NIST IR 8477-Based Set Theory Relationship Mapping (STRM)		**Focal Document:**	**NIST AI 600-1 (AI RMF Generative Artificial Intelligence Profile)**
Reference Document :	Secure Controls Framework (SCF) version 2025.2	**Focal Document URL:**	https://doi.org/10.6028/NIST.AI.600-1
STRM Guidance:	https://securecontrolsframework.com/set-theory-relationship-mapping-strm/	**Published STRM URL:**	https://securecontrolsframework.com/content/strm/scf-strm-us-fed-nist-ai-600-1.pdf

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
GOVERN 1.1	N/A	Legal and regulatory requirements involving AI are understood, managed, and documented.	Functional	Intersects With	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	5	
GOVERN 1.1	N/A	Legal and regulatory requirements involving AI are understood, managed, and documented.	Functional	Intersects With	Cybersecurity & Data Protection Governance Program	GOV-01	Mechanisms exist to facilitate the implementation of cybersecurity & data protection governance controls.	5	
GV-1.1-001	N/A	Align GAI development and use with applicable laws and regulations, including those related to data privacy, copyright and intellectual property law.	Functional	Intersects With	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	5	
GOVERN 1.2	N/A	The characteristics of trustworthy AI are integrated into organizational policies, processes, procedures, and practices.	Functional	Intersects With	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.	5	
GOVERN 1.2	N/A	The characteristics of trustworthy AI are integrated into organizational policies, processes, procedures, and practices.	Functional	Intersects With	Cybersecurity & Data Protection Governance Program	GOV-01	Mechanisms exist to facilitate the implementation of cybersecurity & data protection governance controls.	5	
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.	5	
GV-1.2-001	N/A	Establish transparency policies and processes for documenting the origin and history of training data and generated data for GAI applications to advance digital content transparency, while balancing the proprietary nature of training approaches.	Functional	Intersects With	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.	5	
GV-1.2-002	N/A	Establish policies to evaluate risk-relevant capabilities of GAI and robustness of safety measures, both prior to deployment and on an ongoing basis, through internal and external evaluations.	Functional	Intersects With	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.	5	
GV-1.2-002	N/A	Establish policies to evaluate risk-relevant capabilities of GAI and robustness of safety measures, both prior to deployment and on an ongoing basis, through internal and external evaluations.	Functional	Intersects With	Cybersecurity & Data Protection Governance Program	GOV-01	Mechanisms exist to facilitate the implementation of cybersecurity & data protection governance controls.	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	Standardized Operating Procedures (SOP)	OPS-01.1	Mechanisms exist to identify and document Standardized Operating Procedures (SOP), or similar documentation, to enable the proper execution of day-to-day / assigned tasks.	5	
GV-1.3-001	N/A	Consider the following factors when updating or defining risk tiers for GAIA buses and impacts to information integrity; Dependencies between GAI and other IT or data systems; Harm to fundamental rights or public safety; Presentation of obscene, objectionable, offensive, discriminatory, invalid or untruthful output; Psychological impacts to humans (e.g., anthropomorphization, algorithmic aversion, emotional entanglement); Possibility for malicious use; Whether the system introduces significant new security vulnerabilities; Anticipated system impact on some groups compared to others; Unreliable decision making capabilities, validity, adaptability, and variability of GAI system performance over time.	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
GV-1.3-002	N/A	Establish minimum thresholds for performance or assurance criteria and review as part of deployment approval ("go/"no-go") policies, procedures, and processes, with reviewed processes and approval thresholds reflecting measurement of GAI capabilities and risks.	Functional	Intersects With	Measures of Performance	GOV-05	Mechanisms exist to develop, report and monitor cybersecurity & data privacy program measures of performance.	5	
GV-1.3-002	N/A	Establish minimum thresholds for performance or assurance criteria and review as part of deployment approval ("go/"no-go") policies, procedures, and processes, with reviewed processes and approval thresholds reflecting measurement of GAI capabilities and risks.	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.	5	
GV-1.3-003	N/A	Establish a test plan and response policy, before developing highly capable models, to periodically evaluate whether the model may misuse CBRN information or capabilities and/or offensive cyber capabilities.	Functional	Subset Of	Artificial Intelligence Test, Evaluation, Validation & Verification (AI TEVV)	AAT-10	Mechanisms exist to implement Artificial Intelligence Test, Evaluation, Validation & Verification (AI TEVV) practices to enable Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related security, resilience and compliance-related conformity testing throughout the lifecycle of the AAT.	10	
GV-1.3-004	N/A	Obtain input from stakeholder communities to identify unacceptable use, in accordance with activities in the AI RMF Map 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	
GV-1.3-005	N/A	Maintain an updated hierarchy of identified and expected GAI risks connected to contexts of GAI model advancement and use, potentially including specialized risk levels for GAI systems that address issues such as model collapse and algorithmic monoculture.	Functional	Intersects With	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.	5	
GV-1.3-005	N/A	Maintain an updated hierarchy of identified and expected GAI risks connected to contexts of GAI model advancement and use, potentially including specialized risk levels for GAI systems that address issues such as model collapse and algorithmic monoculture.	Functional	Intersects With	AI & Autonomous Technologies Risk Mapping	AAT-02.1	Mechanisms exist to identify Artificial Intelligence (AI) and Autonomous Technologies (AAT) in use and map those components to potential legal risks, including statutory and regulatory compliance requirements.	5	
GV-1.3-006	N/A	Reevaluate organizational risk tolerances to account for unacceptable negative risk (such as where significant negative impacts are imminent, severe harms are actually occurring, or large-scale risks could occur); and broad GAI negative risks, includingImmature safety or risk cultures related to AI and GAI design, development and deployment, public information integrity risks, including impacts on democratic processes, unknown long-term performance characteristics of GAI.	Functional	Intersects With	AI TEVV Safety Demonstration	AAT-10.4	Mechanisms exist to demonstrate the Artificial Intelligence (AI) and Autonomous Technologies (AAT) to be deployed are safe, residual risk does not exceed the organization's risk tolerance and can fail safely, particularly if made to operate beyond its knowledge limits.	5	
GV-1.3-007	N/A	Devise a plan to halt development or deployment of a GAI system that poses unacceptable negative risk.	Functional	Intersects With	AI & Autonomous Technologies Risk Response	AAT-18.1	Mechanisms exist to prioritize, respond to and remediate Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related risks based on assessments and other analytical output.	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	AI & Autonomous Technologies Risk Management Decisions	AAT-07	Mechanisms exist to leverage decision makers from a diversity of demographics, disciplines, experience, expertise and backgrounds for mapping, measuring and managing Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related risks.	5	
GOVERN 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 Program	RSK-01	Mechanisms exist to facilitate the implementation of strategic, operational and tactical risk management controls.	5	
GV-1.4-001	N/A	Establish policies and mechanisms to prevent GAI systems from generating CSAM, NCII or content that violates the law.	Functional	Intersects With	Cybersecurity & Data Protection Governance Program	GOV-01	Mechanisms exist to facilitate the implementation of cybersecurity & data protection governance controls.	5	
