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

Focal Document: **NIST Cybersecurity Framework (CSF) version 2.0**
Focal Document URL: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf
Published STRM URL: https://securecontrolsframework.com/content/strm/scf-strm-general-nist-csf-2-0.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)
GV	N/A	The organization's cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored.	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	Measures of Performance	GOV-05	Mechanisms exist to develop, report and monitor cybersecurity and data protection program measures of performance.	8	
				subset of	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	10	
				intersects with	Strategic Plan & Objectives	PRM-01.1	Mechanisms exist to establish a strategic cybersecurity and data protection-specific business plan and set of objectives to achieve that plan.	5	
GV.OC	N/A	The circumstances — mission, stakeholder expectations, dependencies, and legal, regulatory, and contractual requirements — surrounding the organization's cybersecurity risk management decisions are understood.	Functional	subset of	Defining Business Context & Mission	GOV-08	Mechanisms exist to define the context of its business model and document the organization's mission.	10	
				intersects with	Asset-Service Dependencies	AST-01.1	Mechanisms exist to identify and assess the security of Technology Assets, Applications and/or Services (TAAS), Applications and/or Services (TAAS) that support more than one critical business function.	5	
				intersects with	Stakeholder Identification & Involvement	AST-01.2	Mechanisms exist to identify and involve pertinent stakeholders of critical Technology Assets, Applications, Services and/or Data (TAASD) to support the ongoing secure management of those assets.	5	
				intersects with	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	5	
				intersects with	Responsible, Accountable, Supportive, Consulted & Informed (RASCI) Matrix	TPM-05.4	Mechanisms exist to document and maintain a Responsible, Accountable, Supportive, Consulted & Informed (RASCI) matrix, or similar documentation, to delineate assignment for cybersecurity and data protection controls between internal stakeholders and External Service Providers (ESPs).	5	
GV.OC-01	N/A	The organizational mission is understood and informs cybersecurity risk management.	Functional	subset of	Defining Business Context & Mission	GOV-08	Mechanisms exist to define the context of its business model and document the organization's mission.	10	
				intersects with	Risk Framing	RSK-01.1	Mechanisms exist to identify: (1) Assumptions affecting risk assessments, risk response and risk monitoring; (2) Constraints affecting risk assessments, risk response and risk monitoring; (3) The organizational risk tolerance; and (4) Priorities, benefits and trade-offs considered by the organization for managing risk.	5	
				intersects with	Threat Modeling	TDA-06.2	Mechanisms exist to perform threat modelling and other secure design techniques, to ensure that threats to software and solutions are identified and accounted for.	4	
GV.OC-02	N/A	Internal and external stakeholders are understood, and their needs and expectations regarding cybersecurity risk management are understood and considered.	Functional	intersects with	Stakeholder Identification & Involvement	AST-01.2	Mechanisms exist to identify and involve pertinent stakeholders of critical Technology Assets, Applications, Services and/or Data (TAASD) to support the ongoing secure management of those assets.	5	
				intersects with	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for cybersecurity and data protection requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	5	
				intersects with	Responsible, Accountable, Supportive, Consulted & Informed (RASCI) Matrix	TPM-05.4	Mechanisms exist to document and maintain a Responsible, Accountable, Supportive, Consulted & Informed (RASCI) matrix, or similar documentation, to delineate assignment for cybersecurity and data protection controls between internal stakeholders and External Service Providers (ESPs).	5	
GV.OC-03	N/A	Legal, regulatory, and contractual requirements regarding cybersecurity — including privacy and civil liberties obligations — are understood and managed.	Functional	subset of	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	10	
				intersects with	Cybersecurity & Data Protection Controls Oversight	CPL-02	Mechanisms exist to provide a cybersecurity and data protection controls oversight function that reports to the organization's executive leadership.	5	
				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	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for cybersecurity and data protection requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	5	
				intersects with	Contract Flow-Down Requirements	TPM-05.2	Mechanisms exist to ensure cybersecurity and data protection requirements are included in contracts that flow-down to applicable sub-contractors and suppliers.	5	
GV.OC-04	N/A	Critical objectives, capabilities, and services that external stakeholders depend on or expect from the organization are understood and communicated.	Functional	intersects with	Defining Business Context & Mission	GOV-08	Mechanisms exist to define the context of its business model and document the organization's mission.	5	
			Functional	intersects with	Identify Critical Assets	BCD-02	Mechanisms exist to identify and document the critical Technology Assets, Applications, Services and/or Data (TAASD) that support essential missions and business functions.	5	
			Functional	intersects with	Strategic Plan & Objectives	PRM-01.1	Mechanisms exist to establish a strategic cybersecurity and data protection-specific business plan and set of objectives to achieve that plan.	5	
			Functional	intersects with	Third-Party Criticality Assessments	TPM-02	Mechanisms exist to identify, prioritize and assess suppliers and partners of critical Technology Assets, Applications and/or Services (TAAS) using a supply chain risk assessment process relative to their importance in supporting the delivery of high-value services.	5	
GV.OC-05	N/A	Outcomes, capabilities, and services that the organization depends on are understood and communicated.	Functional	intersects with	Identify Critical Assets	BCD-02	Mechanisms exist to identify and document the critical Technology Assets, Applications, Services and/or Data (TAASD) that support essential missions and business functions.	5	
				intersects with	Software Bill of Materials (SBOM)	TDA-04.2	Mechanisms exist to generate, or obtain, a Software Bill of Materials (SBOM) for Technology Assets, Applications and/or Services (TAAS) that lists software packages in use, including versions and applicable licenses.	4	
				intersects with	Third-Party Criticality Assessments	TPM-02	Mechanisms exist to identify, prioritize and assess suppliers and partners of critical Technology Assets, Applications and/or Services (TAAS) using a supply chain risk assessment process relative to their importance in supporting the delivery of high-value services.	5	
GV.RM	N/A	The organization's priorities, constraints, risk tolerance and appetite statements, and assumptions are established, communicated, and used to support operational risk decisions.	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 and data protection program.	5	
				intersects with	Cybersecurity & Data Protection Portfolio Management	PRM-01	Mechanisms exist to facilitate the implementation of cybersecurity and data protection-related resource planning controls that define a viable plan for achieving cybersecurity and data protection objectives.	5	
				intersects with	Strategic Plan & Objectives	PRM-01.1	Mechanisms exist to establish a strategic cybersecurity and data protection-specific business plan and set of objectives to achieve that plan.	5	
				intersects with	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	5	
				intersects with	Risk Framing	RSK-01.1	Mechanisms exist to identify: (1) Assumptions affecting risk assessments, risk response and risk monitoring; (2) Constraints affecting risk assessments, risk response and risk monitoring; (3) The organizational risk tolerance; and (4) Priorities, benefits and trade-offs considered by the organization for managing risk.	8	
				intersects with	Risk Tolerance	RSK-01.3	Mechanisms exist to define organizational risk tolerance, the specified range of acceptable results.	8	
				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.	8	
GV.RM-01	N/A	Risk management objectives are established and agreed to by organizational stakeholders.	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	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	
				intersects with	Key Risk Indicators (KRIs)	GOV-05.2	Mechanisms exist to develop, report and monitor Key Risk Indicators (KRIs) to assist senior management in performance monitoring and trend analysis of the cybersecurity and data protection program.	3	
				intersects with	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	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)
GV.RM-02	N/A	Risk appetite and risk tolerance statements are established, communicated, and maintained.	Functional	intersects with	Risk Tolerance	RSK-01.3	Mechanisms exist to define organizational risk tolerance, the specified range of acceptable results.	10	
				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.	10	
GV.RM-03	N/A	Cybersecurity risk management activities and outcomes are included in enterprise risk management processes.	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	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	
				subset of	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	10	
GV.RM-04	N/A	Strategic direction that describes appropriate risk response options is established and communicated.	Functional	subset of	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	10	
				intersects with	Risk Framing	RSK-01.1	Mechanisms exist to identify: (1) Assumptions affecting risk assessments, risk response and risk monitoring; (2) Constraints affecting risk assessments, risk response and risk monitoring; (3) The organizational risk tolerance; and (4) Priorities, benefits and trade-offs considered by the organization for managing risk.	5	
				intersects with	Risk Remediation	RSK-06	Mechanisms exist to remediate risks to an acceptable level.	5	
				superset of	Risk Response	RSK-06.1	Mechanisms exist to respond to findings from cybersecurity and data protection assessments, incidents and audits to ensure proper remediation has been performed.	5	
				intersects with	Compensating Countermeasures	RSK-06.2	Mechanisms exist to identify and implement compensating countermeasures to reduce risk and exposure to threats.	5	
GV.RM-05	N/A	Lines of communication across the organization are established for cybersecurity risks, including risks from suppliers and other third parties.	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 and data protection program.	5	
				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	
				intersects with	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	
				intersects with	Responsible, Accountable, Supportive, Consulted & Informed (RASCI) Matrix	TPM-05.4	Mechanisms exist to document and maintain a Responsible, Accountable, Supportive, Consulted & Informed (RASCI) matrix, or similar documentation, to delineate assignment for cybersecurity and data protection controls between internal stakeholders and External Service Providers (ESPs).	5	
GV.RM-06	N/A	A standardized method for calculating, documenting, categorizing, and prioritizing cybersecurity risks is established and communicated.	Functional	subset of	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	10	
				intersects with	Risk Framing	RSK-01.1	Mechanisms exist to identify: (1) Assumptions affecting risk assessments, risk response and risk monitoring; (2) Constraints affecting risk assessments, risk response and risk monitoring; (3) The organizational risk tolerance; and (4) Priorities, benefits and trade-offs considered by the organization for managing risk.	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).	5	
				intersects with	Risk Register	RSK-04.1	Mechanisms exist to maintain a risk register that facilitates monitoring and reporting of risks.	5	
GV.RM-07	N/A	Strategic opportunities (i.e., positive risks) are characterized and are included in organizational cybersecurity risk discussions.	Functional	subset of	Risk Framing	RSK-01.1	Mechanisms exist to identify: (1) Assumptions affecting risk assessments, risk response and risk monitoring; (2) Constraints affecting risk assessments, risk response and risk monitoring; (3) The organizational risk tolerance; and (4) Priorities, benefits and trade-offs considered by the organization for managing risk.	10	
GV.RR	N/A	Cybersecurity roles, responsibilities, and authorities to foster accountability, performance assessment, and continuous improvement are established and communicated.	Functional	intersects with	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	
				intersects with	Responsible, Accountable, Supportive, Consulted & Informed (RASCI) Matrix	TPM-05.4	Mechanisms exist to document and maintain a Responsible, Accountable, Supportive, Consulted & Informed (RASCI) matrix, or similar documentation, to delineate assignment for cybersecurity and data protection controls between internal stakeholders and External Service Providers (ESPs).	8	
GV.RR-01	N/A	Organizational leadership is responsible and accountable for cybersecurity risk and fosters a culture that is risk-aware, ethical, and continually improving.	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	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.		
				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 and data protection program.	5	
				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	
				intersects with	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	5	
				intersects with	Risk Tolerance	RSK-01.3	Mechanisms exist to define organizational risk tolerance, the specified range of acceptable results.	5	
				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	
				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	
				intersects with	Risk Culture	RSK-12	Mechanisms exist to ensure teams are committed to a culture that considers and communicates technology-related risk.	5	
GV.RR-02	N/A	Roles, responsibilities, and authorities related to cybersecurity risk management are established, communicated, understood, and enforced.	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 and data protection program.	5	
				intersects with	Position Categorization	HRS-02	Mechanisms exist to manage personnel security risk by assigning a risk designation to all positions and establishing screening criteria for individuals filling those positions.		
