Reference Document : Secure Controls Framework (SCF) version 2025.2
STRM Guidance: https://securecontrolsframework.com/set-theory-relationship-mapping-strm/

Focal Document URL: https://nvlpubs.nist.gov/nistpubs/ai/nist.ai.100-1.pdf
Published STRM URL: https://securecontrolsframework.com/content/strm/scf-strm-general-nist-ai-100-1-rmf.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)
GOVERN 1.0	N/A	Policies, processes, procedures, and practices across the organization related to the mapping, measuring, and managing of AI risks are in place, transparent, and implemented effectively.	Functional	intersects with	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	8	
GOVERN 1.0	N/A	Policies, processes, procedures, and practices across the organization related to the mapping, measuring, and managing of AI risks are in place, transparent, and implemented effectively.	Functional	subset of	Artificial Intelligence (AI) & Autonomous Technologies Governance	AAT-01	Mechanisms exist to ensure policies, processes, procedures and practices related to the mapping, measuring and managing of Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related risks are in place, transparent and implemented effectively.	10	
GOVERN 1.0	N/A	Policies, processes, procedures, and practices across the organization related to the mapping, measuring, and managing of AI risks are in place, transparent, and implemented effectively.	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.	8	
GOVERN 1.1	N/A	Legal and regulatory requirements involving AI are understood, managed, and documented.	Functional	intersects with	AI & Autonomous Technologies-Related Legal Requirements Definition	AAT-01.1	Mechanisms exist to identify, understand, document and manage applicable statutory and regulatory requirements for Artificial Intelligence (AI) and Autonomous Technologies (AAT).	5	
GOVERN 1.1	N/A	Legal and regulatory requirements involving AI are understood, managed, and documented.	Functional	intersects with	Stakeholder Identification & Involvement	AST-01.2	Mechanisms exist to identify and involve pertinent stakeholders of critical systems, applications and services to support the ongoing secure management of those assets.	5	
GOVERN 1.1	N/A	Legal and regulatory requirements involving AI are understood, managed, and documented.	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	
GOVERN 1.1	N/A	Legal and regulatory requirements involving AI are understood, managed, and documented.	Functional	intersects with	Compliance Scope	CPL-01.2	Mechanisms exist to document and validate the scope of cybersecurity & data privacy controls that are determined to meet statutory, regulatory and/or contractual compliance obligations.	5	
GOVERN 1.2	N/A	The characteristics of trustworthy AI are integrated into organizational policies, processes, procedures, and practices.	Functional	intersects with	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	8	
GOVERN 1.2	N/A	The characteristics of trustworthy AI are integrated into organizational policies, processes, procedures, and practices.	Functional	intersects with	Trustworthy AI & Autonomous Technologies	AAT-01.2	Mechanisms exist to ensure Artificial Intelligence (AI) and Autonomous Technologies (AAT) are designed to be reliable, safe, fair, secure, resilient, transparent, explainable and data privacy-enhanced to minimize emergent properties or unintended consequences.	5	
GOVERN 1.2	N/A	The characteristics of trustworthy AI are integrated into organizational policies, processes, procedures, and practices.	Functional	subset of	Secure Engineering Principles	SEA-01	Mechanisms exist to facilitate the implementation of industry-recognized cybersecurity & data privacy practices in the specification, design, development, implementation and modification of systems and services.	10	
GOVERN 1.2	N/A	The characteristics of trustworthy AI are integrated into organizational policies, processes, procedures, and practices.	Functional	intersects with	Centralized Management of Cybersecurity & Data Privacy Controls	SEA-01.1	Mechanisms exist to centrally-manage the organization-wide management and implementation of cybersecurity & data privacy controls and related processes.	5	
GOVERN 1.2	N/A	The characteristics of trustworthy AI are integrated into organizational policies, processes, procedures, and practices.	Functional	intersects with	Operations Security	OPS-01	Mechanisms exist to facilitate the implementation of operational security controls.	8	
GOVERN 1.2	N/A	The characteristics of trustworthy AI are integrated into organizational policies, processes, procedures, and practices.	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.	8	
GOVERN 1.2	N/A	The characteristics of trustworthy AI are integrated into organizational policies, processes, procedures, and practices.	Functional	subset of	Technology Development & Acquisition	TDA-01	Mechanisms exist to facilitate the implementation of tailored development and acquisition strategies, contract tools and procurement methods to meet unique business needs.	10	
GOVERN 1.2	N/A	The characteristics of trustworthy AI are integrated into organizational policies, processes, procedures, and practices.	Functional	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 products and/or services 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	
GOVERN 1.3	N/A	Processes, procedures, and practices are in place to determine the needed level of risk management activities based on the organization's risk tolerance.	Functional	intersects with	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	8	
GOVERN 1.3	N/A	Processes, procedures, and practices are in place to determine the needed level of risk management activities based on the organization's risk tolerance.	Functional	intersects with	Assigned Cybersecurity & Data Protection Responsibilities	GOV-04	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide cybersecurity & data protection program.	5	
GOVERN 1.3	N/A	Processes, procedures, and practices are in place to determine the needed level of risk management activities based on the organization's risk tolerance.	Functional	intersects with	Stakeholder Accountability Structure	GOV-04.1	Mechanisms exist to enforce an accountability structure so that appropriate teams and individuals are empowered, responsible and trained for mapping, measuring and managing data and technology-related risks.	5	
GOVERN 1.3	N/A	Processes, procedures, and practices are in place to determine the needed level of risk management activities based on the organization's risk tolerance.	Functional	intersects with	Authoritative Chain of Command	GOV-04.2	Mechanisms exist to establish an authoritative chain of command with clear lines of communication to remove ambiguity from individuals and teams related to managing data and technology-related risks.	5	
GOVERN 1.3	N/A	Processes, procedures, and practices are in place to determine the needed level of risk management activities based on the organization's risk tolerance.	Functional	intersects with	Compliance Scope	CPL-01.2	Mechanisms exist to document and validate the scope of cybersecurity & data privacy controls that are determined to meet statutory, regulatory and/or contractual compliance obligations.	5	
GOVERN 1.3	N/A	Processes, procedures, and practices are in place to determine the needed level of risk management activities based on the organization's risk tolerance.	Functional	subset of	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	10	
GOVERN 1.3	N/A	Processes, procedures, and practices are in place to determine the needed level of risk management activities based on the organization's risk tolerance.	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	
GOVERN 1.3	N/A	Processes, procedures, and practices are in place to determine the needed level of risk management activities based on the organization's risk tolerance.	Functional	intersects with	Risk Management Resourcing	RSK-01.2	Mechanisms exist to reduce the magnitude or likelihood of potential impacts by resourcing the capability required to manage technology-related risks.	5	
GOVERN 1.3	N/A	Processes, procedures, and practices are in place to determine the needed level of risk management activities based on the organization's risk tolerance.	Functional	intersects with	Risk Tolerance	RSK-01.3	Mechanisms exist to define organizational risk tolerance, the specified range of acceptable results.	5	
GOVERN 1.3	N/A	Processes, procedures, and practices are in place to determine the needed level of risk management activities based on the organization's risk tolerance.	Functional	intersects with	Operations Security	OPS-01	Mechanisms exist to facilitate the implementation of operational security controls.	8	
GOVERN 1.3	N/A	Processes, procedures, and practices are in place to determine the needed level of risk management activities based on the organization's risk tolerance.	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.	8	
GOVERN 1.4	N/A	The risk management process and its outcomes are established through transparent policies, procedures, and other controls based on organizational risk priorities.	Functional	intersects with	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	8	
GOVERN 1.4	N/A	The risk management process and its outcomes are established through transparent policies, procedures, and other controls based on organizational risk priorities.	Functional	subset of	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	10	
GOVERN 1.4	N/A	The risk management process and its outcomes are established through transparent policies, procedures, and other controls based on organizational risk priorities.	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	
GOVERN 1.4	N/A	The risk management process and its outcomes are established through transparent policies, procedures, and other controls based on organizational risk priorities.	Functional	intersects with	Risk Management Resourcing	RSK-01.2	Mechanisms exist to reduce the magnitude or likelihood of potential impacts by resourcing the capability required to manage technology-related risks.	5	
GOVERN 1.4	N/A	The risk management process and its outcomes are established through transparent policies, procedures, and other controls based on organizational risk priorities.	Functional	intersects with	Operations Security	OPS-01	Mechanisms exist to facilitate the implementation of operational security controls.	8	
GOVERN 1.4	N/A	The risk management process and its outcomes are established through transparent policies, procedures, and other controls based on organizational risk priorities.	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.	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)
GOVERN 1.5	N/A	Ongoing monitoring and periodic review of the risk management process and its outcomes are planned and organizational roles and responsibilities clearly defined, including determining the frequency of periodic review.	Functional	intersects with	Measures of Performance	GOV-05	Mechanisms exist to develop, report and monitor cybersecurity & data privacy program measures of performance.	5	
GOVERN 1.5	N/A	Ongoing monitoring and periodic review of the risk management process and its outcomes are planned and organizational roles and responsibilities clearly defined, including determining the frequency of periodic review.	Functional	intersects with	Cybersecurity & Data Protection Controls Oversight	CPL-02	Mechanisms exist to provide a cybersecurity & data protection controls oversight function that reports to the organization's executive leadership.	5	
GOVERN 1.5	N/A	Ongoing monitoring and periodic review of the risk management process and its outcomes are planned and organizational roles and responsibilities clearly defined, including determining the frequency of periodic review.	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 & data protection policies, standards and other applicable requirements.	5	
GOVERN 1.5	N/A	Ongoing monitoring and periodic review of the risk management process and its outcomes are planned and organizational roles and responsibilities clearly defined, including determining the frequency of periodic review.	Functional	intersects with	Audit Activities	CPL-04	Mechanisms exist to thoughtfully plan audits by including input from operational risk and compliance partners to minimize the impact of audit-related activities on business operations.	5	
GOVERN 1.5	N/A	Ongoing monitoring and periodic review of the risk management process and its outcomes are planned and organizational roles and responsibilities clearly defined, including determining the frequency of periodic review.	Functional	subset of	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	10	
GOVERN 1.5	N/A	Ongoing monitoring and periodic review of the risk management process and its outcomes are planned and organizational roles and responsibilities clearly defined, including determining the frequency of periodic review.	Functional	intersects with	Risk Assessment	RSK-04	Mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's systems and data.	5	
GOVERN 1.5	N/A	Ongoing monitoring and periodic review of the risk management process and its outcomes are planned and organizational roles and responsibilities clearly defined, including determining the frequency of periodic review.	Functional	intersects with	Risk Register	RSK-04.1	Mechanisms exist to maintain a risk register that facilitates monitoring and reporting of risks.	5	
GOVERN 1.5	N/A	Ongoing monitoring and periodic review of the risk management process and its outcomes are planned and organizational roles and responsibilities clearly defined, including determining the frequency of periodic review.	Functional	intersects with	Business Impact Analysis (BIA)	RSK-08	Mechanisms exist to conduct a Business Impact Analysis (BIA) to identify and assess cybersecurity and data protection risks.	5	
GOVERN 1.6	N/A	Mechanisms are in place to inventory AI systems and are resourced according to organizational risk priorities.	Functional	intersects with	Situational Awareness of AI & Autonomous Technologies	AAT-02	Mechanisms exist to develop and maintain an inventory of Artificial Intelligence (AI) and Autonomous Technologies (AAT) (internal and third-party).	5	
GOVERN 1.6	N/A	Mechanisms are in place to inventory AI systems and are resourced according to organizational risk priorities.	Functional	intersects with	Asset Inventories	AST-02	Mechanisms exist to perform inventories of technology assets that: (1) Accurately reflects the current systems, applications and services 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	
GOVERN 1.6	N/A	Mechanisms are in place to inventory AI systems and are resourced according to organizational risk priorities.	Functional	intersects with	Identify Critical Assets	BCD-02	Mechanisms exist to identify and document the critical systems, applications and services that support essential missions and business functions.	5	
GOVERN 1.6	N/A	Mechanisms are in place to inventory AI systems and are resourced according to organizational risk priorities.	Functional	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	
GOVERN 1.7	N/A	Processes and procedures are in place for decommissioning and phasing out AI systems safely and in a manner that does not increase risks or decrease the organization's trustworthiness.	Functional	intersects with	Secure Disposal, Destruction or Re-Use of Equipment	AST-09	Mechanisms exist to securely dispose of, destroy or repurpose system components using organization-defined techniques and methods to prevent information being recovered from these components.	5	
