\_\_\_\_

 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

Strength of

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 Al 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	Al & 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 Al 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 Al 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 (A) and Autonomous Technologies (AAT) are designed to be reliable, safe, fair, scure, 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. Mechanisms exist to centrally-manage the organization-wide	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 oblications.	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 fisk 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	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-	5	
GOVERN 1.3	N/A	tolerance. Processes, procedures, and practices are in place to determine the needed level of risk management activities based on the organization's risk	Functional	intersects with	Resourcing Risk Tolerance	RSK-01.3	related risks. Mechanisms exist to define organizational risk tolerance, the specified range of acceptable results.	5	
GOVERN 1.3	N/A	tolerance. 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. The risk management process and its outcomes are established through	Functional	intersects with	Operations Security	OPS-01	Mechanisms exist to facilitate the implementation of operational security controls. Mechanisms exist to identify and document Standardized Operating	8	
GOVERN 1.4	N/A	The first management process and its outcomes are estabuished through transparent policies, procedures, and other controls based on organizational risk priorities.	Functional	intersects with	Standardized Operating Procedures (SOP)	OPS-01.1	Procedures (SOP), or similar document standardized operating Procedures (SOP), or similar documentation, to enable the proper execution of day-to-day / assigned tasks.	8	

ibution-NoDerivative

Vers	ion 2025.2
	7/7/2025

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship	Notes (optional)
		Ongoing monitoring and periodic review of the risk management process	Rationale	Relationship			Mechanisms exist to develop, report and monitor cybersecurity & data	(optional)	
GOVERN 1.5	N/A	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	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	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	5	
GOVERN 1.5	N/A	clearly defined, including determining the frequency of periodic review. Ongoing monitoring and periodic review of the risk management process and its outcomes are planned and organizational roles and responsibilities	Functional	intersects with	Risk Register	RSK-04.1	organization's systems and data. Mechanisms exist to maintain a risk register that facilitates monitoring and reporting of risks.	5	
GOVERN 1.5	N/A	clearly defined, including determining the frequency of periodic review. Ongoing monitoring and periodic review of the risk management process and its outcomes are planned and organizational roles and responsibilities	Functional	intersects with	Business Impact Analysis	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	clearly defined, including determining the frequency of periodic review. Mechanisms are in place to inventory Al systems and are resourced according to organizational risk priorities.	Functional	intersects with	(BIA) Situational Awareness of AI & Autonomous	AAT-02	Mechanisms exist to develop and maintain an inventory of Artificial Intelligence (AI) and Autonomous Technologies (AAT) (internal and third-	5	
		according to organizational risk priorities.			Technologies		party). Mechanisms exist to perform inventories of technology assets that:		
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	(1) Accurately reflects the current systems, applications and services in use; (2) Identifies authorized software products, including business justification details; (3) but the level of granularity deemed necessary for tracking and reporting; (4) Includes or gignization-defined information deemed necessary to achieve effective property accountability; and (5) is available for review and audity designated organizational	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	personnel. 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 Al 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 Al 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 Al systems safety 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 mision/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 Al 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 Al 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 Al 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 Al 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 Al 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 Al 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	measuring, and managing Ar insks. 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] Annualit Wherefater.	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	More an addition of the second	5	
GOVERN 2.1	N/A	Roles and responsibilities and lines of communication related to mapping, measuring, and managing Al risks are documented and are clear to individuals and teams throughout the organization.	Functional	intersects with	Stakeholder Accountability Structure	GOV-04.1	protection program. 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	Induced Tasks. 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	Notes (optional)
			Rationale	Relationship			Control Description Mechanisms exist to define and differentiate roles and responsibilities	(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	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	Functional	intersects with	Defined Roles &	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	
		individuals and teams throughout the organization.			Responsibilities		Mechanisms exist to provide role-based cybersecurity & data privacy-		
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	related training: (1) Before authorizing access to the system or performing assigned duties; (2) When required by system changes; and	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	(3) Annually thereafter. 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	Al & Autonomous Technologies Fairness & Bias	AAT-06	Mechanisms exist to prevent Artificial Intelligence (A) and Autonomous Technologies (AD) from unlarity identifying, profiling and/or statistically singling out a segmented population defined by race, religion, gender identify, national origin, religion, disability or any other politically-charged identifier.	10	
GOVERN 3.1	N/A	Decision-making related to mapping, measuring, and managing Al risks throughout the lifecycle is informed by a diverse team (e.g., diversity of demographics, disciplines, experience, expertise, and backgrounds).	Functional	intersects with	Al & 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 demotioned diversities any entry of the angle and believe the second	Functional	subset of	Technology Development & Acquisition	TDA-01	Mechanisms exist to facilitate the implementation of tailored development and acquisition strategies, contract tools and	10	
GOVERN 3.1	N/A	demographics, disciplines, experience, expertise, and backgrounds). 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	procurrement methods to meet unique business needs. Mechanisme soits to design and implement product management processes to proactively gowen the design, development and production of products and/or services across the System Development Life Cycle (BDLC) to: (1) Improve functionality; (2) Enhance security and realisincy 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-Al configurations and oversight of Al 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-Al configurations and oversight of Al 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 (AAT systems.	5	
GOVERN 3.2	N/A	Policies and procedures are in place to define and differentiate roles and responsibilities for human-Al configurations and oversight of Al 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-Al configurations and oversight of Al 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. Mechanisms exist to incorporate cybersecurity & data privacy	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	principles into Business As Usual (BAU) practices through executive leadership involvement. Mechanisms exist to compel data and/or process owners to	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	operationalize cybersecurity & data privacy process owners to application and/or service under their control.	5	
GOVERN 4.0	N/A	Organizational teams are committed to a culture that considers and communicates Al 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 Al 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 Al 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 Al 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 Al 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 Al 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 Al 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 Al 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 Al 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 Al 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 Al 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) for: (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 Al technology they design, develop, deploy, evaluate, and use, and they communicate about the impacts more broadly.	Functional	intersects with	Al & Autonomous Technologies Risk Profiling	AAT-09	Inductioning Sortware. Mechanisms exist to document the risks and potential impacts of Artificial Intelligence (A) 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 procetively 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 oblisations.	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 maticimed software.	5	
GOVERN 4.2	N/A	Organizational teams document the risks and potential impacts of the Al 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 constraint's entry of the constraint of the organization's security (2) Accurately and completely describes the required security functionality and the allocation of security controls among physical and logical components; and call dogical components; and (2) Expresses how individual security functions, mechanisms and services work forgether to provide required security compatibilities and a capabilities and a capabilities and a capabilities and a	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	unified approach to protection. Mechanisms exist to implement Artificial Intelligence Test, Evaluation, Validation & Verification (AI TEV/) practices to enable Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related security, resilience and compliance-related conformity testing throughout the lifeycied 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 Al & 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	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 Al 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. Organizational policies and practices are in place to collect, consider,	Functional	intersects with	AI & Autonomous Technologies Stakeholder Feedback Integration	AAT-11.1	Mechaniams 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). Mechaniams exist to facilitate the implementation of operational	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. Organizational policies and practices are in place to collect, consider,	Functional	intersects with	Operations Security	OPS-01	Prechamisms exist to inclutate the implementation of operational security controls.	8	
GOVERN 5.1	N/A	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	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 that Alystern regarding the potential individual and societal impacts related to Al risks.	Functional	intersects with	Product Management	TDA-01.1	Mechanisms exist to design and implement product management processes to procetively govern the design, development and production of products and/or services across the System Development Life Cycle (SDLC) to: (1) Improve tunctionality; (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 At systems to regularly incorporate adjudicated feedback from relevant AI actors into system design and implementation.	Functional	intersects with	Product Management	TDA-01.1	Nechanisms exist to design and implement product management processes to proceatively govern the design, development and production of products and/or services across the System Development Life Cycle (SUC) (or: (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	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	Notes (optional)
		Policies and procedures are in place to address AI risks and benefits			AI & Autonomous		Mechanisms exist to address Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related risks and benefits arising from	(optional)	
GOVERN 6.0	N/A	arising from third-party software and data and other supply chain issues.	Functional	intersects with	Technologies Supply Chain Impacts	RSK-09.2	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	8	
GOVERN 6.0	N/A	Policies and procedures are in place to address AI risks and banefits arising from third-party software and data and other supply chain issues.	Functional	intersects with	Product Management	TDA-01.1	execution of day-to-day / assigned tasks. Mechanisms oxis to design and implement product management processes to proactively govern the design, development and production of products and/or services across the System Development LFC cycle (SDLC) to: (1) Improve functionality; (2) Enhance security and mailinery capabilities; (3) Correct security and ficiencies; 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	Al & 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 Al 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 Al 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. Mechanisms exist to cover:	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	"Inclinational source 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 Al 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	Al & 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(5) 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 ast of protection needs is obtained. Mechanisms exist to establish and document the context surrounding	5	
MAP 1.1	N/A	Intended Jub Joses, Jose Statistica Viennica uses, Jonicas valencia tears, norms and expectations, and prospective settings in which the AJ system Will be deployed are understood and documented. Considerations includes 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 TEW and system metrics.	Functional	intersects with	AI & Autonomous Technologies Context Definition	AAT-03	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 Al 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 Al system purposes, uses, and risks across the development or product. Al lifecycle; and related TEVV and system metrics.	Functional	intersects with	Al & 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 risk 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 TEVW and system metrics.	Functional	intersects with	Business Impact Analysis (BIA)	RSK-08	Machanisms 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 TEVW and system metrics.	Functional	intersects with	Data Protection Impact Assessment (DPIA)	RSK-10	Mechanisms exist to conduct a Data Protection Impact Assessment (DPM) on systems, applications and sarvices 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 (A) 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	Notes (optional)
		Interdisciplinary AI actors, competencies, skills, and capacities for	Hationato	notationamp	Competency		Mechanisms exist to ensure that all security-related positions are	(optional)	
MAP 1.2	N/A	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	Requirements for Security-Related Positions	HRS-03.2	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	Functional	intersects with	AI & Autonomous Technologies Mission and	AAT-03.1	Mechanisms exist to define and document the organization's mission and defined goals for Artificial Intelligence (AI) and Autonomous	5	
		understood and documented.			Goals Definition Strategic Plan &		Technologies (AAT). Mechanisms exist to establish a strategic cybersecurity & data privacy-		
MAP 1.3	N/A	The organization's mission and relevant goals for Al technology are understood and documented.	Functional	intersects with	Objectives	PRM-01.1	specific business plan and set of objectives to achieve that plan.	5	
							Mechanisms exist to establish and document the context surrounding Artificial Intelligence (AI) and Autonomous Technologies (AAT),		
MAP 1.4	N/A	The business value or context of business use has been clearly defined or -	Functional	intersects with	AI & Autonomous Technologies Context	AAT-03	including: (1) Intended purposes;	5	
		in the case of assessing existing AI systems – re-evaluated.			Definition		<ul><li>(2) Potentially beneficial uses;</li><li>(3) Context-specific laws and regulations;</li></ul>		
							(4) Norms and expectations; and (5) Prospective settings in which the system(s) will be deployed. Mechanisms exist to define and document the organization's mission.		
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		AAT-03.1	and defined goals for Artificial Intelligence (AI) and Autonomous	5	
					Goals Definition		Technologies (AAT). Mechanisms exist to define business processes with consideration for		
MAP 1.4	N/A	The business value or context of business use has been clearly defined or –	Functional	intersects with	Business Process	PRM-06	cybersecurity & data privacy that determines: (1) The resulting risk to organizational operations, assets, individuals and other organizations; and	5	
MAP 1.4	NA	in the case of assessing existing AI systems – re-evaluated.	Functionat	Intersects with	Definition	PRM-00	<ol> <li>Information protection needs arising from the defined business processes and revises the processes as necessary, until an achievable</li> </ol>	5	
							set of protection needs is obtained. Mechanisms exist to define organizational risk tolerance, the specified		
MAP 1.5	N/A	Organizational risk tolerances are determined and documented. System requirements (e.g., "the system shall respect the privacy of its	Functional	equal	Risk Tolerance	RSK-01.3	range of acceptable results. Mechanisms exist to take socio-technical implications into account to	10	
MAP 1.6	N/A	users") are elicited from and understood by relevant Al actors. Design decisions take socio-technical implications into account to address Al	Functional	intersects with	Al & Autonomous Technologies	AAT-14	address risks associated with Artificial Intelligence (AI) and Autonomous Technologies (AAT).	5	
		risks. System requirements (e.g., "the system shall respect the privacy of its			Requirements Definitions		Mechanisms exist to facilitate the implementation and operation of		
MAP 1.6	N/A	users") are elicited from and understood by relevant Al actors. Design decisions take socio-technical implications into account to address Al	Functional	subset of	Data Privacy Program	PRI-01	data protection controls throughout the data lifecycle to ensure all forms of Personal Data (PD) are processed lawfully, fairly and	10	
		risks.					transparently. Mechanisms exist to restrict collecting, receiving, processing, storing,		
		System requirements (e.g., "the system shall respect the privacy of its					transmitting, updating and/or sharing Personna Data (PD) to: (1) The purpose(s) originally collected, consistent with the data privacy		
MAP 1.6	N/A	users") are elicited from and understood by relevant AI actors. Design decisions take socio-technical implications into account to address AI	Functional	intersects with	Usage Restrictions of Personal Data (PD)	PRI-05.4	(2) What is authorized by the data subject, or authorized agent; and	5	
		risks.					(3) What is consistent with applicable laws, regulations and contractual obligations.		