				intersects with	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	
				intersects with	Responsible, Accountable, Supportive, Consulted & Informed (RASCI) Matrix	TPM-05.4	Mechanisms exist to document and maintain a Responsible, Accountable, Supportive, Consulted & Informed (RASCI) matrix, or similar documentation, to delineate assignment for cybersecurity and data protection controls between internal stakeholders and External Service Providers (ESPs).	5	
GV.RR-03	N/A	Adequate resources are allocated commensurate with the cybersecurity risk strategy, roles, responsibilities, and policies.	Functional	intersects with	Cybersecurity & Data Protection Portfolio Management	PRM-01	Mechanisms exist to facilitate the implementation of cybersecurity and data protection-related resource planning controls that define a viable plan for achieving cybersecurity and data protection objectives.	5	
				intersects with	Cybersecurity & Data Protection Resource Management	PRM-02	Mechanisms exist to address all capital planning and investment requests, including the resources needed to implement the cybersecurity and data protection programs and document all exceptions to this requirement.	5	
				equal	Allocation of Resources	PRM-03	Mechanisms exist to identify and allocate resources for management, operational, technical and data protection requirements within business process planning for projects / initiatives.	10	
GV.RR-04	N/A	Cybersecurity is included in human resources practices.	Functional	equal	Human Resources Security Management	HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.	10	
				intersects with	User Awareness	HRS-03.1	Mechanisms exist to communicate with users about their roles and responsibilities to maintain a safe and secure working environment.	5	
GV.PO	N/A	Organizational cybersecurity policy is established, communicated, and enforced.	Functional	subset of	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity and data protection policies, standards and procedures.	10	
				intersects with	Policy Familiarization & Acknowledgement	HRS-05.7	Mechanisms exist to ensure personnel receive recurring familiarization with the organization's cybersecurity and data protection policies and provide acknowledgement.	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)
				intersects with	Personnel Sanctions	HRS-07	Mechanisms exist to sanction personnel failing to comply with established security policies, standards and procedures.	5	
GV.PO-01	N/A	Policy for managing cybersecurity risks is established based on organizational context, cybersecurity strategy, and priorities and is communicated and enforced.	Functional	subset of	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity and data protection policies, standards and procedures.	10	
				intersects with	Policy Familiarization & Acknowledgement	HRS-05.7	Mechanisms exist to ensure personnel receive recurring familiarization with the organization's cybersecurity and data protection policies and provide acknowledgement.	5	
				intersects with	Personnel Sanctions	HRS-07	Mechanisms exist to sanction personnel failing to comply with established security policies, standards and procedures.	5	
GV.PO-02	N/A	Policy for managing cybersecurity risks is reviewed, updated, communicated, and enforced to reflect changes in requirements, threats, technology, and organizational mission.	Functional	intersects with	Periodic Review & Update of Cybersecurity & Data Protection Program	GOV-03	Mechanisms exist to review the cybersecurity and data protection program, including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	8	
				intersects with	Policy Familiarization & Acknowledgement	HRS-05.7	Mechanisms exist to ensure personnel receive recurring familiarization with the organization's cybersecurity and data protection policies and provide acknowledgement.	8	
				intersects with	Personnel Sanctions	HRS-07	Mechanisms exist to sanction personnel failing to comply with established security policies, standards and procedures.	8	
GV.OV	N/A	Results of organization-wide cybersecurity risk management activities and performance are used to inform, improve, and adjust the risk management strategy.	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	
				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.	5	
				intersects with	Measures of Performance	GOV-05	Mechanisms exist to develop, report and monitor cybersecurity and data protection program measures of performance.	5	
				intersects with	Periodic Review & Update of Cybersecurity & Data Protection Program	GOV-03	Mechanisms exist to review the cybersecurity and data protection program, including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	
GV.OV-01	N/A	Cybersecurity risk management strategy outcomes are reviewed to inform and adjust strategy and direction.	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	
				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.	5	
				intersects with	Measures of Performance	GOV-05	Mechanisms exist to develop, report and monitor cybersecurity and data protection program measures of performance.	5	
				intersects with	Periodic Review & Update of Cybersecurity & Data Protection Program	GOV-03	Mechanisms exist to review the cybersecurity and data protection program, including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	5	
				intersects with	Defining Business Context & Mission	GOV-08	Mechanisms exist to define the context of its business model and document the organization's mission.	5	
				intersects with	Strategic Plan & Objectives	PRM-01.1	Mechanisms exist to establish a strategic cybersecurity and data protection-specific business plan and set of objectives to achieve that plan.	5	
GV.OV-02	N/A	The cybersecurity risk management strategy is reviewed and adjusted to ensure coverage of organizational requirements and 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	
				subset of	Periodic Review & Update of Cybersecurity & Data Protection Program	GOV-03	Mechanisms exist to review the cybersecurity and data protection program, including policies, standards and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	10	
				intersects with	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	5	
GV.OV-03	N/A	Organizational cybersecurity risk management performance is evaluated and reviewed for adjustments needed.	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	
				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.	5	
				intersects with	Measures of Performance	GOV-05	Mechanisms exist to develop, report and monitor cybersecurity and data protection program measures of performance.	5	
				intersects with	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	5	
GV.SC	N/A	Cyber supply chain risk management processes are identified, established, managed, monitored, and improved by organizational stakeholders.	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	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	
				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.	5	
				intersects with	Measures of Performance	GOV-05	Mechanisms exist to develop, report and monitor cybersecurity and data protection program measures of performance.	5	
				intersects with	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	5	
				equal	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 Technology Assets, Applications and/or Services (TAAS), including documenting selected mitigating actions and monitoring performance against those plans.	10	
				intersects with	Supply Chain Risk Assessment	RSK-09.1	Mechanisms exist to periodically assess supply chain risks associated with Technology Assets, Applications and/or Services (TAAS).	5	
				intersects with	Supply Chain Risk Management (SCRM)	TPM-03	Mechanisms exist to: (1) Evaluate security risks and threats associated with Technology Assets, Applications and/or Services (TAAS) supply chains; and	8	
GV.SC-01	N/A	A cybersecurity supply chain risk management program, strategy, objectives, policies, and processes are established and agreed to by organizational stakeholders.	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	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	
				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	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	5	
				equal	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 Technology Assets, Applications and/or Services (TAAS), including documenting selected mitigating actions and monitoring performance against those plans.	10	
GV.SC-02	N/A	Cybersecurity roles and responsibilities for suppliers, customers, and partners are established, communicated, and coordinated internally and externally.	Functional	intersects with	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for cybersecurity and data protection requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	8	
				intersects with	Contract Flow-Down Requirements	TPM-05.2	Mechanisms exist to ensure cybersecurity and data protection requirements are included in contracts that flow-down to applicable sub-contractors and suppliers.	8	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
				intersects with	Responsible, Accountable, Supportive, Consulted & Informed (RASCI) Matrix	TPM-05.4	Mechanisms exist to document and maintain a Responsible, Accountable, Supportive, Consulted & Informed (RASCI) matrix, or similar documentation, to delineate assignment for cybersecurity and data protection controls between internal stakeholders and External Service Providers (ESPs).	8	
GV.SC-03	N/A	Cybersecurity supply chain risk management is integrated into cybersecurity and enterprise risk management, risk assessment, and improvement processes.	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	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	
				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	Defining Business Context & Mission	GOV-08	Mechanisms exist to define the context of its business model and document the organization's mission.	5	
				intersects with	Define Control Objectives	GOV-09	Mechanisms exist to establish control objectives as the basis for the selection, implementation and management of the organization's internal control system.	5	
				intersects with	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	5	
				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 Technology Assets, Applications and/or Services (TAAS), including documenting selected mitigating actions and monitoring performance against those plans.	5	
GV.SC-04	N/A	Suppliers are known and prioritized by criticality.	Functional	intersects with	Asset Governance	AST-01	Mechanisms exist to facilitate an IT Asset Management (ITAM) program to implement and manage asset management controls.	5	
				intersects with	Asset-Service Dependencies	AST-01.1	Mechanisms exist to identify and assess the security of Technology Assets, Applications and/or Services (TAAS), Applications and/or Services (TAAS) that support more than one critical business function.	5	
				intersects with	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	5	
				intersects with	Third-Party Inventories	TPM-01.1	Mechanisms exist to maintain a current, accurate and complete list of External Service Providers (ESPs) that can potentially impact the Confidentiality, Integrity, Availability and/or Safety (CIAS) of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	8	
				intersects with	Third-Party Criticality Assessments	TPM-02	Mechanisms exist to identify, prioritize and assess suppliers and partners of critical Technology Assets, Applications and/or Services (TAAS) using a supply chain risk assessment process relative to their importance in supporting the delivery of high-value services.	8	
GV.SC-05	N/A	Requirements to address cybersecurity risks in supply chains are established, prioritized, and integrated into contracts and other types of agreements with suppliers and other relevant third parties.	Functional	intersects with	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	5	
				intersects with	Compliance Scope	CPL-01.2	Mechanisms exist to document and validate the scope of cybersecurity and data protection controls that are determined to meet statutory, regulatory and/or contractual compliance obligations.	5	
				intersects with	Adequate Security for Sensitive / Regulated Data In Support of Contracts	IAO-03.2	Mechanisms exist to protect sensitive / regulated data that is collected, developed, received, transmitted, used or stored in support of the performance of a contract.	5	
				intersects with	Data Privacy Requirements for Contractors & Service Providers	PRI-07.1	Mechanisms exist to include data privacy requirements in contracts and other acquisition-related documents that establish data privacy roles and responsibilities for contractors and service providers.	5	
				intersects with	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	5	
				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 Technology Assets, Applications and/or Services (TAAS), including documenting selected mitigating actions and monitoring performance against those plans.	5	
				intersects with	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for cybersecurity and data protection requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	5	
				intersects with	Contract Flow-Down Requirements	TPM-05.2	Mechanisms exist to ensure cybersecurity and data protection requirements are included in contracts that flow-down to applicable sub-contractors and suppliers.	5	
GV.SC-06	N/A	Planning and due diligence are performed to reduce risks before entering into formal supplier or other third-party relationships.	Functional	intersects with	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	5	
				intersects with	Third-Party Criticality Assessments	TPM-02	Mechanisms exist to identify, prioritize and assess suppliers and partners of critical Technology Assets, Applications and/or Services (TAAS) using a supply chain risk assessment process relative to their importance in supporting the delivery of high-value services.	5	
				intersects with	Supply Chain Risk Management (SCRM)	TPM-03	Mechanisms exist to: (1) Evaluate security risks and threats associated with Technology Assets, Applications and/or Services (TAAS) supply chains; and (2) Take appropriate remediation actions to minimize the organization's exposure to those risks and threats, as necessary.	5	
				intersects with	Limit Potential Harm	TPM-03.2	Mechanisms exist to utilize security safeguards to limit harm from potential adversaries who identify and target the organization's supply chain.	5	
				intersects with	Processes To Address Weaknesses or Deficiencies	TPM-03.3	Mechanisms exist to address identified weaknesses or deficiencies in the security of the supply chain	5	
				intersects with	Third-Party Services	TPM-04	Mechanisms exist to mitigate the risks associated with third-party access to the organization's Technology Assets, Applications, Services and/or Data (TAASD).	5	
				intersects with	Third-Party Risk Assessments & Approvals	TPM-04.1	Mechanisms exist to conduct a risk assessment prior to the acquisition or outsourcing of technology-related Technology Assets, Applications and/or Services (TAAS).	5	
				intersects with	Conflict of Interests	TPM-04.3	Mechanisms exist to ensure that the interests of external service providers are consistent with and reflect organizational interests.	5	
				intersects with	Third-Party Processing, Storage and Service Locations	TPM-04.4	Mechanisms exist to restrict the location of information processing/storage based on business requirements.	5	
				intersects with	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for cybersecurity and data protection requirements with third-parties, reflecting the organization's needs to protect its Technology Assets, Applications, Services and/or Data (TAASD).	5	
				intersects with	Contract Flow-Down Requirements	TPM-05.2	Mechanisms exist to ensure cybersecurity and data protection requirements are included in contracts that flow-down to applicable sub-contractors and suppliers.	5	
				intersects with	Third-Party Authentication Practices	TPM-05.3	Mechanisms exist to ensure External Service Providers (ESPs) use unique authentication factors for each of its customers.	5	
				intersects with	Responsible, Accountable, Supportive, Consulted & Informed (RASCI) Matrix	TPM-05.4	Mechanisms exist to document and maintain a Responsible, Accountable, Supportive, Consulted & Informed (RASCI) matrix, or similar documentation, to delineate assignment for cybersecurity and data protection controls between internal stakeholders and External Service Providers (ESPs).	5	
				intersects with	Third-Party Scope Review	TPM-05.5	Mechanisms exist to perform recurring validation of the Responsible, Accountable, Supportive, Consulted & Informed (RASCI) matrix, or similar documentation, to ensure cybersecurity and data protection control assignments accurately reflect current business practices, compliance obligations, technologies and stakeholders.	5	
				intersects with	First-Party Declaration (1PD)	TPM-05.6	Mechanisms exist to obtain a First-Party Declaration (1PD) from applicable External Service Providers (ESPs) that provides assurance of compliance with specified statutory, regulatory and contractual obligations for cybersecurity and data protection controls, including any flow-down requirements to subcontractors.	5	