GOVERN 1.7	N/A	Processes and procedures are in place for decommissioning and phasing out AI systems safely and in a manner that does not increase risks or decrease the organization's trustworthiness.	Functional	intersects with	Decommissioning	AST-30	Mechanisms exist to ensure systems, applications and services are properly decommissioned so that data is properly transitioned to new systems or archived in accordance with applicable organizational standards, as well as statutory, regulatory and contractual obligations.	5	
GOVERN 1.7	N/A	Processes and procedures are in place for decommissioning and phasing out AI systems safely and in a manner that does not increase risks or decrease the organization's trustworthiness.	Functional	intersects with	Secure Development Life Cycle (SDLC) Management	PRM-07	Mechanisms exist to ensure changes to systems within the Secure Development Life Cycle (SDLC) are controlled through formal change control procedures.	5	
GOVERN 1.7	N/A	Processes and procedures are in place for decommissioning and phasing out AI systems safely and in a manner that does not increase risks or decrease the organization's trustworthiness.	Functional	intersects with	Technical Debt Reviews	SEA-02.3	Mechanisms exist to conduct ongoing "technical debt" reviews of hardware and software technologies to remediate outdated and/or unsupported technologies.	5	
GOVERN 1.7	N/A	Processes and procedures are in place for decommissioning and phasing out AI systems safely and in a manner that does not increase risks or decrease the organization's trustworthiness.	Functional	intersects with	Unsupported Systems	TDA-17	Mechanisms exist to prevent unsupported systems by: (1) Replacing systems 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 system components required to satisfy mission/business needs.	5	
GOVERN 2.0	N/A	Accountability structures are in place so that the appropriate teams and individuals are empowered, responsible, and trained for mapping, measuring, and managing AI risks.	Functional	intersects with	Stakeholder Accountability Structure	GOV-04.1	Mechanisms exist to enforce an accountability structure so that appropriate teams and individuals are empowered, responsible and trained for mapping, measuring and managing data and technology-related risks.	5	
GOVERN 2.0	N/A	Accountability structures are in place so that the appropriate teams and individuals are empowered, responsible, and trained for mapping, measuring, and managing AI risks.	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	
GOVERN 2.0	N/A	Accountability structures are in place so that the appropriate teams and individuals are empowered, responsible, and trained for mapping, measuring, and managing AI risks.	Functional	intersects with	Stakeholder Identification & Involvement	AST-01.2	Mechanisms exist to identify and involve pertinent stakeholders of critical systems, applications and services to support the ongoing secure management of those assets.	5	
GOVERN 2.0	N/A	Accountability structures are in place so that the appropriate teams and individuals are empowered, responsible, and trained for mapping, measuring, and managing AI risks.	Functional	intersects with	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	
GOVERN 2.0	N/A	Accountability structures are in place so that the appropriate teams and individuals are empowered, responsible, and trained for mapping, measuring, and managing AI risks.	Functional	intersects with	Roles With Special Protection Measures	HRS-04.1	Mechanisms exist to ensure that individuals accessing a system that stores, transmits or processes information requiring special protection satisfy organization-defined personnel screening criteria.	5	
GOVERN 2.0	N/A	Accountability structures are in place so that the appropriate teams and individuals are empowered, responsible, and trained for mapping, measuring, and managing AI risks.	Functional	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	
GOVERN 2.0	N/A	Accountability structures are in place so that the appropriate teams and individuals are empowered, responsible, and trained for mapping, measuring, and managing AI risks.	Functional	intersects with	Use of Critical Technologies	HRS-05.4	Mechanisms exist to govern usage policies for critical technologies.	5	
GOVERN 2.0	N/A	Accountability structures are in place so that the appropriate teams and individuals are empowered, responsible, and trained for mapping, measuring, and managing AI risks.	Functional	subset of	Cybersecurity & Data Privacy-Minded Workforce	SAT-01	Mechanisms exist to facilitate the implementation of security workforce development and awareness controls.	10	
GOVERN 2.0	N/A	Accountability structures are in place so that the appropriate teams and individuals are empowered, responsible, and trained for mapping, measuring, and managing AI risks.	Functional	intersects with	Role-Based Cybersecurity & Data Privacy Training	SAT-03	Mechanisms exist to provide role-based cybersecurity & data privacy-related training: (1) Before authorizing access to the system or performing assigned duties; (2) When required by system changes; and (3) Annually thereafter.	5	
GOVERN 2.1	N/A	Roles and responsibilities and lines of communication related to mapping, measuring, and managing AI risks are documented and are clear to individuals and teams throughout the organization.	Functional	intersects with	Assigned Cybersecurity & Data Protection Responsibilities	GOV-04	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide cybersecurity & data protection program.	5	
GOVERN 2.1	N/A	Roles and responsibilities and lines of communication related to mapping, measuring, and managing AI risks are documented and are clear to individuals and teams throughout the organization.	Functional	intersects with	Stakeholder Accountability Structure	GOV-04.1	Mechanisms exist to enforce an accountability structure so that appropriate teams and individuals are empowered, responsible and trained for mapping, measuring and managing data and technology-related risks.	5	
GOVERN 2.1	N/A	Roles and responsibilities and lines of communication related to mapping, measuring, and managing AI risks are documented and are clear to individuals and teams throughout the organization.	Functional	intersects with	Authoritative Chain of Command	GOV-04.2	Mechanisms exist to establish an authoritative chain of command with clear lines of communication to remove ambiguity from individuals and teams related to managing data and technology-related risks.	5	
GOVERN 2.1	N/A	Roles and responsibilities and lines of communication related to mapping, measuring, and managing AI risks are documented and are clear to individuals and teams throughout the organization.	Functional	subset of	Artificial Intelligence (AI) & Autonomous Technologies Governance	AAT-01	Mechanisms exist to ensure policies, processes, procedures and practices related to the mapping, measuring and managing of Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related risks are in place, transparent and implemented effectively.	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)
GOVERN 2.1	N/A	Roles and responsibilities and lines of communication related to mapping, measuring, and managing AI risks are documented and are clear to individuals and teams throughout the organization.	Functional	intersects with	Assigned Responsibilities for AI & Autonomous Technologies	AAT-08	Mechanisms exist to define and differentiate roles and responsibilities for: (1) Artificial Intelligence (AI) and Autonomous Technologies (AAT) configurations; and (2) Oversight of AAT systems.	5	
GOVERN 2.1	N/A	Roles and responsibilities and lines of communication related to mapping, measuring, and managing AI risks are documented and are clear to individuals and teams throughout the organization.	Functional	intersects with	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	
GOVERN 2.2	N/A	The organization's personnel and partners receive AI risk management training to enable them to perform their duties and responsibilities consistent with related policies, procedures, and agreements.	Functional	intersects with	Role-Based Cybersecurity & Data Privacy Training	SAT-03	Mechanisms exist to provide role-based cybersecurity & data privacy-related training: (1) Before authorizing access to the system or performing assigned duties; (2) When required by system changes; and (3) Annually thereafter.	5	
GOVERN 2.2	N/A	The organization's personnel and partners receive AI risk management training to enable them to perform their duties and responsibilities consistent with related policies, procedures, and agreements.	Functional	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	
GOVERN 2.2	N/A	The organization's personnel and partners receive AI risk management training to enable them to perform their duties and responsibilities consistent with related policies, procedures, and agreements.	Functional	intersects with	Cyber Threat Environment	SAT-03.6	Mechanisms exist to provide role-based cybersecurity & data privacy awareness training that is current and relevant to the cyber threats that users might encounter in day-to-day business operations.	5	
GOVERN 2.3	N/A	Executive leadership of the organization takes responsibility for decisions about risks associated with AI system development and deployment.	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	
GOVERN 2.3	N/A	Executive leadership of the organization takes responsibility for decisions about risks associated with AI system development and deployment.	Functional	intersects with	Status Reporting To Governing Body	GOV-01.2	Mechanisms exist to provide governance oversight reporting and recommendations to those entrusted to make executive decisions about matters considered material to the organization's cybersecurity & data protection program.	5	
GOVERN 2.3	N/A	Executive leadership of the organization takes responsibility for decisions about risks associated with AI system development and deployment.	Functional	intersects with	Assigned Cybersecurity & Data Protection Responsibilities	GOV-04	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide cybersecurity & data protection program.	5	
GOVERN 3.0	N/A	Workforce diversity, equity, inclusion, and accessibility processes are prioritized in the mapping, measuring, and managing of AI risks throughout the lifecycle.	Functional	equal	AI & Autonomous Technologies Fairness & Bias	AAT-06	Mechanisms exist to prevent Artificial Intelligence (AI) and Autonomous Technologies (AAT) from unfairly identifying, profiling and/or statistically singling out a segmented population defined by race, religion, gender identity, national origin, religion, disability or any other politically-charged identifier.	10	
GOVERN 3.1	N/A	Decision-making related to mapping, measuring, and managing AI risks throughout the lifecycle is informed by a diverse team (e.g., diversity of demographics, disciplines, experience, expertise, and backgrounds).	Functional	intersects with	AI & Autonomous Technologies Risk Management Decisions	AAT-07	Mechanisms exist to leverage decision makers from a diversity of demographics, disciplines, experience, expertise and backgrounds for mapping, measuring and managing Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related risks.	5	
GOVERN 3.1	N/A	Decision-making related to mapping, measuring, and managing AI risks throughout the lifecycle is informed by a diverse team (e.g., diversity of demographics, disciplines, experience, expertise, and backgrounds).	Functional	subset of	Technology Development & Acquisition	TDA-01	Mechanisms exist to facilitate the implementation of tailored development and acquisition strategies, contract tools and procurement methods to meet unique business needs.	10	
GOVERN 3.1	N/A	Decision-making related to mapping, measuring, and managing AI risks throughout the lifecycle is informed by a diverse team (e.g., diversity of demographics, disciplines, experience, expertise, and backgrounds).	Functional	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 products and/or services 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	
GOVERN 3.2	N/A	Policies and procedures are in place to define and differentiate roles and responsibilities for human-AI configurations and oversight of AI systems.	Functional	intersects with	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	8	
GOVERN 3.2	N/A	Policies and procedures are in place to define and differentiate roles and responsibilities for human-AI configurations and oversight of AI systems.	Functional	intersects with	Assigned Responsibilities for AI & Autonomous Technologies	AAT-08	Mechanisms exist to define and differentiate roles and responsibilities for: (1) Artificial Intelligence (AI) and Autonomous Technologies (AAT) configurations; and (2) Oversight of AAT systems.	5	
GOVERN 3.2	N/A	Policies and procedures are in place to define and differentiate roles and responsibilities for human-AI configurations and oversight of AI systems.	Functional	intersects with	Operations Security	OPS-01	Mechanisms exist to facilitate the implementation of operational security controls.	8	
GOVERN 3.2	N/A	Policies and procedures are in place to define and differentiate roles and responsibilities for human-AI configurations and oversight of AI systems.	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.	8	
GOVERN 4.0	N/A	Organizational teams are committed to a culture that considers and communicates AI risk.	Functional	intersects with	Business As Usual (BAU) Secure Practices	GOV-14	Mechanisms exist to incorporate cybersecurity & data privacy principles into Business As Usual (BAU) practices through executive leadership involvement.	3	
GOVERN 4.0	N/A	Organizational teams are committed to a culture that considers and communicates AI risk.	Functional	intersects with	Operationalizing Cybersecurity & Data Protection Practices	GOV-15	Mechanisms exist to compel data and/or process owners to operationalize cybersecurity & data privacy practices for each system, application and/or service under their control.	5	
GOVERN 4.0	N/A	Organizational teams are committed to a culture that considers and communicates AI risk.	Functional	equal	Risk Culture	RSK-12	Mechanisms exist to ensure teams are committed to a culture that considers and communicates technology-related risk.	10	
GOVERN 4.1	N/A	Organizational policies and practices are in place to foster a critical thinking and safety-first mindset in the design, development, deployment, and uses of AI systems to minimize potential negative impacts.	Functional	intersects with	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	8	
GOVERN 4.1	N/A	Organizational policies and practices are in place to foster a critical thinking and safety-first mindset in the design, development, deployment, and uses of AI systems to minimize potential negative impacts.	Functional	subset of	Artificial Intelligence (AI) & Autonomous Technologies Governance	AAT-01	Mechanisms exist to ensure policies, processes, procedures and practices related to the mapping, measuring and managing of Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related risks are in place, transparent and implemented effectively.	10	
GOVERN 4.1	N/A	Organizational policies and practices are in place to foster a critical thinking and safety-first mindset in the design, development, deployment, and uses of AI systems to minimize potential negative impacts.	Functional	subset of	Human Resources Security Management	HRS-01	Mechanisms exist to facilitate the implementation of personnel security controls.	10	