		System requirements (e.g., "the system shall respect the privacy of its					Mechanisms exist to identify critical system components and functions		
MAP 1.6	N/A	users") are elicited from and understood by relevant Al actors. Design decisions take socio-technical implications into account to address Al	Functional	intersects with	Cybersecurity & Data Privacy Requirements Definition	PRM-05	by performing a criticality analysis for critical systems, system components or services at pre-defined decision points in the Secure	5	
MAP 2.0	N/A	risks. Categorization of the Al system is performed.	Functional	intersects with		AST-31	Development Life Cycle (SDLC). 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	AST-31.1	Mechanisms exist to categorize Artificial Intelligence (AI) and Autonomous Technologies (AAT).	5	
100 2.0	1071	Categorization of the ne system to performed.	ranotionat	intersecto with	Technologies Al & Autonomous			5	
MAP 2.1	N/A	The specific tasks and methods used to implement the tasks that the Al system will support are defined (e.g., classifiers, generative models, recommenders).	Functional	intersects with	Technologies Implementation Tasks	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	
					Definition		Mechanisms exist to define business processes with consideration for		
		The specific tasks and methods used to implement the tasks that the Al			Business Process		cybersecurity & data privacy that determines: (1) The resulting risk to organizational operations, assets, individuals		
MAP 2.1	N/A	system will support are defined (e.g., classifiers, generative models, recommenders).	Functional	intersects with	Definition	PRM-06	and other organizations; and (2) Information protection needs arising from the defined business	5	
							processes and revises the processes as necessary, until an achievable set of protection needs is obtained. 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		
MAP 2.1	N/A	The specific tasks and methods used to implement the tasks that the Al system will support are defined (e.g., classifiers, generative models,	Functional	intersects with	Product Management	TDA-01.1	Development Life Cycle (SDLC) to: (1) Improve functionality;	5	
		recommenders).					(2) Enhance security and resiliency capabilities; (3) Correct security deficiencies; and		
							<ul> <li>(4) Conform with applicable statutory, regulatory and/or contractual obligations.</li> </ul>		
		Information about the AI system's knowledge limits and how system output may be utilized and overseen by humans is documented.	E		Al & Autonomous Technologies Knowledge		Mechanisms exist to identify and document knowledge limits of Artificial Intelligence (AI) and Autonomous Technologies (AAT) to	40	
MAP 2.2	N/A	Documentation provides sufficient information to assist relevant Al actors when making decisions and taking subsequent actions.	Functional	equal	Limits	AAT-14.2	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	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 &	5	
PIAP 2.5	NVA	selection (e.g., availability, representativeness, suitability), system trustworthiness, and construct validation.	Functionat	Intersects with	ALTEVV TOOLS	AA1-10.2	Verification (AI TEVV) practices.	5	
							Mechanisms exist to conduct specialized assessments for: (1) Statutory, regulatory and contractual compliance obligations;		
							(2) Monitoring capabilities; (3) Mobile devices;		
MAP 2.3	N/A	Scientific integrity and TEVV considerations are identified and documented, including those related to experimental design, data collection and colorities of a semiability concentration and semiality of anterpret	Functional	intersects with	Specialized Assessments	IAO-02.2	(4) Databases; (5) Application security;	5	
		selection (e.g., availability, representativeness, suitability), system trustworthiness, and construct validation.					<ul><li>(6) Embedded technologies (e.g., IoT, OT, etc.);</li><li>(7) Vulnerability management;</li></ul>		
							(8) Malicious code; (9) Insider threats; (10) Participant and testing and (as		
							(10) Performance/load testing; and/or (11) Artificial Intelligence and Autonomous Technologies (AAT). Machanisme avist to establish and desument the context surrounding.		
							Mechanisms exist to establish and document the context surrounding Artificial Intelligence (AI) and Autonomous Technologies (AAT), including:		
MAP 3.0	N/A	Al capabilities, targeted usage, goals, and expected benefits and costs compared with appropriate benchmarks are understood.	Functional	intersects with	AI & Autonomous Technologies Context	AAT-03	(1) Intended purposes; (2) Potentially beneficial uses;	5	
					Definition		<ul> <li>(2) Potentially beneficial uses;</li> <li>(3) Context-specific laws and regulations;</li> <li>(4) Norms and expectations; and</li> </ul>		
					AI & Autonomous		(5) Prospective settings in which the system(s) will be deployed. Mechanisms exist to define and document the organization's mission		
MAP 3.0	N/A	Al capabilities, targeted usage, goals, and expected benefits and costs compared with appropriate benchmarks are understood.	Functional	intersects with		AAT-03.1	and defined goals for Artificial Intelligence (AI) and Autonomous Technologies (AAT).	5	
MAP 3.0	N/A	Al capabilities, targeted usage, goals, and expected benefits and costs compared with appropriate benchmarks are understood.	Functional	intersects with	AI & Autonomous Technologies Business	AAT-04	Mechanisms exist to benchmark capabilities, targeted usage, goals and expected benefits and costs of Artificial Intelligence (AI) and	8	
		compared with appropriate benchmarks are understood. Potential benefits of intended AI system functionality and performance are			Case Al & Autonomous		Autonomous Technologies (AAT). Mechanisms exist to benchmark capabilities, targeted usage, goals		
MAP 3.1	N/A	Potential benefits of intended AI system functionality and performance are examined and documented.	Functional	intersects with	Technologies Business Case	AAT-04	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	AAT-04.1	Mechanisms exist to assess the potential benefits of proposed Artificial Intelligence (AI) and Autonomous Technologies (AAT).	8	
		Potential costs, including non-monetary costs, which result from expected			Benefits Analysis AI & Autonomous		Mechanisms exist to benchmark capabilities, targeted usage, goals		
MAP 3.2	N/A	or realized Al errors or system functionality and trustworthiness – as connected to organizational risk tolerance – are examined and documentations of the system of the	Functional	intersects with	Technologies Business Case	AAT-04	and expected benefits and costs of Artificial Intelligence (AI) and Autonomous Technologies (AAT).	5	
		documented. Potential costs, including non-monetary costs, which result from expected or realized AI errors or system functionality and trustworthiness – as			AI & Autonomous		Mechanisms exist to assess potential costs, including non-monetary		
MAP 3.2	N/A	or reauzed AI errors or system functionality and trustwortniness – as connected to organizational risk tolerance – are examined and documented.	Functional	intersects with	Technologies Potential Costs Analysis	AAT-04.2	costs, resulting from expected or realized Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related errors or system functionality and trustworthiness.	8	
II									

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 durance under the system of th	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	documented. Targeted application scope is specified and documented based on the system's capability, established context, and AI system categorization.	Functional	intersects with	Al & 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	Al & Autonomous Technologies Stakeholder Competencies	AAT-13.1	Mechanisms exist to ensure Artificial Intelligence (A) 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	Al & 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 Al technology and logal 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	Al & Autonomous Technologies Risk Mapping	AAT-02.1	Mechanisms exist to identify Artificial Intelligence (AI) and Autonmous 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	Al & 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 (FIRA)).	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 the team that developed or deployed the AI system, or other data are the team that developed or deployed the AI system, or other data are the team that developed or deployed the AI system.	Functional	intersects with	Al & 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	Identified and documented. Likelihood and magnitude of each identified impact (both potentially beneficial and harmful) based on expected use, past uses of Al systems in similar contexts, public incident reports, feedback from those external to the team that developed or deployed the Al 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, fedback 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 Al 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 Al 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 Al 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 Al & 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 Measuring AI &	GOV-05	Mechanisms exist to develop, report and monitor cybersecurity & data privacy program measures of performance. Mechanisms exist to regularly assess the effectiveness of existing	10	
MEASURE 1.0	N/A	Appropriate methods and metrics are identified and applied.	Functional	intersects with	Autonomous Technologies Effectiveness	AAT-16.2	controls, including reports of errors and potential impacts on affected communities. Mechanisms exist to develop, report and monitor cybersecurity & data	8	
MEASURE 1.1	N/A	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. Approaches and metrics for measurement of AI risks enumerated during	Functional	equal	Measures of Performance Measuring AI &	GOV-05	privacy program measures of performance.	10	
MEASURE 1.1	N/A	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	Autonomous Autonomous Technologies Effectiveness	AAT-16.2	controls, including reports of errors and potential impacts on affected communities.	8	
MEASURE 1.1	N/A	Approaches and metrics for measurement of Al risks enumerated during the MAP function are selected for implementation starting with the most significant Al 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, Al actors external to the team that developed or deployed the Al system, and affected communities are consulted in support of assessments as necessary per organizational risk relevance.	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	Al 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	Al 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	

Version	2025.2	
7.	7/2025	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	Notes (optional)
			Rationale	Relationship			Mechanisms exist to formally assess the cybersecurity & data privacy	(optional)	
			1				controls in systems, applications and services through Information Assurance Program (IAP) activities to determine the extent to which the		
MEASURE 2.0	N/A	Al systems are evaluated for trustworthy characteristics.	Functional	equal	Assessments	IAO-02	controls are implemented correctly, operating as intended and	10	
			i.				producing the desired outcome with respect to meeting expected requirements.		
							Mechanisms exist to perform Information Assurance Program (IAP)		
MEASURE 2.0	N/A	Al systems are evaluated for trustworthy characteristics.	Functional	intersects with	Technical Verification	IAO-06	activities to evaluate the design, implementation and effectiveness of technical cybersecurity & data privacy controls.	5	
		Test sets, metrics, and details about the tools used during TEVV are					Mechanisms exist to document test sets, metrics and details about the		
MEASURE 2.1	N/A	documented.	Functional	equal	AI TEVV Tools	AAT-10.2	tools used during Artificial Intelligence Test, Evaluation, Validation & Verification (AI TEVV) practices.	10	
		Evaluations involving human subjects meet applicable requirements			Artificial Intelligence		Mechanisms exist to implement Artificial Intelligence Test, Evaluation,		
MEASURE 2.2	N/A	(including human subject protection) and are representative of the relevant population.	Functional	intersects with	Test, Evaluation,	AAT-10	Validation & Verification (AI TEVV) practices to enable Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related security,	5	
					Validation & Verification (AI TEVV)		resilience and compliance-related conformity testing throughout the	-	
		Evaluations involving human subjects meet applicable requirements					lifecycle of the AAT. Mechanisms exist to proactively prevent harm by regularly identifying		
MEASURE 2.2	N/A	(including human subject protection) and are representative of the relevant	Functional	equal	AI & Autonomous Technologies Harm	AAT-17	and tracking existing, unanticipated and emergent Artificial Intelligence	10	
		population.			Prevention		(AI) and Autonomous Technologies (AAT)-related risks.		