GV-1.4-002	N/A	Establish transparent acceptable use policies for GAI that address illegal use or applications of GAI.	Functional	Intersects With	Cybersecurity & Data Protection Governance Program	GOV-01	Mechanisms exist to facilitate the implementation of cybersecurity & data protection governance controls.	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 are clearly defined, including determining the frequency of periodic review.	Functional	Intersects With	Assigned Responsibilities for AI & Autonomous Technologies	AAT-08	Mechanisms exist to define and differentiate roles and responsibilities for: (1) Artificial Intelligence (AI) and Autonomous Technologies (AAT) configurations; and (2) Oversight of AAT systems.	5	
GOVERN 1.5	N/A	Ongoing monitoring and periodic review of the risk management process and its outcomes are planned, and organizational roles and responsibilities are clearly defined, including determining the frequency of periodic review.	Functional	Intersects With	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	
GV-1.5-001	N/A	Define organizational responsibilities for periodic review of content provenance and incident monitoring for GAI systems.	Functional	Intersects With	Assigned Responsibilities for AI & Autonomous Technologies	AAT-08	Mechanisms exist to define and differentiate roles and responsibilities for: (1) Artificial Intelligence (AI) and Autonomous Technologies (AAT) configurations; and (2) Oversight of AAT systems.	5	
GV-1.5-001	N/A	Define organizational responsibilities for periodic review of content provenance and incident monitoring for GAI systems.	Functional	Intersects With	Data Source Identification	AAT-12.1	Mechanisms exist to identify and document data sources utilized in the training and/or operation of Artificial Intelligence and Autonomous Technologies (AAT).	5	
GV-1.5-001	N/A	Define organizational responsibilities for periodic review of content provenance and incident monitoring for GAI systems.	Functional	Intersects With	Defined Roles & Responsibilities	HRS-03	Mechanisms exist to define cybersecurity roles & responsibilities for all personnel.	5	
GV-1.5-002	N/A	Establish organizational policies and procedures for after action reviews of GAI system incident response and incident disclosures, to identify gaps; Update incident response and incident disclosure processes as required.	Functional	Intersects With	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.	8	
GV-1.5-002	N/A	Establish organizational policies and procedures for after action reviews of GAI system incident response and incident disclosures, to identify gaps; Update incident response and incident disclosure processes as required.	Functional	Intersects With	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	8	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
GV-1.5-002	N/A	Establish organizational policies and procedures for after action reviews of GAI system incident response and incident disclosures, to identify gaps; Update incident response and incident disclosure processes as required.	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	
GV-1.5-003	N/A	Maintain a document retention policy to keep history for test, evaluation, validation, and verification (TEVV), and digital content transparency methods for GAI.	Functional	Intersects With	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.	5	
GV-1.5-003	N/A	Maintain a document retention policy to keep history for test, evaluation, validation, and verification (TEVV), and digital content transparency methods for GAI.	Functional	Intersects With	Artificial Intelligence Test, Evaluation, Validation & Verification (AI TEVV)	AAT-10	Mechanisms exist to implement Artificial Intelligence Test, Evaluation, Validation & Verification (AI TEVV) practices to enable Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related security, resilience and compliance-related conformity testing throughout the lifecycle of the AAT.	8	
GV-1.5-003	N/A	Maintain a document retention policy to keep history for test, evaluation, validation, and verification (TEVV), and digital content transparency methods for GAI.	Functional	Intersects With	Media & Data Retention	DCH-18	Mechanisms exist to retain media and data in accordance with applicable statutory, regulatory and contractual obligations.	8	
GOVERN 1.6	N/A	Mechanisms are in place to inventory AI systems and are resourced according to organizational risk priorities.	Functional	Intersects With	Situational Awareness of AI & Autonomous Technologies	AAT-02	Mechanisms exist to develop and maintain an inventory of Artificial Intelligence (AI) and Autonomous Technologies (AAT) (internal and third-party).	5	
GOVERN 1.6	N/A	Mechanisms are in place to inventory AI systems and are resourced according to organizational risk priorities.	Functional	Intersects With	Asset Inventories	AST-02	Mechanisms exist to perform inventories of technology assets that: (1) Accurately reflects the current systems, applications and services in use; (2) Identifies authorized software products, including business justification details; (3) Is at the level of granularity deemed necessary for tracking and reporting; (4) Includes organization-defined information deemed necessary to achieve effective property accountability; and (5) Is available for review and audit by designated organizational personnel.	5	
GV-1.6-001	N/A	Enumerate organizational GAI systems for incorporation into AI system inventory and adjust AI system inventory requirements to account for GAI risks.	Functional	Intersects With	Situational Awareness of AI & Autonomous Technologies	AAT-02	Mechanisms exist to develop and maintain an inventory of Artificial Intelligence (AI) and Autonomous Technologies (AAT) (internal and third-party).	5	
GV-1.6-001	N/A	Enumerate organizational GAI systems for incorporation into AI system inventory and adjust AI system inventory requirements to account for GAI risks.	Functional	Intersects With	Asset Inventories	AST-02	Mechanisms exist to perform inventories of technology assets that: (1) Accurately reflects the current systems, applications and services in use; (2) Identifies authorized software products, including business justification details; (3) Is at the level of granularity deemed necessary for tracking and reporting; (4) Includes organization-defined information deemed necessary to achieve effective property accountability; and (5) Is available for review and audit by designated organizational personnel.	5	
GV-1.6-002	N/A	Define any inventory exemptions in organizational policies for GAI systems embedded into application software.	Functional	Intersects With	Situational Awareness of AI & Autonomous Technologies	AAT-02	Mechanisms exist to develop and maintain an inventory of Artificial Intelligence (AI) and Autonomous Technologies (AAT) (internal and third-party).	5	
GV-1.6-002	N/A	Define any inventory exemptions in organizational policies for GAI systems embedded into application software.	Functional	Intersects With	Asset Inventories	AST-02	Mechanisms exist to perform inventories of technology assets that: (1) Accurately reflects the current systems, applications and services in use; (2) Identifies authorized software products, including business justification details; (3) Is at the level of granularity deemed necessary for tracking and reporting; (4) Includes organization-defined information deemed necessary to achieve effective property accountability; and (5) Is available for review and audit by designated organizational personnel.	8	
GV-1.6-003	N/A	In addition to general model, governance, and risk information, consider the following items in GAI system inventory entriesData provenance information (e.g., source, signatures, versioning, watermarks); Known issues reported from internal bug tracking or external information sharing resources (e.g., AI incident database, AVID, CVE, NVD, or OECD AI incident monitor); Human oversight roles and responsibilities; Special rights and considerations for intellectual property, licensed works, or personal, privileged, proprietary or sensitive data; Underlying foundation models, versions of underlying models, and access modes.	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
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	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.	5	
GOVERN 1.7	N/A	Processes and procedures are in place for decommissioning and phasing out AI systems safely and in a manner that does not increase risks or decrease the organization's trustworthiness.	Functional	Intersects With	Decommissioning	AST-30	Mechanisms exist to ensure systems, applications and services are properly decommissioned so that data is properly transitioned to new systems or archived in accordance with applicable organizational standards, as well as statutory, regulatory and contractual obligations.	5	
GV-1.7-001	N/A	Protocols are put in place to ensure GAI systems are able to be deactivated whennecessary.	Functional	Intersects With	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.	5	