GOVERN 4.1	N/A	Organizational policies and practices are in place to foster a critical thinking and safety-first mindset in the design, development, deployment, and uses of AI systems to minimize potential negative impacts.	Functional	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	
GOVERN 4.1	N/A	Organizational policies and practices are in place to foster a critical thinking and safety-first mindset in the design, development, deployment, and uses of AI systems to minimize potential negative impacts.	Functional	intersects with	Competency Requirements for Security-Related Positions	HRS-03.2	Mechanisms exist to ensure that all security-related positions are staffed by qualified individuals who have the necessary skill set.	5	
GOVERN 4.1	N/A	Organizational policies and practices are in place to foster a critical thinking and safety-first mindset in the design, development, deployment, and uses of AI systems to minimize potential negative impacts.	Functional	intersects with	Roles With Special Protection Measures	HRS-04.1	Mechanisms exist to ensure that individuals accessing a system that stores, transmits or processes information requiring special protection satisfy organization-defined personnel screening criteria.	5	
GOVERN 4.1	N/A	Organizational policies and practices are in place to foster a critical thinking and safety-first mindset in the design, development, deployment, and uses of AI systems to minimize potential negative impacts.	Functional	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	
GOVERN 4.1	N/A	Organizational policies and practices are in place to foster a critical thinking and safety-first mindset in the design, development, deployment, and uses of AI systems to minimize potential negative impacts.	Functional	intersects with	Use of Critical Technologies	HRS-05.4	Mechanisms exist to govern usage policies for critical technologies.	5	
GOVERN 4.1	N/A	Organizational policies and practices are in place to foster a critical thinking and safety-first mindset in the design, development, deployment, and uses of AI systems to minimize potential negative impacts.	Functional	intersects with	Operations Security	OPS-01	Mechanisms exist to facilitate the implementation of operational security controls.	8	
GOVERN 4.1	N/A	Organizational policies and practices are in place to foster a critical thinking and safety-first mindset in the design, development, deployment, and uses of AI systems to minimize potential negative impacts.	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.	8	
GOVERN 4.1	N/A	Organizational policies and practices are in place to foster a critical thinking and safety-first mindset in the design, development, deployment, and uses of AI systems to minimize potential negative impacts.	Functional	subset of	Cybersecurity & Data Privacy-Minded Workforce	SAT-01	Mechanisms exist to facilitate the implementation of security workforce development and awareness 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)
GOVERN 4.1	N/A	Organizational policies and practices are in place to foster a critical thinking and safety-first mindset in the design, development, deployment, and uses of AI systems to minimize potential negative impacts.	Functional	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 products and/or services 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	
GOVERN 4.1	N/A	Organizational policies and practices are in place to foster a critical thinking and safety-first mindset in the design, development, deployment, and uses of AI systems to minimize potential negative impacts.	Functional	intersects with	Development Methods, Techniques & Processes	TDA-02.3	Mechanisms exist to require software developers to ensure that their software development processes employ industry-recognized secure practices for secure programming, engineering methods, quality control processes and validation techniques to minimize flawed and/or malformed software.	5	
GOVERN 4.2	N/A	Organizational teams document the risks and potential impacts of the AI technology they design, develop, deploy, evaluate, and use, and they communicate about the impacts more broadly.	Functional	intersects with	AI & Autonomous Technologies Risk Profiling	AAT-09	Mechanisms exist to document the risks and potential impacts of Artificial Intelligence (AI) and Autonomous Technologies (AAT) that are: (1) Designed; (2) Developed; (3) Deployed; (4) Evaluated; and/or (5) Used.	5	
GOVERN 4.2	N/A	Organizational teams document the risks and potential impacts of the AI technology they design, develop, deploy, evaluate, and use, and they communicate about the impacts more broadly.	Functional	subset of	Technology Development & Acquisition	TDA-01	Mechanisms exist to facilitate the implementation of tailored development and acquisition strategies, contract tools and procurement methods to meet unique business needs.	10	
GOVERN 4.2	N/A	Organizational teams document the risks and potential impacts of the AI technology they design, develop, deploy, evaluate, and use, and they communicate about the impacts more broadly.	Functional	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 products and/or services 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	
GOVERN 4.2	N/A	Organizational teams document the risks and potential impacts of the AI technology they design, develop, deploy, evaluate, and use, and they communicate about the impacts more broadly.	Functional	intersects with	Development Methods, Techniques & Processes	TDA-02.3	Mechanisms exist to require software developers to ensure that their software development processes employ industry-recognized secure practices for secure programming, engineering methods, quality control processes and validation techniques to minimize flawed and/or malformed software.	5	
GOVERN 4.2	N/A	Organizational teams document the risks and potential impacts of the AI technology they design, develop, deploy, evaluate, and use, and they communicate about the impacts more broadly.	Functional	intersects with	Documentation Requirements	TDA-04	Mechanisms exist to obtain, protect and distribute administrator documentation for systems that describe: (1) Secure configuration, installation and operation of the system; (2) Effective use and maintenance of security features/functions; and (3) Known vulnerabilities regarding configuration and use of administrative (e.g., privileged) functions.	5	
GOVERN 4.2	N/A	Organizational teams document the risks and potential impacts of the AI technology they design, develop, deploy, evaluate, and use, and they communicate about the impacts more broadly.	Functional	intersects with	Developer Architecture & Design	TDA-05	Mechanisms exist to require the developers of systems, system components or services to produce a design specification and security architecture that: (1) Is consistent with and supportive of the organization's security architecture which is established within and is an integrated part of the organization's enterprise architecture; (2) Accurately and completely describes the required security functionality and the allocation of security controls among physical and logical components; and (3) Expresses how individual security functions, mechanisms and services work together to provide required security capabilities and a unified approach to protection.	5	
GOVERN 4.3	N/A	Organizational practices are in place to enable AI testing, identification of incidents, and information sharing.	Functional	intersects with	Artificial Intelligence Test, Evaluation, Validation & Verification (AI TEVV)	AAT-10	Mechanisms exist to implement Artificial Intelligence Test, Evaluation, Validation & Verification (AI TEVV) practices to enable Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related security, resilience and compliance-related conformity testing throughout the lifecycle of the AAT.	5	
GOVERN 4.3	N/A	Organizational practices are in place to enable AI testing, identification of incidents, and information sharing.	Functional	subset of	Information Assurance (IA) Operations	IAO-01	Mechanisms exist to facilitate the implementation of cybersecurity & data privacy assessment and authorization controls.	10	
GOVERN 5.0	N/A	Processes are in place for robust engagement with relevant AI actors.	Functional	intersects with	Assigned Cybersecurity & Data Protection Responsibilities	GOV-04	Mechanisms exist to assign one or more qualified individuals with the mission and resources to centrally-manage, coordinate, develop, implement and maintain an enterprise-wide cybersecurity & data protection program.	5	
GOVERN 5.0	N/A	Processes are in place for robust engagement with relevant AI actors.	Functional	intersects with	Stakeholder Accountability Structure	GOV-04.1	Mechanisms exist to enforce an accountability structure so that appropriate teams and individuals are empowered, responsible and trained for mapping, measuring and managing data and technology-related risks.	5	
GOVERN 5.0	N/A	Processes are in place for robust engagement with relevant AI actors.	Functional	intersects with	Robust Stakeholder Engagement for AI & Autonomous Technologies	AAT-11	Mechanisms exist to compel ongoing engagement with relevant Artificial Intelligence (AI) and Autonomous Technologies (AAT) stakeholders to encourage feedback about positive, negative and unanticipated impacts.	5	
GOVERN 5.0	N/A	Processes are in place for robust engagement with relevant AI actors.	Functional	intersects with	Stakeholder Identification & Involvement	AST-01.2	Mechanisms exist to identify and involve pertinent stakeholders of critical systems, applications and services to support the ongoing secure management of those assets.	5	
GOVERN 5.0	N/A	Processes are in place for robust engagement with relevant AI actors.	Functional	intersects with	Stakeholder Notification of Changes	CHG-05	Mechanisms exist to ensure stakeholders are made aware of and understand the impact of proposed changes.	5	
GOVERN 5.1	N/A	Organizational policies and practices are in place to collect, consider, prioritize, and integrate feedback from those external to the team that developed or deployed the AI system regarding the potential individual and societal impacts related to AI risks.	Functional	intersects with	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	8	
GOVERN 5.1	N/A	Organizational policies and practices are in place to collect, consider, prioritize, and integrate feedback from those external to the team that developed or deployed the AI system regarding the potential individual and societal impacts related to AI risks.	Functional	intersects with	AI & Autonomous Technologies Stakeholder Feedback Integration	AAT-11.1	Mechanisms exist to regularly collect, consider, prioritize and integrate risk-related feedback from those external to the team that developed or deployed Artificial Intelligence (AI) and Autonomous Technologies (AAT).	5	
GOVERN 5.1	N/A	Organizational policies and practices are in place to collect, consider, prioritize, and integrate feedback from those external to the team that developed or deployed the AI system regarding the potential individual and societal impacts related to AI risks.	Functional	intersects with	Operations Security	OPS-01	Mechanisms exist to facilitate the implementation of operational security controls.	8	
GOVERN 5.1	N/A	Organizational policies and practices are in place to collect, consider, prioritize, and integrate feedback from those external to the team that developed or deployed the AI system regarding the potential individual and societal impacts related to AI risks.	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.	8	
GOVERN 5.1	N/A	Organizational policies and practices are in place to collect, consider, prioritize, and integrate feedback from those external to the team that developed or deployed the AI system regarding the potential individual and societal impacts related to AI risks.	Functional	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 products and/or services 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	
GOVERN 5.2	N/A	Mechanisms are established to enable the team that developed or deployed AI systems to regularly incorporate adjudicated feedback from relevant AI actors into system design and implementation.	Functional	intersects with	AI & Autonomous Technologies Stakeholder Feedback Integration	AAT-11.1	Mechanisms exist to regularly collect, consider, prioritize and integrate risk-related feedback from those external to the team that developed or deployed Artificial Intelligence (AI) and Autonomous Technologies (AAT).	5	
GOVERN 5.2	N/A	Mechanisms are established to enable the team that developed or deployed AI systems to regularly incorporate adjudicated feedback from relevant AI actors into system design and implementation.	Functional	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 products and/or services 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	
GOVERN 6.0	N/A	Policies and procedures are in place to address AI risks and benefits arising from third-party software and data and other supply chain issues.	Functional	intersects with	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	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)
GOVERN 6.0	N/A	Policies and procedures are in place to address AI risks and benefits arising from third-party software and data and other supply chain issues.	Functional	intersects with	AI & Autonomous Technologies Supply Chain Impacts	RSK-09.2	Mechanisms exist to address Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related risks and benefits arising from the organization's supply chain, including third-party software and data.	5	
GOVERN 6.0	N/A	Policies and procedures are in place to address AI risks and benefits arising from third-party software and data and other supply chain issues.	Functional	intersects with	Operations Security	OPS-01	Mechanisms exist to facilitate the implementation of operational security controls.	8	
GOVERN 6.0	N/A	Policies and procedures are in place to address AI risks and benefits arising from third-party software and data and other supply chain issues.	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.	8	
GOVERN 6.0	N/A	Policies and procedures are in place to address AI risks and benefits arising from third-party software and data and other supply chain issues.	Functional	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 products and/or services 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	
GOVERN 6.1	N/A	Policies and procedures are in place that address AI risks associated with third-party entities, including risks of infringement of a third-party's intellectual property or other rights.	Functional	intersects with	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	8	
GOVERN 6.1	N/A	Policies and procedures are in place that address AI risks associated with third-party entities, including risks of infringement of a third-party's intellectual property or other rights.	Functional	intersects with	AI & Autonomous Technologies Intellectual Property Infringement Protections	AAT-12	Mechanisms exist to prevent third-party Intellectual Property (IP) rights infringement by Artificial Intelligence (AI) and Autonomous Technologies (AAT).	5	
GOVERN 6.1	N/A	Policies and procedures are in place that address AI risks associated with third-party entities, including risks of infringement of a third-party's intellectual property or other rights.	Functional	intersects with	Operations Security	OPS-01	Mechanisms exist to facilitate the implementation of operational security controls.	8	