				intersects with	Break Clauses	TPM-05.7	Mechanisms exist to include "break clauses" within contracts for failure to meet contract criteria for cybersecurity and/or data privacy controls.	5	
				intersects with	Third-Party Personnel Security	TPM-06	Mechanisms exist to control personnel security requirements including security roles and responsibilities for third-party providers.	5	
				intersects with	Third-Party Deficiency Remediation	TPM-09	Mechanisms exist to address weaknesses or deficiencies in supply chain elements identified during independent or organizational assessments of such elements.	5	
				intersects with	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	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)
GV.SC-07	N/A	The risks posed by a supplier, their products and services, and other third parties are understood, recorded, prioritized, assessed, responded to, and monitored over the course of the relationship.	Functional	intersects with	Third-Party Inventories	TPM-01.1	Mechanisms exist to maintain a current, accurate and complete list of External Service Providers (ESPs) that can potentially impact the Confidentiality, Integrity, Availability and/or Safety (CIAS) of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	5	
				intersects with	Third-Party Criticality Assessments	TPM-02	Mechanisms exist to identify, prioritize and assess suppliers and partners of critical Technology Assets, Applications and/or Services (TAAS) using a supply chain risk assessment process relative to their importance in supporting the delivery of high-value services.	5	
				intersects with	Supply Chain Risk Management (SCRM)	TPM-03	Mechanisms exist to: (1) Evaluate security risks and threats associated with Technology Assets, Applications and/or Services (TAAS) supply chains; and	5	
				intersects with	Limit Potential Harm	TPM-03.2	Mechanisms exist to utilize security safeguards to limit harm from potential adversaries who identify and target the organization's supply chain.	5	
				intersects with	Processes To Address Weaknesses or Deficiencies	TPM-03.3	Mechanisms exist to address identified weaknesses or deficiencies in the security of the supply chain	5	
				intersects with	Third-Party Services	TPM-04	Mechanisms exist to mitigate the risks associated with third-party access to the organization's Technology Assets, Applications, Services and/or Data (TAASD).	5	
				intersects with	Third-Party Risk Assessments & Approvals	TPM-04.1	Mechanisms exist to conduct a risk assessment prior to the acquisition or outsourcing of technology-related Technology Assets, Applications and/or Services (TAAS).	5	
				intersects with	Review of Third-Party Services	TPM-08	Mechanisms exist to monitor, regularly review and assess External Service Providers (ESPs) for compliance with established contractual requirements for cybersecurity and data protection controls.	5	
				intersects with	Third-Party Deficiency Remediation	TPM-09	Mechanisms exist to address weaknesses or deficiencies in supply chain elements identified during independent or organizational assessments of such elements.	5	
GV.SC-08	N/A	Relevant suppliers and other third parties are included in incident planning, response, and recovery activities.	Functional	intersects with	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	5	
				intersects with	Coordinate With External Service Providers	BCD-01.2	Mechanisms exist to coordinate internal contingency plans with the contingency plans of external service providers to ensure that contingency requirements can be satisfied.	5	
				intersects with	Incident Response Operations	IRO-01	Mechanisms exist to implement and govern processes and documentation to facilitate an organization-wide response capability for cybersecurity and data protection-related incidents.	5	
				intersects with	Incident Handling	IRO-02	Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Eradication; and (6) Recovery.	5	
				intersects with	Correlation with External Organizations	IRO-02.5	Mechanisms exist to coordinate with approved third-parties to achieve a cross-organization perspective on incident awareness and more effective incident responses.	5	
				intersects with	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	5	
				intersects with	Third-Party Inventories	TPM-01.1	Mechanisms exist to maintain a current, accurate and complete list of External Service Providers (ESPs) that can potentially impact the Confidentiality, Integrity, Availability and/or Safety (CIAS) of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	5	
				intersects with	Third-Party Criticality Assessments	TPM-02	Mechanisms exist to identify, prioritize and assess suppliers and partners of critical Technology Assets, Applications and/or Services (TAAS) using a supply chain risk assessment process relative to their importance in supporting the delivery of high-value services.	5	
				intersects with	Third-Party Deficiency Remediation	TPM-09	Mechanisms exist to address weaknesses or deficiencies in supply chain elements identified during independent or organizational assessments of such elements.	5	
				intersects with	Managing Changes To Third-Party Services	TPM-10	Mechanisms exist to control changes to services by suppliers, taking into account the criticality of business Technology Assets, Applications, Services and/or Data (TAASD) that are in scope by the third-party.	5	
				intersects with	Third-Party Incident Response & Recovery Capabilities	TPM-11	Mechanisms exist to ensure response/recovery planning and testing are conducted with critical suppliers/providers.	5	
GV.SC-09	N/A	Supply chain security practices are integrated into cybersecurity and enterprise risk management programs, and their performance is monitored throughout the technology product and service life cycle.	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	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	
				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.	5	
				intersects with	Measures of Performance	GOV-05	Mechanisms exist to develop, report and monitor cybersecurity and data protection program measures of performance.	5	
				intersects with	Secure Development Life Cycle (SDLC) Management	PRM-07	Mechanisms exist to ensure changes to Technology Assets, Applications and/or Services (TAAS) within the Secure Development Life Cycle (SDLC) are controlled through formal change control procedures.	5	
				intersects with	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	5	
				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 Technology Assets, Applications and/or Services (TAAS), including documenting selected mitigating actions and monitoring performance against those plans.	5	
				intersects with	Supply Chain Risk Assessment	RSK-09.1	Mechanisms exist to periodically assess supply chain risks associated with Technology Assets, Applications and/or Services (TAAS).	5	
				intersects with	Technology Lifecycle Management	SEA-07.1	Mechanisms exist to manage the usable lifecycles of technology assets.	5	
				intersects with	Product Management	TDA-01.1	Mechanisms exist to design and implement product management processes to proactively govern the design, development and production of Technology Assets, Applications and/or Services (TAAS) across the System Development Life Cycle (SDLC) to:	5	
GV.SC-10	N/A	Cybersecurity supply chain risk management plans include provisions for activities that occur after the conclusion of a partnership or service agreement.	Functional	subset of	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 Technology Assets, Applications and/or Services (TAAS), including documenting selected mitigating actions and monitoring performance against those plans.	10	
				intersects with	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	5	
				intersects with	Contract Flow-Down Requirements	TPM-05.2	Mechanisms exist to ensure cybersecurity and data protection requirements are included in contracts that flow-down to applicable sub-contractors and suppliers.	5	
				intersects with	Third-Party Authentication Practices	TPM-05.3	Mechanisms exist to ensure External Service Providers (ESPs) use unique authentication factors for each of its customers.	5	
				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	
				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.	5	
				intersects with	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	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)
ID	N/A	The organization's current cybersecurity risks are understood.	Functional	intersects with	Risk Framing	RSK-01.1	Mechanisms exist to identify: (1) Assumptions affecting risk assessments, risk response and risk monitoring; (2) Constraints affecting risk assessments, risk response and risk monitoring; (3) The organizational risk tolerance; and (4) Priorities, benefits and trade-offs considered by the organization for managing risk.	5	
				intersects with	Risk Identification	RSK-03	Mechanisms exist to identify and document risks, both internal and external.	5	
				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	
				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).	5	
				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 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	
				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 Technology Assets, Applications and/or Services (TAAS), including documenting selected mitigating actions and monitoring performance against those plans.	5	
ID.AM	N/A	Assets (e.g., data, hardware, software, systems, facilities, services, people) that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.	Functional	subset of	Asset Governance	AST-01	Mechanisms exist to facilitate an IT Asset Management (ITAM) program to implement and manage asset management controls.	10	
				intersects with	Asset-Service Dependencies	AST-01.1	Mechanisms exist to identify and assess the security of Technology Assets, Applications and/or Services (TAAS), Applications and/or Services (TAAS) that support more than one critical business function.	5	
				intersects with	Stakeholder Identification & Involvement	AST-01.2	Mechanisms exist to identify and involve pertinent stakeholders of critical Technology Assets, Applications, Services and/or Data (TAASD) to support the ongoing secure management of those assets.	5	
				intersects with	Asset Inventories	AST-02	Mechanisms exist to perform inventories of Technology Assets, Applications, Services and/or Data (TAASD) that: (1) Accurately reflects the current TAASD in use; (2) Identifies authorized software products, including business justification details; (3) Is at the level of granularity deemed necessary for tracking and reporting; (4) Includes organization-defined information deemed necessary to achieve effective property accountability; and (5) Is available for review and audit by designated organizational personnel.	5	
				intersects with	Asset Ownership Assignment	AST-03	Mechanisms exist to ensure asset ownership responsibilities are assigned, tracked and managed at a team, individual, or responsible organization level to establish a common understanding of requirements for asset protection.	5	
				intersects with	Accountability Information	AST-03.1	Mechanisms exist to include capturing the name, position and/or role of individuals responsible/accountable for administering assets as part of the technology asset inventory process.	5	
				intersects with	Human Resources Security Management	HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.	5	
				intersects with	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	
				intersects with	Terms of Employment	HRS-05	Mechanisms exist to require all employees and contractors to apply cybersecurity and data protection principles in their daily work.	5	
				intersects with	Rules of Behavior	HRS-05.1	Mechanisms exist to define acceptable and unacceptable rules of behavior for the use of technologies, including consequences for unacceptable behavior.	5	
				intersects with	Physical & Environmental Protections	PES-01	Mechanisms exist to facilitate the operation of physical and environmental protection controls.	5	
				intersects with	Risk-Based Security Categorization	RSK-02	Mechanisms exist to categorize Technology Assets, Applications, Services and/or Data (TAASD) in accordance with applicable laws, regulations and contractual obligations that: (1) Document the security categorization results (including supporting rationale) in the security plan for systems; and (2) Ensure the security categorization decision is reviewed and approved by the asset owner.	5	
				intersects with	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	5	
				intersects with	Third-Party Inventories	TPM-01.1	Mechanisms exist to maintain a current, accurate and complete list of External Service Providers (ESPs) that can potentially impact the Confidentiality, Integrity, Availability and/or Safety (CIAS) of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	5	
				intersects with	Responsible, Accountable, Supportive, Consulted & Informed (RASCI) Matrix	TPM-05.4	Mechanisms exist to document and maintain a Responsible, Accountable, Supportive, Consulted & Informed (RASCI) matrix, or similar documentation, to delineate assignment for cybersecurity and data protection controls between internal stakeholders and External Service Providers (ESPs).	5	
				intersects with	Third-Party Personnel Security	TPM-06	Mechanisms exist to control personnel security requirements including security roles and responsibilities for third-party providers.	5	
ID.AM-01	N/A	Inventories of hardware managed by the organization are maintained.	Functional	subset of	Asset Inventories	AST-02	Mechanisms exist to perform inventories of Technology Assets, Applications, Services and/or Data (TAASD) that: (1) Accurately reflects the current TAASD in use; (2) Identifies authorized software products, including business justification details; (3) Is at the level of granularity deemed necessary for tracking and reporting; (4) Includes organization-defined information deemed necessary to achieve effective property accountability; and (5) Is available for review and audit by designated organizational personnel.	10	
				intersects with	Third-Party Inventories	TPM-01.1	Mechanisms exist to maintain a current, accurate and complete list of External Service Providers (ESPs) that can potentially impact the Confidentiality, Integrity, Availability and/or Safety (CIAS) of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	5	
ID.AM-02	N/A	Inventories of software, services, and systems managed by the organization are maintained.	Functional	subset of	Asset Inventories	AST-02	Mechanisms exist to perform inventories of Technology Assets, Applications, Services and/or Data (TAASD) that: (1) Accurately reflects the current TAASD in use; (2) Identifies authorized software products, including business justification details; (3) Is at the level of granularity deemed necessary for tracking and reporting; (4) Includes organization-defined information deemed necessary to achieve effective property accountability; and (5) Is available for review and audit by designated organizational personnel.	10	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
				intersects with	Third-Party Inventories	TPM-01.1	Mechanisms exist to maintain a current, accurate and complete list of External Service Providers (ESPs) that can potentially impact the Confidentiality, Integrity, Availability and/or Safety (CIAS) of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	5	
ID.AM-03	N/A	Representations of the organization's authorized network communication and internal and external network data flows are maintained.	Functional	intersects with	Network Diagrams & Data Flow Diagrams (DFDs)	AST-04	Mechanisms exist to maintain network architecture diagrams that: (1) Contain sufficient detail to assess the security of the network's architecture; (2) Reflect the current architecture of the network environment; and (3) Document all sensitive/regulated data flows.	5	
				intersects with	Control Applicability Boundary Graphical Representation	AST-04.2	Mechanisms exist to ensure control applicability is appropriately-determined for Technology Assets, Applications and/or Services (TAAS) and third parties by graphically representing applicable boundaries.	5	
				intersects with	Geographic Location of Data	DCH-19	Mechanisms exist to inventory, document and maintain data flows for data that is resident (permanently or temporarily) within a service's geographically distributed applications (physical and virtual), infrastructure, systems components and/or shared with other third-parties.	5	
ID.AM-04	N/A	Inventories of services provided by suppliers are maintained.	Functional	equal	Third-Party Inventories	TPM-01.1	Mechanisms exist to maintain a current, accurate and complete list of External Service Providers (ESPs) that can potentially impact the Confidentiality, Integrity, Availability and/or Safety (CIAS) of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	10	
ID.AM-05	N/A	Assets are prioritized based on classification, criticality, resources, and impact on the mission.	Functional	intersects with	Asset Scope Classification	AST-04.1	Mechanisms exist to determine cybersecurity and data protection control applicability by identifying, assigning and documenting the appropriate asset scope categorization for all Technology Assets, Applications and/or Services (TAAS) and personnel (internal and third-parties).	5	