GV-1.7-002	N/A	Consider the following factors when decommissioning GAI systemsData retention requirements; Data security, e.g., containment, protocols, Data leakage after decommissioning; Dependencies between upstream, downstream, or other data, internet of things (IOT) or AI systems; Use of open-source data or models; Users' emotional entanglement with GAI functions.	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
GOVERN 2.1	N/A	Roles and responsibilities and lines of communication related to mapping, measuring, and managing AI risks are documented and are clear to individuals and teams throughout the organization.	Functional	Intersects With	Assigned Responsibilities for AI & Autonomous Technologies	AAT-08	Mechanisms exist to define and differentiate roles and responsibilities for: (1) Artificial Intelligence (AI) and Autonomous Technologies (AAT) configurations; and (2) Oversight of AAT systems.	5	
GV-2.1-001	N/A	Establish organizational roles, policies, and procedures for communicating GAI incidents and performance to AI Actors and downstream stakeholders (including those potentially impacted), via community or official resources (e.g., AI incident database, AVID, CVE, NVD, or OECD AI incident monitor).	Functional	Intersects With	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.	5	
GV-2.1-001	N/A	Establish organizational roles, policies, and procedures for communicating GAI incidents and performance to AI Actors and downstream stakeholders (including those potentially impacted), via community or official resources (e.g., AI incident database, AVID, CVE, NVD, or OECD AI incident monitor).	Functional	Intersects With	Assigned Responsibilities for AI & Autonomous Technologies	AAT-08	Mechanisms exist to define and differentiate roles and responsibilities for: (1) Artificial Intelligence (AI) and Autonomous Technologies (AAT) configurations; and (2) Oversight of AAT systems.	5	
GV-2.1-002	N/A	Establish procedures to engage teams for GAI system incident response with diverse composition and responsibilities based on the particular incident type.	Functional	Intersects With	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.	5	
GV-2.1-002	N/A	Establish procedures to engage teams for GAI system incident response with diverse composition and responsibilities based on the particular incident type.	Functional	Intersects With	Assigned Responsibilities for AI & Autonomous Technologies	AAT-08	Mechanisms exist to define and differentiate roles and responsibilities for: (1) Artificial Intelligence (AI) and Autonomous Technologies (AAT) configurations; and (2) Oversight of AAT systems.	5	
GV-2.1-003	N/A	Establish processes to verify the AI Actors conducting GAI incident response tasks demonstrate and maintain the appropriate skills and training.	Functional	Intersects With	AI & Autonomous Technologies Training	AAT-05	Mechanisms exist to ensure personnel and external stakeholders are provided with position-specific risk management training for Artificial Intelligence (AI) and Autonomous Technologies (AAT).	5	
GV-2.1-004	N/A	When systems may raise national security risks, involve national security professionals in mapping, measuring, and managing those risks.	Functional	Subset Of	Artificial Intelligence (AI) & Autonomous Technologies Governance	AAT-01	Mechanisms exist to ensure policies, processes, procedures and practices related to the mapping, measuring and managing of Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related risks are in place, transparent and implemented effectively.	10	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
GV-2.1-004	N/A	When systems may raise national security risks, involve national security professionals in mapping, measuring, and managing those risks.	Functional	Intersects With	AI & Autonomous Technologies High Risk Designations	AAT-09.1	Mechanisms exist to designate Artificial Intelligence (AI) and Autonomous Technologies (AAT) "High Risk" if one(1), or more, of the follow criteria are met: (1) AAT is used as a safety component of a product or service; (2) AAT poses a significant risk of harm to an individual's health, safety or fundamental rights; and/or (3) AAT materially influences the outcome of an individual's decision making.	8	
GV-2.1-004	N/A	When systems may raise national security risks, involve national security professionals in mapping, measuring, and managing those risks.	Functional	Intersects With	Serious Incident Reporting For AI & Autonomous Technologies	AAT-16.9	Mechanisms exist to report any serious incident involving operational Artificial Intelligence (AI) and Autonomous Technologies (AAT) to relevant authorities as to when and where the serious incident occurred, in accordance with mandated reporting timelines.	3	
GV-2.1-004	N/A	When systems may raise national security risks, involve national security professionals in mapping, measuring, and managing those risks.	Functional	Intersects With	Contacts With Authorities	GOV-06	Mechanisms exist to identify and document appropriate contacts with relevant law enforcement and regulatory bodies.	5	
GV-2.1-005	N/A	Create mechanisms to provide protections for whistleblowers who report, based on reasonable belief, when the organization violates relevant laws or poses a specific and empirically well-substantiated negative risk to public safety (or has already caused harm).	Functional	Intersects With	Reporting Suspicious Activities	HRS-15	Mechanisms exist to enable personnel to report suspicious activities and/or behavior without fear of reprisal or other negative consequences (e.g., whistleblower protections).	5	
GOVERN 3.2	N/A	Policies and procedures are in place to define and differentiate roles and responsibilities for human-AI configurations and oversight of AI systems.	Functional	Intersects With	Assigned Responsibilities for AI & Autonomous Technologies	AAT-08	Mechanisms exist to define and differentiate roles and responsibilities for: (1) Artificial Intelligence (AI) and Autonomous Technologies (AAT) configurations; and (2) Oversight of AAT systems.	5	
GV-3.2-001	N/A	Policies are in place to bolster oversight of GAI systems with independent evaluations or assessments of GAI models or systems where the type and robustness of evaluations are proportional to the identified risks.	Functional	Intersects With	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.	5	
GV-3.2-002	N/A	Consider adjustment of organizational roles and components across lifecycle stages of large or complex GAI systems, including Test and evaluation, validation, and red-teaming of GAI systems; GAI content moderation; GAI system development and engineering; Increased accessibility of GAI tools, interfaces, and systems, Incident response and containment.	Functional	No relationship	N/A	N/A	No applicable SCF control	N/A	
GV-3.2-003	N/A	Define acceptable use policies for GAI interfaces, modalities, and human-AI configurations (i.e., for chatbots and decision-making tasks), including criteria for the kinds of queries GAI applications should refuse to respond to.	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	
GV-3.2-003	N/A	Define acceptable use policies for GAI interfaces, modalities, and human-AI configurations (i.e., for chatbots and decision-making tasks), including criteria for the kinds of queries GAI applications should refuse to respond to.	Functional	Intersects With	Product Conformity Governance	TDA-21	Mechanisms exist to ensure developed products and/or services conform to applicable statutory and regulatory requirements, based on the product's and/or service's: (1) Use case(s); and (2) Geographic markets.	8	
GV-3.2-004	N/A	Establish policies for user feedback mechanisms for GAI systems which include thorough instructions and any mechanisms for recourse.	Functional	Intersects With	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.	5	
GV-3.2-004	N/A	Establish policies for user feedback mechanisms for GAI systems which include thorough instructions and any mechanisms for recourse.	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.	5	
GV-3.2-005	N/A	Engage in threat modeling to anticipate potential risks from GAI systems.	Functional	Intersects With	Threat Modeling	TDA-06.2	Mechanisms exist to perform threat modelling and other secure design techniques, to ensure that threats to software and solutions are identified and accounted for.	5	
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	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.	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	Cybersecurity & Data Protection Governance Program	GOV-01	Mechanisms exist to facilitate the implementation of cybersecurity & data protection governance controls.	5	
GV-4.1-001	N/A	Establish policies and procedures that address continual improvement processes for GAI risk measurement. Address general risks associated with a lack of explainability and transparency in GAI systems by using ample documentation and techniques such asapplication of gradient-based attributions, occlusion/term reduction, counterfactual prompts and prompt engineering, and analysis of embeddings; Assess and update risk measurement approaches at regular cadences.	Functional	Intersects With	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.	5	