GOVERN 6.1	N/A	Policies and procedures are in place that address AI risks associated with third-party entities, including risks of infringement of a third-party's intellectual property or other rights.	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.	8	
GOVERN 6.2	N/A	Contingency processes are in place to handle failures or incidents in third-party data or AI systems deemed to be high-risk.	Functional	subset of	Business Continuity Management System (BCMS)	BCD-01	Mechanisms exist to facilitate the implementation of contingency planning controls to help ensure resilient assets and services (e.g., Continuity of Operations Plan (COOP) or Business Continuity & Disaster Recovery (BC/DR) playbooks).	10	
GOVERN 6.2	N/A	Contingency processes are in place to handle failures or incidents in third-party data or AI systems deemed to be high-risk.	Functional	intersects with	AI & Autonomous Technologies Incidents	BCD-16	Mechanisms exist to handle failures or incidents with Artificial Intelligence (AI) and Autonomous Technologies (AAT) deemed to be high-risk.	5	
GOVERN 6.2	N/A	Contingency processes are in place to handle failures or incidents in third-party data or AI systems deemed to be high-risk.	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 & data privacy-related incidents.	10	
GOVERN 6.2	N/A	Contingency processes are in place to handle failures or incidents in third-party data or AI systems deemed to be high-risk.	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	
GOVERN 6.2	N/A	Contingency processes are in place to handle failures or incidents in third-party data or AI systems deemed to be high-risk.	Functional	intersects with	Incident Classification & Prioritization	IRO-02.4	Mechanisms exist to identify classes of incidents and actions to take to ensure the continuation of organizational missions and business functions.	5	
GOVERN 6.2	N/A	Contingency processes are in place to handle failures or incidents in third-party data or AI systems deemed to be high-risk.	Functional	intersects with	Incident Response Plan (IRP)	IRO-04	Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.	5	
MAP 1.0	N/A	Context is established and understood.	Functional	intersects with	AI & Autonomous Technologies Context Definition	AAT-03	Mechanisms exist to establish and document the context surrounding Artificial Intelligence (AI) and Autonomous Technologies (AAT), including: (1) Intended purposes; (2) Potentially beneficial uses; (3) Context-specific laws and regulations; (4) Norms and expectations; and (5) Prospective settings in which the system(s) will be deployed.	5	
MAP 1.0	N/A	Context is established and understood.	Functional	intersects with	Business Process Definition	PRM-06	Mechanisms exist to define business processes with consideration for cybersecurity & data privacy that determines: (1) The resulting risk to organizational operations, assets, individuals and other organizations; and (2) Information protection needs arising from the defined business processes and revises the processes as necessary, until an achievable set of protection needs is obtained.	5	
MAP 1.1	N/A	Intended purposes, potentially beneficial uses, context specific laws, norms and expectations, and prospective settings in which the AI system will be deployed are understood and documented. Considerations include: the specific set or types of users along with their expectations; potential positive and negative impacts of system uses to individuals, communities, organizations, society, and the planet; assumptions and related limitations about AI system purposes, uses, and risks across the development or product AI lifecycle; and related TEVV and system metrics.	Functional	intersects with	AI & Autonomous Technologies Context Definition	AAT-03	Mechanisms exist to establish and document the context surrounding Artificial Intelligence (AI) and Autonomous Technologies (AAT), including: (1) Intended purposes; (2) Potentially beneficial uses; (3) Context-specific laws and regulations; (4) Norms and expectations; and (5) Prospective settings in which the system(s) will be deployed.	5	
MAP 1.1	N/A	Intended purposes, potentially beneficial uses, context specific laws, norms and expectations, and prospective settings in which the AI system will be deployed are understood and documented. Considerations include: the specific set or types of users along with their expectations; potential positive and negative impacts of system uses to individuals, communities, organizations, society, and the planet; assumptions and related limitations about AI system purposes, uses, and risks across the development or product AI lifecycle; and related TEVV and system metrics.	Functional	intersects with	AI & Autonomous Technologies Business Case	AAT-04	Mechanisms exist to benchmark capabilities, targeted usage, goals and expected benefits and costs of Artificial Intelligence (AI) and Autonomous Technologies (AAT).	5	
MAP 1.1	N/A	Intended purposes, potentially beneficial uses, context specific laws, norms and expectations, and prospective settings in which the AI system will be deployed are understood and documented. Considerations include: the specific set or types of users along with their expectations; potential positive and negative impacts of system uses to individuals, communities, organizations, society, and the planet; assumptions and related limitations about AI system purposes, uses, and risks across the development or product AI lifecycle; and related TEVV and system metrics.	Functional	intersects with	Business Process Definition	PRM-06	Mechanisms exist to define business processes with consideration for cybersecurity & data privacy that determines: (1) The resulting risk to organizational operations, assets, individuals and other organizations; and (2) Information protection needs arising from the defined business processes and revises the processes as necessary, until an achievable set of protection needs is obtained.	5	
MAP 1.1	N/A	Intended purposes, potentially beneficial uses, context specific laws, norms and expectations, and prospective settings in which the AI system will be deployed are understood and documented. Considerations include: the specific set or types of users along with their expectations; potential positive and negative impacts of system uses to individuals, communities, organizations, society, and the planet; assumptions and related limitations about AI system purposes, uses, and risks across the development or product AI lifecycle; and related TEVV and system metrics.	Functional	intersects with	Business Impact Analysis (BIA)	RSK-08	Mechanisms exist to conduct a Business Impact Analysis (BIA) to identify and assess cybersecurity and data protection risks.	3	
MAP 1.1	N/A	Intended purposes, potentially beneficial uses, context specific laws, norms and expectations, and prospective settings in which the AI system will be deployed are understood and documented. Considerations include: the specific set or types of users along with their expectations; potential positive and negative impacts of system uses to individuals, communities, organizations, society, and the planet; assumptions and related limitations about AI system purposes, uses, and risks across the development or product AI lifecycle; and related TEVV and system metrics.	Functional	intersects with	Data Protection Impact Assessment (DPIA)	RSK-10	Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on systems, applications and services that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.	3	
MAP 1.2	N/A	Interdisciplinary AI actors, competencies, skills, and capacities for establishing context reflect demographic diversity and broad domain and user experience expertise, and their participation is documented. Opportunities for interdisciplinary collaboration are prioritized.	Functional	intersects with	Assigned Responsibilities for AI & Autonomous Technologies	AAT-08	Mechanisms exist to define and differentiate roles and responsibilities for: (1) Artificial Intelligence (AI) and Autonomous Technologies (AAT) configurations; and (2) Oversight of AAT systems.	5	
MAP 1.2	N/A	Interdisciplinary AI actors, competencies, skills, and capacities for establishing context reflect demographic diversity and broad domain and user experience expertise, and their participation is documented. Opportunities for interdisciplinary collaboration are prioritized.	Functional	intersects with	AI & Autonomous Technologies Stakeholder Diversity	AAT-13	Mechanisms exist to ensure Artificial Intelligence (AI) and Autonomous Technologies (AAT) stakeholder competencies, skills and capacities incorporate demographic diversity, broad domain and user experience expertise.	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)
MAP 1.2	N/A	Interdisciplinary AI actors, competencies, skills, and capacities for establishing context reflect demographic diversity and broad domain and user experience expertise, and their participation is documented. Opportunities for interdisciplinary collaboration are prioritized.	Functional	intersects with	Competency Requirements for Security-Related Positions	HRS-03.2	Mechanisms exist to ensure that all security-related positions are staffed by qualified individuals who have the necessary skill set.	5	
MAP 1.3	N/A	The organization's mission and relevant goals for AI technology are understood and documented.	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	
MAP 1.3	N/A	The organization's mission and relevant goals for AI technology are understood and documented.	Functional	intersects with	AI & Autonomous Technologies Mission and Goals Definition	AAT-03.1	Mechanisms exist to define and document the organization's mission and defined goals for Artificial Intelligence (AI) and Autonomous Technologies (AAT).	5	
MAP 1.3	N/A	The organization's mission and relevant goals for AI technology are understood and documented.	Functional	intersects with	Strategic Plan & Objectives	PRM-01.1	Mechanisms exist to establish a strategic cybersecurity & data privacy-specific business plan and set of objectives to achieve that plan.	5	
MAP 1.4	N/A	The business value or context of business use has been clearly defined or – in the case of assessing existing AI systems – re-evaluated.	Functional	intersects with	AI & Autonomous Technologies Context Definition	AAT-03	Mechanisms exist to establish and document the context surrounding Artificial Intelligence (AI) and Autonomous Technologies (AAT), including: (1) Intended purposes; (2) Potentially beneficial uses; (3) Context-specific laws and regulations; (4) Norms and expectations; and (5) Prospective settings in which the system(s) will be deployed.	5	
MAP 1.4	N/A	The business value or context of business use has been clearly defined or – in the case of assessing existing AI systems – re-evaluated.	Functional	intersects with	AI & Autonomous Technologies Mission and Goals Definition	AAT-03.1	Mechanisms exist to define and document the organization's mission and defined goals for Artificial Intelligence (AI) and Autonomous Technologies (AAT).	5	
MAP 1.4	N/A	The business value or context of business use has been clearly defined or – in the case of assessing existing AI systems – re-evaluated.	Functional	intersects with	Business Process Definition	PRM-06	Mechanisms exist to define business processes with consideration for cybersecurity & data privacy that determines: (1) The resulting risk to organizational operations, assets, individuals and other organizations; and (2) Information protection needs arising from the defined business processes and revises the processes as necessary, until an achievable set of protection needs is obtained.	5	
MAP 1.5	N/A	Organizational risk tolerances are determined and documented.	Functional	equal	Risk Tolerance	RSK-01.3	Mechanisms exist to define organizational risk tolerance, the specified range of acceptable results.	10	
MAP 1.6	N/A	System requirements (e.g., "the system shall respect the privacy of its users") are elicited from and understood by relevant AI actors. Design decisions take socio-technical implications into account to address AI risks.	Functional	intersects with	AI & Autonomous Technologies Requirements Definitions	AAT-14	Mechanisms exist to take socio-technical implications into account to address risks associated with Artificial Intelligence (AI) and Autonomous Technologies (AAT).	5	
MAP 1.6	N/A	System requirements (e.g., "the system shall respect the privacy of its users") are elicited from and understood by relevant AI actors. Design decisions take socio-technical implications into account to address AI risks.	Functional	subset of	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.	10	
MAP 1.6	N/A	System requirements (e.g., "the system shall respect the privacy of its users") are elicited from and understood by relevant AI actors. Design decisions take socio-technical implications into account to address AI risks.	Functional	intersects with	Usage Restrictions of Personal Data (PD)	PRI-05.4	Mechanisms exist to restrict collecting, receiving, processing, storing, transmitting, updating and/or sharing Personal Data (PD) to: (1) The purpose(s) originally collected, consistent with the data privacy notice(s); (2) What is authorized by the data subject, or authorized agent; and (3) What is consistent with applicable laws, regulations and contractual obligations.	5	
MAP 1.6	N/A	System requirements (e.g., "the system shall respect the privacy of its users") are elicited from and understood by relevant AI actors. Design decisions take socio-technical implications into account to address AI risks.	Functional	intersects with	Cybersecurity & Data Privacy Requirements Definition	PRM-05	Mechanisms exist to identify critical system components and functions by performing a criticality analysis for critical systems, system components or services at pre-defined decision points in the Secure Development Life Cycle (SDLC).	5	
MAP 2.0	N/A	Categorization of the AI system is performed.	Functional	intersects with	Asset Categorization	AST-31	Mechanisms exist to categorize technology assets.	5	
MAP 2.0	N/A	Categorization of the AI system is performed.	Functional	intersects with	Categorize Artificial Intelligence (AI)-Related Technologies	AST-31.1	Mechanisms exist to categorize Artificial Intelligence (AI) and Autonomous Technologies (AAT).	5	
MAP 2.1	N/A	The specific tasks and methods used to implement the tasks that the AI system will support are defined (e.g., classifiers, generative models, recommenders).	Functional	intersects with	AI & Autonomous Technologies Implementation Tasks Definition	AAT-14.1	Mechanisms exist to define the tasks that Artificial Intelligence (AI) and Autonomous Technologies (AAT) will support (e.g., classifiers, generative models, recommenders).	5	
MAP 2.1	N/A	The specific tasks and methods used to implement the tasks that the AI system will support are defined (e.g., classifiers, generative models, recommenders).	Functional	intersects with	Business Process Definition	PRM-06	Mechanisms exist to define business processes with consideration for cybersecurity & data privacy that determines: (1) The resulting risk to organizational operations, assets, individuals and other organizations; and (2) Information protection needs arising from the defined business processes and revises the processes as necessary, until an achievable set of protection needs is obtained.	5	
MAP 2.1	N/A	The specific tasks and methods used to implement the tasks that the AI system will support are defined (e.g., classifiers, generative models, recommenders).	Functional	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 products and/or services 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	