				intersects with	Identify Critical Assets	BCD-02	Mechanisms exist to identify and document the critical Technology Assets, Applications, Services and/or Data (TAASD) that support essential missions and business functions.	5	
				intersects with	Data & Asset Classification	DCH-02	Mechanisms exist to ensure data and assets are categorized in accordance with applicable statutory, regulatory and contractual requirements.	5	
				intersects with	Third-Party Criticality Assessments	TPM-02	Mechanisms exist to identify, prioritize and assess suppliers and partners of critical Technology Assets, Applications and/or Services (TAAS) using a supply chain risk assessment process relative to their importance in supporting the delivery of high-value services.	5	
ID.AM-07	N/A	Inventories of data and corresponding metadata for designated data types are maintained.	Functional	intersects with	Media Storage	DCH-06	Mechanisms exist to: (1) Physically control and securely store digital and non-digital media within controlled areas using organization-defined security measures; and (2) Protect system media until the media are destroyed or sanitized using approved equipment, techniques and procedures.	5	
				intersects with	Sensitive Data Inventories	DCH-06.2	Mechanisms exist to maintain inventory logs of all sensitive media and conduct sensitive media inventories at least annually.	5	
				intersects with	Periodic Scans for Sensitive / Regulated Data	DCH-06.3	Mechanisms exist to periodically scan unstructured data sources for sensitive/regulated data or data requiring special protection measures by statutory, regulatory or contractual obligations.	5	
				intersects with	Personal Data (PD) Retention & Disposal	PRI-05	Mechanisms exist to: (1) Retain Personal Data (PD), including metadata, for an organization-defined time period to fulfill the purpose(s) identified in the notice or as required by law; (2) Dispose of, destroys, erases, and/or anonymizes the PD, regardless of the method of storage; and (3) Use organization-defined techniques or methods to ensure secure deletion or destruction of PD (including originals, copies and archived records).	5	
				intersects with	Inventory of Personal Data (PD)	PRI-05.5	Mechanisms exist to establish and maintain a current inventory of all Technology Assets, Applications and/or Services (TAAS) that collect, receive, process, store, transmit, update and/or share Personal Data (PD).	5	
ID.AM-08	N/A	Systems, hardware, software, services, and data are managed throughout their life cycles.	Functional	subset of	Asset Governance	AST-01	Mechanisms exist to facilitate an IT Asset Management (ITAM) program to implement and manage asset management controls.	10	
				intersects with	Stakeholder Identification & Involvement	AST-01.2	Mechanisms exist to identify and involve pertinent stakeholders of critical Technology Assets, Applications, Services and/or Data (TAASD) to support the ongoing secure management of those assets.	5	
				intersects with	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	5	
				intersects with	Data Stewardship	DCH-01.1	Mechanisms exist to ensure data stewardship is assigned, documented and communicated.	5	
				intersects with	Secure Development Life Cycle (SDLC) Management	PRM-07	Mechanisms exist to ensure changes to Technology Assets, Applications and/or Services (TAAS) within the Secure Development Life Cycle (SDLC) are controlled through formal change control procedures.	5	
				intersects with	Predictable Failure Analysis	SEA-07	Mechanisms exist to determine the Mean Time to Failure (MTTF) for system components in specific environments of operation.	5	
				intersects with	Technology Lifecycle Management	SEA-07.1	Mechanisms exist to manage the usable lifecycles of technology assets.	5	
ID.RA	N/A	The cybersecurity risk to the organization, assets, and individuals is understood by the organization.	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	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	
				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	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	5	
				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 Technology Assets, Applications and/or Services (TAAS), including documenting selected mitigating actions and monitoring performance against those plans.	5	
ID.RA-01	N/A	Vulnerabilities in assets are identified, validated, and recorded.	Functional	intersects with	Information Assurance (IA) Operations	IAO-01	Mechanisms exist to facilitate the implementation of cybersecurity and data protection assessment and authorization controls.	5	
				intersects with	Assessments	IAO-02	Mechanisms exist to formally assess the cybersecurity and data protection controls in Technology Assets, Applications and/or Services (TAAS) through Information Assurance Program (IAP) activities to determine the extent to which the controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting expected requirements.	5	
				intersects with	Plan of Action & Milestones (POA&M)	IAO-05	Mechanisms exist to generate a Plan of Action and Milestones (POA&M), or similar risk register, to document planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities.	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).	5	
				intersects with	Risk Register	RSK-04.1	Mechanisms exist to maintain a risk register that facilitates monitoring and reporting of risks.	5	
				intersects with	Cybersecurity & Data Protection Testing Throughout Development	TDA-09	Mechanisms exist to require system developers/integrators consult with cybersecurity and data protection personnel to: (1) Create and implement a Security Testing and Evaluation (ST&E) plan, or similar capability; (2) Implement a verifiable flaw remediation process to correct weaknesses and deficiencies identified during the security testing and evaluation process; and (3) Document the results of the security testing/evaluation and flaw remediation processes.	5	
				subset of	Vulnerability & Patch Management Program (VPMP)	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	10	
				intersects with	Vulnerability Scanning	VPM-06	Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications.	5	
ID.RA-02	N/A	Cyber threat intelligence is received from information sharing forums and sources.	Functional	intersects with	Contacts With Groups & Associations	GOV-07	Mechanisms exist to establish contact with selected groups and associations within the cybersecurity and data protection communities to: (1) Facilitate ongoing cybersecurity and data protection education and training for organizational personnel; (2) Maintain currency with recommended cybersecurity and data protection practices, techniques and technologies; and (3) Share current cybersecurity and/or data privacy-related information including threats, vulnerabilities and incidents.	5	
				intersects with	Threat Intelligence Feeds Feeds	THR-03	Mechanisms exist to maintain situational awareness of vulnerabilities and evolving threats by leveraging the knowledge of attacker tactics, techniques and procedures to facilitate the implementation of preventative and compensating controls.	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)
ID.RA-03	N/A	Internal and external threats to the organization are identified and recorded.	Functional	subset of	Threat Intelligence Feeds Program	THR-01	Mechanisms exist to implement a threat intelligence program that includes a cross-organization information-sharing capability that can influence the development of the system and security architectures, selection of security solutions, monitoring, threat hunting, response and recovery activities.	10	
				intersects with	Indicators of Exposure (IOE)	THR-02	Mechanisms exist to develop Indicators of Exposure (IOE) to understand the potential attack vectors that attackers could use to attack the organization.	5	
				intersects with	Threat Intelligence Feeds Feeds	THR-03	Mechanisms exist to maintain situational awareness of vulnerabilities and evolving threats by leveraging the knowledge of attacker tactics, techniques and procedures to facilitate the implementation of preventative and compensating controls.	5	
				intersects with	Insider Threat Program	THR-04	Mechanisms exist to implement an insider threat program that includes a cross-discipline insider threat incident handling team.	5	
				intersects with	Insider Threat Awareness	THR-05	Mechanisms exist to utilize security awareness training on recognizing and reporting potential indicators of insider threat.	5	
				intersects with	Threat Hunting	THR-07	Mechanisms exist to perform cyber threat hunting that uses Indicators of Compromise (IoC) to detect, track and disrupt threats that evade existing security controls.	5	
				intersects with	Threat Catalog	THR-09	Mechanisms exist to develop and keep current a catalog of applicable internal and external threats to the organization, both natural and manmade.	5	
ID.RA-04	N/A	Potential impacts and likelihoods of threats exploiting vulnerabilities are identified and recorded.	Functional	intersects with	Threat Catalog	THR-09	Mechanisms exist to develop and keep current a catalog of applicable internal and external threats to the organization, both natural and manmade.	5	
				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	
ID.RA-05	N/A	Threats, vulnerabilities, likelihoods, and impacts are used to understand inherent risk and inform risk response prioritization.	Functional	intersects with	Risk Framing	RSK-01.1	Mechanisms exist to identify: (1) Assumptions affecting risk assessments, risk response and risk monitoring; (2) Constraints affecting risk assessments, risk response and risk monitoring; (3) The organizational risk tolerance; and (4) Priorities, benefits and trade-offs considered by the organization for managing risk.	5	
				intersects with	Impact-Level Prioritization	RSK-02.1	Mechanisms exist to prioritize the impact level for Technology Assets, Applications and/or Services (TAAS) to prevent potential disruptions.	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).	5	
				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	
				intersects with	Risk Remediation	RSK-06	Mechanisms exist to remediate risks to an acceptable level.	5	
				intersects with	Risk Response	RSK-06.1	Mechanisms exist to respond to findings from cybersecurity and data protection assessments, incidents and audits to ensure proper remediation has been performed.	5	
				intersects with	Indicators of Exposure (IOE)	THR-02	Mechanisms exist to develop Indicators of Exposure (IOE) to understand the potential attack vectors that attackers could use to attack the organization.	5	
				intersects with	Threat Catalog	THR-09	Mechanisms exist to develop and keep current a catalog of applicable internal and external threats to the organization, both natural and manmade.	5	
				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	
ID.RA-06	N/A	Risk responses are chosen, prioritized, planned, tracked, and communicated.	Functional	intersects with	Risk Framing	RSK-01.1	Mechanisms exist to identify: (1) Assumptions affecting risk assessments, risk response and risk monitoring; (2) Constraints affecting risk assessments, risk response and risk monitoring; (3) The organizational risk tolerance; and (4) Priorities, benefits and trade-offs considered by the organization for managing risk.	5	
				intersects with	Impact-Level Prioritization	RSK-02.1	Mechanisms exist to prioritize the impact level for Technology Assets, Applications and/or Services (TAAS) to prevent potential disruptions.	5	
				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	
				intersects with	Risk Remediation	RSK-06	Mechanisms exist to remediate risks to an acceptable level.	5	
				intersects with	Risk Response	RSK-06.1	Mechanisms exist to respond to findings from cybersecurity and data protection assessments, incidents and audits to ensure proper remediation has been performed.	5	
				intersects with	Compensating Countermeasures	RSK-06.2	Mechanisms exist to identify and implement compensating countermeasures to reduce risk and exposure to threats.	5	
ID.RA-07	N/A	Changes and exceptions are managed, assessed for risk impact, recorded, and tracked.	Functional	subset of	Change Management Program	CHG-01	Mechanisms exist to facilitate the implementation of a change management program.	10	
				intersects with	Configuration Change Control	CHG-02	Mechanisms exist to govern the technical configuration change control processes.	5	
				intersects with	Prohibition Of Changes	CHG-02.1	Mechanisms exist to prohibit unauthorized changes, unless organization-approved change requests are received.	5	
				intersects with	Test, Validate & Document Changes	CHG-02.2	Mechanisms exist to appropriately test and document proposed changes in a non-production environment before changes are implemented in a production environment.	5	
				intersects with	Security Impact Analysis for Changes	CHG-03	Mechanisms exist to analyze proposed changes for potential security impacts, prior to the implementation of the change.	5	
				intersects with	Access Restriction For Change	CHG-04	Mechanisms exist to enforce configuration restrictions in an effort to restrict the ability of users to conduct unauthorized changes.	5	
				intersects with	Exception Management	GOV-02.1	Mechanisms exist to prohibit exceptions to standards, except when the exception has been formally assessed for risk impact, approved and recorded.	5	
ID.RA-08	N/A	Processes for receiving, analyzing, and responding to vulnerability disclosures are established.	Functional	intersects with	Threat Intelligence Feeds Program	THR-01	Mechanisms exist to implement a threat intelligence program that includes a cross-organization information-sharing capability that can influence the development of the system and security architectures, selection of security solutions, monitoring, threat hunting, response and recovery activities.	5	
				intersects with	Indicators of Exposure (IOE)	THR-02	Mechanisms exist to develop Indicators of Exposure (IOE) to understand the potential attack vectors that attackers could use to attack the organization.	5	
				intersects with	Threat Intelligence Feeds Feeds	THR-03	Mechanisms exist to maintain situational awareness of vulnerabilities and evolving threats by leveraging the knowledge of attacker tactics, techniques and procedures to facilitate the implementation of preventative and compensating controls.	5	
				intersects with	Vulnerability & Patch Management Program (VPMP)	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	5	
				intersects with	Vulnerability Remediation Process	VPM-02	Mechanisms exist to ensure that vulnerabilities are properly identified, tracked and remediated.	5	
				intersects with	Vulnerability Ranking	VPM-03	Mechanisms exist to identify and assign a risk ranking to newly discovered security vulnerabilities using reputable outside sources for security vulnerability information.	5	
ID.RA-09	N/A	The authenticity and integrity of hardware and software are assessed prior to acquisition and use.	Functional	intersects with	Logical Tampering Protection	AST-15	Mechanisms exist to verify logical configuration settings and the physical integrity of critical technology assets throughout their lifecycle.	5	
				intersects with	Roots of Trust Protection	AST-18	Mechanisms exist to provision and protect the confidentiality, integrity and authenticity of product supplier keys and data that can be used as a "roots of trust" basis for integrity verification.	5	
				intersects with	Technology Development & Acquisition	TDA-01	Mechanisms exist to facilitate the implementation of tailored development and acquisition strategies, contract tools and procurement methods to meet unique business needs.	5	
				intersects with	Integrity Mechanisms for Software / Firmware Updates	TDA-01.2	Mechanisms exist to utilize integrity validation mechanisms for security updates.	5	
				intersects with	Developer Configuration Management	TDA-14	Mechanisms exist to require system developers and integrators to perform configuration management during system design, development, implementation and operation.	5	
				intersects with	Software / Firmware Integrity Verification	TDA-14.1	Mechanisms exist to require developers of Technology Assets, Applications and/or Services (TAAS) to enable integrity verification of software and firmware components.	5	
				intersects with	Hardware Integrity Verification	TDA-14.2	Mechanisms exist to require developers of Technology Assets, Applications and/or Services (TAAS) to enable integrity verification of hardware components.	5	
ID.RA-10	N/A	Critical suppliers are assessed prior to acquisition.	Functional	intersects with	Third-Party Inventories	TPM-01.1	Mechanisms exist to maintain a current, accurate and complete list of External Service Providers (ESPs) that can potentially impact the Confidentiality, Integrity, Availability and/or Safety (CIAS) of the organization's Technology Assets, Applications, Services and/or Data (TAASD).	5	