MEASURE 2.2	N/A	Evaluations involving human subjects meet applicable requirements (including human subject protection) and are representative of the relevant	Functional	equal	AI & Autonomous Technologies Human	AAT-17.1	Mechanisms exist to protect human subjects from harm.	10	
		population.			Subject Protections				
		Al system performance or assurance criteria are measured qualitatively or quantitatively and demonstrated for conditions similar to deployment	i .		AI TEVV Comparable		Mechanisms exist to evaluate Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related performance or the assurance		
MEASURE 2.3	N/A	setting(s). Measures are documented.	Functional	equal	Deployment Settings	AAT-10.12	criteria demonstrated for conditions similar to deployment settings.	10	
		The functionality and behavior of the AI system and its components – as					Mechanisms exist to proactively and continuously monitor deployed		
MEASURE 2.4	N/A	identified in the MAP function – are monitored when in production.	Functional	intersects with	AI TEVV Post-Deployment Monitoring	AAT-10.13	Artificial Intelligence (AI) and Autonomous Technologies (AAT).	5	
		The functionality and behavior of the Al system and its components – as			Al & Autonomous		Mechanisms exist to monitor the functionality and behavior of the		
MEASURE 2.4	N/A	identified in the MAP function – are monitored when in production.	Functional	intersects with	Technologies Production	AAT-16	deployed Artificial Intelligence (AI) and Autonomous Technologies	8	
		The AI system to be deployed is demonstrated to be valid and reliable.		-	Monitoring		(AAT). Mechanisms exist to ensure Artificial Intelligence (AI) and Autonomous		
		Limitations of the generalizability beyond the conditions under which the			Trustworthy AI &		Technologies (AAT) are designed to be reliable, safe, fair, secure,	-	
MEASURE 2.5	N/A	technology was developed are documented.	Functional	intersects with	Autonomous Technologies	AAT-01.2	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	Functional	intersects with	Al & Autonomous Technologies Model	AAT-10.9	Mechanisms exist to validate the Artificial Intelligence (AI) and Autonomous Technologies (AAT) model.	8	
		technology was developed are documented.		<b> </b>	Validation		Mechanisms exist to demonstrate the Astiliaid Intelligence (AD and		
		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		1			Mechanisms exist to demonstrate the Artificial Intelligence (AI) and Autonomous Technologies (AAT) to be deployed are safe, residual risk		
MEASURE 2.6	N/A	residual negative risk does not exceed the risk tolerance, and it can fail safely, particularly if made to operate beyond its knowledge limits. Safety	Functional	intersects with	AI TEVV Safety Demonstration	AAT-10.4	does not exceed the organization's risk tolerance and can fail safely, particularly if made to operate beyond its knowledge limits.	8	
		metrics reflect system reliability and robustness, real-time monitoring, and			Demonstration		particularly in made to operate beyond its knowledge timits.		
		response times for AI system failures. The AI system is evaluated regularly for safety risks – as identified in the					Mechanisms exist to conduct regular assessments of Artificial		
		MAP function. The AI system to be deployed is demonstrated to be safe, its	i.		AI & Autonomous		Intelligence (AI) and Autonomous Technologies (AAT) with independent		
MEASURE 2.6	N/A	residual negative risk does not exceed the risk tolerance, and it can fail safely, particularly if made to operate beyond its knowledge limits. Safety	Functional	intersects with	Technologies Ongoing	AAT-11.2	assessors and stakeholders not involved in the development of the AAT.	5	
		metrics reflect system reliability and robustness, real-time monitoring, and	i.		Assessments				
		response times for AI system failures. The AI system is evaluated regularly for safety risks – as identified in the		-			Mechanisms exist to proactively and continuously monitor deployed		
		MAP function. The AI system to be deployed is demonstrated to be safe, its					Artificial Intelligence (AI) and Autonomous Technologies (AAT).		
MEASURE 2.6	N/A	residual negative risk does not exceed the risk tolerance, and it can fail safely, particularly if made to operate beyond its knowledge limits. Safety	Functional	intersects with	AI TEVV Post-Deployment Monitoring	AAT-10.13		5	
		metrics reflect system reliability and robustness, real-time monitoring, and			_				
		response times for AI system failures. AI system security and resilience – as identified in the MAP function – are			ALTERA/ Security 8		Mechanisms exist to evaluate the security and resilience of Artificial		
MEASURE 2.7	N/A	evaluated and documented.	Functional	equal	AI TEVV Security & Resiliency Assessment	AAT-10.5	Intelligence (AI) and Autonomous Technologies (AAT) to be deployed.	10	
MEASURE 2.7	N/A	Al system security and resilience – as identified in the MAP function – are	Functional	intersects with	Achieving Resilience	SEA-01.2	Mechanisms exist to achieve resilience requirements in normal and	5	
MEASONE 2.7	NVA.	evaluated and documented. Risks associated with transparency and accountability – as identified in	Tunctionat	Intersects with	Requirements AI TEVV Transparency &	3LA-01.2	adverse situations. Mechanisms exist to examine risks associated with transparency and	5	
MEASURE 2.8	N/A	the MAP function – are examined and documented.	Functional	equal	Accountability	AAT-10.6	accountability of Artificial Intelligence (AI) and Autonomous	10	
		The AI model is explained, validated, and documented, and AI system			Assessment AI & Autonomous		Technologies (AAT) to be deployed. Mechanisms exist to validate the Artificial Intelligence (AI) and		
MEASURE 2.9	N/A	output is interpreted within its context - as identified in the MAP function -	Functional	equal	Technologies Model	AAT-10.9	Autonomous Technologies (AAT) model.	10	
		to inform responsible use and governance. Privacy risk of the AI system – as identified in the MAP function – is		-	Validation		Mechanisms exist to examine the data privacy risk of Artificial		
MEASURE 2.10	N/A	examined and documented.	Functional	equal	AI TEVV Privacy Assessment	AAT-10.7	Intelligence (AI) and Autonomous Technologies (AAT) to be deployed.	10	
		Privacy risk of the AI system – as identified in the MAP function – is							
MEASURE 2.10	N/A						Mechanisms exist to conduct a Data Protection Impact Assessment		
		examined and documented.	Functional	intersects with	Data Protection Impact	RSK-10	(DPIA) on systems, applications and services that store, process	8	
			Functional	intersects with	Data Protection Impact Assessment (DPIA)	RSK-10		8	
MEASURE 0.44	N/A	examined and documented. Fairness and bias - as identified in the MAP function - are evaluated and					(DPIA) on systems, applications and services that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks. Mechanisms exist to examine fairness and bias of Artificial Intelligence		
MEASURE 2.11	N/A	examined and documented.	Functional	intersects with equal	Assessment (DPIA)		(DPIA) on systems, applications and services that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks.	8	
		examined and documented. Fairness and bias – as identified in the MAP function – are evaluated and results are documented. Environmental impact and sustainability of AI model training and	Functional		Assessment (DPIA) Al TEVV Fairness & Bias Assessment Al & Autonomous	AAT-10.8	(DPA) on systems, applications and services that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks. Machanisms exist to examine fairness and bias of Artificial Intelligence (A) and Autonomus Technologies (ART) to be deployed. Mechanisms exist to essess and document the environmental impacts	10	
MEASURE 2.11 MEASURE 2.12	N/A N/A	examined and documented. Fairness and bias – as identified in the MAP function – are evaluated and results are documented.			Assessment (DPIA) Al TEVV Fairness & Bias Assessment Al & Autonomous Technologies Environmental Impact &		(DPIA) on systems, applications and services that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-accected risks. Mechanisms exist to examine failmess and bias of Artificial Intelligence (AI) and Autonomous Technologies (AAT) to be deployed.		
		examined and documented. Fairness and bias – as identified in the MAP function – are evaluated and results are documented. Environmental impact and sustainability of AI model training and management activities – as identified in the MAP function – are assessed and documented.	Functional	equal	Assessment (DPIA) AI TEVV Fairness & Bias Assessment AI & Autonomous Technologies	AAT-10.8	(DPA) on systems, applications and services that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks. Mechanisme exist to examine failness and bias of Artificial Intelligence (A) and Autonomous Technologies (AAT) to be deployed. Mechanisms exist to assess and document the environmental impacts and sustainability of Artificial Intelligence (A) and Autonomous Technologies (AAT).	10	
MEASURE 2.12	N/A	examined and documented. Fairness and bias – as identified in the MAP function – are evaluated and results are documented. Environmental impact and sustainability of AI model training and management activities – as identified in the MAP function – are assessed	Functional	equal	Assessment (DPIA) AI TEVV Fairness & Bias Assessment AI & Autonomous Technologies Environmental Impact & Sustainability AI TEVV Results	AAT-10.8	(DPA) on systems, applications and services that store, process and/or transmit Personal Data (PD) to identify and remediate masonably-expected risks. Machanisms exist to examine failness and bias of Artificial Intelligence (A) and Autonomous Technologies (AT) to be deployed. Machanisms exist to assess and document the environmental impacts and sustainability of Artificial Intelligence (AI) and Autonomous Technologies (AT). Machanisms exist to evaluate the results of Artificial Intelligence Test, Evaluation, Validation & Verification (AI TEVV) to determine the viability	10	
		examined and documented. Fairness and bias – as identified in the MAP function – are evaluated and results are documented. Environmental impact and sustainability of AI model training and management activities – as identified in the MAP function – are assessed and documented. Effectiveness of the employed TEVV metrics and processes in the	Functional	equal	Assessment (DPIA) AI TEVV Fairness & Bias Assessment AI & Autonomous Technologies Environmental Impact & Sustainability	AAT-10.8 AAT-17.2	(IDPA) on systems, applications and services that store, process and/or transmit Personal Data (PD) to identify and remediate <u>reasonably-expected risks</u> . Mechanisms exist to examine fairness and bias of Artificial Intelligence (AI) and Autonomous Technologies (AAT) to be deployed. Mechanisms exist to assess and document the environmental impacts and sustainability of Artificial Intelligence (AI) and Autonomous Technologies (AAT). Mechanisms exist to evaluate the results of Artificial Intelligence Test, Evaluation, Validation & Verification (AI TEVV) to determine the viability of the proposed Artificial Intelligence (A) and Autonomous	10	
MEASURE 2.12 MEASURE 2.13	N/A N/A	examined and documented. Fairness and bias – as identified in the MAP function – are evaluated and results are documented. Environmental impact and sustainability of AI model training and management activities – as identified in the MAP function – are assessed and documented. Effectiveness of the employed TEVV metrics and processes in the MEASURE function are evaluated and documented. Effectiveness of the employed TEVV metrics and processes in the	Functional Functional Functional	equal equal intersects with	Assessment (DPIA) AI TEVV Fairness & Bias Assessment AI & Autonomous Technologies Environmental Impact & Sustainability AI TEVV Results Evaluation	AAT-10.8 AAT-17.2 AAT-10.10	(IDPA) on systems, applications and services that store, process and/or transmit Personal Data (PD) to identify and remediate <u>reasonably-expected risks</u> . Mechanisms exist to examine fairness and bias of Artificial Intelligence (AI) and Autonomous Technologies (AAT) to be deployed. Mechanisms exist to assess and document the environmental impacts and sustainability of Artificial Intelligence (A) and Autonomous Technologies (AAT). Mechanisms exist to evaluate the results of Artificial Intelligence Test, Evaluation, Validation & Verification (A) TEVV to determine the vability of the proposed Artificial Intelligence (A) and Autonomous Technologies (AAT).	10 10 8	
MEASURE 2.12	N/A	examined and documented. Fairness and bias – as identified in the MAP function – are evaluated and results are documented. Environmental impact and sustainability of AI model training and management activities – as identified in the MAP function – are assessed and documented. Effectiveness of the employed TEVV metrics and processes in the MEASURE function are evaluated and documented.	Functional	equal	Assessment (DPIA) AI TEVV Fairness & Bias Assessment AI & Autonomous Technologies Environmental Impact & Sustainability AI TEVV Results	AAT-10.8 AAT-17.2	(DPA) on systems, applications and services that store, process and/or transmit Personal Data (PD) to identify and remediate measonably-expected risks. Mechanisms exist to examine failness and bias of Artificial Intelligence (A) and Autonomous Technologies (AAT) to be deployed. Mechanisms exist to assess and document the environmental impacts and sustainability of Artificial Intelligence (AI) and Autonomous Technologies (AAT). 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 (IAT).	10	
MEASURE 2.12 MEASURE 2.13	N/A N/A	examined and documented. Fairness and bias – as identified in the MAP function – are evaluated and results are documented. Environmental impact and sustainability of AI model training and management activities – as identified in the MAP function – are assessed and documented. Effectiveness of the employed TEVV metrics and processes in the MEASURE function are evaluated and documented. Effectiveness of the employed TEVV metrics and processes in the	Functional Functional Functional	equal equal intersects with	Assessment (DPIA) Al TEVV Fairness & Bias Assessment Al & Autonomous Technologies Environmental Impact & Sustainability Al TEVV Results Evaluation Al TEVV Effectiveness Measuring Al &	AAT-10.8 AAT-17.2 AAT-10.10	(DPA) on systems, applications and services that store, process and/or transmit Personal Data (PD) to identify and remediate measonably-expected risks. Machanisms exist to examine failmess and bias of Artificial Intelligence (A) and Autonomous Technologies (AR) to be deployed. Mechanisms exist to essess and document the environmental impacts and sustainability of Artificial Intelligence (AI) and Autonomous Technologies (AR). Machanisms 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 (ART). Machanisms exist to evaluate the effectiveness of the processes utilized to perform Artificial Intelligence Test, Sulation, Validation & Verification (AI TEVV).	10 10 8	