GV-4.1-002	N/A	Establish policies, procedures, and processes detailing risk measurement in context of use with standardized measurement protocols and structured public feedback exercises such as AI red-teaming or independent external evaluations.	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.	5	
GV-4.1-002	N/A	Establish policies, procedures, and processes detailing risk measurement in context of use with standardized measurement protocols and structured public feedback exercises such as AI red-teaming or independent external evaluations.	Functional	Intersects With	AI & Autonomous Technologies Risk Mapping	AAT-02.1	Mechanisms exist to identify Artificial Intelligence (AI) and Autonomous Technologies (AAT) in use and map those components to potential legal risks, including statutory and regulatory compliance requirements.	8	
GV-4.1-002	N/A	Establish policies, procedures, and processes detailing risk measurement in context of use with standardized measurement protocols and structured public feedback exercises such as AI red-teaming or independent external evaluations.	Functional	Intersects With	AI & Autonomous Technologies Likelihood & Impact Risk Analysis	AAT-07.2	Mechanisms exist to define the potential likelihood and impact of each identified risk based on expected use and past uses of Artificial Intelligence (AI) and Autonomous Technologies (AAT) in similar contexts.	8	
GV-4.1-002	N/A	Establish policies, procedures, and processes detailing risk measurement in context of use with standardized measurement protocols and structured public feedback exercises such as AI red-teaming or independent external evaluations.	Functional	Intersects With	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.	3	
GV-4.1-002	N/A	Establish policies, procedures, and processes detailing risk measurement in context of use with standardized measurement protocols and structured public feedback exercises such as AI red-teaming or independent external evaluations.	Functional	Intersects With	Responsibility To Supersede, Deactivate and/or Disengage AI & Autonomous Technologies	AAT-15.2	Mechanisms exist to define the criteria and responsible party(ies) for superseding, disengaging or deactivating Artificial Intelligence (AI) and Autonomous Technologies (AAT) that demonstrate performance or outcomes inconsistent with intended use.	3	
GV-4.1-003	N/A	Establish policies, procedures, and processes for oversight functions (e.g., senior leadership, legal, compliance, including internal evaluation) across the GAI lifecycle, from problem formulation and supply chains to system decommission.	Functional	Intersects With	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.	5	
GV-4.1-003	N/A	Establish policies, procedures, and processes for oversight functions (e.g., senior leadership, legal, compliance, including internal evaluation) across the GAI lifecycle, from problem formulation and supply chains to system decommission.	Functional	Intersects With	Robust Stakeholder Engagement for AI & Autonomous Technologies	AAT-11	Mechanisms exist to compel ongoing engagement with relevant Artificial Intelligence (AI) and Autonomous Technologies (AAT) stakeholders to encourage feedback about positive, negative and unanticipated impacts.	5	
GOVERN 4.2	N/A	Organizational teams document the risks and potential impacts of the AI technology they design, develop, deploy, evaluate, and use, and they communicate about the impacts more broadly.	Functional	Intersects With	AI & Autonomous Technologies 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	

GOVERN 4.2	N/A	Organizational teams document the risks and potential impacts of the AI technology they design, develop, deploy, evaluate, and use, and they communicate about the impacts more broadly.	Functional	Intersects With	AI & Autonomous Technologies Risk Profiling	AAT-09	Mechanisms exist to document the risks and potential impacts of Artificial Intelligence (AI) and Autonomous Technologies (AAT) that are:
							(1) Designed;
							(2) Developed;
							(3) Deployed;
							(4) Evaluated; and/or
							(5) Used.
								5	

GV-4.2-001	N/A	Establish terms of use and terms of service for GAI systems.	Functional	Intersects With	Robust Stakeholder Engagement for AI & Autonomous Technologies	AAT-11	Mechanisms exist to compel ongoing engagement with relevant Artificial Intelligence (AI) and Autonomous Technologies (AAT) stakeholders to encourage feedback about positive, negative and unanticipated impacts.	3	
GV-4.2-001	N/A	Establish terms of use and terms of service for GAI systems.	Functional	Intersects With	Use of Critical Technologies	HRS-05.4	Mechanisms exist to govern usage policies for critical technologies.	8	
GV-4.2-002	N/A	Include relevant AI Actors in the GAI system risk identification process.	Functional	Intersects With	AI & Autonomous Technologies Risk Mapping	AAT-02.1	Mechanisms exist to identify Artificial Intelligence (AI) and Autonomous Technologies (AAT) in use and map those components to potential legal risks, including statutory and regulatory compliance requirements.	8	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)

GV-4.2-002	N/A	Include relevant AI Actors in the GAI system risk identification process.	Functional	Intersects With	AI & Autonomous Technologies Risk Profiling	AAT-09	Mechanisms exist to document the risks and potential impacts of Artificial Intelligence (AI) and Autonomous Technologies (AAT) that are:
							(1) Designed;
							(2) Developed;
							(3) Deployed;
							(4) Evaluated; and/or
							(5) Used.
								3	

GV-4.2-002	N/A	Include relevant AI Actors in the GAI system risk identification process.	Functional	Intersects With	Robust Stakeholder Engagement for AI & Autonomous Technologies	AAT-11	Mechanisms exist to compel ongoing engagement with relevant Artificial Intelligence (AI) and Autonomous Technologies (AAT) stakeholders to encourage feedback about positive, negative and unanticipated impacts.	5	
GV-4.2-002	N/A	Include relevant AI Actors in the GAI system risk identification process.	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.	5	
GV-4.2-002	N/A	Include relevant AI Actors in the GAI system risk identification process.	Functional	Intersects With	Risk Identification	RSK-03	Mechanisms exist to identify and document risks, both internal and external.	5	
GV-4.2-003	N/A	Verify that downstream GAI system impacts (such as the use of third-party plugins) are included in the impact documentation process.	Functional	Intersects With	AI & Autonomous Technologies Impact Assessment	AAT-07.1	Mechanisms exist to assess the impact(s) of proposed Artificial Intelligence (AI) and Autonomous Technologies (AAT) on individuals, groups, communities, organizations and society (e.g., Fundamental Rights Impact Assessment (FRIA)).	10	
GOVERN 4.3	N/A	Organizational practices are in place to enable AI testing, identification of incidents, and information sharing.	Functional	Intersects With	Artificial Intelligence Test, Evaluation, Validation & Verification (AI TEVV)	AAT-10	Mechanisms exist to implement Artificial Intelligence Test, Evaluation, Validation & Verification (AI TEVV) practices to enable Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related security, resilience and compliance-related conformity testing throughout the lifecycle of the AAT.	5	
GV4.3--001	N/A	Establish policies for measuring the effectiveness of employed content provenance methodologies (e.g., cryptography, watermarking, steganography, etc.)	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	
GV-4.3-002	N/A	Establish organizational practices to identify the minimum set of criteria necessary for GAI system incident reporting such as System ID (auto-generated most likely), Title, Reporter, System/Source, Data Reported, Date of Incident, Description, Impact(s), Stakeholder(s) Impacted.	Functional	Intersects With	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.	8	
GV-4.3-002	N/A	Establish organizational practices to identify the minimum set of criteria necessary for GAI system incident reporting such as System ID (auto-generated most likely), Title, Reporter, System/Source, Data Reported, Date of Incident, Description, Impact(s), Stakeholder(s) Impacted.	Functional	Intersects With	AI & Autonomous Technologies Event Logging	AAT-16.8	Mechanisms exist to ensure Artificial Intelligence (AI) and Autonomous Technologies (AAT) system event logging capabilities at a minimum provide: (1) Start date, start time, end date and end time for each use; (2) Database(s) against which input data has been checked by the system; (3) Input data for which the search has led to a match; and (4) Identification of individual(s) involved in the verification of the results.	8	