				intersects with	Third-Party Criticality Assessments	TPM-02	Mechanisms exist to identify, prioritize and assess suppliers and partners of critical Technology Assets, Applications and/or Services (TAAS) using a supply chain risk assessment process relative to their importance in supporting the delivery of high-value services.	5	
				intersects with	Third-Party Risk Assessments & Approvals	TPM-04.1	Mechanisms exist to conduct a risk assessment prior to the acquisition or outsourcing of technology-related Technology Assets, Applications and/or Services (TAAS).	5	
				intersects with	Operations Security	OPS-01	Mechanisms exist to facilitate the implementation of operational security controls.	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)
ID.IM	N/A	Improvements to organizational cybersecurity risk management processes, procedures and activities are identified across all CSF Functions.	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	
				subset of	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	10	
				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 Technology Assets, Applications and/or Services (TAAS), including documenting selected mitigating actions and monitoring performance against those plans.	5	
ID.IM-01	N/A	Improvements are identified from evaluations.	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	Functional Review Of Cybersecurity & Data Protection Controls	CPL-03.2	Mechanisms exist to regularly review technology assets for adherence to the organization's cybersecurity and data protection policies and standards.	5	
				intersects with	Assessments	IAO-02	Mechanisms exist to formally assess the cybersecurity and data protection controls in Technology Assets, Applications and/or Services (TAAS) through Information Assurance Program (IAP) activities to determine the extent to which the controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting expected requirements.	5	
				intersects with	Security Assessment Report (SAR)	IAO-02.4	Mechanisms exist to produce a Security Assessment Report (SAR) at the conclusion of a security assessment to certify the results of the assessment and assist with any remediation actions.	5	
				intersects with	Plan of Action & Milestones (POA&M)	IAO-05	Mechanisms exist to generate a Plan of Action and Milestones (POA&M), or similar risk register, to document planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities.	5	
				intersects with	Cybersecurity & Data Protection Testing Throughout Development	TDA-09	Mechanisms exist to require system developers/integrators consult with cybersecurity and data protection personnel to: (1) Create and implement a Security Testing and Evaluation (ST&E) plan, or similar capability; (2) Implement a verifiable flaw remediation process to correct weaknesses and deficiencies identified during the security testing and evaluation process; and (3) Document the results of the security testing/evaluation and flaw remediation processes.	5	
				intersects with	Continuous Monitoring Plan	TDA-09.1	Mechanisms exist to require the developers of Technology Assets, Applications and/or Services (TAAS) to produce a plan for the continuous monitoring of cybersecurity and data protection control effectiveness.	5	
				intersects with	Third-Party Risk Assessments & Approvals	TPM-04.1	Mechanisms exist to conduct a risk assessment prior to the acquisition or outsourcing of technology-related Technology Assets, Applications and/or Services (TAAS).	5	
				intersects with	Review of Third-Party Services	TPM-08	Mechanisms exist to monitor, regularly review and assess External Service Providers (ESPs) for compliance with established contractual requirements for cybersecurity and data protection controls.	5	
ID.IM-02	N/A	Improvements are identified from security tests and exercises, including those done in coordination with suppliers and relevant third parties.	Functional	intersects with	Contingency Plan Root Cause Analysis (RCA) & Lessons Learned	BCD-05	Mechanisms exist to conduct a Root Cause Analysis (RCA) and "lessons learned" activity every time the contingency plan is activated.	5	
				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	Functional Review Of Cybersecurity & Data Protection Controls	CPL-03.2	Mechanisms exist to regularly review technology assets for adherence to the organization's cybersecurity and data protection policies and standards.	5	
				intersects with	Assessments	IAO-02	Mechanisms exist to formally assess the cybersecurity and data protection controls in Technology Assets, Applications and/or Services (TAAS) through Information Assurance Program (IAP) activities to determine the extent to which the controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting expected requirements.	5	
				intersects with	Security Assessment Report (SAR)	IAO-02.4	Mechanisms exist to produce a Security Assessment Report (SAR) at the conclusion of a security assessment to certify the results of the assessment and assist with any remediation actions.	5	
				intersects with	Plan of Action & Milestones (POA&M)	IAO-05	Mechanisms exist to generate a Plan of Action and Milestones (POA&M), or similar risk register, to document planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities.	5	
				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.	5	
				intersects with	Cybersecurity & Data Protection Testing Throughout Development	TDA-09	Mechanisms exist to require system developers/integrators consult with cybersecurity and data protection personnel to: (1) Create and implement a Security Testing and Evaluation (ST&E) plan, or similar capability; (2) Implement a verifiable flaw remediation process to correct weaknesses and deficiencies identified during the security testing and evaluation process; and (3) Document the results of the security testing/evaluation and flaw remediation processes.	5	
				intersects with	Continuous Monitoring Plan	TDA-09.1	Mechanisms exist to require the developers of Technology Assets, Applications and/or Services (TAAS) to produce a plan for the continuous monitoring of cybersecurity and data protection control effectiveness.	5	
				intersects with	Third-Party Risk Assessments & Approvals	TPM-04.1	Mechanisms exist to conduct a risk assessment prior to the acquisition or outsourcing of technology-related Technology Assets, Applications and/or Services (TAAS).	5	
				intersects with	Review of Third-Party Services	TPM-08	Mechanisms exist to monitor, regularly review and assess External Service Providers (ESPs) for compliance with established contractual requirements for cybersecurity and data protection controls.	5	
ID.IM-03	N/A	Improvements are identified from execution of operational processes, procedures, and activities.	Functional	intersects with	Measures of Performance	GOV-05	Mechanisms exist to develop, report and monitor cybersecurity and data protection program measures of performance.	5	
				intersects with	Contingency Plan Root Cause Analysis (RCA) & Lessons Learned	BCD-05	Mechanisms exist to conduct a Root Cause Analysis (RCA) and "lessons learned" activity every time the contingency plan is activated.	5	
				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.	5	
ID.IM-04	N/A	Incident response plans and other cybersecurity plans that affect operations are established, communicated, maintained, and improved.	Functional	intersects with	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	5	
				intersects with	Ongoing Contingency Planning	BCD-06	Mechanisms exist to update contingency plans due to changes affecting: (1) People (e.g., personnel changes); (2) Processes (e.g., new, altered or decommissioned business practices, including	5	
				intersects with	Incident Response Plan (IRP)	IRO-04	Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.	5	
				intersects with	IRP Update	IRO-04.2	Mechanisms exist to regularly review and modify incident response practices to incorporate lessons learned, business process changes and industry developments, as necessary.	5	
PR	N/A	Safeguards to manage the organization's cybersecurity risks are used.	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	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	
				intersects with	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	5	
				intersects with	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	5	
				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 Technology Assets, Applications and/or Services (TAAS), including documenting selected mitigating actions and monitoring performance against those plans.	5	
				intersects with	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	5	
				intersects with	Authenticate, Authorize and Audit (AAA)	IAC-01.2	Mechanisms exist to strictly govern the use of Authenticate, Authorize and Audit (AAA) solutions, both on-premises and those hosted by an External Service Provider (ESP).	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)
PR.AA	N/A	Access to physical and logical assets is limited to authorized users, services, and hardware and managed commensurate with the assessed risk of unauthorized access.	Functional	intersects with	Physical & Environmental Protections	PES-01	Mechanisms exist to facilitate the operation of physical and environmental protection controls.	5	
				intersects with	Physical Access Authorizations	PES-02	Physical access control mechanisms exist to maintain a current list of personnel with authorized access to organizational facilities (except for those areas within the facility officially designated as publicly accessible).	5	
				intersects with	Physical Access Control	PES-03	Physical access control mechanisms exist to enforce physical access authorizations for all physical access points (including designated entry/exit points) to facilities (excluding those areas within the facility officially designated as publicly accessible).	5	
PR.AA-01	N/A	Identities and credentials for authorized users, services, and hardware are managed by the organization.	Functional	intersects with	Identification & Authentication for Organizational Users	IAC-02	Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) organizational users and processes acting on behalf of organizational users.	5	
				intersects with	Identification & Authentication for Non-Organizational Users	IAC-03	Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) third-party users and processes that provide services to the organization.	5	
				intersects with	Identification & Authentication for Devices	IAC-04	Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) devices before establishing a connection using bidirectional authentication that is cryptographically- based and replay resistant.	5	
				intersects with	Identification & Authentication for Third-Party Technology Assets, Applications and/or Services (TAAS)	IAC-05	Mechanisms exist to identify and authenticate third-party Technology Assets, Applications and/or Services (TAAS).	5	
PR.AA-02	N/A	Identities are proofed and bound to credentials based on the context of interactions.	Functional	equal	Identity Proofing (Identity Verification)	IAC-28	Mechanisms exist to verify the identity of a user before issuing authenticators or modifying access permissions.	10	
PR.AA-03	N/A	Users, services, and hardware are authenticated.	Functional	subset of	Authenticate, Authorize and Audit (AAA)	IAC-01.2	Mechanisms exist to strictly govern the use of Authenticate, Authorize and Audit (AAA) solutions, both on-premises and those hosted by an External Service Provider (ESP).	10	
				intersects with	Identification & Authentication for Organizational Users	IAC-02	Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) organizational users and processes acting on behalf of organizational users.	5	
				intersects with	Identification & Authentication for Non-Organizational Users	IAC-03	Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) third-party users and processes that provide services to the organization.	5	
				intersects with	Identification & Authentication for Devices	IAC-04	Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) devices before establishing a connection using bidirectional authentication that is cryptographically- based and replay resistant.	5	
				intersects with	Identification & Authentication for Third-Party Technology Assets, Applications and/or Services (TAAS)	IAC-05	Mechanisms exist to identify and authenticate third-party Technology Assets, Applications and/or Services (TAAS).	5	
PR.AA-04	N/A	Identity assertions are protected, conveyed, and verified.	Functional	intersects with	Authenticate, Authorize and Audit (AAA)	IAC-01.2	Mechanisms exist to strictly govern the use of Authenticate, Authorize and Audit (AAA) solutions, both on-premises and those hosted by an External Service Provider (ESP).	5	
				intersects with	Replay-Resistant Authentication	IAC-02.2	Automated mechanisms exist to employ replay-resistant authentication.	5	
				intersects with	Acceptance of External Authenticators	IAC-03.5	Mechanisms exist to restrict the use of external authenticators to those that are National Institute of Standards and Technology (NIST)-compliant and maintain a list of accepted external authenticators.	5	
PR.AA-05	N/A	Access permissions, entitlements, and authorizations are defined in a policy, managed, enforced, and reviewed, and incorporate the principles of least privilege and separation of duties.	Functional	intersects with	Position Categorization	HRS-02	Mechanisms exist to manage personnel security risk by assigning a risk designation to all positions and establishing screening criteria for individuals filling those positions.	5	
				intersects with	Separation of Duties (SoD)	HRS-11	Mechanisms exist to implement and maintain Separation of Duties (SoD) to prevent potential inappropriate activity without collusion.	5	
				subset of	Identity & Access Management (IAM)	IAC-01	Mechanisms exist to facilitate the implementation of identification and access management controls.	10	
				intersects with	Authenticate, Authorize and Audit (AAA)	IAC-01.2	Mechanisms exist to strictly govern the use of Authenticate, Authorize and Audit (AAA) solutions, both on-premises and those hosted by an External Service Provider (ESP).	5	
				intersects with	Identification & Authentication for Organizational Users	IAC-02	Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) organizational users and processes acting on behalf of organizational users.	5	
				intersects with	Identification & Authentication for Non-Organizational Users	IAC-03	Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) third-party users and processes that provide services to the organization.	5	
				intersects with	Identification & Authentication for Devices	IAC-04	Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) devices before establishing a connection using bidirectional authentication that is cryptographically- based and replay resistant.	5	
				intersects with	Identification & Authentication for Third-Party Technology Assets, Applications and/or Services (TAAS)	IAC-05	Mechanisms exist to identify and authenticate third-party Technology Assets, Applications and/or Services (TAAS).	5	
				intersects with	Role-Based Access Control (RBAC)	IAC-08	Mechanisms exist to enforce Role-Based Access Control (RBAC) for Technology Assets, Applications, Services and/or Data (TAASD) to restrict access to individuals assigned specific roles with legitimate business needs.	5	
				intersects with	Least Privilege	IAC-21	Mechanisms exist to utilize the concept of least privilege, allowing only authorized access to processes necessary to accomplish assigned tasks in accordance with organizational business functions.	5	
PR.AA-06	N/A	Physical access to assets is managed, monitored, and enforced commensurate with risk.	Functional	subset of	Physical & Environmental Protections	PES-01	Mechanisms exist to facilitate the operation of physical and environmental protection controls.	10	
				intersects with	Physical Access Authorizations	PES-02	Physical access control mechanisms exist to maintain a current list of personnel with authorized access to organizational facilities (except for those areas within the facility officially designated as publicly accessible).	5	
				intersects with	Role-Based Physical Access	PES-02.1	Physical access control mechanisms exist to authorize physical access to facilities based on the position or role of the individual.	5	
				intersects with	Physical Access Control	PES-03	Physical access control mechanisms exist to enforce physical access authorizations for all physical access points (including designated entry/exit points) to facilities (excluding those areas within the facility officially designated as publicly accessible).	5	
PR.AT	N/A	The organization's personnel are provided with cybersecurity awareness and training so that they can perform their cybersecurity-related tasks.	Functional	subset of	Cybersecurity & Data Protection-Minded Workforce	SAT-01	Mechanisms exist to facilitate the implementation of security workforce development and awareness controls.	10	
				intersects with	Cybersecurity & Data Protection Awareness Training	SAT-02	Mechanisms exist to provide all employees and contractors appropriate awareness education and training that is relevant for their job function.	5	
				intersects with	Role-Based Cybersecurity & Data Protection Training	SAT-03	Mechanisms exist to provide role-based cybersecurity and data protection-related training: (1) Before authorizing access to the system or performing assigned duties; (2) When required by system changes; and (3) Annually thereafter.	5	