MEASURE 2.12 MEASURE 2.13	N/A N/A	examined and documented. Fairness and bias – as identified in the MAP function – are evaluated and results are documented. Environmental impact and sustainability of AI model training and management activities – as identified in the MAP function – are assessed and documented. Effectiveness of the employed TEVV metrics and processes in the MEASURE function are evaluated and documented. Effectiveness of the employed TEVV metrics and processes in the MEASURE function are evaluated and documented.	Functional Functional Functional	equal equal intersects with	Assessment (DPIA) AI TEVV Fairness & Bias Assessment AI & Autonomous Technologies Environmental Impact & Sustainability AI TEVV Results Evaluation AI TEVV Effectiveness Measuring AI & Autonomous	AAT-10.8 AAT-17.2 AAT-10.10	(IDPA) on systems, applications and services that store, process and/or transmit Personal Data (PD) to identify and remediate <u>reasonably-expected risks</u> . Mechanisms exist to examine fairness and bias of Artificial Intelligence (AI) and Autonomous Technologies (AAT) to be deployed. Mechanisms exist to assess and document the environmental impacts and sustainability of Artificial Intelligence (AI) and Autonomous Technologies (AAT). Mechanisms exist to evaluate the results of Artificial Intelligence Test, Evaluation, Validation & Verification (AI) TeVV to determine the vability of the proposed Artificial Intelligence (AI) and Autonomous Technologies (AAT).	10 10 8	
MEASURE 2.12 MEASURE 2.13 MEASURE 2.13	N/A N/A N/A	examined and documented. Fairness and bias as identified in the MAP function are evaluated and results are documented. Environmental impact and sustainability of AI model training and management activities as identified in the MAP function are assessed and documented. Effectiveness of the employed TEVV metrics and processes in the MEASURE function are evaluated and documented. Effectiveness of the employed TEVV metrics and processes in the MEASURE function are evaluated and documented. Effectiveness of the employed TEVV metrics and processes in the MEASURE function are evaluated and documented. Mechanisms for tracking identified AI risks over time are in place.	Functional Functional Functional Functional	equal equal intersects with equal	Assessment (DPIA) Al TEVV Fairness & Bias Assessment Al & Autonomous Technologies Environmental Impact & Sustainability Al TEVV Results Evaluation Al TEVV Effectiveness Measuring Al &	AAT-10.8 AAT-17.2 AAT-10.10 AAT-10.11	(IDPA) on systems, applications and services that store, process and/or transmit Personal Data (PD) to identify and remediate <u>reasonably-expected rinks</u> . Mechanisms exist to examine fairness and bias of Artificial Intelligence (AI) and Autonomous Technologies (AAT) to be deployed. Mechanisms exist to examine fairness and bias of Artificial Intelligence Technologies (AAT). Mechanisms exist to evaluate the results of Artificial Intelligence Test, Evaluation, Validation (AI) and Autonomous Technologies (AAT). Mechanisms exist to evaluate the results of Artificial Intelligence Test, Evaluation, Validation (AI) and Autonomous Technologies (AAT). Mechanisms exist to evaluate the effectiveness of the processes utilized to perform Artificial Intelligence Test, Evaluation, Validation & Verification (AI TEVV). Mechanisms exist to regularly assess the effectiveness of existing controls, including reports of errors and potential impacts on affected communities.	10 10 8 10	
MEASURE 2.12 MEASURE 2.13 MEASURE 2.13	N/A N/A N/A	examined and documented. Fairness and bias – as identified in the MAP function – are evaluated and results are documented. Environmental impact and sustainability of AI model training and management activities – as identified in the MAP function – are assessed and documented. Effectiveness of the employed TEVV metrics and processes in the MEASURE function are evaluated and documented. Effectiveness of the employed TEVV metrics and processes in the MEASURE function are evaluated and documented.	Functional Functional Functional Functional	equal equal intersects with equal	Assessment (DPIA) AI TEVV Fairness & Bias Assessment AI & Autonomous Technologies Environmental Impact & Sustainability AI TEVV Effectiveness Measuring AI & Autonomous Technologies Effectiveness	AAT-10.8 AAT-17.2 AAT-10.10 AAT-10.11	(IDPA) on systems, applications and services that store, process and/or transmit Personal Data (PD) to identify and remediate <u>reasonably-expected rinks</u> . Michanisms exist to examine fairness and bias of Artificial Intelligence (AI) and Autonomous Technologies (AAT) to be deployed. Mechanisms exist to ease and document the environmental impacts and sustainability of Artificial Intelligence (AI) and Autonomous Technologies (AAT). Mechanisms exist to evaluate the results of Artificial Intelligence Test, Evaluation, Validation eXIII and Intelligence (AI) and Autonomous Technologies (AAT). Mechanisms exist to evaluate the effectiveness of the proceeder of the proposed Artificial Intelligence Test, Evaluation, Validation & Verification (AI TEVV). Mechanisms exist to regulate the effectiveness of the processes utilized to perform Artificial Intelligence Test, Evaluation, Validation & Verification (AI TEVV).	10 10 8 10	
MEASURE 2.12 MEASURE 2.13 MEASURE 2.13	N/A N/A N/A	examined and documented. Fairness and bias as identified in the MAP function are evaluated and results are documented. Environmental impact and sustainability of AI model training and management activities as identified in the MAP function are assessed and documented. Effectiveness of the employed TEVV metrics and processes in the MEASURE function are evaluated and documented. Effectiveness of the employed TEVV metrics and processes in the MEASURE function are evaluated and documented. Effectiveness of the employed TEVV metrics and processes in the MEASURE function are evaluated and documented. Mechanisms for tracking identified AI risks over time are in place.	Functional Functional Functional Functional	equal equal intersects with equal	Assessment (DPIA) AI TEVV Fairness & Bias Assessment AI & Autonomous Technologies Environmental Impact & Sustainability AI TEVV Results Evaluation AI TEVV Effectiveness Measuring AI & Autonomous Technologies	AAT-10.8 AAT-17.2 AAT-10.10 AAT-10.11	(DPA) on systems, applications and services that store, process and/or transmit Bersonal Data (PD) to identify and remediate massnabby-expected rinks. Machanisms exist to examine fairness and bias of Artificial Intelligence (A) and Autonomous Technologies (AR1) to be deployed. Machanisms exist to essess and document the environmental impacts and sustainability of Artificial Intelligence (A) and Autonomous Technologies (AR1). Machanisms exist to evaluate the results of Artificial Intelligence Test, Evaluation, Validation & Verification (A) TEVV to determine the viability of the proposed Artificial Intelligence (A) and Autonomous Technologies (AR1). Machanisms exist to evaluate the feativeness of the processes utilized to perform Artificial Intelligence Test, Evaluation, Validation & Verification (AI TEVV). Machanisms exist to valuate the effectiveness of existing controls, including reports of errors and potential impacts on affected communities.	10 10 8 10	
MEASURE 2.12 MEASURE 2.13 MEASURE 2.13 MEASURE 3.0	N/A N/A N/A	examined and documented. Fairness and bias – as identified in the MAP function – are evaluated and results are documented. Environmental impact and sustainability of AI model training and management activities – as identified in the MAP function – are assessed and documented. Effectiveness of the employed TEVV metrics and processes in the MEASURE function are evaluated and documented. Effectiveness of the employed TEVV metrics and processes in the MEASURE function are evaluated and documented. Effectiveness of the employed TEVV metrics and processes in the MEASURE function are evaluated and documented. Mechanisms for tracking identified AI risks over time are in place. Mechanisms for tracking identified AI risks over time are in place.	Functional Functional Functional Functional Functional	equal equal intersects with equal intersects with	Assessment (DPIA) AI TEVV Fairness & Blas Assessment AI & Autonomous Technologies Environmental Impact & Sustainability AI TEVV Results Evaluation AI TEVV Effectiveness Measuring AI & Autonomous Technologies Effectiveness Plan of Action &	AAT-10.8 AAT-17.2 AAT-10.10 AAT-10.11 AAT-16.2	(DPA) on systems, applications and services that store, process and/or transmit Bersonal Data (PD) to identify and remediate <u>masonably-sepscted risks</u> . Machanisms exist to examine fairness and bias of Artificial Intelligence (A) and Autonomous Technologies (AR1) to be deployed. Machanisms exist to assess and document the environmental impacts and sustainability of Artificial Intelligence (A) and Autonomous Technologies (AR1). Machanisms exist to evaluate the results of Artificial Intelligence Test, Evaluation, Validation & Verification (A) TEVV to determine the viability of the proposed Artificial Intelligence (A) and Autonomous Technologies (AR1). Machanisms exist to evaluate the feativeness of the processes utilized to perform Artificial Intelligence Test, Evaluation, Validation & Verification (AI TEVV). Machanisms exist to valuate the defectiveness of the processes utilized to perform Artificial Intelligence Test, Evaluation, Validation & Verification (AI TEVV). Machanisms exist to regularly assess the effectiveness of existing controls, including reports of errors and potential impacts on affected communities. Machanisms exist to generate a Plan of Action and Milestones (POA&M), or similar risk register, to document planned remedial actions to correct wavenesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known winerabilities.	10 10 8 10 3	
MEASURE 2.12 MEASURE 2.13 MEASURE 2.13 MEASURE 3.0	N/A N/A N/A	examined and documented. Fairness and bias as identified in the MAP function are evaluated and results are documented. Environmental impact and sustainability of AI model training and management activities as identified in the MAP function are assessed and documented. Effectiveness of the employed TEVV metrics and processes in the MEASURE function are evaluated and documented. Effectiveness of the employed TEVV metrics and processes in the MEASURE function are evaluated and documented. Effectiveness of the employed TEVV metrics and processes in the MEASURE function are evaluated and documented. Mechanisms for tracking identified AI risks over time are in place.	Functional Functional Functional Functional Functional	equal equal intersects with equal intersects with	Assessment (DPIA) AI TEVV Fairness & Blas Assessment AI & Autonomous Technologies Environmental Impact & Sustainability AI TEVV Results Evaluation AI TEVV Effectiveness Measuring AI & Autonomous Technologies Effectiveness Plan of Action &	AAT-10.8 AAT-17.2 AAT-10.10 AAT-10.11 AAT-16.2	(DPA) on systems, applications and services that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected rinks. Mechanisms exist to examine fairness and bias of Artificial Intelligence (AI) and Autonomous Technologies (AAT) to be deployed. Mechanisms exist to examine fairness and bias of Artificial Intelligence and sustainability of Artificial Intelligence (AI) and Autonomous Technologies (AAT). Mechanisms exist to evaluate the results of Artificial Intelligence Test, Evaluation, Validation & Verification (AI) TEV/) to determine the valulity of the proposed Artificial Intelligence (AI) and Autonomous Technologies (AAT). Mechanisms exist to evaluate the effectiveness of the processes utilized to perform Artificial Intelligence Test, Evaluation, Validation & Verification (AITEV). Mechanisms exist to regular the effectiveness of the processes utilized to perform Artificial Intelligence Test, Evaluation, Validation & Verification (AITEV). Mechanisms exist to regularly assess the effectiveness of existing controls, Including reports of enrors and potential Impacts on affected communities. Mechanisms exist to generate a Plan of Action and Milestones (POAM), or similar risk register, to document planned remedial actions to correct weaknesses or deficiencies noted during the exessment of the security controls and to reduce or eliminate horow valuerabilities.	10 10 8 10 3	
MEASURE 2.12 MEASURE 2.13 MEASURE 2.13 MEASURE 3.0 MEASURE 3.0	N/A N/A N/A N/A	examined and documented. Fairness and bias – as identified in the MAP function – are evaluated and results are documented. Environmental impact and sustainability of AI model training and management activities – as identified in the MAP function – are assessed and documented. Effectiveness of the employed TEVV metrics and processes in the MEASURE function are evaluated and documented. Effectiveness of the employed TEVV metrics and processes in the MEASURE function are evaluated and documented. Effectiveness of the employed TEVV metrics and processes in the MEASURE function are evaluated and documented. Mechanisms for tracking identified AI risks over time are in place. Mechanisms for tracking identified AI risks over time are in place.	Functional Functional Functional Functional Functional	equal equal intersects with equal intersects with intersects with	Assessment (DPIA) AI TEVV Fairness & Bias Assessment AI & Autonomous Technologies Environmental Impact & Sustainability AI TEVV Effectiveness Measuring AI & Autonomous Technologies Effectiveness Plan of Action & Milestones (POA&M) Risk Register	AAT-10.8 AAT-17.2 AAT-10.10 AAT-10.11 AAT-16.2 IAO-05	(DPA) on systems, applications and services that store, process and/or transmit Bersonal Data (PD) to identify and remediate <u>masonably-sepscted risks</u> . Machanisms exist to examine fairness and bias of Artificial Intelligence (A) and Autonomous Technologies (AR1) to be deployed. Machanisms exist to assess and document the environmental impacts and sustainability of Artificial Intelligence (A) and Autonomous Technologies (AR1). Machanisms exist to evaluate the results of Artificial Intelligence Test, Evaluation, Validation & Verification (A) TEVV to determine the viability of the proposed Artificial Intelligence (A) and Autonomous Technologies (AR1). Machanisms exist to evaluate the feativeness of the processes utilized to perform Artificial Intelligence Test, Evaluation, Validation & Verification (AI TEVV). Machanisms exist to valuate the feativeness of the processes utilized to perform Artificial Intelligence Test, Evaluation, Validation & Verification (AI TEVV). Machanisms exist to regularly assess the effectiveness of existing controls, including reports of errors and potential impacts on affected communities.	10 10 8 10 3 5	