GV-4.3-002	N/A	Establish organizational practices to identify the minimum set of criteria necessary for GAI system incident reporting such as System ID (auto-generated most likely), Title, Reporter, System/Source, Data Reported, Date of Incident, Description, Impact(s), Stakeholder(s) Impacted.	Functional	Intersects With	Serious Incident Reporting For AI & Autonomous Technologies	AAT-16.9	Mechanisms exist to report any serious incident involving operational Artificial Intelligence (AI) and Autonomous Technologies (AAT) to relevant authorities as to when and where the serious incident occurred, in accordance with mandated reporting timelines.	5	
GV-4.3-002	N/A	Establish organizational practices to identify the minimum set of criteria necessary for GAI system incident reporting such as System ID (auto-generated most likely), Title, Reporter, System/Source, Data Reported, Date of Incident, Description, Impact(s), Stakeholder(s) Impacted.	Functional	Intersects With	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	8	
GV-4.3-003	N/A	Verify information sharing and feedback mechanisms among individuals and organizations regarding any negative impact from GAI systems.	Functional	Intersects With	Artificial Intelligence Test, Evaluation, Validation & Verification (AI TEVV)	AAT-10	Mechanisms exist to implement Artificial Intelligence Test, Evaluation, Validation & Verification (AI TEVV) practices to enable Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related security, resilience and compliance-related conformity testing throughout the lifecycle of the AAT.	5	
GV-4.3-003	N/A	Verify information sharing and feedback mechanisms among individuals and organizations regarding any negative impact from GAI systems.	Functional	Intersects With	Robust Stakeholder Engagement for AI & Autonomous Technologies	AAT-11	Mechanisms exist to compel ongoing engagement with relevant Artificial Intelligence (AI) and Autonomous Technologies (AAT) stakeholders to encourage feedback about positive, negative and unanticipated impacts.	5	
GOVERN 5.1	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	Robust Stakeholder Engagement for AI & Autonomous Technologies	AAT-11	Mechanisms exist to compel ongoing engagement with relevant Artificial Intelligence (AI) and Autonomous Technologies (AAT) stakeholders to encourage feedback about positive, negative and unanticipated impacts.	5	
GV-5.1-001	N/A	Allocate time and resources for outreach, feedback, and recourse processes in GAI system development.	Functional	Intersects With	Robust Stakeholder Engagement for AI & Autonomous Technologies	AAT-11	Mechanisms exist to compel ongoing engagement with relevant Artificial Intelligence (AI) and Autonomous Technologies (AAT) stakeholders to encourage feedback about positive, negative and unanticipated impacts.	5	
GV-5.1-001	N/A	Allocate time and resources for outreach, feedback, and recourse processes in GAI system development.	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	
GV-5.1-001	N/A	Allocate time and resources for outreach, feedback, and recourse processes in GAI system development.	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.	5	
GV-5.1-002	N/A	Document interactions with GAI systems to users prior to interactive activities, particularly in contexts involving more significant risks.	Functional	Intersects With	AI & Autonomous Technologies Likelihood & Impact Risk Analysis	AAT-07.2	Mechanisms exist to define the potential likelihood and impact of each identified risk based on expected use and past uses of Artificial Intelligence (AI) and Autonomous Technologies (AAT) in similar contexts.	5	
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	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.	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	AI & Autonomous Technologies Intellectual Property Infringement Protections	AAT-12	Mechanisms exist to prevent third-party Intellectual Property (IP) rights infringement by Artificial Intelligence (AI) and Autonomous Technologies (AAT).	5	
GV-6.1-001	N/A	Categorize different types of GAI content with associated third-party rights (e.g., copyright, intellectual property, data privacy).	Functional	Intersects With	AI & Autonomous Technologies Intellectual Property Infringement Protections	AAT-12	Mechanisms exist to prevent third-party Intellectual Property (IP) rights infringement by Artificial Intelligence (AI) and Autonomous Technologies (AAT).	5	
GV-6.1-001	N/A	Categorize different types of GAI content with associated third-party rights (e.g., copyright, intellectual property, data privacy).	Functional	Intersects With	Data Source Identification	AAT-12.1	Mechanisms exist to identify and document data sources utilized in the training and/or operation of Artificial Intelligence and Autonomous Technologies (AAT).	5	
GV-6.1-002	N/A	Conduct joint educational activities and events in collaboration with third parties to promote best practices for managing GAI risks.	Functional	Subset Of	Cybersecurity & Data Privacy Awareness Training	SAT-02	Mechanisms exist to provide all employees and contractors appropriate awareness education and training that is relevant for their job function.	10	
GV-6.1-003	N/A	Develop and validate approaches for measuring the success of content provenance management efforts with third parties (e.g., incidents detected and response times).	Functional	Intersects With	AI TEVV Benchmarking Content Provenance	AAT-10.17	Mechanisms exist to benchmark the verifiable lineage and origin of content used by Artificial Intelligence (AI) and Autonomous Technologies (AAT) according to industry -recognized standards.	8	
GV-6.1-003	N/A	Develop and validate approaches for measuring the success of content provenance management efforts with third parties (e.g., incidents detected and response times).	Functional	Intersects With	Data Source Identification	AAT-12.1	Mechanisms exist to identify and document data sources utilized in the training and/or operation of Artificial Intelligence and Autonomous Technologies (AAT).	8	
GV-6.1-004	N/A	Draft and maintain well-defined contracts and service level agreements (SLAs) that specify content ownership, usage rights, quality standards, security requirements, and content provenance expectations for GAI systems.	Functional	Intersects With	Data Source Identification	AAT-12.1	Mechanisms exist to identify and document data sources utilized in the training and/or operation of Artificial Intelligence and Autonomous Technologies (AAT).	5	
GV-6.1-004	N/A	Draft and maintain well-defined contracts and service level agreements (SLAs) that specify content ownership, usage rights, quality standards, security requirements, and content provenance expectations for GAI systems.	Functional	Intersects With	Adequate Security for Sensitive / Regulated Data In Support of Contracts	IAO-03.2	Mechanisms exist to protect sensitive / regulated data that is collected, developed, received, transmitted, used or stored in support of the performance of a contract.	5	
GV-6.1-004	N/A	Draft and maintain well-defined contracts and service level agreements (SLAs) that specify content ownership, usage rights, quality standards, security requirements, and content provenance expectations for GAI systems.	Functional	Subset Of	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for cybersecurity & data privacy requirements with third-parties, reflecting the organization's needs to protect its systems, processes and data.	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)
GV-6.1-005	N/A	Implement a use-cased based supplier risk assessment framework to evaluate and monitor third-party entities' performance and adherence to content provenance standards and technologies to detect anomalies and unauthorized changes; services acquisition and value chain risk management; and legal compliance.	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.	5	
GV-6.1-006	N/A	Include clauses in contracts which allow an organization to evaluate third-party GAI processes and standards.	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.	5	
GV-6.1-007	N/A	Inventory all third-party entities with access to organizational content and establish approved GAI technology and service provider lists.	Functional	Intersects With	Third-Party Inventories	TPM-01.1	Mechanisms exist to maintain a current, accurate and complete list of External Service Providers (ESPs) that can potentially impact the Confidentiality, Integrity, Availability and/or Safety (CIAS) of the organization's systems, applications, services and data.	5	
GV-6.1-008	N/A	Maintain records of changes to content made by third parties to promote content provenance, including sources, timestamps, metadata.	Functional	Intersects With	Data Source Identification	AAT-12.1	Mechanisms exist to identify and document data sources utilized in the training and/or operation of Artificial Intelligence and Autonomous Technologies (AAT).	5	