PR.AT-01	N/A	Personnel are provided with awareness and training so that they possess the knowledge and skills to perform general tasks with cybersecurity risks in mind.	Functional	intersects with	Cybersecurity & Data Protection Awareness Training	SAT-02	Mechanisms exist to provide all employees and contractors appropriate awareness education and training that is relevant for their job function.	5	
				intersects with	Role-Based Cybersecurity & Data Protection Training	SAT-03	Mechanisms exist to provide role-based cybersecurity and data protection-related training: (1) Before authorizing access to the system or performing assigned duties; (2) When required by system changes; and (3) Annually thereafter.	5	
				intersects with	Cyber Threat Environment	SAT-03.6	Mechanisms exist to provide role-based cybersecurity and data protection awareness training that is current and relevant to the cyber threats that users might encounter in day-to-day business operations.	5	
PR.AT-02	N/A	Individuals in specialized roles are provided with awareness and training so that they possess the knowledge and skills to perform relevant tasks with cybersecurity risks in mind.	Functional	intersects with	Role-Based Cybersecurity & Data Protection Training	SAT-03	Mechanisms exist to provide role-based cybersecurity and data protection-related training: (1) Before authorizing access to the system or performing assigned duties; (2) When required by system changes; and (3) Annually thereafter.	5	
				intersects with	Privileged Users	SAT-03.5	Mechanisms exist to provide specific training for privileged users to ensure privileged users understand their unique roles and responsibilities	5	
				intersects with	Cyber Threat Environment	SAT-03.6	Mechanisms exist to provide role-based cybersecurity and data protection awareness training that is current and relevant to the cyber threats that users might encounter in day-to-day business operations.	5	
				intersects with	Continuing Professional Education (CPE) - Cybersecurity & Data Protection Personnel	SAT-03.7	Mechanisms exist to ensure cybersecurity and data protection personnel receive Continuing Professional Education (CPE) training to maintain currency and proficiency with industry-recognized secure practices that are pertinent to their assigned roles and responsibilities.	5	
				subset of	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	10	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
PR.DS	N/A	Data are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	Functional	intersects with	Data Stewardship	DCH-01.1	Mechanisms exist to ensure data stewardship is assigned, documented and communicated.	5	
				intersects with	Sensitive / Regulated Data Protection	DCH-01.2	Mechanisms exist to protect sensitive/regulated data wherever it is stored.	5	
				intersects with	Sensitive / Regulated Media Records	DCH-01.3	Mechanisms exist to ensure media records for sensitive/regulated data contain sufficient information to determine the potential impact in the event of a data loss incident.	5	
				intersects with	Defining Access Authorizations for Sensitive/Regulated Data	DCH-01.4	Mechanisms exist to explicitly define authorizations for specific individuals and/or roles for logical and /or physical access to sensitive/regulated data.	5	
				intersects with	Data & Asset Classification	DCH-02	Mechanisms exist to ensure data and assets are categorized in accordance with applicable statutory, regulatory and contractual requirements.	5	
				intersects with	Media Access	DCH-03	Mechanisms exist to control and restrict access to digital and non-digital media to authorized individuals.	5	
PR.DS-01	N/A	The confidentiality, integrity, and availability of data-at-rest are protected.	Functional	subset of	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	10	
				intersects with	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	5	
				intersects with	Alternate Physical Protection	CRY-01.1	Cryptographic mechanisms exist to prevent unauthorized disclosure of information as an alternative to physical safeguards.	5	
				intersects with	Encrypting Data At Rest	CRY-05	Cryptographic mechanisms exist to prevent unauthorized disclosure of data at rest.	5	
PR.DS-02	N/A	The confidentiality, integrity, and availability of data-in-transit are protected.	Functional	subset of	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	10	
				intersects with	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	5	
				intersects with	Transmission Confidentiality	CRY-03	Cryptographic mechanisms exist to protect the confidentiality of data being transmitted.	5	
				intersects with	Transmission Integrity	CRY-04	Cryptographic mechanisms exist to protect the integrity of data being transmitted.	5	
PR.DS-10	N/A	The confidentiality, integrity, and availability of data-in-use are protected.	Functional	subset of	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	10	
				intersects with	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	5	
				intersects with	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	5	
				intersects with	Least Privilege	IAC-21	Mechanisms exist to utilize the concept of least privilege, allowing only authorized access to processes necessary to accomplish assigned tasks in accordance with organizational business functions.	5	
PR.DS-11	N/A	Backups of data are created, protected, maintained, and tested.	Functional	intersects with	Data Backups	BCD-11	Mechanisms exist to create recurring backups of data, software and/or system images, as well as verify the integrity of these backups, to ensure the availability of the data to satisfy Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	5	
				intersects with	Testing for Reliability & Integrity	BCD-11.1	Mechanisms exist to routinely test backups that verify the reliability of the backup process, as well as the integrity and availability of the data.	5	
				intersects with	Test Restoration Using Sampling	BCD-11.5	Mechanisms exist to utilize sampling of available backups to test recovery capabilities as part of business continuity plan testing.	5	
				intersects with	Transfer to Alternate Storage Site	BCD-11.6	Mechanisms exist to transfer backup data to the alternate storage site at a rate that is capable of meeting both Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	5	
PR.PS	N/A	The hardware, software (e.g., firmware, operating systems, applications), and services of physical and virtual platforms are managed consistent with the organization's risk strategy to protect their confidentiality, integrity, and availability.	Functional	intersects with	Configuration Management Program	CFG-01	Mechanisms exist to facilitate the implementation of configuration management controls.	5	
				intersects with	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	5	
				intersects with	Reviews & Updates	CFG-02.1	Mechanisms exist to review and update baseline configurations: (1) At least annually; (2) When required due to so; or (3) As part of system component installations and upgrades.	5	
				intersects with	Configure Technology Assets, Applications and/or Services (TAAS) for High-Risk Areas	CFG-02.5	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) utilized in high-risk areas with more restrictive baseline configurations.	5	
				intersects with	Maintenance Operations	MNT-01	Mechanisms exist to develop, disseminate, review & update procedures to facilitate the implementation of maintenance controls across the enterprise.	5	
				intersects with	Controlled Maintenance	MNT-02	Mechanisms exist to conduct controlled maintenance activities throughout the lifecycle of the system, application or service.	5	
PR.PS-01	N/A	Configuration management practices are established and applied.	Functional	equal	Configuration Management Program	CFG-01	Mechanisms exist to facilitate the implementation of configuration management controls.	10	
PR.PS-02	N/A	Software is maintained, replaced, and removed commensurate with risk.	Functional	intersects with	Maintenance Operations	MNT-01	Mechanisms exist to develop, disseminate, review & update procedures to facilitate the implementation of maintenance controls across the enterprise.	5	
				intersects with	Controlled Maintenance	MNT-02	Mechanisms exist to conduct controlled maintenance activities throughout the lifecycle of the system, application or service.	5	
				intersects with	Timely Maintenance	MNT-03	Mechanisms exist to obtain maintenance support and/or spare parts for Technology Assets, Applications and/or Services (TAAS) within a defined Recovery Time Objective (RTO).	5	
				intersects with	Preventative Maintenance	MNT-03.1	Mechanisms exist to perform preventive maintenance on critical Technology Assets, Applications and/or Services (TAAS).	5	
				intersects with	Secure Development Life Cycle (SDLC) Management	PRM-07	Mechanisms exist to ensure changes to Technology Assets, Applications and/or Services (TAAS) within the Secure Development Life Cycle (SDLC) are controlled through formal change control procedures.	5	
				intersects with	Technology Lifecycle Management	SEA-07.1	Mechanisms exist to manage the usable lifecycles of technology assets.	5	
				intersects with	Unsupported Technology Assets, Applications and/or Services (TAAS)	TDA-17	Mechanisms exist to prevent unsupported Technology Assets, Applications and/or Services (TAAS) by: (1) Removing and/or replacing TAAS when support for the components is no longer available from the developer, vendor or manufacturer; and (2) Requiring justification and documented approval for the continued use of unsupported TAAS required to satisfy mission/business needs.	5	
				intersects with	Vulnerability & Patch Management Program (VPMP)	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	5	
				intersects with	Attack Surface Scope	VPM-01.1	Mechanisms exist to define and manage the scope for its attack surface management activities.	5	
				intersects with	Vulnerability Remediation Process	VPM-02	Mechanisms exist to ensure that vulnerabilities are properly identified, tracked and remediated.	5	
				intersects with	Software & Firmware Patching	VPM-05	Mechanisms exist to conduct software patching for all deployed Technology Assets, Applications and/or Services (TAAS), including firmware.	5	
PR.PS-03	N/A	Hardware is maintained, replaced, and removed commensurate with risk.	Functional	intersects with	Maintenance Operations	MNT-01	Mechanisms exist to develop, disseminate, review & update procedures to facilitate the implementation of maintenance controls across the enterprise.	5	
				intersects with	Controlled Maintenance	MNT-02	Mechanisms exist to conduct controlled maintenance activities throughout the lifecycle of the system, application or service.	5	
				intersects with	Timely Maintenance	MNT-03	Mechanisms exist to obtain maintenance support and/or spare parts for Technology Assets, Applications and/or Services (TAAS) within a defined Recovery Time Objective (RTO).	5	
				intersects with	Preventative Maintenance	MNT-03.1	Mechanisms exist to perform preventive maintenance on critical Technology Assets, Applications and/or Services (TAAS).	5	
				intersects with	Secure Development Life Cycle (SDLC) Management	PRM-07	Mechanisms exist to ensure changes to Technology Assets, Applications and/or Services (TAAS) within the Secure Development Life Cycle (SDLC) are controlled through formal change control procedures.	5	
				intersects with	Technology Lifecycle Management	SEA-07.1	Mechanisms exist to manage the usable lifecycles of technology assets.	5	
				intersects with	Unsupported Technology Assets, Applications and/or Services (TAAS)	TDA-17	Mechanisms exist to prevent unsupported Technology Assets, Applications and/or Services (TAAS) by: (1) Removing and/or replacing TAAS when support for the components is no longer available from the developer, vendor or manufacturer; and (2) Requiring justification and documented approval for the continued use of unsupported TAAS required to satisfy mission/business needs.	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)
PR.PS-04	N/A	Log records are generated and made available for continuous monitoring.	Functional	subset of	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	10	
				intersects with	System Generated Alerts	MON-01.4	Mechanisms exist to generate, monitor, correlate and respond to alerts from physical, cybersecurity, data privacy and supply chain activities to achieve integrated situational awareness.	5	
				intersects with	Content of Event Logs	MON-03	Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) to produce event logs that contain sufficient information to, at a minimum: (1) Establish what type of event occurred; (2) When (date and time) the event occurred; (3) Where the event occurred; (4) The source of the event; (5) The outcome (success or failure) of the event; and (6) The identity of any user/subject associated with the event.	5	
PR.PS-05	N/A	Installation and execution of unauthorized software are prevented.	Functional	intersects with	Configuration Management Program	CFG-01	Mechanisms exist to facilitate the implementation of configuration management controls.	5	
				intersects with	Secure Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	5	
				intersects with	Least Functionality	CFG-03	Mechanisms exist to configure systems to provide only essential capabilities by specifically prohibiting or restricting the use of ports, protocols, and/or services.	5	
				intersects with	Prevent Unauthorized Software Execution	CFG-03.2	Mechanisms exist to configure systems to prevent the execution of unauthorized software programs.	5	
				intersects with	User-Installed Software	CFG-05	Mechanisms exist to restrict the ability of non-privileged users to install unauthorized software.	5	
				intersects with	Prohibit Installation Without Privileged Status	END-03	Automated mechanisms exist to prohibit software installations without explicitly assigned privileged status.	5	
PR.PS-06	N/A	Secure software development practices are integrated, and their performance is monitored throughout the software development life cycle.	Functional	intersects with	Technology Development & Acquisition	TDA-01	Mechanisms exist to facilitate the implementation of tailored development and acquisition strategies, contract tools and procurement methods to meet unique business needs.	5	
				intersects with	Product Management	TDA-01.1	Mechanisms exist to design and implement product management processes to proactively govern the design, development and production of Technology Assets, Applications and/or Services (TAAS) across the System Development Life Cycle (SDLC) to: (1) Improve functionality; (2) Enhance security and resiliency capabilities; (3) Correct security deficiencies; and (4) Conform with applicable statutory, regulatory and/or contractual obligations.	5	
				intersects with	Secure Software Development Practices (SSDP)	TDA-06	Mechanisms exist to develop applications based on Secure Software Development Practices (SSDP).	5	
				intersects with	Criticality Analysis	TDA-06.1	Mechanisms exist to require the developer of the system, system component or service to perform a criticality analysis at organization-defined decision points in the Secure Development Life Cycle (SDLC).	5	
				intersects with	Threat Modeling	TDA-06.2	Mechanisms exist to perform threat modelling and other secure design techniques, to ensure that threats to software and solutions are identified and accounted for.	5	
				intersects with	Software Assurance Maturity Model (SAMM)	TDA-06.3	Mechanisms exist to utilize a Software Assurance Maturity Model (SAMM) to govern a secure development lifecycle for the development of Technology Assets, Applications and/or Services (TAAS).	5	
				intersects with	Cybersecurity & Data Protection Testing Throughout Development	TDA-09	Mechanisms exist to require system developers/integrators consult with cybersecurity and data protection personnel to: (1) Create and implement a Security Testing and Evaluation (ST&E) plan, or similar capability; (2) Implement a verifiable flaw remediation process to correct weaknesses and deficiencies identified during the security testing and evaluation process; and (3) Document the results of the security testing/evaluation and flaw remediation processes.	5	
PR.IR	N/A	Security architectures are managed with the organization's risk strategy to protect asset confidentiality, integrity, and availability, and organizational resilience.	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	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	
				intersects with	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	5	
				subset of	Secure Engineering Principles	SEA-01	Mechanisms exist to facilitate the implementation of industry-recognized cybersecurity and data protection practices in the specification, design, development, implementation and modification of Technology Assets, Applications and/or Services (TAAS).	10	
				intersects with	Centralized Management of Cybersecurity & Data Protection Controls	SEA-01.1	Mechanisms exist to centrally-manage the organization-wide management and implementation of cybersecurity and data protection controls and related processes.	5	