MEASURE 2.12 MEASURE 2.13 MEASURE 2.13 MEASURE 3.0 MEASURE 3.0	N/A N/A N/A N/A	examined and documented. Fairness and bias – as identified in the MAP function – are evaluated and results are documented. Environmental impact and sustainability of AI model training and management activities – as identified in the MAP function – are assessed and documented. Effectiveness of the employed TEVV metrics and processes in the MEASURE function are evaluated and documented. Effectiveness of the employed TEVV metrics and processes in the MEASURE function are evaluated and documented. Effectiveness of the employed TEVV metrics and processes in the MEASURE function are evaluated and documented. Mechanisms for tracking identified AI risks over time are in place. Mechanisms for tracking identified AI risks over time are in place. Approaches, parsonnel, and documentation are in place to regularly identify and track existing, unanticipated, and emergent AI risks based on	Functional Functional Functional Functional Functional	equal equal intersects with equal intersects with intersects with	Assessment (DPIA) AI TEVV Fairness & Bias Assessment AI & Autonomous Technologies Environmental Impact & Sustainability AI TEVV Effectiveness Measuring AI & Autonomous Technologies Effectiveness Plan of Action & Milestones (POA&M) Risk Register AI & Autonomous Technologies Harm	AAT-10.8 AAT-17.2 AAT-10.10 AAT-10.11 AAT-16.2 IAO-05	(IDPA) on systems, applications and services that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected riaks. Mechanisms exist to examine fairness and bias of Artificial Intelligence (A) and Autonomous Technologies (AAT) to be deployed. Mechanisms exist to easess and document the environmental impacts and sustainability of Artificial Intelligence (AI) and Autonomous Technologies (AAT). 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). Mechanisms exist to evaluate the effectiveness of the processes utilized to perform Artificial Intelligence Test, Evaluation, Validation & Verification (AI TEVV). Mechanisms exist to regularly assess the effectiveness of a siting controls, including reports of errors and potential impacts on affected communities. 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 untensismisms exist to maintain a risk register that facilitates monitoring and reporting of risko.	10 10 8 10 3 5	
MEASURE 2.12 MEASURE 2.13 MEASURE 2.13 MEASURE 3.0 MEASURE 3.0 MEASURE 3.0	N/A N/A N/A N/A N/A	examined and documented. Fairness and bias – as identified in the MAP function – are evaluated and results are documented. Environmental impact and sustainability of AI model training and management activities – as identified in the MAP function – are assessed and documented. Effectiveness of the employed TEVV metrics and processes in the MEASURE function are evaluated and documented. Effectiveness of the employed TEVV metrics and processes in the MEASURE function are evaluated and documented. Effectiveness of the employed TEVV metrics and processes in the MEASURE function are evaluated and documented. Mechanisms for tracking identified AI risks over time are in place. Mechanisms for tracking identified AI risks over time are in place. Approaches, parsonnel, 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 Functional Functional Functional Functional Functional	equal equal intersects with equal intersects with equal	Assessment (DPIA) Al TEVV Fairness & Bias Assessment Al & Autonomous Technologies Environmental Impact & Sustainability Al TEVV Effectiveness Measuring Al & Autonomous Technologies Effectiveness Plan of Action & Milestones (POA&M) Risk Register Al & Autonomous	AAT-10.8 AAT-17.2 AAT-10.10 AAT-10.11 AAT-16.2 IAO-05 RSK-04.1	(IDPA) on systems, applications and services that store, process and/or transmit Personal Data (PD) to identify and remediate <u>reasonably-expected risks</u> . Mechanisms exist to examine fairness and bias of Artificial Intelligence (A) and Autonomous Technologies (AAT) to be deployed. Mechanisms exist to examine fairness and bias of Artificial Intelligence (A) and Autonomous Technologies (AAT) to be deployed. Mechanisms exist to exaluate the results of Artificial Intelligence Test, Technologies (AAT). Mechanisms exist to evaluate the results of Artificial Intelligence Test, Evaluation, Validation & Verification (A) TEVV to determine the viability of the proposed Artificial Intelligence (A) and Autonomous Technologies (AAT). Mechanisms exist to evaluate the effectiveness of the processes utilized to perform Artificial Intelligence Test, Evaluation, Validiation & Verification (AI TEVV). Mechanisms exist to regularly assess the effectiveness of a sifting controls, including reports of errors and potential impacts on affected communities. Mechanisms exist to generate a Plan of Action and Milestones (POA&M), or similar risk register, to document planned remedial assessment of the security controls and to reduce or eliminate known untenabilities. Mechanisms exist to maintain a risk register that facilitates monitoring and reporting of risko.	10 10 8 10 3 5 5 10	
MEASURE 2.12 MEASURE 2.13 MEASURE 2.13 MEASURE 3.0 MEASURE 3.0 MEASURE 3.0	N/A N/A N/A N/A N/A	examined and documented. Fairness and bias – as identified in the MAP function – are evaluated and results are documented. Environmental impact and sustainability of AI model training and management activities – as identified in the MAP function – are evaluated and documented. Effectiveness of the employed TEVV metrics and processes in the MEASURE function are evaluated and documented. Effectiveness of the employed TEVV metrics and processes in the MEASURE function are evaluated and documented. Effectiveness of the employed TEVV metrics and processes in the MEASURE function are evaluated and documented.  Effectiveness of the employed TEVV metrics and processes in the MEASURE function are evaluated and documented.  Mechanisms for tracking identified AI risks over time are in place.  Mechanisms for tracking identified AI risks over time are in place.  Approaches, personnel, and documentation are in place to regularly identify and track existing, unanticipated, and emergent AI risks based on Approaches, personnel, and documentation are in place to regularly	Functional Functional Functional Functional Functional Functional	equal equal intersects with equal intersects with equal	Assessment (DPIA) AI TEVV Fairness & Bias Assessment AI & Autonomous Technologies Environmental Impact & Sustainability AI TEVV Effectiveness Measuring AI & Autonomous Technologies Effectiveness Plan of Action & Milestones (POA&M) Risk Register AI & Autonomous Technologies Harm	AAT-10.8 AAT-17.2 AAT-10.10 AAT-10.11 AAT-16.2 IAO-05 RSK-04.1	(DPA) on systems, applications and services that store, process and/or transmit Personal Data (P) to identify and remediate trassonably-expected rinks. Mechanisms exist to examine fairness and bias of Artificial Intelligence (AI) and Autonomous Technologies (AAT) to be deployed. Mechanisms exist to examine fairness and bias of Artificial Intelligence and sustainability of Artificial Intelligence (AI) and Autonomous Technologies (AAT). Mechanisms exist to evaluate the results of Artificial Intelligence Test, Evaluation, Validation & Verification (AI) and Autonomous Technologies (AAT). Mechanisms exist to evaluate the results of Artificial Intelligence Test, Evaluation, Validation & Verification (AI) and Autonomous Technologies (AAT). Mechanisms exist to evaluate the effectiveness of the processes utilized to perform Artificial Intelligence Test, Evaluation, Validation & Verification (AIT EVV). Mechanisms exist to regularly assess the effectiveness of existing controls, including reports of errors and potential Impacts on affected communities. Mechanisms exist to generate a Plan of Action and Milestones (POAM), or similar risk register, to document planned remedial actions to correct weaknesses or deficiencies noted during the exessment of the security controls and to reduce or eliminate horvan unsersbillities. Mechanisms exist to proactively prevent harm by regularly identifying and tractum a ternologies (AAT)-related trificial Intelligence (AI) and Autonomus Technologies (AT)-related trificial Intelligence (AI) and Autonomus Technologies	10 10 8 10 3 5 5 10	
MEASURE 2.12 MEASURE 2.13 MEASURE 2.13 MEASURE 3.0 MEASURE 3.0 MEASURE 3.0	N/A N/A N/A N/A N/A	examined and documented. Fairness and bias – as identified in the MAP function – are evaluated and results are documented. Environmental impact and sustainability of AI model training and management activities – as identified in the MAP function – are assessed and documented. Effectiveness of the employed TEVV metrics and processes in the MEASURE function are evaluated and documented. Effectiveness of the employed TEVV metrics and processes in the MEASURE function are evaluated and documented. Effectiveness of the employed TEVV metrics and processes in the MEASURE function are evaluated and documented. Mechanisms for tracking identified AI risks over time are in place. Mechanisms for tracking identified AI risks over time are in place. Approaches, parsonnel, 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 Functional Functional Functional Functional Functional	equal equal intersects with equal intersects with equal	Assessment (DPIA) AI TEVV Fairness & Bias Assessment AI & Autonomous Technologies Environmental Impact & Sustainability AI TEVV Effectiveness Measuring AI & Autonomous Technologies Effectiveness Plan of Action & Milestones (POA&M) Risk Register AI & Autonomous Technologies Harm	AAT-10.8 AAT-17.2 AAT-10.10 AAT-10.11 AAT-16.2 IAO-05 RSK-04.1	(DPA) on systems, applications and services that store, process and/or transmit Personal Data (P) to identify and remediate reasonably-expected rinks. Mechanisms exist to examine fairness and bias of Artificial Intelligence (AI) and Autonomous Technologies (AAT) to be deployed. Mechanisms exist to examine fairness and bias of Artificial Intelligence and sustainability of Artificial Intelligence (AI) and Autonomous Technologies (AAT). Mechanisms exist to evaluate the results of Artificial Intelligence Test, Evaluation, Validation & Verification (AI) and Autonomous Technologies (AAT). Mechanisms exist to evaluate the results of Artificial Intelligence Test, Evaluation, Validation & Verification (AI) and Autonomous Technologies (AAT). Mechanisms exist to evaluate the effectiveness of the processes utilized to perform Artificial Intelligence Test, Evaluation, Validation & Verification (AIT EVV). Mechanisms exist to regularly assess the effectiveness of existing controls, including reports of errors and potential Impacts and controls, including reports of errors and potential Impacts on affected communities. Mechanisms exist to generate a Plan of Action and Milestones (POAM), or similar risk register, to document planned remedial actions to correct weaknesses or deficiencies noted during the exessment of the socurity controls and to reduce or eliminate horvor unsersebilities. Mechanisms exist to proactively prevent harm by regularly identifying and trackning exist to proactively prevent harm by regularly identifying and trackning exist to proactively prevent harm by regularly identifying and tracking exist to proactively prevent harm by regularly identifying and tracking exist to conduct specialized assessment for: (1) Statutory, regulatory and contractual compliance obligations; (2) Montoring capabilities;	10 10 8 10 3 5 5 10	
MEASURE 2.12 MEASURE 2.13 MEASURE 2.13 MEASURE 3.0 MEASURE 3.0 MEASURE 3.0	N/A N/A N/A N/A N/A	examined and documented. Fairness and bias – as identified in the MAP function – are evaluated and results are documented. Environmental impact and sustainability of AI model training and management activities – as identified in the MAP function – are assessed and documented. Effectiveness of the employed TEVV metrics and processes in the MEASURE function are evaluated and documented. Effectiveness of the employed TEVV metrics and processes in the MEASURE function are evaluated and documented. Effectiveness of the employed TEVV metrics and processes in the MEASURE function are evaluated and documented. Effectiveness of the employed TEVV metrics and processes in the MEASURE function are evaluated and documented. Mechanisms for tracking identified AI risks over time are in place. Mechanisms for tracking identified AI risks over time are in place. Approaches, personnel, and documentation are in place to regularly identify and track skiting, unanticipated, and emergent AI risks based on factors such as intended and actual performance in deployed contexts. Approaches, personnel, and documentation are in place to regularly identify and track skiting, unanticipated, and emergent AI risks based on factors such as intended and actual performance in deployed contexts.	Functional Functional Functional Functional Functional Functional	equal equal intersects with equal intersects with equal	Assessment (DPIA) AI TEVV Fairness & Bias Assessment AI & Autonomous Technologies Environmental Impact & Sustainability AI TEVV Effectiveness Measuring AI & Autonomous Technologies Effectiveness Plan of Action & Milestones (POA&M) Risk Register AI & Autonomous Technologies Harm	AAT-10.8 AAT-17.2 AAT-10.10 AAT-10.11 AAT-16.2 IAO-05 RSK-04.1	(IDPA) on systems, applications and services that store, process and/or transmit Personal Data (PD) to identify and remediate <u>reasonably-expected risks</u> . Mechanisms exist to examine fairness and bias of Artificial Intelligence (AI) and Autonomous Technologies (AAT) to be deployed. Mechanisms exist to exastess and document the environmental impacts and sustainability of Artificial Intelligence (AI) and Autonomous Technologies (AAT). 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). Mechanisms exist to evaluate the effectiveness of the proceed Artificial Intelligence Test, Evaluation, Validation & Verification (AI) TEVV to determine the viability of the proposed Artificial Intelligence Test, Evaluation, Validation & Verification (AI TEVV). Mechanisms exist to evaluate the effectiveness of the proceeds controls, including reports of errors and potential impacts on affected communities. Mechanisms exist to generate a Plan of Action and Milestones (POAM), or similar risk register, to document planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the eacurity controls and to reduce or eliminate known valmerabilities. Mechanisms exist to maintain a risk register that facilitates monitoring and rucking existito proceed and emergent Artificial Intelligence (A) and Autonomous Technologies (AAT)-related risks. Mechanisms exist to conduct specialized assessment of for: (1) Statutory, register on altificial reliations exister (2) Mohile devices;	10 10 8 10 3 5 5 10	