MAP 2.2	N/A	Information about the AI system's knowledge limits and how system output may be utilized and overseen by humans is documented. Documentation provides sufficient information to assist relevant AI actors when making decisions and taking subsequent actions.	Functional	equal	AI & Autonomous Technologies Knowledge Limits	AAT-14.2	Mechanisms exist to identify and document knowledge limits of Artificial Intelligence (AI) and Autonomous Technologies (AAT) to provide sufficient information to assist relevant stakeholder decision making.	10	
MAP 2.3	N/A	Scientific integrity and TEVV considerations are identified and documented, including those related to experimental design, data collection and selection (e.g., availability, representativeness, suitability), system trustworthiness, and construct validation.	Functional	intersects with	AI TEVV Tools	AAT-10.2	Mechanisms exist to document test sets, metrics and details about the tools used during Artificial Intelligence Test, Evaluation, Validation & Verification (AI TEVV) practices.	5	
MAP 2.3	N/A	Scientific integrity and TEVV considerations are identified and documented, including those related to experimental design, data collection and selection (e.g., availability, representativeness, suitability), system trustworthiness, and construct validation.	Functional	intersects with	Specialized Assessments	IAO-02.2	Mechanisms exist to conduct specialized assessments for: (1) Statutory, regulatory and contractual compliance obligations; (2) Monitoring capabilities; (3) Mobile devices; (4) Databases; (5) Application security; (6) Embedded technologies (e.g., IoT, OT, etc.); (7) Vulnerability management; (8) Malicious code; (9) Insider threats; (10) Performance/load testing; and/or (11) Artificial Intelligence and Autonomous Technologies (AAT).	5	
MAP 3.0	N/A	AI capabilities, targeted usage, goals, and expected benefits and costs compared with appropriate benchmarks are understood.	Functional	intersects with	AI & Autonomous Technologies Context Definition	AAT-03	Mechanisms exist to establish and document the context surrounding Artificial Intelligence (AI) and Autonomous Technologies (AAT), including: (1) Intended purposes; (2) Potentially beneficial uses; (3) Context-specific laws and regulations; (4) Norms and expectations; and (5) Prospective settings in which the system(s) will be deployed.	5	
MAP 3.0	N/A	AI capabilities, targeted usage, goals, and expected benefits and costs compared with appropriate benchmarks are understood.	Functional	intersects with	AI & Autonomous Technologies Mission and Goals Definition	AAT-03.1	Mechanisms exist to define and document the organization's mission and defined goals for Artificial Intelligence (AI) and Autonomous Technologies (AAT).	5	
MAP 3.0	N/A	AI capabilities, targeted usage, goals, and expected benefits and costs compared with appropriate benchmarks are understood.	Functional	intersects with	AI & Autonomous Technologies Business Case	AAT-04	Mechanisms exist to benchmark capabilities, targeted usage, goals and expected benefits and costs of Artificial Intelligence (AI) and Autonomous Technologies (AAT).	8	
MAP 3.1	N/A	Potential benefits of intended AI system functionality and performance are examined and documented.	Functional	intersects with	AI & Autonomous Technologies Business Case	AAT-04	Mechanisms exist to benchmark capabilities, targeted usage, goals and expected benefits and costs of Artificial Intelligence (AI) and Autonomous Technologies (AAT).	5	
MAP 3.1	N/A	Potential benefits of intended AI system functionality and performance are examined and documented.	Functional	intersects with	AI & Autonomous Technologies Potential Benefits Analysis	AAT-04.1	Mechanisms exist to assess the potential benefits of proposed Artificial Intelligence (AI) and Autonomous Technologies (AAT).	8	
MAP 3.2	N/A	Potential costs, including non-monetary costs, which result from expected or realized AI errors or system functionality and trustworthiness – as connected to organizational risk tolerance – are examined and documented.	Functional	intersects with	AI & Autonomous Technologies Business Case	AAT-04	Mechanisms exist to benchmark capabilities, targeted usage, goals and expected benefits and costs of Artificial Intelligence (AI) and Autonomous Technologies (AAT).	5	
MAP 3.2	N/A	Potential costs, including non-monetary costs, which result from expected or realized AI errors or system functionality and trustworthiness – as connected to organizational risk tolerance – are examined and documented.	Functional	intersects with	AI & Autonomous Technologies Potential Costs Analysis	AAT-04.2	Mechanisms exist to assess potential costs, including non-monetary costs, resulting from expected or realized Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related errors or system functionality and trustworthiness.	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)
MAP 3.2	N/A	Potential costs, including non-monetary costs, which result from expected or realized AI errors or system functionality and trustworthiness – as connected to organizational risk tolerance – are examined and documented.	Functional	intersects with	Risk Tolerance	RSK-01.3	Mechanisms exist to define organizational risk tolerance, the specified range of acceptable results.	5	
MAP 3.3	N/A	Targeted application scope is specified and documented based on the system's capability, established context, and AI system categorization.	Functional	intersects with	AI & Autonomous Technologies Targeted Application Scope	AAT-04.3	Mechanisms exist to specify and document the targeted application scope of the proposed use and operation of Artificial Intelligence (AI) and Autonomous Technologies (AAT).	8	
MAP 3.3	N/A	Targeted application scope is specified and documented based on the system's capability, established context, and AI system categorization.	Functional	intersects with	Compliance Scope	CPL-01.2	Mechanisms exist to document and validate the scope of cybersecurity & data privacy controls that are determined to meet statutory, regulatory and/or contractual compliance obligations.	5	
MAP 3.4	N/A	Processes for operator and practitioner proficiency with AI system performance and trustworthiness – and relevant technical standards and certifications – are defined, assessed, and documented.	Functional	intersects with	AI & Autonomous Technologies Stakeholder Competencies	AAT-13.1	Mechanisms exist to ensure Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related operator and practitioner proficiency requirements for Artificial Intelligence (AI) and Autonomous Technologies (AAT) are defined, assessed and documented.	8	
MAP 3.4	N/A	Processes for operator and practitioner proficiency with AI system performance and trustworthiness – and relevant technical standards and certifications – are defined, assessed, and documented.	Functional	intersects with	Competency Requirements for Security-Related Positions	HRS-03.2	Mechanisms exist to ensure that all security-related positions are staffed by qualified individuals who have the necessary skill set.	5	
MAP 3.5	N/A	Processes for human oversight are defined, assessed, and documented in accordance with organizational policies from the GOVERN function.	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	
MAP 3.5	N/A	Processes for human oversight are defined, assessed, and documented in accordance with organizational policies from the GOVERN function.	Functional	intersects with	Status Reporting To Governing Body	GOV-01.2	Mechanisms exist to provide governance oversight reporting and recommendations to those entrusted to make executive decisions about matters considered material to the organization's cybersecurity & data protection program.	5	
MAP 3.5	N/A	Processes for human oversight are defined, assessed, and documented in accordance with organizational policies from the GOVERN function.	Functional	intersects with	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	8	
MAP 3.5	N/A	Processes for human oversight are defined, assessed, and documented in accordance with organizational policies from the GOVERN function.	Functional	subset of	Artificial Intelligence (AI) & Autonomous Technologies Governance	AAT-01	Mechanisms exist to ensure policies, processes, procedures and practices related to the mapping, measuring and managing of Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related risks are in place, transparent and implemented effectively.	10	
MAP 3.5	N/A	Processes for human oversight are defined, assessed, and documented in accordance with organizational policies from the GOVERN function.	Functional	intersects with	Operations Security	OPS-01	Mechanisms exist to facilitate the implementation of operational security controls.	8	
MAP 3.5	N/A	Processes for human oversight are defined, assessed, and documented in accordance with organizational policies from the GOVERN function.	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.	8	
MAP 4.0	N/A	Risks and benefits are mapped for all components of the AI system including third-party software and data.	Functional	equal	AI & Autonomous Technologies Cost / Benefit Mapping	AAT-04.4	Mechanisms exist to map risks and benefits for all components of Artificial Intelligence (AI) and Autonomous Technologies (AAT), including third-party software and data.	10	
MAP 4.1	N/A	Approaches for mapping AI technology and legal risks of its components – including the use of third-party data or software – are in place, followed, and documented, as are risks of infringement of a third party's intellectual property or other rights.	Functional	equal	AI & Autonomous Technologies Risk Mapping	AAT-02.1	Mechanisms exist to identify Artificial Intelligence (AI) and Autonomous Technologies (AAT) in use and map those components to potential legal risks, including statutory and regulatory compliance requirements.	10	
MAP 4.2	N/A	Internal risk controls for components of the AI system, including third-party AI technologies, are identified and documented.	Functional	equal	AI & Autonomous Technologies Internal Controls	AAT-02.2	Mechanisms exist to identify and document internal cybersecurity & data privacy controls for Artificial Intelligence (AI) and Autonomous Technologies (AAT).	10	
MAP 5.0	N/A	Impacts to individuals, groups, communities, organizations, and society are characterized.	Functional	equal	AI & Autonomous Technologies Impact Assessment	AAT-07.1	Mechanisms exist to assess the impact(s) of proposed Artificial Intelligence (AI) and Autonomous Technologies (AAT) on individuals, groups, communities, organizations and society (e.g., Fundamental Rights Impact Assessment (FRIA)).	10	
MAP 5.1	N/A	Likelihood and magnitude of each identified impact (both potentially beneficial and harmful) based on expected use, past uses of AI systems in similar contexts, public incident reports, feedback from those external to the team that developed or deployed the AI system, or other data are identified and documented.	Functional	intersects with	AI & Autonomous Technologies Likelihood & Impact Risk Analysis	AAT-07.2	Mechanisms exist to define the potential likelihood and impact of each identified risk based on expected use and past uses of Artificial Intelligence (AI) and Autonomous Technologies (AAT) in similar contexts.	5	
MAP 5.1	N/A	Likelihood and magnitude of each identified impact (both potentially beneficial and harmful) based on expected use, past uses of AI systems in similar contexts, public incident reports, feedback from those external to the team that developed or deployed the AI system, or other data are identified and documented.	Functional	intersects with	Impact-Level Prioritization	RSK-02.1	Mechanisms exist to prioritize the impact level for systems, applications and/or services to prevent potential disruptions.	5	
MAP 5.1	N/A	Likelihood and magnitude of each identified impact (both potentially beneficial and harmful) based on expected use, past uses of AI systems in similar contexts, public incident reports, feedback from those external to the team that developed or deployed the AI system, or other data are identified and documented.	Functional	intersects with	Business Impact Analysis (BIA)	RSK-08	Mechanisms exist to conduct a Business Impact Analysis (BIA) to identify and assess cybersecurity and data protection risks.	5	
MAP 5.2	N/A	Practices and personnel for supporting regular engagement with relevant AI actors and integrating feedback about positive, negative, and unanticipated impacts are in place and documented.	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	
MAP 5.2	N/A	Practices and personnel for supporting regular engagement with relevant AI actors and integrating feedback about positive, negative, and unanticipated impacts are in place and documented.	Functional	intersects with	Measures of Performance	GOV-05	Mechanisms exist to develop, report and monitor cybersecurity & data privacy program measures of performance.	5	
MAP 5.2	N/A	Practices and personnel for supporting regular engagement with relevant AI actors and integrating feedback about positive, negative, and unanticipated impacts are in place and documented.	Functional	subset of	Artificial Intelligence (AI) & Autonomous Technologies Governance	AAT-01	Mechanisms exist to ensure policies, processes, procedures and practices related to the mapping, measuring and managing of Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related risks are in place, transparent and implemented effectively.	10	
MAP 5.2	N/A	Practices and personnel for supporting regular engagement with relevant AI actors and integrating feedback about positive, negative, and unanticipated impacts are in place and documented.	Functional	intersects with	Robust Stakeholder Engagement for AI & Autonomous Technologies	AAT-11	Mechanisms exist to compel ongoing engagement with relevant Artificial Intelligence (AI) and Autonomous Technologies (AAT) stakeholders to encourage feedback about positive, negative and unanticipated impacts.	5	
MEASURE 1.0	N/A	Appropriate methods and metrics are identified and applied.	Functional	equal	Measures of Performance	GOV-05	Mechanisms exist to develop, report and monitor cybersecurity & data privacy program measures of performance.	10	
MEASURE 1.0	N/A	Appropriate methods and metrics are identified and applied.	Functional	intersects with	Measuring AI & Autonomous Technologies Effectiveness	AAT-16.2	Mechanisms exist to regularly assess the effectiveness of existing controls, including reports of errors and potential impacts on affected communities.	8	
MEASURE 1.1	N/A	Approaches and metrics for measurement of AI risks enumerated during the MAP function are selected for implementation starting with the most significant AI risks. The risks or trustworthiness characteristics that will not – or cannot – be measured are properly documented.	Functional	equal	Measures of Performance	GOV-05	Mechanisms exist to develop, report and monitor cybersecurity & data privacy program measures of performance.	10	
MEASURE 1.1	N/A	Approaches and metrics for measurement of AI risks enumerated during the MAP function are selected for implementation starting with the most significant AI risks. The risks or trustworthiness characteristics that will not – or cannot – be measured are properly documented.	Functional	intersects with	Measuring AI & Autonomous Technologies Effectiveness	AAT-16.2	Mechanisms exist to regularly assess the effectiveness of existing controls, including reports of errors and potential impacts on affected communities.	8	