				intersects with	Achieving Resilience Requirements	SEA-01.2	Mechanisms exist to achieve resilience requirements in normal and adverse situations.	5	
				intersects with	Alignment With Enterprise Architecture	SEA-02	Mechanisms exist to develop an enterprise architecture, aligned with industry-recognized leading practices, with consideration for cybersecurity and data protection principles that addresses risk to organizational operations, assets, individuals, other organizations.	5	
PR.IR-01	N/A	Networks and environments are protected from unauthorized logical access and usage.	Functional	subset of	Network Security Controls (NSC)	NET-01	Mechanisms exist to develop, govern & update procedures to facilitate the implementation of Network Security Controls (NSC).	10	
				intersects with	Layered Network Defenses	NET-02	Mechanisms exist to implement security functions as a layered structure that minimizes interactions between layers of the design and avoids any dependence by lower layers on the functionality or correctness of higher layers.	5	
				intersects with	Secure Engineering Principles	SEA-01	Mechanisms exist to facilitate the implementation of industry-recognized cybersecurity and data protection practices in the specification, design, development, implementation and modification of Technology Assets, Applications and/or Services (TAAS).	5	
				intersects with	Alignment With Enterprise Architecture	SEA-02	Mechanisms exist to develop an enterprise architecture, aligned with industry-recognized leading practices, with consideration for cybersecurity and data protection principles that addresses risk to organizational operations, assets, individuals, other organizations.	5	
PR.IR-02	N/A	The organization's technology assets are protected from environmental threats.	Functional	intersects with	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	5	
				subset of	Physical & Environmental Protections	PES-01	Mechanisms exist to facilitate the operation of physical and environmental protection controls.	10	
				intersects with	Supporting Utilities	PES-07	Facility security mechanisms exist to protect power equipment and power cabling for the system from damage and destruction.	5	
				intersects with	Water Damage Protection	PES-07.5	Facility security mechanisms exist to protect systems from damage resulting from water leakage by providing master shutoff valves that are accessible, working properly and known to key personnel.	5	
				intersects with	Fire Protection	PES-08	Facility security mechanisms exist to utilize and maintain fire suppression and detection devices/systems for the system that are supported by an independent energy source.	5	
				intersects with	Temperature & Humidity Controls	PES-09	Facility security mechanisms exist to maintain and monitor temperature and humidity levels within the facility.	5	
				intersects with	Achieving Resilience Requirements	SEA-01.2	Mechanisms exist to achieve resilience requirements in normal and adverse situations.	5	
				intersects with	Threat Catalog	THR-09	Mechanisms exist to develop and keep current a catalog of applicable internal and external threats to the organization, both natural and manmade.	5	
PR.IR-03	N/A	Mechanisms are implemented to achieve resilience requirements in normal and adverse situations.	Functional	subset of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	
				intersects with	Secure Engineering Principles	SEA-01	Mechanisms exist to facilitate the implementation of industry-recognized cybersecurity and data protection practices in the specification, design, development, implementation and modification of Technology Assets, Applications and/or Services (TAAS).	5	
				intersects with	Alignment With Enterprise Architecture	SEA-02	Mechanisms exist to develop an enterprise architecture, aligned with industry-recognized leading practices, with consideration for cybersecurity and data protection principles that addresses risk to organizational operations, assets, individuals, other organizations.	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)
				intersects with	Achieving Resilience Requirements	SEA-01.2	Mechanisms exist to achieve resilience requirements in normal and adverse situations.	5	
PR.IR-04	N/A	Adequate resource capacity to ensure availability is maintained.	Functional	subset of	Capacity & Performance Management	CAP-01	Mechanisms exist to facilitate the implementation of capacity management controls to ensure optimal system performance to meet expected and anticipated future capacity requirements.	10	
				intersects with	Resource Priority	CAP-02	Mechanisms exist to control resource utilization of Technology Assets, Applications and/or Services (TAAS) that are susceptible to Denial of Service (DoS) attacks to limit and prioritize the use of resources.	5	
				intersects with	Capacity Planning	CAP-03	Mechanisms exist to conduct capacity planning so that necessary capacity for information processing, telecommunications and environmental support will exist during contingency operations.	5	
				intersects with	Performance Monitoring	CAP-04	Automated mechanisms exist to centrally-monitor and alert on the operating state and health status of critical Technology Assets, Applications and/or Services (TAAS).	5	
				intersects with	Elastic Expansion	CAP-05	Mechanisms exist to automatically scale the resources available for Technology Assets, Applications and/or Services (TAAS), as demand conditions change.	5	
DE	N/A	Possible cybersecurity attacks and compromises are found and analyzed.	Functional	subset of	Threat Intelligence Feeds Program	THR-01	Mechanisms exist to implement a threat intelligence program that includes a cross-organization information-sharing capability that can influence the development of the system and security architectures, selection of security solutions, monitoring, threat hunting, response and recovery activities.	10	
				intersects with	Indicators of Exposure (IOE)	THR-02	Mechanisms exist to develop Indicators of Exposure (IOE) to understand the potential attack vectors that attackers could use to attack the organization.	5	
				intersects with	Threat Intelligence Feeds Feeds	THR-03	Mechanisms exist to maintain situational awareness of vulnerabilities and evolving threats by leveraging the knowledge of attacker tactics, techniques and procedures to facilitate the implementation of preventative and compensating controls.	5	
				intersects with	Threat Hunting	THR-07	Mechanisms exist to perform cyber threat hunting that uses Indicators of Compromise (IoC) to detect, track and disrupt threats that evade existing security controls.	5	
				intersects with	Threat Catalog	THR-09	Mechanisms exist to develop and keep current a catalog of applicable internal and external threats to the organization, both natural and manmade.	5	
				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	
DE.CM	N/A	Assets are monitored to find anomalies, indicators of compromise, and other potentially adverse events.	Functional	intersects with	Monitoring for Indicators of Compromise (IOC)	MON-11.3	Automated mechanisms exist to identify and alert on Indicators of Compromise (IoC).	5	
				intersects with	Anomalous Behavior	MON-16	Mechanisms exist to utilize User & Entity Behavior Analytics (UEBA) and/or User Activity Monitoring (UAM) solutions to detect and respond to anomalous behavior that could indicate account compromise or other malicious activities.	5	
				intersects with	Indicators of Compromise (IOC)	IRO-03	Mechanisms exist to define specific Indicators of Compromise (IOC) to identify the signs of potential cybersecurity events.	5	
				intersects with	Indicators of Exposure (IOE)	THR-02	Mechanisms exist to develop Indicators of Exposure (IOE) to understand the potential attack vectors that attackers could use to attack the organization.	5	
DE.CM-01	N/A	Networks and network services are monitored to find potentially adverse events.	Functional	subset of	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	10	
				intersects with	Intrusion Detection & Prevention Systems (IDS & IPS)	MON-01.1	Mechanisms exist to implement Intrusion Detection / Prevention Systems (IDS / IPS) technologies on critical systems, key network segments and network choke points.	5	
				intersects with	Inbound & Outbound Communications Traffic	MON-01.3	Mechanisms exist to continuously monitor inbound and outbound communications traffic for unusual or unauthorized activities or conditions.	5	
				intersects with	System Generated Alerts	MON-01.4	Mechanisms exist to generate, monitor, correlate and respond to alerts from physical, cybersecurity, data privacy and supply chain activities to achieve integrated situational awareness.	5	
				intersects with	Security Event Monitoring	MON-01.8	Mechanisms exist to review event logs on an ongoing basis and escalate incidents in accordance with established timelines and procedures.	5	
DE.CM-02	N/A	The physical environment is monitored to find potentially adverse events.	Functional	intersects with	Physical & Environmental Protections	PES-01	Mechanisms exist to facilitate the operation of physical and environmental protection controls.	5	
				intersects with	Physical Access Control	PES-03	Physical access control mechanisms exist to enforce physical access authorizations for all physical access points (including designated entry/exit points) to facilities (excluding those areas within the facility officially designated as publicly accessible).	5	
				intersects with	Physical Access Logs	PES-03.3	Physical access control mechanisms generate a log entry for each access attempt through controlled ingress and egress points.	5	
				intersects with	Monitoring Physical Access	PES-05	Physical access control mechanisms exist to monitor for, detect and respond to physical security incidents.	5	
DE.CM-03	N/A	Personnel activity and technology usage are monitored to find potentially adverse events.	Functional	intersects with	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	5	
				intersects with	Anomalous Behavior	MON-16	Mechanisms exist to utilize User & Entity Behavior Analytics (UEBA) and/or User Activity Monitoring (UAM) solutions to detect and respond to anomalous behavior that could indicate account compromise or other malicious activities.	5	
				intersects with	Insider Threats	MON-16.1	Mechanisms exist to monitor internal personnel activity for potential security incidents.	5	
				intersects with	Unauthorized Activities	MON-16.3	Mechanisms exist to monitor for unauthorized activities, accounts, connections, devices and software.	5	
				intersects with	DNS & Content Filtering	NET-18	Mechanisms exist to force Internet-bound network traffic through a proxy device (e.g., Policy Enforcement Point (PEP)) for URL content filtering and DNS filtering to limit a user's ability to connect to dangerous or prohibited Internet sites.	5	
DE.CM-06	N/A	External service provider activities and services are monitored to find potentially adverse events.	Functional	intersects with	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	5	
				intersects with	Third-Party Threats	MON-16.2	Mechanisms exist to monitor third-party personnel activity for potential security incidents.	5	
				intersects with	Account Creation and Modification Logging	MON-16.4	Automated mechanisms exist to generate event logs for permissions changes to privileged accounts and/or groups.	5	
DE.CM-09	N/A	Computing hardware and software, runtime environments, and their data are monitored to find potentially adverse events.	Functional	intersects with	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	5	
				intersects with	File Integrity Monitoring (FIM)	MON-01.7	Mechanisms exist to utilize a File Integrity Monitor (FIM), or similar change-detection technology, on critical assets to generate alerts for unauthorized modifications.	5	
				intersects with	Enterprise Device Management (EDM)	END-01	Mechanisms exist to facilitate the implementation of Enterprise Device Management (EDM) controls.	5	
				intersects with	Malicious Code Protection (Anti-Malware)	END-04	Mechanisms exist to utilize antimalware technologies to detect and eradicate malicious code.	5	
				intersects with	Endpoint File Integrity Monitoring (FIM)	END-06	Mechanisms exist to utilize File Integrity Monitor (FIM), or similar technologies, to detect and report on unauthorized changes to selected files and configuration settings.	5	
DE.AE	N/A	Anomalies, indicators of compromise, and other potentially adverse events are analyzed to characterize the events and detect cybersecurity incidents.	Functional	intersects with	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	5	
				intersects with	Security Event Monitoring	MON-01.8	Mechanisms exist to review event logs on an ongoing basis and escalate incidents in accordance with established timelines and procedures.	5	
				intersects with	Automated Alerts	MON-01.12	Mechanisms exist to automatically alert incident response personnel to inappropriate or anomalous activities that have potential security incident implications.	5	
				subset of	Incident Response Operations	IRO-01	Mechanisms exist to implement and govern processes and documentation to facilitate an organization-wide response capability for cybersecurity and data protection-related incidents.	10	
				intersects with	Incident Handling	IRO-02	Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Eradication; and (6) Recovery.	5	
				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	
DE.AE-02	N/A	Potentially adverse events are analyzed to better understand associated activities.	Functional	intersects with	Incident Handling	IRO-02	Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Eradication; and (6) Recovery.	5	
				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	
				intersects with	Centralized Collection of Security Event Logs	MON-02	Mechanisms exist to utilize a Security Incident Event Manager (SIEM) or similar automated tool, to support the centralized collection of security-related event logs.	8	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
DE.AE-03	N/A	Information is correlated from multiple sources.	Functional	intersects with	Correlate Monitoring Information	MON-02.1	Automated mechanisms exist to correlate both technical and non-technical information from across the enterprise by a Security Incident Event Manager (SIEM) or similar automated tool, to enhance organization-wide situational awareness.	10	
				intersects with	Incident Handling	IRO-02	Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Eradication; and (6) Recovery.	3	
				intersects with	Correlation with External Organizations	IRO-02.5	Mechanisms exist to coordinate with approved third-parties to achieve a cross-organization perspective on incident awareness and more effective incident responses.	5	
DE.AE-04	N/A	The estimated impact and scope of adverse events are understood.	Functional	intersects with	Incident Handling	IRO-02	Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Eradication; and (6) Recovery.	5	
				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	
				intersects with	Materiality Determination	GOV-16	Mechanisms exist to define materiality threshold criteria capable of designating an incident as material.	5	
DE.AE-06	N/A	Information on adverse events is provided to authorized staff and tools.	Functional	intersects with	Security Event Monitoring	MON-01.8	Mechanisms exist to review event logs on an ongoing basis and escalate incidents in accordance with established timelines and procedures.	5	
				intersects with	Automated Alerts	MON-01.12	Mechanisms exist to automatically alert incident response personnel to inappropriate or anomalous activities that have potential security incident implications.	5	
				intersects with	Centralized Collection of Security Event Logs	MON-02	Mechanisms exist to utilize a Security Incident Event Manager (SIEM) or similar automated tool, to support the centralized collection of security-related event logs.	5	
				intersects with	Correlate Monitoring Information	MON-02.1	Automated mechanisms exist to correlate both technical and non-technical information from across the enterprise by a Security Incident Event Manager (SIEM) or similar automated tool, to enhance organization-wide situational awareness.	5	
				intersects with	Incident Handling	IRO-02	Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Eradication; and (6) Recovery.	5	
				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	
				intersects with	Incident Response Plan (IRP)	IRO-04	Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.	5	
				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 and data protection incident response operations.	5	
				intersects with	Situational Awareness For Incidents	IRO-09	Mechanisms exist to document, monitor and report the status of cybersecurity and data protection incidents to internal stakeholders all the way through the resolution of the incident.	5	
				intersects with	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable: (1) Internal stakeholders; (2) Affected clients & third-parties; and (3) Regulatory authorities.	5	
DE.AE-07	N/A	Cyber threat intelligence and other contextual information are integrated into the analysis.	Functional	subset of	Threat Intelligence Feeds Program	THR-01	Mechanisms exist to implement a threat intelligence program that includes a cross-organization information-sharing capability that can influence the development of the system and security architectures, selection of security solutions, monitoring, threat hunting, response and recovery activities.	10	