MEASURE 2.12 MEASURE 2.13 MEASURE 2.13 MEASURE 3.0 MEASURE 3.0 MEASURE 3.1	N/A N/A N/A N/A N/A N/A	examined and documented. Fairness and bias – as identified in the MAP function – are evaluated and results are documented. Environmental impact and sustainability of AI model training and management activities – as identified in the MAP function – are assessed and documented. Effectiveness of the employed TEVV metrics and processes in the MEASURE function are evaluated and documented. Effectiveness of the employed TEVV metrics and processes in the MEASURE function are evaluated and documented. Effectiveness of the employed TEVV metrics and processes in the MEASURE function are evaluated and documented. Effectiveness of the employed TEVV metrics and processes in the MEASURE function are evaluated and documented. Mechanisms for tracking identified AI risks over time are in place. Mechanisms for tracking identified AI risks over time are in place. Approaches, personnel, and documentation are in place to regularly identify and track skiting, unanticipated, and emergent AI risks based on factors such as intended and actual performance in deployed contexts. Approaches, personnel, and documentation are in place to regularly identify and track skiting, unanticipated, and emergent AI risks based on factors such as intended and actual performance in deployed contexts.	Functional Functional Functional Functional Functional Functional Functional Functional Functional	equal equal intersects with intersects with intersects with equal equal	Assessment (DPIA) Al TEVV Fairness & Bias Assessment Al & Autonomous Technologies Environmental Impact & Sustainability Al TEVV Effectiveness Measuring Al & Autonomous Technologies Effectiveness Plan of Action & Milestones (POA&M) Risk Register Al & Autonomous Technologies Harm Prevention	AAT-10.8 AAT-17.2 AAT-10.10 AAT-10.11 AAT-16.2 IAO-05 RSK-04.1 AAT-17	(DPA) on systems, applications and services that store, process and/or transmit Personal Data (PD) to identify and remediate <u>reasonably-expected risks</u> . Mechanisms exist to examine fairness and bias of Artificial Intelligence (AI) and Autonomous Technologies (AAT) to be deployed. Mechanisms exist to exastess and document the environmental impacts and sustainability of Artificial Intelligence (AI) and Autonomous Technologies (AAT). Mechanisms exist to evaluate the results of Artificial Intelligence Test, Evaluation, Validation & Verification (AI) TeVV to determine the viability of the proposed Artificial Intelligence Test, Evaluation, Validation & Verification (AI) Mechanisms exist to evaluate the effectiveness of the proceeds to evaluate the proposed Artificial Intelligence Test, Evaluation, Validation & Verification (AI TEVV). Mechanisms exist to regularly assess the effectiveness of existing controls, including reports of errors and potential impacts on affected communities. Mechanisms exist to generate a Plan of Action and Milestones (POAM), or similar risk register, to document planned remedial actions to correct weaknesses or deficiencies noted during the sessessment of the security controls and to reduce or eliminate known valorstabilities. Mechanisms exist to proactively prevent harm by regularly identifying and racing equilatory and contructual compliance obligations; (1) Statutory, regulatory and contructual compliance obligations; (2) Mohile devices; (4) Databases; (5) Application security;	10 10 8 10 3 5 10 10 10	
MEASURE 2.12 MEASURE 2.13 MEASURE 2.13 MEASURE 3.0 MEASURE 3.0 MEASURE 3.0	N/A N/A N/A N/A N/A	examined and documented. Fairness and bias – as identified in the MAP function – are evaluated and results are documented. Environmental impact and sustainability of AI model training and management activities – as identified in the MAP function – are assessed and documented. Effectiveness of the employed TEVV metrics and processes in the MEASURE function are evaluated and documented. Effectiveness of the employed TEVV metrics and processes in the MEASURE function are evaluated and documented. Effectiveness of the employed TEVV metrics and processes in the MEASURE function are evaluated and documented. Effectiveness of the employed TEVV metrics and processes in the MEASURE function are evaluated and documented. Mechanisms for tracking identified AI risks over time are in place. Mechanisms for tracking identified AI risks over time are in place. Approaches, personnel, and documentation are in place to regularly identify and track skiting, unanticipated, and emergent AI risks based on factors such as intended and actual performance in deployed contexts. Approaches, personnel, and documentation are in place to regularly identify and track skiting, unanticipated, and emergent AI risks based on factors such as intended and actual performance in deployed contexts.	Functional Functional Functional Functional Functional Functional	equal equal intersects with intersects with intersects with equal equal	Assessment (DPIA) AI TEVV Fairness & Bias Assessment AI & Autonomous Technologies Environmental Impact & Sustainability AI TEVV Effectiveness Measuring AI & Autonomous Technologies Effectiveness Plan of Action & Milestones (POA&M) Risk Register AI & Autonomous Technologies Harm	AAT-10.8 AAT-17.2 AAT-10.10 AAT-10.11 AAT-16.2 IAO-05 RSK-04.1 AAT-17	(DPA) on systems, applications and services that store, process and/or transmit Personal Data (PD) to identify and remediate <u>masonably-expected risks</u> . Mechanisms exist to examine fairness and bias of Artificial Intelligence (A) and Autonomous Technologies (AAT) to be deployed. Mechanisms exist to examine fairness and bias of Artificial Intelligence (A) and Autonomous Technologies (AAT) to be deployed. Mechanisms exist to examine fairness and bias of Artificial Intelligence Test, Erchnologies (AAT). Mechanisms exist to evaluate the results of Artificial Intelligence Test, Evaluation, Validation & Verification (A) TEVV to determine the viability of the proposed Artificial Intelligence (A) and Autonomous Technologies (AAT). Mechanisms exist to evaluate the effectiveness of the processes utilized to perform Artificial Intelligence Test, Evaluation, Validation & Verification (AI TEVV). Mechanisms exist to equalute the effectiveness of desisting controls, including reports of errors and potential impacts on affected communities. Mechanisms exist to generate a Plan of Action and Milestones (POA&M), or similar risk register, to document planned remedial actions to correct wakenesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities. Mechanisms exist to maintain a risk register that facilitates monitoring and reporting of risks. Mechanisms exist to conduct specialized assessments for: (1) Statutory, regulatory and contractual compliance obligations; (2) Monitoring capabilities; (3) Applications security; (4) Databases; (5) Applications security;	10 10 8 10 3 5 5 10	
MEASURE 2.12 MEASURE 2.13 MEASURE 2.13 MEASURE 3.0 MEASURE 3.0 MEASURE 3.1	N/A N/A N/A N/A N/A N/A	examined and documented. Fairness and bias – as identified in the MAP function – are evaluated and results are documented. Environmental impact and sustainability of AI model training and management activities – as identified in the MAP function – are assessed and documented. Effectiveness of the employed TEVV metrics and processes in the MEASURE function are evaluated and documented. Effectiveness of the employed TEVV metrics and processes in the MEASURE function are evaluated and documented. Effectiveness of the employed TEVV metrics and processes in the MEASURE function are evaluated and documented. Effectiveness of the employed TEVV metrics and processes in the MEASURE function are evaluated and documented. Mechanisms for tracking identified AI risks over time are in place. Mechanisms for tracking identified AI risks over time are in place. Approaches, personnel, and documentation are in place to regularly identify and track skiting, unanticipated, and emergent AI risks based on factors such as intended and actual performance in deployed contexts. Approaches, personnel, and documentation are in place to regularly identify and track skiting, unanticipated, and emergent AI risks based on factors such as intended and actual performance in deployed contexts.	Functional Functional Functional Functional Functional Functional Functional Functional Functional	equal equal intersects with intersects with intersects with equal equal	Assessment (DPIA) Al TEVV Fairness & Bias Assessment Al & Autonomous Technologies Environmental Impact & Sustainability Al TEVV Effectiveness Measuring Al & Autonomous Technologies Effectiveness Plan of Action & Milestones (POA&M) Risk Register Al & Autonomous Technologies Harm Prevention	AAT-10.8 AAT-17.2 AAT-10.10 AAT-10.11 AAT-16.2 IAO-05 RSK-04.1 AAT-17	(DPA) on systems, applications and services that store, process and/or transmit Personal Data (PD) to identify and remediate masonabby-expected rinks. Mechanisms exist to examine fairness and bias of Artificial Intelligence (A) and Autonomous Technologies (AAT) to be deployed. Mechanisms exist to examine fairness and bias of Artificial Intelligence (A) and Autonomous Technologies (AAT) to be deployed. Mechanisms exist to exaluate the results of Artificial Intelligence Test, Erchnologies (AAT). Mechanisms exist to evaluate the results of Artificial Intelligence Test, Evaluation, Validation & Verification (A) TEVV to determine the viability of the proposed Artificial Intelligence (A) and Autonomous Technologies (AAT). Mechanisms exist to evaluate the effectiveness of the processes utilized to perform Artificial Intelligence Test, Evaluation, Validation & Verification (AI TEVV). Mechanisms exist to regularly assess the effectiveness of existing controls, including reports of errors and potential impacts on affected communities. Mechanisms exist to generate a Plan of Action and Milestones (POA&M), or similar risk register, to document planned remedial actions to correct wakenesses or deficiencies noted funding the assessment of the security controls and to reduce or eliminate known vulnerabilities, unanticipated and emergent Artifical Intelligence (AI) and Autonomous Technologies (AAT)-related risks. Mechanisms exist to conduct specialized assessments for: (1) Statutory, regulatory and contractual compliance obligations; (2) Monitoring capabilities; (3) Application security; (4) Autoneability management; (5) Application security; (5) Embeddet technologies (a.g., IoT, OT, etc.); (7) Vulnerability management;	10 10 8 10 3 5 10 10 10	
MEASURE 2.12 MEASURE 2.13 MEASURE 2.13 MEASURE 3.0 MEASURE 3.0 MEASURE 3.1	N/A N/A N/A N/A N/A N/A	examined and documented. Fairness and bias – as identified in the MAP function – are evaluated and results are documented. Environmental impact and sustainability of AI model training and management activities – as identified in the MAP function – are assessed and documented. Effectiveness of the employed TEVV metrics and processes in the MEASURE function are evaluated and documented. Effectiveness of the employed TEVV metrics and processes in the MEASURE function are evaluated and documented. Effectiveness of the employed TEVV metrics and processes in the MEASURE function are evaluated and documented. Effectiveness of the employed TEVV metrics and processes in the MEASURE function are evaluated and documented. Mechanisms for tracking identified AI risks over time are in place. Mechanisms for tracking identified AI risks over time are in place. Approaches, personnel, and documentation are in place to regularly identify and track skiting, unanticipated, and emergent AI risks based on factors such as intended and actual performance in deployed contexts. Approaches, personnel, and documentation are in place to regularly identify and track skiting, unanticipated, and emergent AI risks based on factors such as intended and actual performance in deployed contexts.	Functional Functional Functional Functional Functional Functional Functional Functional Functional	equal equal intersects with intersects with intersects with equal equal	Assessment (DPIA) Al TEVV Fairness & Bias Assessment Al & Autonomous Technologies Environmental Impact & Sustainability Al TEVV Effectiveness Measuring Al & Autonomous Technologies Effectiveness Plan of Action & Milestones (POA&M) Risk Register Al & Autonomous Technologies Harm Prevention	AAT-10.8 AAT-17.2 AAT-10.10 AAT-10.11 AAT-16.2 IAO-05 RSK-04.1 AAT-17	(IDPA) on systems, applications and services that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks. Mechanisms exist to examine fairness and bias of Artificial Intelligence (AI) and Autonomous Technologies (AAT) to be deployed. Mechanisms exist to examine fairness and bias of Artificial Intelligence Technologies (AAT). Mechanisms exist to evaluate the results of Artificial Intelligence Test, Evaluation, Validation 4(AT). Mechanisms exist to evaluate the results of Artificial Intelligence Test, Evaluation, Validation 4(AT). Mechanisms exist to evaluate the effectiveness of the proceeder attribution and the effectiveness of the processes utilized to perform Artificial Intelligence Test, Evaluation, Validation 5 Verification (AT EVV). Mechanisms exist to evaluate the effectiveness of the processes utilized to perform Artificial Intelligence Test, Evaluation, Validation 6 Verification (AT EVV). Mechanisms exist to regularly assess the effectiveness of existing controls, including reports of errors and potential impacts on affected communities. Mechanisms exist to generate a Plan of Action and Milestones (POAM), or similar risk register, to document planned remedial actions to correct weaknesses or deficiencies noted during the seasesment of the security controls and to reduce or eliminate known vulnerabilities. (A) and Autonomous Technologies (AAT)-related risks. Mechanisms exist to conduct specialized assessments for: (1) Statutory, regulatory and contructual compliance obligations; (2) Mohiel devices; (3) Applications security; (6) Embedded technologies (e.g., IoT, OT, etc.); (7) Vulnerability management; (6) Mailcous code; (6) Inside torsocode; (6) Inside torsocode; (7) Inside torsocode; (7) Inside torsocode; (8) Antiones and the set is torsocode; (8) Antiones and the set is torsocode; (8) Antiones and the se	10 10 8 10 3 5 10 10 10	