GV-6.1-008	N/A	Maintain records of changes to content made by third parties to promote content provenance, including sources, timestamps, metadata.	Functional	Intersects With	Digital Content Modification Logging	AAT-12.4	Mechanisms exist to ensure Artificial Intelligence and Autonomous Technologies (AAT): (1) Enable auditing of content modifications; and (2) Generate event logs for content-related changes.	8	
GV-6.1-009	N/A	Update and integrate due diligence processes for GAI acquisition and procurement vendor assessments to include intellectual property, data privacy, security, and other risks. For example, update processes to Address solutions that may rely on embedded GAI technologies; Address ongoing monitoring, assessments, and alerting, dynamic risk assessments, and real-time reporting tools for monitoring third-party GAI risks; Consider policy adjustments across GAI modeling libraries, tools and APIs, fine-tuned models, and embedded tools; Assess GAI vendors, open-source or proprietary GAI tools, or GAI service providers against incident or vulnerability databases.	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	
GV-6.1-009	N/A	Update and integrate due diligence processes for GAI acquisition and procurement vendor assessments to include intellectual property, data privacy, security, and other risks. For example, update processes to Address solutions that may rely on embedded GAI technologies; Address ongoing monitoring, assessments, and alerting, dynamic risk assessments, and real-time reporting tools for monitoring third-party GAI risks; Consider policy adjustments across GAI modeling libraries, tools and APIs, fine-tuned models, and embedded tools; Assess GAI vendors, open-source or proprietary GAI tools, or GAI service providers against incident or vulnerability databases.	Functional	Intersects With	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	8	
GV-6.1-009	N/A	Update and integrate due diligence processes for GAI acquisition and procurement vendor assessments to include intellectual property, data privacy, security, and other risks. For example, update processes to Address solutions that may rely on embedded GAI technologies; Address ongoing monitoring, assessments, and alerting, dynamic risk assessments, and real-time reporting tools for monitoring third-party GAI risks; Consider policy adjustments across GAI modeling libraries, tools and APIs, fine-tuned models, and embedded tools; Assess GAI vendors, open-source or proprietary GAI tools, or GAI service providers against incident or vulnerability databases.	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.	5	
GV-6.1-010	N/A	Update GAI acceptable use policies to address proprietary and open-source GAI technologies and data, and contractors, consultants, and other third-party personnel.	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.	8	
GV-6.1-010	N/A	Update GAI acceptable use policies to address proprietary and open-source GAI technologies and data, and contractors, consultants, and other third-party personnel.	Functional	Intersects With	Technology Use Restrictions	HRS-05.3	Mechanisms exist to establish usage restrictions and implementation guidance for organizational technologies based on the potential to cause damage to systems, if used maliciously.	8	
GV-6.1-010	N/A	Update GAI acceptable use policies to address proprietary and open-source GAI technologies and data, and contractors, consultants, and other third-party personnel.	Functional	Intersects With	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for cybersecurity & data privacy requirements with third-parties, reflecting the organization's needs to protect its systems, processes and data.	5	
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	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.	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	Artificial Intelligence Test, Evaluation, Validation & Verification (AI TEVV)	AAT-10	Mechanisms exist to implement Artificial Intelligence Test, Evaluation, Validation & Verification (AI TEVV) practices to enable Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related security, resilience and compliance-related conformity testing throughout the lifecycle of the AAT.	5	
GOVERN 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 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.	5	
GV-6.2-001	N/A	Document GAI risks associated with system value chain to identify over-reliance on third-party data and to identify fallbacks.	Functional	Intersects With	AI & Autonomous Technologies System Value Chain	AAT-25	Mechanisms exist to document the sequence of events and relevant stakeholders involved in creating and deploying Artificial Intelligence (AI) and Autonomous Technologies (AAT).	5	
GV-6.2-001	N/A	Document GAI risks associated with system value chain to identify over-reliance on third-party data and to identify fallbacks.	Functional	Intersects With	AI & Autonomous Technologies System Value Chain Fallbacks	AAT-25.1	Mechanisms exist to identify: (1) Over-reliance on third-party data with Artificial Intelligence (AI) and Autonomous Technologies (AAT); and (2) Fallback methods to address the inability to access third-party data, as necessary.	5	
GV-6.2-002	N/A	Document incidents involving third-party GAI data and systems, including open- data and open-source software.	Functional	Intersects With	Open Source Software	CFG-04.1	Mechanisms exist to establish parameters for the secure use of open source software.	5	
GV-6.2-002	N/A	Document incidents involving third-party GAI data and systems, including open- data and open-source software.	Functional	Intersects With	Third-Party Services	TPM-04	Mechanisms exist to mitigate the risks associated with third-party access to the organization's systems and data.	5	
GV-6.2-003	N/A	Establish incident response plans for third-party GAI technologies Align incident response plans with impacts enumerated in MAP 5.1; Communicate third-party GAI incident response plans to all relevant AI Actors; Define ownership of GAI incident response functions; Rehearse third-party GAI incident response plans at a regular cadence; Improve incident response plans based on retrospective learning; Review incident response plans for alignment with relevant breach reporting, data protection, data privacy, or other laws.	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	
GV-6.2-003	N/A	Establish incident response plans for third-party GAI technologies Align incident response plans with impacts enumerated in MAP 5.1; Communicate third-party GAI incident response plans to all relevant AI Actors; Define ownership of GAI incident response functions; Rehearse third-party GAI incident response plans at a regular cadence; Improve incident response plans based on retrospective learning; Review incident response plans for alignment with relevant breach reporting, data protection, data privacy, or other laws.	Functional	Intersects With	Incident Response Testing	IRO-06	Mechanisms exist to formally test incident response capabilities through realistic exercises to determine the operational effectiveness of those capabilities.	5	
GV-6.2-003	N/A	Establish incident response plans for third-party GAI technologies Align incident response plans with impacts enumerated in MAP 5.1; Communicate third-party GAI incident response plans to all relevant AI Actors; Define ownership of GAI incident response functions; Rehearse third-party GAI incident response plans at a regular cadence; Improve incident response plans based on retrospective learning; Review incident response plans for alignment with relevant breach reporting, data protection, data privacy, or other laws.	Functional	Intersects With	Third-Party Incident Response & Recovery Capabilities	TPM-11	Mechanisms exist to ensure response/recovery planning and testing are conducted with critical suppliers/providers.	5	
GV-6.2-004	N/A	Establish policies and procedures for continuous monitoring of third-party GAI systems in deployment.	Functional	Intersects With	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	5	
GV-6.2-005	N/A	Establish policies and procedures that address GAI data redundancy, including model weights and other system artifacts.	Functional	Intersects With	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.	8	

GV-6.2-005	N/A	Establish policies and procedures that address GAI data redundancy, including model weights and other system artifacts.	Functional	Intersects With	AI & Autonomous Technologies Risk Profiling	AAT-09	Mechanisms exist to document the risks and potential impacts of Artificial Intelligence (AI) and Autonomous Technologies (AAT) that are:
							(1) Designed;
							(2) Developed;
							(3) Deployed;
							(4) Evaluated; and/or
							(5) Used.