MEASURE 1.1	N/A	Approaches and metrics for measurement of AI risks enumerated during the MAP function are selected for implementation starting with the most significant AI risks. The risks or trustworthiness characteristics that will not – or cannot – be measured are properly documented.	Functional	intersects with	Unmeasurable AI & Autonomous Technologies Risks	AAT-16.3	Mechanisms exist to identify and document unmeasurable risks or trustworthiness characteristics.	8	
MEASURE 1.2	N/A	Appropriateness of AI metrics and effectiveness of existing controls are regularly assessed and updated, including reports of errors and potential impacts on affected communities.	Functional	equal	Measures of Performance	GOV-05	Mechanisms exist to develop, report and monitor cybersecurity & data privacy program measures of performance.	10	
MEASURE 1.2	N/A	Appropriateness of AI metrics and effectiveness of existing controls are regularly assessed and updated, including reports of errors and potential impacts on affected communities.	Functional	intersects with	Measuring AI & Autonomous Technologies Effectiveness	AAT-16.2	Mechanisms exist to regularly assess the effectiveness of existing controls, including reports of errors and potential impacts on affected communities.	8	
MEASURE 1.3	N/A	Internal experts who did not serve as front-line developers for the system and/or independent assessors are involved in regular assessments and updates. Domain experts, users, AI actors external to the team that developed or deployed the AI system, and affected communities are consulted in support of assessments as necessary per organizational risk tolerance.	Functional	equal	AI & Autonomous Technologies Ongoing Assessments	AAT-11.2	Mechanisms exist to conduct regular assessments of Artificial Intelligence (AI) and Autonomous Technologies (AAT) with independent assessors and stakeholders not involved in the development of the AAT.	10	
MEASURE 2.0	N/A	AI systems are evaluated for trustworthy characteristics.	Functional	equal	AI TEVV Trustworthiness Assessment	AAT-10.1	Mechanisms exist to evaluate Artificial Intelligence (AI) and Autonomous Technologies (AAT) for trustworthy behavior and operation including security, anonymization and disaggregation of captured and stored data for approved purposes.	10	
MEASURE 2.0	N/A	AI systems are evaluated for trustworthy characteristics.	Functional	intersects with	AI TEVV Trustworthiness Demonstration	AAT-10.3	Mechanisms exist to demonstrate the Artificial Intelligence (AI) and Autonomous Technologies (AAT) to be deployed are: (1) Valid; (2) Reliable; and (3) Operate as intended, based on approved designs.	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)
MEASURE 2.0	N/A	AI systems are evaluated for trustworthy characteristics.	Functional	equal	Assessments	IAO-02	Mechanisms exist to formally assess the cybersecurity & data privacy controls in systems, applications and services 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.	10	
MEASURE 2.0	N/A	AI systems are evaluated for trustworthy characteristics.	Functional	intersects with	Technical Verification	IAO-06	Mechanisms exist to perform Information Assurance Program (IAP) activities to evaluate the design, implementation and effectiveness of technical cybersecurity & data privacy controls.	5	
MEASURE 2.1	N/A	Test sets, metrics, and details about the tools used during TEVV are documented.	Functional	equal	AI TEVV Tools	AAT-10.2	Mechanisms exist to document test sets, metrics and details about the tools used during Artificial Intelligence Test, Evaluation, Validation & Verification (AI TEVV) practices.	10	
MEASURE 2.2	N/A	Evaluations involving human subjects meet applicable requirements (including human subject protection) and are representative of the relevant population.	Functional	intersects with	Artificial Intelligence Test, Evaluation, Validation & Verification (AI TEVV)	AAT-10	Mechanisms exist to implement Artificial Intelligence Test, Evaluation, Validation & Verification (AI TEVV) practices to enable Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related security, resilience and compliance-related conformity testing throughout the lifecycle of the AAT.	5	
MEASURE 2.2	N/A	Evaluations involving human subjects meet applicable requirements (including human subject protection) and are representative of the relevant population.	Functional	equal	AI & Autonomous Technologies Harm Prevention	AAT-17	Mechanisms exist to proactively prevent harm by regularly identifying and tracking existing, unanticipated and emergent Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related risks.	10	
MEASURE 2.2	N/A	Evaluations involving human subjects meet applicable requirements (including human subject protection) and are representative of the relevant population.	Functional	equal	AI & Autonomous Technologies Human Subject Protections	AAT-17.1	Mechanisms exist to protect human subjects from harm.	10	
MEASURE 2.3	N/A	AI system performance or assurance criteria are measured qualitatively or quantitatively and demonstrated for conditions similar to deployment setting(s). Measures are documented.	Functional	equal	AI TEVV Comparable Deployment Settings	AAT-10.12	Mechanisms exist to evaluate Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related performance or the assurance criteria demonstrated for conditions similar to deployment settings.	10	
MEASURE 2.4	N/A	The functionality and behavior of the AI system and its components – as identified in the MAP function – are monitored when in production.	Functional	intersects with	AI TEVV Post-Deployment Monitoring	AAT-10.13	Mechanisms exist to proactively and continuously monitor deployed Artificial Intelligence (AI) and Autonomous Technologies (AAT).	5	
MEASURE 2.4	N/A	The functionality and behavior of the AI system and its components – as identified in the MAP function – are monitored when in production.	Functional	intersects with	AI & Autonomous Technologies Production Monitoring	AAT-16	Mechanisms exist to monitor the functionality and behavior of the deployed Artificial Intelligence (AI) and Autonomous Technologies (AAT).	8	
MEASURE 2.5	N/A	The AI system to be deployed is demonstrated to be valid and reliable. Limitations of the generalizability beyond the conditions under which the technology was developed are documented.	Functional	intersects with	Trustworthy AI & Autonomous Technologies	AAT-01.2	Mechanisms exist to ensure Artificial Intelligence (AI) and Autonomous Technologies (AAT) are designed to be reliable, safe, fair, secure, resilient, transparent, explainable and data privacy-enhanced to minimize emergent properties or unintended consequences.	5	
MEASURE 2.5	N/A	The AI system to be deployed is demonstrated to be valid and reliable. Limitations of the generalizability beyond the conditions under which the technology was developed are documented.	Functional	intersects with	AI & Autonomous Technologies Model Validation	AAT-10.9	Mechanisms exist to validate the Artificial Intelligence (AI) and Autonomous Technologies (AAT) model.	8	
MEASURE 2.6	N/A	The AI system is evaluated regularly for safety risks – as identified in the MAP function. The AI system to be deployed is demonstrated to be safe, its residual negative risk does not exceed the risk tolerance, and it can fail safely, particularly if made to operate beyond its knowledge limits. Safety metrics reflect system reliability and robustness, real-time monitoring, and response times for AI system failures.	Functional	intersects with	AI TEVV Safety Demonstration	AAT-10.4	Mechanisms exist to demonstrate the Artificial Intelligence (AI) and Autonomous Technologies (AAT) to be deployed are safe, residual risk does not exceed the organization's risk tolerance and can fail safely, particularly if made to operate beyond its knowledge limits.	8	
MEASURE 2.6	N/A	The AI system is evaluated regularly for safety risks – as identified in the MAP function. The AI system to be deployed is demonstrated to be safe, its residual negative risk does not exceed the risk tolerance, and it can fail safely, particularly if made to operate beyond its knowledge limits. Safety metrics reflect system reliability and robustness, real-time monitoring, and response times for AI system failures.	Functional	intersects with	AI & Autonomous Technologies Ongoing Assessments	AAT-11.2	Mechanisms exist to conduct regular assessments of Artificial Intelligence (AI) and Autonomous Technologies (AAT) with independent assessors and stakeholders not involved in the development of the AAT.	5	
MEASURE 2.6	N/A	The AI system is evaluated regularly for safety risks – as identified in the MAP function. The AI system to be deployed is demonstrated to be safe, its residual negative risk does not exceed the risk tolerance, and it can fail safely, particularly if made to operate beyond its knowledge limits. Safety metrics reflect system reliability and robustness, real-time monitoring, and response times for AI system failures.	Functional	intersects with	AI TEVV Post-Deployment Monitoring	AAT-10.13	Mechanisms exist to proactively and continuously monitor deployed Artificial Intelligence (AI) and Autonomous Technologies (AAT).	5	
MEASURE 2.7	N/A	AI system security and resilience – as identified in the MAP function – are evaluated and documented.	Functional	equal	AI TEVV Security & Resiliency Assessment	AAT-10.5	Mechanisms exist to evaluate the security and resilience of Artificial Intelligence (AI) and Autonomous Technologies (AAT) to be deployed.	10	
MEASURE 2.7	N/A	AI system security and resilience – as identified in the MAP function – are evaluated and documented.	Functional	intersects with	Achieving Resilience Requirements	SEA-01.2	Mechanisms exist to achieve resilience requirements in normal and adverse situations.	5	
MEASURE 2.8	N/A	Risks associated with transparency and accountability – as identified in the MAP function – are examined and documented.	Functional	equal	AI TEVV Transparency & Accountability Assessment	AAT-10.6	Mechanisms exist to examine risks associated with transparency and accountability of Artificial Intelligence (AI) and Autonomous Technologies (AAT) to be deployed.	10	
MEASURE 2.9	N/A	The AI model is explained, validated, and documented, and AI system output is interpreted within its context – as identified in the MAP function – to inform responsible use and governance.	Functional	equal	AI & Autonomous Technologies Model Validation	AAT-10.9	Mechanisms exist to validate the Artificial Intelligence (AI) and Autonomous Technologies (AAT) model.	10	
MEASURE 2.10	N/A	Privacy risk of the AI system – as identified in the MAP function – is examined and documented.	Functional	equal	AI TEVV Privacy Assessment	AAT-10.7	Mechanisms exist to examine the data privacy risk of Artificial Intelligence (AI) and Autonomous Technologies (AAT) to be deployed.	10	
MEASURE 2.10	N/A	Privacy risk of the AI system – as identified in the MAP function – is examined and documented.	Functional	intersects with	Data Protection Impact Assessment (DPIA)	RSK-10	Mechanisms exist to conduct a Data Protection Impact Assessment (DPIA) on systems, applications and services that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.	8	
MEASURE 2.11	N/A	Fairness and bias – as identified in the MAP function – are evaluated and results are documented.	Functional	equal	AI TEVV Fairness & Bias Assessment	AAT-10.8	Mechanisms exist to examine fairness and bias of Artificial Intelligence (AI) and Autonomous Technologies (AAT) to be deployed.	10	
MEASURE 2.12	N/A	Environmental impact and sustainability of AI model training and management activities – as identified in the MAP function – are assessed and documented.	Functional	equal	AI & Autonomous Technologies Environmental Impact & Sustainability	AAT-17.2	Mechanisms exist to assess and document the environmental impacts and sustainability of Artificial Intelligence (AI) and Autonomous Technologies (AAT).	10	
MEASURE 2.13	N/A	Effectiveness of the employed TEVV metrics and processes in the MEASURE function are evaluated and documented.	Functional	intersects with	AI TEVV Results Evaluation	AAT-10.10	Mechanisms exist to evaluate the results of Artificial Intelligence Test, Evaluation, Validation & Verification (AI TEVV) to determine the viability of the proposed Artificial Intelligence (AI) and Autonomous Technologies (AAT).	8	
MEASURE 2.13	N/A	Effectiveness of the employed TEVV metrics and processes in the MEASURE function are evaluated and documented.	Functional	equal	AI TEVV Effectiveness	AAT-10.11	Mechanisms exist to evaluate the effectiveness of the processes utilized to perform Artificial Intelligence Test, Evaluation, Validation & Verification (AI TEVV).	10	
MEASURE 3.0	N/A	Mechanisms for tracking identified AI risks over time are in place.	Functional	intersects with	Measuring AI & Autonomous Technologies Effectiveness	AAT-16.2	Mechanisms exist to regularly assess the effectiveness of existing controls, including reports of errors and potential impacts on affected communities.	3	
MEASURE 3.0	N/A	Mechanisms for tracking identified AI risks over time are in place.	Functional	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	
MEASURE 3.0	N/A	Mechanisms for tracking identified AI risks over time are in place.	Functional	equal	Risk Register	RSK-04.1	Mechanisms exist to maintain a risk register that facilitates monitoring and reporting of risks.	10	
MEASURE 3.1	N/A	Approaches, personnel, and documentation are in place to regularly identify and track existing, unanticipated, and emergent AI risks based on factors such as intended and actual performance in deployed contexts.	Functional	equal	AI & Autonomous Technologies Harm Prevention	AAT-17	Mechanisms exist to proactively prevent harm by regularly identifying and tracking existing, unanticipated and emergent Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related risks.	10	
MEASURE 3.1	N/A	Approaches, personnel, and documentation are in place to regularly identify and track existing, unanticipated, and emergent AI risks based on factors such as intended and actual performance in deployed contexts.	Functional	intersects with	Specialized Assessments	IAO-02.2	Mechanisms exist to conduct specialized assessments for: (1) Statutory, regulatory and contractual compliance obligations; (2) Monitoring capabilities; (3) Mobile devices; (4) Databases; (5) Application security; (6) Embedded technologies (e.g., IoT, OT, etc.); (7) Vulnerability management; (8) Malicious code; (9) Insider threats; (10) Performance/load testing; and/or (11) Artificial Intelligence and Autonomous Technologies (AAT).	3	
MEASURE 3.1	N/A	Approaches, personnel, and documentation are in place to regularly identify and track existing, unanticipated, and emergent AI risks based on factors such as intended and actual performance in deployed contexts.	Functional	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	

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)
MEASURE 3.1	N/A	Approaches, personnel, and documentation are in place to regularly identify and track existing, unanticipated, and emergent AI risks based on factors such as intended and actual performance in deployed contexts.	Functional	intersects with	Risk Register	RSK-04.1	Mechanisms exist to maintain a risk register that facilitates monitoring and reporting of risks.	5	