MEASURE 2.12 MEASURE 2.13 MEASURE 2.13 MEASURE 3.0 MEASURE 3.0 MEASURE 3.1	N/A N/A N/A N/A N/A N/A	examined and documented. Fairness and bias - as identified in the MAP function - are evaluated and results are documented. Environmental impact and sustainability of AI model training and management activities - as identified in the MAP function - are evaluated and documented. Effectiveness of the employed TEVV metrics and processes in the MEASURE function are evaluated and documented. Effectiveness of the employed TEVV metrics and processes in the MEASURE function are evaluated and documented. Effectiveness of the employed TEVV metrics and processes in the MEASURE function are evaluated and documented. Effectiveness of the employed TEVV metrics and processes in the MEASURE function are evaluated and documented. Mechanisms for tracking identified AI risks over time are in place. 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 Functional Functional Functional Functional Functional Functional Functional Functional	equal equal intersects with intersects with intersects with equal equal	Assessment (DPIA) Al TEVV Fairness & Bias Assessment Al & Autonomous Technologies Environmental Impact & Sustainability Al TEVV Effectiveness Measuring Al & Autonomous Technologies Effectiveness Plan of Action & Milestones (POA&M) Risk Register Al & Autonomous Technologies Harm Prevention	AAT-10.8 AAT-17.2 AAT-10.10 AAT-10.11 AAT-16.2 IAO-05 RSK-04.1 AAT-17	(IDPA) on systems, applications and services that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks. Mechanisms exist to examine fairness and bias of Artificial Intelligence (AI) and Autonomous Technologies (AAT) to be deployed. Mechanisms exist to examine fairness and bias of Artificial Intelligence Technologies (AAT). Mechanisms exist to evaluate the results of Artificial Intelligence Test, Evaluation, Validation (AI). Mechanisms exist to evaluate the results of Artificial Intelligence Test, Evaluation, Validation (AI). Mechanisms exist to evaluate the effectiveness of the proceeds of the proposed Artificial Intelligence Test, Evaluation, Validation & Verification (AITEV). Mechanisms exist to evaluate the effectiveness of the processes utilized to perform Artificial Intelligence Test, Evaluation, Validation & Verification (AITEV). Mechanisms exist to evaluate the effectiveness of existing controls, including reports of errors and potential impacts on affected communities. Mechanisms exist to generate a Plan of Action and Milestones (POAM), or similar risk register, to document planned remedial actions to correct weaknesses or deficiencies noted during the seasesment of the security controls and to reduce or eliminate known valuenzabilities. (A) and Autonomous Technologies (AAT)-related risks. Mechanisms exist to conduct specialized assessments for: (1) Statutory, regulatory and contructual compliance obligations; (2) Mohile durone; (3) Abbile durone; (4) Databases; (5) Application security; (6) Embedded technologies (AAT)-related risks. (1) Mohile durone; (1) Artificial Intelligence and; (3) Mohile durone; (4) Patribases; (3) Mohile durone; (4) Patribases; (4) Patribases; (5) Application security; (6) Embedded technologies (AAT)-related risks.	10 10 8 10 3 5 10 10 10	
MEASURE 2.12 MEASURE 2.13 MEASURE 2.13 MEASURE 3.0 MEASURE 3.0 MEASURE 3.1	N/A N/A N/A N/A N/A N/A	examined and documented. Fairness and bias – as identified in the MAP function – are evaluated and results are documented. Environmental impact and sustainability of AI model training and management activities – as identified in the MAP function – are assessed and documented. Effectiveness of the employed TEVV metrics and processes in the MEASURE function are evaluated and documented. Effectiveness of the employed TEVV metrics and processes in the MEASURE function are evaluated and documented. Effectiveness of the employed TEVV metrics and processes in the MEASURE function are evaluated and documented. Mechanisms for tracking identified AI risks over time are in place. Mechanisms for tracking identified AI risks over time are in place. Approaches, personnel, and documentation are in place to regularly identity and track existing, unanticipated, and emergent AI risks based on factors such as intended and actual performance in deployed contexts. Approaches, personnel, and documentation are in place to regularly identity and track existing, unanticipated, and emergent AI risks based on factors such as intended and actual performance in deployed contexts. Approaches, personnel, and documentation are in place to regularly identity and track existing, unanticipated, and emergent AI risks based on factors such as intended and actual performance in deployed contexts. Approaches, personnel, and documentation are in place to regularly identity and track existing.	Functional Functional Functional Functional Functional Functional Functional Functional Functional	equal equal intersects with intersects with intersects with equal equal	Assessment (DPIA) Al TEVV Fairness & Bias Assessment I als Autonomous Technologies Environmental impact & Sustainability Al TEVV Effectiveness Measuring Al & Autonomous Technologies Effectiveness Plan of Action & Milestones (POA&M) Risk Register Al & Autonomous Technologies Harm Prevention Specialized Assessments	AAT-10.8 AAT-17.2 AAT-10.10 AAT-10.11 AAT-16.2 IAO-05 RSK-04.1 AAT-17	(DPA) on systems, applications and services that store, process and/or transmit Personal Data (PD) to identify and remediate masonabby-expected rinks. Mechanisms exist to examine fairness and bias of Artificial Intelligence (A) and Autonomous Technologies (AAT) to be deployed. Mechanisms exist to examine fairness and bias of Artificial Intelligence (A) and Autonomous Technologies (AAT) to be deployed. Mechanisms exist to exaluate the results of Artificial Intelligence Test, Exclusion, Validation & Verification (A) TEVV to determine the viability of the proposed Artificial Intelligence (A) and Autonomous Technologies (AAT). Mechanisms exist to evaluate the results of Artificial Intelligence Test, Evaluation, Validation & Verification (A) TEVV to determine the viability of the proposed Artificial Intelligence (A) and Autonomous Technologies (AAT). Mechanisms exist to evaluate the effectiveness of the proceeds utilized to perform Artificial Intelligence Test, Evaluation, Validation & Verification (A) TEVV). Mechanisms exist to regulate the effectiveness of existing controls, including reports of errors and potential impacts on affected communities. 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 dification is outrig mechanisms exist to maintain a risk register that facilitates monoting and reporting or risks. Mechanisms exist to contact specialized and emergent Artifica Intelligence (A) and Autonomous Technologies (AAT)-related risks. Mechanisms exist to conduct specialized and emergent Artifica Intelligence (A) and autonomous Technologies (AAT)-related risks. Mechanisms exist to generate 1 and Autonomous Technologies (AAT). () Mechanisms exist to generate 1 and Autonomous Technologies (AAT). () Mechanisms exist to generate 1 and Autonomous Technologies (AAT). () Mechanisms exist to generate 1 and Autonomous Technologies (AAT). () Mechanisme to togenet to generate 1 and Autonomous Technologies (AAT). () Me	10 10 8 10 3 5 10 10 10	
MEASURE 2.12 MEASURE 2.13 MEASURE 2.13 MEASURE 3.0 MEASURE 3.0 MEASURE 3.1	N/A N/A N/A N/A N/A N/A	examined and documented. Fairness and bias - as identified in the MAP function - are evaluated and results are documented. Environmental impact and sustainability of AI model training and management activities - as identified in the MAP function - are evaluated and documented. Effectiveness of the employed TEVV metrics and processes in the MEASURE function are evaluated and documented. Effectiveness of the employed TEVV metrics and processes in the MEASURE function are evaluated and documented. Effectiveness of the employed TEVV metrics and processes in the MEASURE function are evaluated and documented. Effectiveness of the employed TEVV metrics and processes in the MEASURE function are evaluated and documented. Mechanisms for tracking identified AI risks over time are in place. 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 Functional Functional Functional Functional Functional Functional Functional Functional	equal equal intersects with intersects with intersects with equal equal	Assessment (DPIA) Al TEVV Fairness & Bias Assessment Al & Autonomous Technologies Environmental Impact & Sustainability Al TEVV Effectiveness Measuring Al & Autonomous Technologies Effectiveness Plan of Action & Milestones (POA&M) Risk Register Al & Autonomous Technologies Harm Prevention	AAT-10.8 AAT-17.2 AAT-10.10 AAT-10.11 AAT-16.2 IAO-05 RSK-04.1 AAT-17	(IDPA) on systems, applications and services that store, process and/or transmit Personal Data (PD) to identify and remediate reasonably-expected risks. Mechanisms exist to examine fairness and bias of Artificial Intelligence (AI) and Autonomous Technologies (AAT) to be deployed. Mechanisms exist to examine fairness and bias of Artificial Intelligence Technologies (AAT). Mechanisms exist to evaluate the results of Artificial Intelligence Test, Evaluation, Validation (AI). Mechanisms exist to evaluate the results of Artificial Intelligence Test, Evaluation, Validation (AI). Mechanisms exist to evaluate the effectiveness of the proceeds of the proposed Artificial Intelligence Test, Evaluation, Validation & Verification (AITEV). Mechanisms exist to evaluate the effectiveness of the processes utilized to perform Artificial Intelligence Test, Evaluation, Validation & Verification (AITEV). Mechanisms exist to evaluate the effectiveness of existing controls, including reports of errors and potential impacts on affected communities. Mechanisms exist to generate a Plan of Action and Milestones (POAM), or similar risk register, to document planned remedial actions to correct weaknesses or deficiencies noted during the seasesment of the security controls and to reduce or eliminate known valuenzabilities. (A) and Autonomous Technologies (AAT)-related risks. Mechanisms exist to conduct specialized assessments for: (1) Statutory, regulatory and contructual compliance obligations; (2) Mohile durone; (3) Abbile durone; (4) Databases; (5) Application security; (6) Embedded technologies (AAT)-related risks. (1) Mohile durone; (1) Artificial Intelligence and; (3) Mohile durone; (4) Patribases; (3) Mohile durone; (4) Patribases; (4) Patribases; (5) Application security; (6) Embedded technologies (AAT)-related risks.	10 10 8 10 3 5 10 10 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)
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	Al & 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	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	available. Jexclandrom sxist to conduct specialized assessments for: (1) Statutory, regulatory and contractual compliance obligations; (2) Motionic graphilities; (3) Motibile devices; (4) Databases; (5) Application security; (6) Embedded tochnologies (e.g., IoT, OT, etc.); (7) Vulnerability management; (8) Maticious 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 wuherabilities.	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	Al & 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	Al & Autonomous Technologies Domain Expert Reviews	AAT-16.5	Mechanisms exist to utilize input from domain experts and newant 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 Al 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 Al 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 tread analysis of the cybersecurity & data privacy program.	3	
MEASURE 4.3	N/A	Measurable performance improvements or declines based on consultations with relevant Al 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 Al actors, including affected communities, and field data about context relevant risks and trustworthiness characteristics are identified and documented.	Functional	equal	Al & 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. AI risks based on assessments and other analytical output from the MAP	Functional	equal	Al & 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. Mechanisms exist to facilitate the implementation of strategic,	10	
MANAGE 1.0	N/A	and MEASURE functions are prioritized, responded to, and managed. Al risks based on assessments and other analytical output from the MAP	Functional	subset of	Risk Management Program	RSK-01	operational and tactical risk management controls. Mechanisms exist to identify and document risks, both internal and	10	
MANAGE 1.0	N/A	and MEASURE functions are prioritized, responded to, and managed.	Functional	intersects with	Risk Identification	RSK-03	external.	8	
MANAGE 1.0	N/A	Al 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	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 vaectivating Artificial Intelligence (A) 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. A determination is made as to whether the AI system achieves its intended	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	purposes and stated objectives and whether its development or deployment should proceed.	Functional	intersects with	Plan of Action & Milestones (POA&M)	IAO-05	(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 Al & Autonomous Technologies	AAT-15.2	Mechanisms exist to define the criteria and responsible partylies) for superseding, disengaging or deactivating Artificial Intelligence (AI) and Autonomous Technologies (AI) that demonstrate performance or outcomes inconsistent with intended use.	5	

Versior	12	20	12	5	.2
7	7	7	20	12	25

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM	STRM	SCF Control	SCF #	Secure Controls Framework (SCF)	Strength of Relationship	Notes (optional)
		Treatment of documented AI risks is prioritized based on impact,	Rationale	Relationship			Control Description Mechanisms exist to generate a Plan of Action and Milestones	(optional)	
MANAGERS	N/A	likelihood, and available resources or methods.	Functional	intersects with	Plan of Action &	IAO-05	(POA&M), or similar risk register, to document planned remedial actions to correct weaknesses or deficiencies noted during the	8	
MANAGE 1.2	N/A		Functional	Intersects with	Milestones (POA&M)	IAO-05	assessment of the security controls and to reduce or eliminate known	8	
		Treatment of documented AI risks is prioritized based on impact,			Impact-Level		vulnerabilities. Mechanisms exist to prioritize the impact level for systems,		
MANAGE 1.2	N/A	likelihood, and available resources or methods.	Functional	intersects with	Prioritization	RSK-02.1	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	3	
		Treatment of documented AI risks is prioritized based on impact,					practices. Mechanisms exist to remediate risks to an acceptable level.		