				intersects with	Threat Intelligence Feeds Feeds	THR-03	Mechanisms exist to maintain situational awareness of vulnerabilities and evolving threats by leveraging the knowledge of attacker tactics, techniques and procedures to facilitate the implementation of preventative and compensating controls.	5	
				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	
DE.AE-08	N/A	Incidents are declared when adverse events meet the defined incident criteria.	Functional	intersects with	Incident Handling	IRO-02	Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Eradication; and (6) Recovery.	5	
				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	
RS	N/A	Actions regarding a detected cybersecurity incident are taken.	Functional	subset of	Incident Response Operations	IRO-01	Mechanisms exist to implement and govern processes and documentation to facilitate an organization-wide response capability for cybersecurity and data protection-related incidents.	10	
				intersects with	Incident Handling	IRO-02	Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Eradication; and (6) Recovery.	5	
				intersects with	Incident Response Plan (IRP)	IRO-04	Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.	5	
				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 and data protection incident response operations.	5	
				intersects with	Situational Awareness For Incidents	IRO-09	Mechanisms exist to document, monitor and report the status of cybersecurity and data protection incidents to internal stakeholders all the way through the resolution of the incident.	5	
				intersects with	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable: (1) Internal stakeholders; (2) Affected clients & third-parties; and (3) Regulatory authorities.	5	
RS.MA	N/A	Responses to detected cybersecurity incidents are managed.	Functional	intersects with	Incident Handling	IRO-02	Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Eradication; and (6) Recovery.	5	
				intersects with	Incident Response Plan (IRP)	IRO-04	Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.	5	
				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 and data protection incident response operations.	5	
RS.MA-01	N/A	The incident response plan is executed in coordination with relevant third parties once an incident is declared.	Functional	intersects with	Incident Handling	IRO-02	Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Eradication; and (6) Recovery.	5	
				intersects with	Correlation with External Organizations	IRO-02.5	Mechanisms exist to coordinate with approved third-parties to achieve a cross-organization perspective on incident awareness and more effective incident responses.	5	
				intersects with	Incident Response Plan (IRP)	IRO-04	Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.	5	
				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 and data protection incident response operations.	5	
				intersects with	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable: (1) Internal stakeholders; (2) Affected clients & third-parties; and (3) Regulatory authorities.	5	

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)
RS.MA-02	N/A	Incident reports are triaged and validated.	Functional	intersects with	Incident Handling	IRO-02	Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Eradication; and (6) Recovery.	5	
				intersects with	Incident Response Plan (IRP)	IRO-04	Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.	5	
RS.MA-03	N/A	Incidents are categorized and prioritized.	Functional	equal	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.	10	
RS.MA-04	N/A	Incidents are escalated or elevated as needed.	Functional	intersects with	Incident Handling	IRO-02	Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Eradication; and (6) Recovery.	5	
				intersects with	Incident Response Plan (IRP)	IRO-04	Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.	5	
				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 and data protection incident response operations.	5	
RS.MA-05	N/A	The criteria for initiating incident recovery are applied.	Functional	intersects with	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	5	
				intersects with	Recovery Operations Criteria	BCD-01.5	Mechanisms exist to define spefic criteria necessary that must be met to execute Disaster Recover / Business Continuity (BC/DR) plans to facilitate business continuity operations capable of meeting applicable Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	5	
RS.AN	N/A	Investigations are conducted to ensure effective response and support forensics and recovery activities.	Functional	intersects with	Incident Handling	IRO-02	Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Eradication; and (6) Recovery.	5	
				intersects with	Chain of Custody & Forensics	IRO-08	Mechanisms exist to perform digital forensics and maintain the integrity of the chain of custody, in accordance with applicable laws, regulations and industry-recognized secure practices.	5	
RS.AN-03	N/A	Analysis is performed to establish what has taken place during an incident and the root cause of the incident.	Functional	equal	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.	10	
RS.AN-06	N/A	Actions performed during an investigation are recorded, and the records' integrity and provenance are preserved.	Functional	intersects with	Incident Handling	IRO-02	Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Eradication; and (6) Recovery.	5	
				intersects with	Chain of Custody & Forensics	IRO-08	Mechanisms exist to perform digital forensics and maintain the integrity of the chain of custody, in accordance with applicable laws, regulations and industry-recognized secure practices.	5	
				intersects with	Situational Awareness For Incidents	IRO-09	Mechanisms exist to document, monitor and report the status of cybersecurity and data protection incidents to internal stakeholders all the way through the resolution of the incident.	5	
RS.AN-07	N/A	Incident data and metadata are collected, and their integrity and provenance are preserved.	Functional	subset of	Chain of Custody & Forensics	IRO-08	Mechanisms exist to perform digital forensics and maintain the integrity of the chain of custody, in accordance with applicable laws, regulations and industry-recognized secure practices.	10	
RS.AN-08	N/A	An incident's magnitude is estimated and validated.	Functional	equal	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.	10	
RS.CO	N/A	Response activities are coordinated with internal and external stakeholders as required by laws, regulations, or policies.	Functional	intersects with	Incident Handling	IRO-02	Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Eradication; and (6) Recovery.	5	
				intersects with	Correlation with External Organizations	IRO-02.5	Mechanisms exist to coordinate with approved third-parties to achieve a cross-organization perspective on incident awareness and more effective incident responses.	5	
				intersects with	Coordination with Related Plans	IRO-06.1	Mechanisms exist to coordinate incident response testing with organizational elements responsible for related plans.	5	
				intersects with	Situational Awareness For Incidents	IRO-09	Mechanisms exist to document, monitor and report the status of cybersecurity and data protection incidents to internal stakeholders all the way through the resolution of the incident.	5	
				intersects with	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable: (1) Internal stakeholders; (2) Affected clients & third-parties; and (3) Regulatory authorities.	5	
				intersects with	Cyber Incident Reporting for Sensitive Data	IRO-10.2	Mechanisms exist to report sensitive/regulated data incidents in a timely manner.	5	
				intersects with	Supply Chain Coordination	IRO-10.4	Mechanisms exist to provide cybersecurity and data protection incident information to the provider of the Technology Assets, Applications and/or Services (TAAS) and other organizations involved in the supply chain for TAAS related to the incident.	5	
RS.CO-02	N/A	Internal and external stakeholders are notified of incidents.	Functional	intersects with	Incident Handling	IRO-02	Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Eradication; and (6) Recovery.	5	
				intersects with	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable: (1) Internal stakeholders; (2) Affected clients & third-parties; and (3) Regulatory authorities.	5	
				intersects with	Cyber Incident Reporting for Sensitive Data	IRO-10.2	Mechanisms exist to report sensitive/regulated data incidents in a timely manner.	5	
				intersects with	Supply Chain Coordination	IRO-10.4	Mechanisms exist to provide cybersecurity and data protection incident information to the provider of the Technology Assets, Applications and/or Services (TAAS) and other organizations involved in the supply chain for TAAS related to the incident.	5	
RS.CO-03	N/A	Information is shared with designated internal and external stakeholders.	Functional	intersects with	Incident Handling	IRO-02	Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Eradication; and (6) Recovery.	5	
				intersects with	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable: (1) Internal stakeholders; (2) Affected clients & third-parties; and (3) Regulatory authorities.	5	
				intersects with	Cyber Incident Reporting for Sensitive Data	IRO-10.2	Mechanisms exist to report sensitive/regulated data incidents in a timely manner.	5	
				intersects with	Supply Chain Coordination	IRO-10.4	Mechanisms exist to provide cybersecurity and data protection incident information to the provider of the Technology Assets, Applications and/or Services (TAAS) and other organizations involved in the supply chain for TAAS related to the incident.	5	
RS.MI	N/A	Activities are performed to prevent expansion of an event and mitigate its effects.	Functional	intersects with	Incident Response Operations	IRO-01	Mechanisms exist to implement and govern processes and documentation to facilitate an organization-wide response capability for cybersecurity and data protection-related incidents.	5	
				intersects with	Incident Handling	IRO-02	Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Eradication; and (6) Recovery.	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)
				intersects with	Incident Response Plan (IRP)	IRO-04	Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.	5	
RS.MI-01	N/A	Incidents are contained.	Functional	subset of	Incident Handling	IRO-02	Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Eradication; and (6) Recovery.	10	
RS.MI-02	N/A	Incidents are eradicated.	Functional	subset of	Incident Handling	IRO-02	Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Eradication; and (6) Recovery.	10	
RC	N/A	Assets and operations affected by a cybersecurity incident are restored.	Functional	subset of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	
				intersects with	Technology Assets, Applications and/or Services (TAAS) Recovery & Reconstitution	BCD-12	Mechanisms exist to ensure the secure recovery and reconstitution of Technology Assets, Applications and/or Services (TAAS) to a known state after a disruption, compromise or failure.	5	
RC.RP	N/A	Restoration activities are performed to ensure operational availability of systems and services affected by cybersecurity incidents.	Functional	subset of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	
				intersects with	Recovery Time / Point Objectives (RTO / RPO)	BCD-01.4	Mechanisms exist to facilitate recovery operations in accordance with Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	5	
				intersects with	Identify Critical Assets	BCD-02	Mechanisms exist to identify and document the critical Technology Assets, Applications, Services and/or Data (TAASD) that support essential missions and business functions.	5	
				intersects with	Resume All Missions & Business Functions	BCD-02.1	Mechanisms exist to resume all missions and business functions within Recovery Time Objectives (RTOs) of the contingency plan's activation.	5	
RC.RP-01	N/A	The recovery portion of the incident response plan is executed once initiated from the incident response process.	Functional	intersects with	Recovery Operations Criteria	BCD-01.5	Mechanisms exist to define spefic criteria necessary that must be met to execute Disaster Recover / Business Continuity (BC/DR) plans to facilitate business continuity operations capable of meeting applicable Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	5	
				intersects with	Technology Assets, Applications and/or Services (TAAS) Recovery & Reconstitution	BCD-12	Mechanisms exist to ensure the secure recovery and reconstitution of Technology Assets, Applications and/or Services (TAAS) to a known state after a disruption, compromise or failure.	5	
RC.RP-02	N/A	Recovery actions are selected, scoped, prioritized, and performed.	Functional	subset of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	
				intersects with	Recovery Time / Point Objectives (RTO / RPO)	BCD-01.4	Mechanisms exist to facilitate recovery operations in accordance with Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	5	
				intersects with	Identify Critical Assets	BCD-02	Mechanisms exist to identify and document the critical Technology Assets, Applications, Services and/or Data (TAASD) that support essential missions and business functions.	5	
				intersects with	Resume All Missions & Business Functions	BCD-02.1	Mechanisms exist to resume all missions and business functions within Recovery Time Objectives (RTOs) of the contingency plan's activation.	5	
RC.RP-03	N/A	The integrity of backups and other restoration assets is verified before using them for restoration.	Functional	intersects with	Backup & Restoration Hardware Protection	BCD-13	Mechanisms exist to protect backup and restoration hardware and software.	5	
				intersects with	Restoration Integrity Verification	BCD-13.1	Mechanisms exist to verify the integrity of backups and other restoration assets prior to using them for restoration.	5	
RC.RP-04	N/A	Critical mission functions and cybersecurity risk management are considered to establish post-incident operational norms.	Functional	subset of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient Technology Assets, Applications and/or Services (TAAS) (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	
				intersects with	Recovery Time / Point Objectives (RTO / RPO)	BCD-01.4	Mechanisms exist to facilitate recovery operations in accordance with Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	5	
				intersects with	Identify Critical Assets	BCD-02	Mechanisms exist to identify and document the critical Technology Assets, Applications, Services and/or Data (TAASD) that support essential missions and business functions.	5	
				intersects with	Resume All Missions & Business Functions	BCD-02.1	Mechanisms exist to resume all missions and business functions within Recovery Time Objectives (RTOs) of the contingency plan's activation.	5	
RC.RP-05	N/A	The integrity of restored assets is verified, systems and services are restored, and normal operating status is confirmed.	Functional	subset of	Technology Assets, Applications and/or Services (TAAS) Recovery & Reconstitution	BCD-12	Mechanisms exist to ensure the secure recovery and reconstitution of Technology Assets, Applications and/or Services (TAAS) to a known state after a disruption, compromise or failure.	10	
RC.RP-06	N/A	The end of incident recovery is declared based on criteria, and incident related documentation is completed.	Functional	intersects with	Incident Handling	IRO-02	Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Eradication; and (6) Recovery.	5	
				intersects with	Situational Awareness For Incidents	IRO-09	Mechanisms exist to document, monitor and report the status of cybersecurity and data protection incidents to internal stakeholders all the way through the resolution of the incident.	5	
RC.CO	N/A	Restoration activities are coordinated with internal and external parties.	Functional	intersects with	Coordinate with Related Plans	BCD-01.1	Mechanisms exist to coordinate contingency plan development with internal and external elements responsible for related plans.	5	
				intersects with	Coordinate With External Service Providers	BCD-01.2	Mechanisms exist to coordinate internal contingency plans with the contingency plans of external service providers to ensure that contingency requirements can be satisfied.	5	
RC.CO-03	N/A	Recovery activities and progress in restoring operational capabilities are communicated to designated internal and external stakeholders.	Functional	equal	Recovery Operations Communications	BCD-01.6	Mechanisms exist to communicate the status of recovery activities and progress in restoring operational capabilities to designated internal and external stakeholders.	10	
RC.CO-04	N/A	Public updates on incident recovery are shared using approved methods and messaging.	Functional	subset of	Public Relations & Reputation Repair	IRO-16	Mechanisms exist to proactively manage public relations associated with incidents and employ appropriate measures to prevent further reputational damage and develop plans to repair any damage to the organization's reputation.	10	