								5	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
GV-6.2-005	N/A	Establish policies and procedures that address GAI data redundancy, including model weights and other system artifacts.	Functional	Intersects With	Product Management	TDA-01.1	Mechanisms exist to design and implement product management processes to proactively govern the design, development and production of products and/or services across the System Development Life Cycle (SDLC) to: (1) Improve functionality; (2) Enhance security and resiliency capabilities; (3) Correct security deficiencies; and (4) Conform with applicable statutory, regulatory and/or contractual obligations.	8	
GV-6.2-006	N/A	Establish policies and procedures to test and manage risks related to rollover and fallback technologies for GAI systems, acknowledging that rollover and fallback may include manual processing.	Functional	Intersects With	AI & Autonomous Technologies System Value Chain Fallbacks	AAT-25.1	Mechanisms exist to identify: (1) Over-reliance on third-party data with Artificial Intelligence (AI) and Autonomous Technologies (AAT); and (2) Fallback methods to address the inability to access third-party data, as necessary.	5	
GV-6.2-007	N/A	Review vendor contracts and avoid arbitrary or capricious termination of critical GAI technologies or vendor services and non-standard terms that may amplify or defer liability in unexpected ways and/or contribute to unauthorized data collection by vendors or third-parties (e.g., secondary data use). Consider Clear assignment of liability and responsibility for incidents, GAI system changes over time (e.g., fine-tuning, drift, decay); RequestNotification and disclosure for serious incidents arising from third-party data and systems; Service Level Agreements (SLAs) in vendor contracts that address incident response, response times, and availability of critical support.	Functional	Subset Of	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	10	
GV-6.2-007	N/A	Review vendor contracts and avoid arbitrary or capricious termination of critical GAI technologies or vendor services and non-standard terms that may amplify or defer liability in unexpected ways and/or contribute to unauthorized data collection by vendors or third-parties (e.g., secondary data use). Consider Clear assignment of liability and responsibility for incidents, GAI system changes over time (e.g., fine-tuning, drift, decay); RequestNotification and disclosure for serious incidents arising from third-party data and systems; Service Level Agreements (SLAs) in vendor contracts that address incident response, response times, and availability of critical support.	Functional	Intersects With	Third-Party Contract Requirements	TPM-05	Mechanisms exist to require contractual requirements for cybersecurity & data privacy requirements with third-parties, reflecting the organization's needs to protect its systems, processes and data.	8	
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 includethe specific set or types of users along with their expectations; potential positive and negative impacts of system uses to individuals, communities, organizations, society, and the planet; assumptions and related limitations about AI system purposes, uses, and risks across the development or product AI lifecycle; and related TEVV and system metrics.	Functional	Intersects With	AI & Autonomous Technologies Context Definition	AAT-03	Mechanisms exist to establish and document the context surrounding Artificial Intelligence (AI) and Autonomous Technologies (AAT), including: (1) Intended purposes; (2) Potentially beneficial uses; (3) Context-specific laws and regulations; (4) Norms and expectations; and (5) Prospective settings in which the system(s) will be deployed.	5	
MP-1.1-001	N/A	When identifying intended purposes, consider factors such as internal vs. external use, narrow vs. broad application scope, fine-tuning, and varieties of data sources (e.g., grounding, retrieval-augmented generation).	Functional	Intersects With	AI & Autonomous Technologies Context Definition	AAT-03	Mechanisms exist to establish and document the context surrounding Artificial Intelligence (AI) and Autonomous Technologies (AAT), including: (1) Intended purposes; (2) Potentially beneficial uses; (3) Context-specific laws and regulations; (4) Norms and expectations; and (5) Prospective settings in which the system(s) will be deployed.	5	
MP-1.1-002	N/A	Determine and document the expected and acceptable GAI system context of use in collaboration with socio-cultural and other domain experts, by assessing Assumptions and limitations; Direct value to the organization; Intended operational environment and observed usage patterns; Potential positive and negative impacts to individuals, public safety, groups, communities, organizations, democratic institutions, and the physical environment; Social norms and expectations.	Functional	Intersects With	AI & Autonomous Technologies Context Definition	AAT-03	Mechanisms exist to establish and document the context surrounding Artificial Intelligence (AI) and Autonomous Technologies (AAT), including: (1) Intended purposes; (2) Potentially beneficial uses; (3) Context-specific laws and regulations; (4) Norms and expectations; and (5) Prospective settings in which the system(s) will be deployed.	5	
MP-1.1-002	N/A	Determine and document the expected and acceptable GAI system context of use in collaboration with socio-cultural and other domain experts, by assessing Assumptions and limitations; Direct value to the organization; Intended operational environment and observed usage patterns; Potential positive and negative impacts to individuals, public safety, groups, communities, organizations, democratic institutions, and the physical environment; Social norms and expectations.	Functional	Intersects With	AI & Autonomous Technologies Likelihood & Impact Risk Analysis	AAT-07.2	Mechanisms exist to define the potential likelihood and impact of each identified risk based on expected use and past uses of Artificial Intelligence (AI) and Autonomous Technologies (AAT) in similar contexts.	5	
MP-1.1-003	N/A	Document risk measurement plans to address identified risks. Plans may include, as applicable Individual and group cognitive biases (e.g., confirmation bias, funding bias, groupthink) for AI Actors involved in the design, implementation, and use of GAI systems; Known past GAI system incidents and failure modes; In-context use and foreseeable misuse, abuse, and off-label use; Over reliance on quantitative metrics and methodologies without sufficient awareness of their limitations in the context(s) of use; Standard measurement and structured human feedback approaches; Anticipated human-AI configurations.	Functional	Intersects With	AI & Autonomous Technologies Risk Management Decisions	AAT-07	Mechanisms exist to leverage decision makers from a diversity of demographics, disciplines, experience, expertise and backgrounds for mapping, measuring and managing Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related risks.	5	

MP-1.1-003	N/A	Document risk measurement plans to address identified risks. Plans may include, as applicable Individual and group cognitive biases (e.g., confirmation bias, funding bias, groupthink) for AI Actors involved in the design, implementation, and use of GAI systems; Known past GAI system incidents and failure modes; In-context use and foreseeable misuse, abuse, and off-label use; Over reliance on quantitative metrics and methodologies without sufficient awareness of their limitations in the context(s) of use; Standard measurement and structured human feedback approaches; Anticipated human-AI configurations.	Functional	Intersects With	AI & Autonomous Technologies Risk Profiling	AAT-09	Mechanisms exist to document the risks and potential impacts of Artificial Intelligence (AI) and Autonomous Technologies (AAT) that are:
							(1) Designed;
							(2) Developed;
							(3) Deployed;
							(4) Evaluated; and/or
							(5) Used.
								5	

MP-1.1-004	N/A	Identify and document foreseeable illegal uses or applications of the GAI system that surpass organizational risk tolerances.	Functional	Intersects With	AI & Autonomous Technologies Risk Mapping	AAT-02.1	Mechanisms exist to identify Artificial Intelligence (AI) and Autonomous Technologies (AAT) in use and map those components to potential legal risks, including statutory and regulatory compliance requirements.	5	

MP-1.1-004	N/A	Identify and document foreseeable illegal uses or applications of the GAI system that surpass organizational risk tolerances.	Functional	Intersects With	AI & Autonomous Technologies Risk Profiling	AAT-09	Mechanisms exist to document the risks and potential impacts of Artificial Intelligence (AI) and Autonomous Technologies (AAT) that are:
							(1) Designed;
							(2) Developed;
							(3) Deployed;
							(4) Evaluated; and/or
							(5) Used.
								8	

MP-1.1-004	N/A	Identify and document foreseeable illegal uses or applications of the GAI system that surpass organizational risk tolerances.	Functional	Intersects With	AI & Autonomous Technologies Output Filtering	AAT-27	Mechanisms exist to prevent Artificial Intelligence (AI) and Autonomous Technologies (AAT) from generating content that is:
							(1) Inappropriate;
							(2) Harmful;
							(3) False;
							(4) Illegal; and/or
							(5) Violent.