MEASURE 3.2	N/A	Risk tracking approaches are considered for settings where AI risks are difficult to assess using currently available measurement techniques or where metrics are not yet available.	Functional	equal	AI & Autonomous Technologies Risk Tracking Approaches	AAT-18	Mechanisms exist to track Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related risks are difficult to assess using currently available measurement techniques or where metrics are not yet available.	10	
MEASURE 3.2	N/A	Risk tracking approaches are considered for settings where AI risks are difficult to assess using currently available measurement techniques or where metrics are not yet available.	Functional	intersects with	Specialized Assessments	IAO-02.2	Mechanisms exist to conduct specialized assessments for: (1) Statutory, regulatory and contractual compliance obligations; (2) Monitoring capabilities; (3) Mobile devices; (4) Databases; (5) Application security; (6) Embedded technologies (e.g., IoT, OT, etc.); (7) Vulnerability management; (8) Malicious code; (9) Insider threats; (10) Performance/load testing; and/or (11) Artificial Intelligence and Autonomous Technologies (AAT).	3	
MEASURE 3.2	N/A	Risk tracking approaches are considered for settings where AI risks are difficult to assess using currently available measurement techniques or where metrics are not yet available.	Functional	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	
MEASURE 3.2	N/A	Risk tracking approaches are considered for settings where AI risks are difficult to assess using currently available measurement techniques or where metrics are not yet available.	Functional	intersects with	Risk Register	RSK-04.1	Mechanisms exist to maintain a risk register that facilitates monitoring and reporting of risks.	5	
MEASURE 3.3	N/A	Feedback processes for end users and impacted communities to report problems and appeal system outcomes are established and integrated into AI system evaluation metrics.	Functional	equal	AI & Autonomous Technologies End User Feedback	AAT-11.3	Mechanisms exist to collect and integrate feedback from end users and impacted communities into Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related system evaluation metrics.	10	
MEASURE 4.0	N/A	Feedback about efficacy of measurement is gathered and assessed.	Functional	intersects with	Measures of Performance	GOV-05	Mechanisms exist to develop, report and monitor cybersecurity & data privacy program measures of performance.	8	
MEASURE 4.0	N/A	Feedback about efficacy of measurement is gathered and assessed.	Functional	equal	Efficacy of AI & Autonomous Technologies Measurement	AAT-16.4	Mechanisms exist to gather and assess feedback about the efficacy of Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related measurements.	10	
MEASURE 4.1	N/A	Measurement approaches for identifying AI risks are connected to deployment context(s) and informed through consultation with domain experts and other end users. Approaches are documented.	Functional	intersects with	Key Performance Indicators (KPIs)	GOV-05.1	Mechanisms exist to develop, report and monitor Key Performance Indicators (KPIs) to assist organizational management in performance monitoring and trend analysis of the cybersecurity & data privacy program.	3	
MEASURE 4.1	N/A	Measurement approaches for identifying AI risks are connected to deployment context(s) and informed through consultation with domain experts and other end users. Approaches are documented.	Functional	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 & data privacy program.	3	
MEASURE 4.1	N/A	Measurement approaches for identifying AI risks are connected to deployment context(s) and informed through consultation with domain experts and other end users. Approaches are documented.	Functional	equal	AI & Autonomous Technologies Measurement Approaches	AAT-16.1	Mechanisms exist to measure Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related risks to deployment context(s) through review and consultation with industry experts, domain specialists and end users.	10	
MEASURE 4.2	N/A	Measurement results regarding AI system trustworthiness in deployment context(s) and across the AI lifecycle are informed by input from domain experts and relevant AI actors to validate whether the system is performing consistently as intended. Results are documented.	Functional	equal	AI & Autonomous Technologies Domain Expert Reviews	AAT-16.5	Mechanisms exist to utilize input from domain experts and relevant stakeholders to validate whether the Artificial Intelligence (AI) and Autonomous Technologies (AAT) perform consistently, as intended.	10	
MEASURE 4.3	N/A	Measurable performance improvements or declines based on consultations with relevant AI actors, including affected communities, and field data about context relevant risks and trustworthiness characteristics are identified and documented.	Functional	intersects with	Measures of Performance	GOV-05	Mechanisms exist to develop, report and monitor cybersecurity & data privacy program measures of performance.	8	
MEASURE 4.3	N/A	Measurable performance improvements or declines based on consultations with relevant AI actors, including affected communities, and field data about context relevant risks and trustworthiness characteristics are identified and documented.	Functional	intersects with	Key Performance Indicators (KPIs)	GOV-05.1	Mechanisms exist to develop, report and monitor Key Performance Indicators (KPIs) to assist organizational management in performance monitoring and trend analysis of the cybersecurity & data privacy program.	3	
MEASURE 4.3	N/A	Measurable performance improvements or declines based on consultations with relevant AI actors, including affected communities, and field data about context relevant risks and trustworthiness characteristics are identified and documented.	Functional	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 & data privacy program.	3	
MEASURE 4.3	N/A	Measurable performance improvements or declines based on consultations with relevant AI actors, including affected communities, and field data about context relevant risks and trustworthiness characteristics are identified and documented.	Functional	equal	AI & Autonomous Technologies Performance Changes	AAT-16.6	Mechanisms exist to evaluate performance improvements or declines with domain experts and relevant stakeholders to define context-relevant risks and trustworthiness issues.	10	
MANAGE 1.0	N/A	AI risks based on assessments and other analytical output from the MAP and MEASURE functions are prioritized, responded to, and managed.	Functional	equal	AI & Autonomous Technologies Risk Response	AAT-18.1	Mechanisms exist to prioritize, respond to and remediate Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related risks based on assessments and other analytical output.	10	
MANAGE 1.0	N/A	AI risks based on assessments and other analytical output from the MAP and MEASURE functions are prioritized, responded to, and managed.	Functional	subset of	Risk Management Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	10	
MANAGE 1.0	N/A	AI risks based on assessments and other analytical output from the MAP and MEASURE functions are prioritized, responded to, and managed.	Functional	intersects with	Risk Identification	RSK-03	Mechanisms exist to identify and document risks, both internal and external.	8	
MANAGE 1.0	N/A	AI risks based on assessments and other analytical output from the MAP and MEASURE functions are prioritized, responded to, and managed.	Functional	intersects with	Risk Assessment	RSK-04	Mechanisms exist to conduct recurring assessments of risk that includes the likelihood and magnitude of harm, from unauthorized access, use, disclosure, disruption, modification or destruction of the organization's systems and data.	8	
MANAGE 1.1	N/A	A determination is made as to whether the AI system achieves its intended purposes and stated objectives and whether its development or deployment should proceed.	Functional	intersects with	AI TEVV Results Evaluation	AAT-10.10	Mechanisms exist to evaluate the results of Artificial Intelligence Test, Evaluation, Validation & Verification (AI TEVV) to determine the viability of the proposed Artificial Intelligence (AI) and Autonomous Technologies (AAT).	5	
MANAGE 1.1	N/A	A determination is made as to whether the AI system achieves its intended purposes and stated objectives and whether its development or deployment should proceed.	Functional	equal	AI & Autonomous Technologies Viability Decisions	AAT-15	Mechanisms exist to define the criteria as to whether Artificial Intelligence (AI) and Autonomous Technologies (AAT) achieved intended purposes and stated objectives to determine whether its development or deployment should proceed.	10	
MANAGE 1.1	N/A	A determination is made as to whether the AI system achieves its intended purposes and stated objectives and whether its development or deployment should proceed.	Functional	intersects with	AI & Autonomous Technologies Negative Residual Risks	AAT-15.1	Mechanisms exist to identify and document negative, residual risks (defined as the sum of all unmitigated risks) to both downstream acquirers and end users of Artificial Intelligence (AI) and Autonomous Technologies (AAT).	8	
MANAGE 1.1	N/A	A determination is made as to whether the AI system achieves its intended purposes and stated objectives and whether its development or deployment should proceed.	Functional	intersects with	Responsibility To Supersede, Deactivate and/or Disengage AI & Autonomous Technologies	AAT-15.2	Mechanisms exist to define the criteria and responsible party(ies) for superseding, disengaging or deactivating Artificial Intelligence (AI) and Autonomous Technologies (AAT) that demonstrate performance or outcomes inconsistent with intended use.	3	
MANAGE 1.1	N/A	A determination is made as to whether the AI system achieves its intended purposes and stated objectives and whether its development or deployment should proceed.	Functional	subset of	Information Assurance (IA) Operations	IAO-01	Mechanisms exist to facilitate the implementation of cybersecurity & data privacy assessment and authorization controls.	10	
MANAGE 1.1	N/A	A determination is made as to whether the AI system achieves its intended purposes and stated objectives and whether its development or deployment should proceed.	Functional	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.	3	
MANAGE 1.1	N/A	A determination is made as to whether the AI system achieves its intended purposes and stated objectives and whether its development or deployment should proceed.	Functional	intersects with	Security Authorization	IAO-07	Mechanisms exist to ensure systems, projects and services are officially authorized prior to "go live" in a production environment.	8	
MANAGE 1.2	N/A	Treatment of documented AI risks is prioritized based on impact, likelihood, and available resources or methods.	Functional	intersects with	AI & Autonomous Technologies Negative Residual Risks	AAT-15.1	Mechanisms exist to identify and document negative, residual risks (defined as the sum of all unmitigated risks) to both downstream acquirers and end users of Artificial Intelligence (AI) and Autonomous Technologies (AAT).	5	
MANAGE 1.2	N/A	Treatment of documented AI risks is prioritized based on impact, likelihood, and available resources or methods.	Functional	intersects with	Responsibility To Supersede, Deactivate and/or Disengage AI & Autonomous Technologies	AAT-15.2	Mechanisms exist to define the criteria and responsible party(ies) for superseding, disengaging or deactivating Artificial Intelligence (AI) and Autonomous Technologies (AAT) that demonstrate performance or outcomes inconsistent with intended use.	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
MANAGE 1.2	N/A	Treatment of documented AI risks is prioritized based on impact, likelihood, and available resources or methods.	Functional	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.	8	
MANAGE 1.2	N/A	Treatment of documented AI risks is prioritized based on impact, likelihood, and available resources or methods.	Functional	intersects with	Impact-Level Prioritization	RSK-02.1	Mechanisms exist to prioritize the impact level for systems, applications and/or services to prevent potential disruptions.	3	
MANAGE 1.2	N/A	Treatment of documented AI risks is prioritized based on impact, likelihood, and available resources or methods.	Functional	intersects with	Risk Ranking	RSK-05	Mechanisms exist to identify and assign a risk ranking to newly discovered security vulnerabilities that is based on industry-recognized practices.	3	
MANAGE 1.2	N/A	Treatment of documented AI risks is prioritized based on impact, likelihood, and available resources or methods.	Functional	intersects with	Risk Remediation	RSK-06	Mechanisms exist to remediate risks to an acceptable level.	3	
MANAGE 1.3	N/A	Responses to the AI risks deemed high priority, as identified by the MAP function, are developed, planned, and documented. Risk response options can include mitigating, transferring, avoiding, or accepting.	Functional	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.	3	
MANAGE 1.3	N/A	Responses to the AI risks deemed high priority, as identified by the MAP function, are developed, planned, and documented. Risk response options can include mitigating, transferring, avoiding, or accepting.	Functional	equal	Risk Response	RSK-06.1	Mechanisms exist to respond to findings from cybersecurity & data privacy assessments, incidents and audits to ensure proper remediation has been performed.	10	
MANAGE 1.4	N/A	Negative residual risks (defined as the sum of all unmitigated risks) to both downstream acquirers of AI systems and end users are documented.	Functional	equal	AI & Autonomous Technologies Negative Residual Risks	AAT-15.1	Mechanisms exist to identify and document negative, residual risks (defined as the sum of all unmitigated risks) to both downstream acquirers and end users of Artificial Intelligence (AI) and Autonomous Technologies (AAT).	10	
MANAGE 1.4	N/A	Negative residual risks (defined as the sum of all unmitigated risks) to both downstream acquirers of AI systems and end users are documented.	Functional	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.	8	
MANAGE 1.4	N/A	Negative residual risks (defined as the sum of all unmitigated risks) to both downstream acquirers of AI systems and end users are documented.	Functional	intersects with	Risk Register	RSK-04.1	Mechanisms exist to maintain a risk register that facilitates monitoring and reporting of risks.	8	
MANAGE 2.0	N/A	Strategies to maximize AI benefits and minimize negative impacts are planned, prepared, implemented, documented, and informed by input from relevant AI actors.	Functional	equal	AI & Autonomous Technologies Continuous Improvements	AAT-07.3	Mechanisms exist to continuously improve Artificial Intelligence (AI) and Autonomous Technologies (AAT) capabilities to maximize benefits and minimize negative impacts associated with AAT.	10	
MANAGE 2.0	N/A	Strategies to maximize AI benefits and minimize negative impacts are planned, prepared, implemented, documented, and informed by input from relevant AI actors.	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.	3	
MANAGE 2.0	N/A	Strategies to maximize AI benefits and minimize negative impacts are planned, prepared, implemented, documented, and informed by input from relevant AI actors.	Functional	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 products and/or services 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.	8	