MANAGE 1.2	N/A	likelihood, and available resources or methods.	Functional	intersects with	Risk Remediation	RSK-06		3	
		Responses to the AI risks deemed high priority, as identified by the MAP function, are developed, planned, and documented. Risk response options			Disc. (Astro-0		Mechanisms exist to generate a Plan of Action and Milestones (POA&M), or similar risk register, to document planned remedial		
MANAGE 1.3	N/A	can include mitigating, transferring, avoiding, or accepting.	Functional	intersects with	Plan of Action & Milestones (POA&M)	IAO-05	actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known	3	
							vulnerabilities.		
		Responses to the AI risks deemed high priority, as identified by the MAP function, are developed, planned, and documented. Risk response options					Mechanisms exist to respond to findings from cybersecurity & data privacy assessments, incidents and audits to ensure proper		
MANAGE 1.3	N/A	can include mitigating, transferring, avoiding, or accepting.	Functional	equal	Risk Response	RSK-06.1	remediation has been performed.	10	
					AI & Autonomous		Mechanisms exist to identify and document negative, residual risks		
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	Technologies Negative	AAT-15.1	(defined as the sum of all unmitigated risks) to both downstream acquirers and end users of Artificial Intelligence (AI) and Autonomous	10	
					Residual Risks		Technologies (AAT). Mechanisms exist to generate a Plan of Action and Milestones		
		Negative residual risks (defined as the sum of all unmitigated risks) to both			Plan of Action &		(POA&M), or similar risk register, to document planned remedial		
MANAGE 1.4	N/A	downstream acquirers of AI systems and end users are documented.	Functional	intersects with	Milestones (POA&M)	IAO-05	actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known	8	
							vulnerabilities.		
MANAGE 1.4	N/A	Negative residual risks (defined as the sum of all unmitigated risks) to both	Functional	intersects with	Risk Register	RSK-04.1	Mechanisms exist to maintain a risk register that facilitates monitoring and reporting of risks.	8	
		downstream acquirers of AI systems and end users are documented. Strategies to maximize AI benefits and minimize negative impacts are					Mechanisms exist to continuously improve Artificial Intelligence (AI)		
MANAGE 2.0	N/A	planned, prepared, implemented, documented, and informed by input	Functional	equal	AI & Autonomous Technologies Continuous	AAT-07.3	and Autonomous Technologies (AAT) capabilities to maximize benefits	10	
		from relevant AI actors.	tronut	- 4001	Improvements		and minimize negative impacts associated with AAT.		
MANAGE 2.0	N/A	Strategies to maximize Al benefits and minimize negative impacts are	Functional	intersects with	Technology Development	TDA-01	Mechanisms exist to facilitate the implementation of tailored development and acquisition strategies, contract tools and	3	
MANAGE 2.0	N/A	planned, prepared, implemented, documented, and informed by input from relevant Al actors.	Functional	Intersects with	& Acquisition	TDA-01	procurement and acquisition strategies, contract tools and procurement methods to meet unique business needs.	3	
		Strategies to maximize AI benefits and minimize negative impacts are planned, prepared, implemented, documented, and informed by input					Mechanisms exist to design and implement product management processes to proactively govern the design, development and		
		from relevant Al actors.					production of products and/or services across the System		
MANAGE 2.0	N/A		Functional	intersects with	Product Management	TDA-01.1	Development Life Cycle (SDLC) to: (1) Improve functionality;	8	
							(2) Enhance security and resiliency capabilities;		
							<ul> <li>(3) Correct security deficiencies; and</li> <li>(4) Conform with applicable statutory, regulatory and/or contractual</li> </ul>		
		Resources required to manage AI risks are taken into account – along with			Cybersecurity & Data		obligations. Mechanisms exist to facilitate the implementation of cybersecurity &		
MANAGE 2.1	N/A	viable non-Al alternative systems, approaches, or methods - to reduce the	Functional	intersects with	Privacy Portfolio	PRM-01	data privacy-related resource planning controls that define a viable	8	
		magnitude or likelihood of potential impacts. Resources required to manage AI risks are taken into account – along with			Management		plan for achieving cybersecurity & data privacy objectives. Mechanisms exist to address all capital planning and investment		
MANAGE 2.1	N/A	viable non-Al alternative systems, approaches, or methods - to reduce the	Functional	equal	Cybersecurity & Data Privacy Resource	PRM-02	requests, including the resources needed to implement the	10	
100000211		magnitude or likelihood of potential impacts.			Management		cybersecurity & data privacy programs and document all exceptions to this requirement.		
MANAGE 2.1	N/A	Resources required to manage AI risks are taken into account - along with	Functional	intersects with	Allocation of Resources	PRM-03	Mechanisms exist to identify and allocate resources for management,	8	
MANAGE 2.1	N/A	viable non-Al alternative systems, approaches, or methods – to reduce the magnitude or likelihood of potential impacts.	Functionat	Intersects with	Autocation of Resources	PRM-03	operational, technical and data privacy requirements within business process planning for projects / initiatives.	0	
MANAGE 2.1 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	Functional	intersects with	Risk Management	RSK-01.2	Mechanisms exist to reduce the magnitude or likelihood of potential impacts by resourcing the capability required to manage technology-	8	
		magnitude or likelihood of potential impacts.			Resourcing		related risks.		
	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	Functional	intersects with	Compensating Countermeasures	RSK-06.2	Mechanisms exist to identify and implement compensating countermeasures to reduce risk and exposure to threats.	8	
		magnitude or likelihood of potential impacts. Mechanisms are in place and applied to sustain the value of deployed Al			AI & Autonomous		Mechanisms exist to sustain the value of deployed Artificial Intelligence		
MANAGE 2.2	N/A	systems.	Functional	equal	Technologies Value	AAT-01.3	(Al) and Autonomous Technologies (AAT).	10	
		Mechanisms are in place and applied to sustain the value of deployed Al			Sustainment Cybersecurity & Data		Mechanisms exist to facilitate the implementation of cybersecurity &		
MANAGE 2.2	N/A	systems.	Functional	intersects with	Privacy Portfolio Management	PRM-01	data privacy-related resource planning controls that define a viable plan for achieving cybersecurity & data privacy objectives.	8	
		Mechanisms are in place and applied to sustain the value of deployed Al			Secure Development Life		Mechanisms exist to ensure changes to systems within the Secure		
MANAGE 2.2	N/A	systems.	Functional	intersects with	Cycle (SDLC) Management	PRM-07	Development Life Cycle (SDLC) are controlled through formal change control procedures.	5	
		Mechanisms are in place and applied to sustain the value of deployed AI			Č.		Mechanisms exist to design and implement product management		
		systems.					processes to proactively govern the design, development and production of products and/or services across the System		
MANAGE 2.2	N/A		Functional	intercects with	Product Management	TDA 01 1	Development Life Cycle (SDLC) to: (1) Improve functionality;	5	
PIANAGE 2.2	NVA		runctionat	Intersects with	Froduct Hallagement	104-01.1	<li>(2) Enhance security and resiliency capabilities;</li>	5	
							<ul> <li>(3) Correct security deficiencies; and</li> <li>(4) Conform with applicable statutory, regulatory and/or contractual</li> </ul>		
		Procedures are followed to research to and real sectors in the			Previously Unknown AI &		obligations.		
MANAGE 2.3	N/A	Procedures are followed to respond to and recover from a previously unknown risk when it is identified.	Functional	equal	Autonomous	AAT-17.3	Mechanisms exist to respond to and recover from a previously unknown Artificial Intelligence (AI) and Autonomous Technologies (AAT)-	10	
UL 2.3	100		- anotionat	oqudi	Technologies Threats & Risks	/011-1/.0	related risk when it is identified.	10	
		Procedures are followed to respond to and recover from a previously	Europe in		Incident Response	105	Mechanisms exist to implement and govern processes and		
MANAGE 2.3	N/A	unknown risk when it is identified.	Functional	intersects with	Operations	IRO-01	documentation to facilitate an organization-wide response capability for cybersecurity & data privacy-related incidents.	3	
		Procedures are followed to respond to and recover from a previously unknown risk when it is identified.					Mechanisms exist to cover: (1) Preparation;		
							(2) Automated event detection or manual incident report intake;		
MANAGE 2.3	N/A		Functional	intersects with	Incident Handling	IRO-02	<ul><li>(3) Analysis;</li><li>(4) Containment;</li></ul>	3	
							(5) Eradication; and		
MANAGE 2.3	N/A	Procedures are followed to respond to and recover from a previously	Functional	intersects with	Risk Identification	RSK-03	(6) Recovery. Mechanisms exist to identify and document risks, both internal and	5	
100002.0		unknown risk when it is identified. Procedures are followed to respond to and recover from a previously	- anotionat		reactorithication		external. Mechanisms exist to respond to findings from cybersecurity & data	~	
MANAGE 2.3	N/A	unknown risk when it is identified.	Functional	intersects with	Risk Response	RSK-06.1	privacy assessments, incidents and audits to ensure proper	8	
		Mechanisms are in place and applied, and responsibilities are assigned		1			remediation has been performed. Mechanisms exist to enforce an accountability structure so that		
MANAGE 2.4	N/A	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	appropriate teams and individuals are empowered, responsible and trained for mapping, measuring and managing data and technology-	8	
							related risks.		
		Mechanisms are in place and applied, and responsibilities are assigned and understood, to supersede, disengage, or deactivate AI systems that			Responsibility To Supersede, Deactivate		Mechanisms exist to define the criteria and responsible party(ies) for superseding, disengaging or deactivating Artificial Intelligence (AI) and		
MANAGE 2.4	N/A	demonstrate performance or outcomes inconsistent with intended use.	Functional	equal	and/or Disengage AI &	AAT-15.2	Autonomous Technologies (AAT) that demonstrate performance or	10	
				L	Autonomous Technologies		outcomes inconsistent with intended use.		
		Mechanisms are in place and applied, and responsibilities are assigned					Mechanisms exist to implement and govern processes and		
MANAGE 2.4	N/A	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	documentation to facilitate an organization-wide response capability for cybersecurity & data privacy-related incidents.	3	
		Mechanisms are in place and applied, and responsibilities are assigned					Mechanisms exist to cover:		
		and understood, to supersede, disengage, or deactivate AI systems that					(1) Preparation;		
	N/A	demonstrate performance or outcomes inconsistent with intended use.	Functional	intersects with	Incident Handling	IRO-02	<ul> <li>(2) Automated event detection or manual incident report intake;</li> <li>(3) Analysis;</li> </ul>	5	
MANAGE 2.4				1			(4) Containment;		
MANAGE 2.4							(5) Eradication; and		

\_

Versio	on	2	02	5	.2
	7/	7	12	02	25

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	Al risks and benefits from third-party entities are managed.	Functional	intersects with	Supply Chain Risk Management (SCRM) Plan	RSK-09	Nechanisms 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	Al risks and benefits from third-party entities are managed.	Functional	equal	Al & 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	Al 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	Al 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	Al 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 Mitestones (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	Al 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	Al risks and benefits from third-party resources are regularly monitored, and risk controls are applied and documented.	Functional	intersects with	Al & 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	Al 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	Al 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 Al 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 kay 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 Al 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 wuharabilities.	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	Al 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	Al & 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 Al system monitoring plans are implemented, including mechanisms for capturing and evaluating input from users and other relevant Al 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 Al system updates and include regular engagement with interested parties, including relevant Al 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	Al & 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	