MANAGE 2.1	N/A	Resources required to manage AI risks are taken into account – along with viable non-AI alternative systems, approaches, or methods – to reduce the magnitude or likelihood of potential impacts.	Functional	intersects with	Cybersecurity & Data Privacy Portfolio Management	PRM-01	Mechanisms exist to facilitate the implementation of cybersecurity & data privacy-related resource planning controls that define a viable plan for achieving cybersecurity & data privacy objectives.	8	
MANAGE 2.1	N/A	Resources required to manage AI risks are taken into account – along with viable non-AI alternative systems, approaches, or methods – to reduce the magnitude or likelihood of potential impacts.	Functional	equal	Cybersecurity & Data Privacy Resource Management	PRM-02	Mechanisms exist to address all capital planning and investment requests, including the resources needed to implement the cybersecurity & data privacy programs and document all exceptions to this requirement.	10	
MANAGE 2.1	N/A	Resources required to manage AI risks are taken into account – along with viable non-AI alternative systems, approaches, or methods – to reduce the magnitude or likelihood of potential impacts.	Functional	intersects with	Allocation of Resources	PRM-03	Mechanisms exist to identify and allocate resources for management, operational, technical and data privacy requirements within business process planning for projects / initiatives.	8	
MANAGE 2.1	N/A	Resources required to manage AI risks are taken into account – along with viable non-AI alternative systems, approaches, or methods – to reduce the magnitude or likelihood of potential impacts.	Functional	intersects with	Risk Management Resourcing	RSK-01.2	Mechanisms exist to reduce the magnitude or likelihood of potential impacts by resourcing the capability required to manage technology-related risks.	8	
MANAGE 2.1	N/A	Resources required to manage AI risks are taken into account – along with viable non-AI alternative systems, approaches, or methods – to reduce the magnitude or likelihood of potential impacts.	Functional	intersects with	Compensating Countermeasures	RSK-06.2	Mechanisms exist to identify and implement compensating countermeasures to reduce risk and exposure to threats.	8	
MANAGE 2.2	N/A	Mechanisms are in place and applied to sustain the value of deployed AI systems.	Functional	equal	AI & Autonomous Technologies Value Sustainment	AAT-01.3	Mechanisms exist to sustain the value of deployed Artificial Intelligence (AI) and Autonomous Technologies (AAT).	10	
MANAGE 2.2	N/A	Mechanisms are in place and applied to sustain the value of deployed AI systems.	Functional	intersects with	Cybersecurity & Data Privacy Portfolio Management	PRM-01	Mechanisms exist to facilitate the implementation of cybersecurity & data privacy-related resource planning controls that define a viable plan for achieving cybersecurity & data privacy objectives.	8	
MANAGE 2.2	N/A	Mechanisms are in place and applied to sustain the value of deployed AI systems.	Functional	intersects with	Secure Development Life Cycle (SDLC) Management	PRM-07	Mechanisms exist to ensure changes to systems within the Secure Development Life Cycle (SDLC) are controlled through formal change control procedures.	5	
MANAGE 2.2	N/A	Mechanisms are in place and applied to sustain the value of deployed AI systems.	Functional	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 products and/or services 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	
MANAGE 2.3	N/A	Procedures are followed to respond to and recover from a previously unknown risk when it is identified.	Functional	equal	Previously Unknown AI & Autonomous Technologies Threats & Risks	AAT-17.3	Mechanisms exist to respond to and recover from a previously unknown Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related risk when it is identified.	10	
MANAGE 2.3	N/A	Procedures are followed to respond to and recover from a previously unknown risk when it is identified.	Functional	intersects with	Incident Response Operations	IRO-01	Mechanisms exist to implement and govern processes and documentation to facilitate an organization-wide response capability for cybersecurity & data privacy-related incidents.	3	
MANAGE 2.3	N/A	Procedures are followed to respond to and recover from a previously unknown risk when it is identified.	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.	3	
MANAGE 2.3	N/A	Procedures are followed to respond to and recover from a previously unknown risk when it is identified.	Functional	intersects with	Risk Identification	RSK-03	Mechanisms exist to identify and document risks, both internal and external.	5	
MANAGE 2.3	N/A	Procedures are followed to respond to and recover from a previously unknown risk when it is identified.	Functional	intersects with	Risk Response	RSK-06.1	Mechanisms exist to respond to findings from cybersecurity & data privacy assessments, incidents and audits to ensure proper remediation has been performed.	8	
MANAGE 2.4	N/A	Mechanisms are in place and applied, and responsibilities are assigned and understood, to supersede, disengage, or deactivate AI systems that demonstrate performance or outcomes inconsistent with intended use.	Functional	intersects with	Stakeholder Accountability Structure	GOV-04.1	Mechanisms exist to enforce an accountability structure so that appropriate teams and individuals are empowered, responsible and trained for mapping, measuring and managing data and technology-related risks.	8	
MANAGE 2.4	N/A	Mechanisms are in place and applied, and responsibilities are assigned and understood, to supersede, disengage, or deactivate AI systems that demonstrate performance or outcomes inconsistent with intended use.	Functional	equal	Responsibility To Supersede, Deactivate and/or Disengage AI & Autonomous Technologies	AAT-15.2	Mechanisms exist to define the criteria and responsible party(ies) for superseding, disengaging or deactivating Artificial Intelligence (AI) and Autonomous Technologies (AAT) that demonstrate performance or outcomes inconsistent with intended use.	10	
MANAGE 2.4	N/A	Mechanisms are in place and applied, and responsibilities are assigned and understood, to supersede, disengage, or deactivate AI systems that demonstrate performance or outcomes inconsistent with intended use.	Functional	intersects with	Incident Response Operations	IRO-01	Mechanisms exist to implement and govern processes and documentation to facilitate an organization-wide response capability for cybersecurity & data privacy-related incidents.	3	
MANAGE 2.4	N/A	Mechanisms are in place and applied, and responsibilities are assigned and understood, to supersede, disengage, or deactivate AI systems that demonstrate performance or outcomes inconsistent with intended use.	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	

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)
MANAGE 2.4	N/A	Mechanisms are in place and applied, and responsibilities are assigned and understood, to supersede, disengage, or deactivate AI systems that demonstrate performance or outcomes inconsistent with intended use.	Functional	intersects with	Risk Response	RSK-06.1	Mechanisms exist to respond to findings from cybersecurity & data privacy assessments, incidents and audits to ensure proper remediation has been performed.	8	
MANAGE 3.0	N/A	AI risks and benefits from third-party entities are managed.	Functional	intersects with	Supply Chain Risk Management (SCRM) Plan	RSK-09	Mechanisms exist to develop a plan for Supply Chain Risk Management (SCRM) associated with the development, acquisition, maintenance and disposal of systems, system components and services, including documenting selected mitigating actions and monitoring performance against those plans.	8	
MANAGE 3.0	N/A	AI risks and benefits from third-party entities are managed.	Functional	equal	AI & Autonomous Technologies Supply Chain Impacts	RSK-09.2	Mechanisms exist to address Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related risks and benefits arising from the organization's supply chain, including third-party software and data.	10	
MANAGE 3.0	N/A	AI risks and benefits from third-party entities are managed.	Functional	subset of	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	10	
MANAGE 3.0	N/A	AI risks and benefits from third-party entities are managed.	Functional	intersects with	Review of Third-Party Services	TPM-08	Mechanisms exist to monitor, regularly review and assess External Service Providers (ESPs) for compliance with established contractual requirements for cybersecurity & data privacy controls.	5	
MANAGE 3.1	N/A	AI risks and benefits from third-party resources are regularly monitored, and risk controls are applied and documented.	Functional	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.	8	
MANAGE 3.1	N/A	AI risks and benefits from third-party resources are regularly monitored, and risk controls are applied and documented.	Functional	intersects with	Supply Chain Risk Assessment	RSK-09.1	Mechanisms exist to periodically assess supply chain risks associated with systems, system components and services.	8	
MANAGE 3.1	N/A	AI risks and benefits from third-party resources are regularly monitored, and risk controls are applied and documented.	Functional	intersects with	AI & Autonomous Technologies Supply Chain Impacts	RSK-09.2	Mechanisms exist to address Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related risks and benefits arising from the organization's supply chain, including third-party software and data.	5	
MANAGE 3.1	N/A	AI risks and benefits from third-party resources are regularly monitored, and risk controls are applied and documented.	Functional	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 services.	8	
MANAGE 3.1	N/A	AI risks and benefits from third-party resources are regularly monitored, and risk controls are applied and documented.	Functional	intersects with	Review of Third-Party Services	TPM-08	Mechanisms exist to monitor, regularly review and assess External Service Providers (ESPs) for compliance with established contractual requirements for cybersecurity & data privacy controls.	5	
MANAGE 3.2	N/A	Pre-trained models which are used for development are monitored as part of AI system regular monitoring and maintenance.	Functional	equal	Pre-Trained AI & Autonomous Technologies Models	AAT-16.7	Mechanisms exist to validate the information source(s) and quality of pre-trained models used in Artificial Intelligence (AI) and Autonomous Technologies (AAT) training, maintenance and improvement-related activities.	10	
MANAGE 4.0	N/A	Risk treatments, including response and recovery, and communication plans for the identified and measured AI risks are documented and monitored regularly	Functional	intersects with	Incident Response Plan (IRP)	IRO-04	Mechanisms exist to maintain and make available a current and viable Incident Response Plan (IRP) to all stakeholders.	5	
MANAGE 4.0	N/A	Risk treatments, including response and recovery, and communication plans for the identified and measured AI risks are documented and monitored regularly	Functional	intersects with	System Security & Privacy Plan (SSPP)	IAO-03	Mechanisms exist to generate System Security & Privacy Plans (SSPPs), or similar document repositories, to identify and maintain key architectural information on each critical system, application or service, as well as influence inputs, entities, systems, applications and processes, providing a historical record of the data and its origins.	8	
MANAGE 4.0	N/A	Risk treatments, including response and recovery, and communication plans for the identified and measured AI risks are documented and monitored regularly	Functional	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	
MANAGE 4.0	N/A	Risk treatments, including response and recovery, and communication plans for the identified and measured AI risks are documented and monitored regularly	Functional	intersects with	Risk Remediation	RSK-06	Mechanisms exist to remediate risks to an acceptable level.	8	
MANAGE 4.0	N/A	Risk treatments, including response and recovery, and communication plans for the identified and measured AI risks are documented and monitored regularly	Functional	intersects with	Risk Response	RSK-06.1	Mechanisms exist to respond to findings from cybersecurity & data privacy assessments, incidents and audits to ensure proper remediation has been performed.	5	
MANAGE 4.1	N/A	Post-deployment AI system monitoring plans are implemented, including mechanisms for capturing and evaluating input from users and other relevant AI actors, appeal and override, decommissioning, incident response, recovery, and change management.	Functional	intersects with	AI TEVV Post-Deployment Monitoring	AAT-10.13	Mechanisms exist to proactively and continuously monitor deployed Artificial Intelligence (AI) and Autonomous Technologies (AAT).	8	
MANAGE 4.1	N/A	Post-deployment AI system monitoring plans are implemented, including mechanisms for capturing and evaluating input from users and other relevant AI actors, appeal and override, decommissioning, incident response, recovery, and change management.	Functional	intersects with	AI & Autonomous Technologies Stakeholder Feedback Integration	AAT-11.1	Mechanisms exist to regularly collect, consider, prioritize and integrate risk-related feedback from those external to the team that developed or deployed Artificial Intelligence (AI) and Autonomous Technologies (AAT).	8	
MANAGE 4.1	N/A	Post-deployment AI system monitoring plans are implemented, including mechanisms for capturing and evaluating input from users and other relevant AI actors, appeal and override, decommissioning, incident response, recovery, and change management.	Functional	intersects with	AI & Autonomous Technologies Ongoing Assessments	AAT-11.2	Mechanisms exist to conduct regular assessments of Artificial Intelligence (AI) and Autonomous Technologies (AAT) with independent assessors and stakeholders not involved in the development of the AAT.	8	
MANAGE 4.1	N/A	Post-deployment AI system monitoring plans are implemented, including mechanisms for capturing and evaluating input from users and other relevant AI actors, appeal and override, decommissioning, incident response, recovery, and change management.	Functional	intersects with	AI & Autonomous Technologies End User Feedback	AAT-11.3	Mechanisms exist to collect and integrate feedback from end users and impacted communities into Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related system evaluation metrics.	8	
MANAGE 4.2	N/A	Measurable activities for continual improvements are integrated into AI system updates and include regular engagement with interested parties, including relevant AI actors.	Functional	equal	Updating AI & Autonomous Technologies	AAT-10.14	Mechanisms exist to integrate continual improvements for deployed Artificial Intelligence (AI) and Autonomous Technologies (AAT).	10	
MANAGE 4.3	N/A	Incidents and errors are communicated to relevant AI actors, including affected communities. Processes for tracking, responding to, and recovering from incidents and errors are followed and documented.	Functional	equal	AI & Autonomous Technologies Incident & Error Reporting	AAT-11.4	Mechanisms exist to communicate Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related incidents and/or errors to relevant stakeholders, including affected communities.	10	
MANAGE 4.3	N/A	Incidents and errors are communicated to relevant AI actors, including affected communities. Processes for tracking, responding to, and recovering from incidents and errors are followed and documented.	Functional	intersects with	Incident Stakeholder Reporting	IRO-10	Mechanisms exist to timely-report incidents to applicable: (1) Internal stakeholders; (2) Affected clients & third-parties; and (3) Regulatory authorities.	8	