								8	

MP-1.1-004	N/A	Identify and document foreseeable illegal uses or applications of the GAI system that surpass organizational risk tolerances.	Functional	Subset Of	Product Management	TDA-01.1	Mechanisms exist to design and implement product management processes to proactively govern the design, development and production of products and/or services across the System Development Life Cycle (SDLC) to: (1) Improve functionality; (2) Enhance security and resiliency capabilities; (3) Correct security deficiencies; and (4) Conform with applicable statutory, regulatory and/or contractual obligations.	10	
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 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	
MP-1.2-001	N/A	Establish and empower interdisciplinary teams that reflect a wide range of capabilities, competencies, demographic groups, domain expertise, educational backgrounds, lived experiences, professions, and skills across the enterprise to inform and conduct risk measurement and management functions.	Functional	Intersects With	AI & Autonomous Technologies Risk Management Decisions	AAT-07	Mechanisms exist to leverage decision makers from a diversity of demographics, disciplines, experience, expertise and backgrounds for mapping, measuring and managing Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related risks.	5	

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)
MP-1.2-002	N/A	Verify that data or benchmarks used in risk measurement, and users, participants, or subjects involved in structured GAI public feedback exercises are representative of diverse in-context user populations.	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	
MP-1.2-002	N/A	Verify that data or benchmarks used in risk measurement, and users, participants, or subjects involved in structured GAI public feedback exercises are representative of diverse in-context user populations.	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.	5	
MAP 2.1	N/A	The specific tasks and methods used to implement the tasks that the AI system will support are defined (e.g., classifiers, generative models, recommenders).	Functional	Intersects With	AI & Autonomous Technologies Implementation Tasks Definition	AAT-14.1	Mechanisms exist to define the tasks that Artificial Intelligence (AI) and Autonomous Technologies (AAT) will support (e.g., classifiers, generative models, recommenders).	5	
MP-2.1-001	N/A	Establish known assumptions and practices for determining data origin and content lineage, for documentation and evaluation purposes.	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.	3	
MP-2.1-001	N/A	Establish known assumptions and practices for determining data origin and content lineage, for documentation and evaluation purposes.	Functional	Subset Of	Data Source Identification	AAT-12.1	Mechanisms exist to identify and document data sources utilized in the training and/or operation of Artificial Intelligence and Autonomous Technologies (AAT).	10	
MP-2.1-001	N/A	Establish known assumptions and practices for determining data origin and content lineage, for documentation and evaluation purposes.	Functional	Intersects With	Data Source Lineage & Origin Disclosure	AAT-12.3	Mechanisms exist to ensure Artificial Intelligence and Autonomous Technologies (AAT) publicly disclose information with sufficient detail to assess: (1) Content lineage; and (2) The origin of data used by the AAT.	5	
MP-2.1-002	N/A	Institute test and evaluation for data and content flows within the GAI system, including but not limited to, original data sources, data transformations, and decision-making criteria.	Functional	Intersects With	Data Source Identification	AAT-12.1	Mechanisms exist to identify and document data sources utilized in the training and/or operation of Artificial Intelligence and Autonomous Technologies (AAT).	5	
MP-2.1-002	N/A	Institute test and evaluation for data and content flows within the GAI system, including but not limited to, original data sources, data transformations, and decision-making criteria.	Functional	Intersects With	Data Source Integrity	AAT-12.2	Mechanisms exist to protect the integrity of source data to prevent accidental contamination or malicious corruption (e.g., data poisoning) that could compromise the performance of Artificial Intelligence and Autonomous Technologies (AAT).	5	
MAP 2.2	N/A	Information about the AI system's knowledge limits and how system output may be utilized and overseen by humans is documented. Documentation provides sufficient information to assist relevant AI Actors when making decisions and taking subsequent actions.	Functional	Intersects With	AI & Autonomous Technologies Knowledge Limits	AAT-14.2	Mechanisms exist to identify and document knowledge limits of Artificial Intelligence (AI) and Autonomous Technologies (AAT) to provide sufficient information to assist relevant stakeholder decision making.	5	
MP-2.2-001	N/A	Identify and document how the system relies on upstream data sources, including for content provenance, and if it serves as an upstream dependency for other systems.	Functional	Intersects With	Data Source Identification	AAT-12.1	Mechanisms exist to identify and document data sources utilized in the training and/or operation of Artificial Intelligence and Autonomous Technologies (AAT).	5	
MP-2.2-002	N/A	Observe and analyze how the GAI system interacts with external networks, and identify any potential for negative externalities, particularly where content provenance might be compromised.	Functional	Intersects With	AI & Autonomous Technologies Transparency	AAT-20.1	Mechanisms exist to ensure Artificial Intelligence (AI) and Autonomous Technologies (AAT) are designed and developed so its operation is sufficiently transparent such that output can be easily interpreted by personnel implementing the AAT.	8	
MP-2.2-002	N/A	Observe and analyze how the GAI system interacts with external networks, and identify any potential for negative externalities, particularly where content provenance might be compromised.	Functional	Intersects With	External System Connections	NET-05.1	Mechanisms exist to prohibit the direct connection of a sensitive system to an external network without the use of an organization-defined boundary protection device.	5	
MAP 2.3	N/A	Scientific integrity and TEVV considerations are identified and documented, including those related to experimental design, data collection and selection (e.g., availability, representativeness, suitability), system trustworthiness, and construct validation	Functional	Intersects With	Artificial Intelligence Test, Evaluation, Validation & Verification (AI TEVV)	AAT-10	Mechanisms exist to implement Artificial Intelligence Test, Evaluation, Validation & Verification (AI TEVV) practices to enable Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related security, resilience and compliance-related conformity testing throughout the lifecycle of the AAT.	5	
MAP 2.3	N/A	Scientific integrity and TEVV considerations are identified and documented, including those related to experimental design, data collection and selection (e.g., availability, representativeness, suitability), system trustworthiness, and construct validation	Functional	Intersects With	Data Source Integrity	AAT-12.2	Mechanisms exist to protect the integrity of source data to prevent accidental contamination or malicious corruption (e.g., data poisoning) that could compromise the performance of Artificial Intelligence and Autonomous Technologies (AAT).	5	
MP-2.3-001	N/A	Assess the accuracy, quality, reliability, and authenticity of GAI output by comparing it to a set of known ground truth data and by using a variety of evaluation methods (e.g., human oversight and automated evaluation, proven cryptographic techniques, review of content inputs).	Functional	Intersects With	AI & Autonomous Technologies Domain Expert Reviews	AAT-16.5	Mechanisms exist to utilize input from domain experts and relevant stakeholders to validate whether the Artificial Intelligence (AI) and Autonomous Technologies (AAT) perform consistently, as intended.	5	
MP-2.3-002	N/A	Review and document accuracy, representativeness, relevance, suitability of data used at different stages of AI life cycle.	Functional	Intersects With	AI TEVV Post-Deployment Monitoring	AAT-10.13	Mechanisms exist to proactively and continuously monitor deployed Artificial Intelligence (AI) and Autonomous Technologies (AAT).	5	
MP-2.3-003	N/A	Deploy and document fact-checking techniques to verify the accuracy and veracity of information generated by GAI systems, especially when the information comes from multiple (or unknown) sources.	Functional	Intersects With	AI & Autonomous Technologies Testing Techniques	AAT-26	Mechanisms exist to develop and implement fact-checking techniques to verify the accuracy and veracity of information generated by Artificial Intelligence (AI) and Autonomous Technologies (AAT).	5	
MP-2.3-004	N/A	Develop and implement testing techniques to identify GAI produced content (e.g., synthetic media) that might be indistinguishable from human-generated content.	Functional	Intersects With	Generative Artificial Intelligence (GAI) Identification	AAT-26.1	Mechanisms exist to develop and implement testing techniques to identify Generative Artificial Intelligence (GAI) produced content (e.g., synthetic media).	5	
MP-2.3-005	N/A	Implement plans for GAI systems to undergo regular adversarial testing to identify vulnerabilities and potential manipulation or misuse.	Functional	Subset Of	Artificial Intelligence Test, Evaluation, Validation & Verification (AI TEVV)	AAT-10	Mechanisms exist to implement Artificial Intelligence Test, Evaluation, Validation & Verification (AI TEVV) practices to enable Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related security, resilience and compliance-related conformity testing throughout the lifecycle of the AAT.	10	
MAP 3.4	N/A	Processes for operator and practitioner proficiency with AI system performance and trustworthiness – and relevant technical standards and certifications – are defined, assessed, and documented.	Functional	Intersects With	AI 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.	5	
MP-3.4-001	N/A	Evaluate whether GAI operators and end-users can accurately understand content lineage and origin.	Functional	Subset Of	Data Source Lineage & Origin Disclosure	AAT-12.3	Mechanisms exist to ensure Artificial Intelligence and Autonomous Technologies (AAT) publicly disclose information with sufficient detail to assess: (1) Content lineage; and (2) The origin of data used by the AAT.	10	
MP-3.4-002	N/A	Adapt existing training programs to include modules on digital content transparency.	Functional	Intersects With	Maintaining Workforce Development Relevancy	SAT-01.1	Mechanisms exist to periodically review security workforce development and awareness training to account for changes to: (1) Organizational policies, standards and procedures; (2) Assigned roles and responsibilities; (3) Relevant threats and risks; and (4) Technological developments.	8	
MP-3.4-003	N/A	Develop certification programs that test proficiency in managing GAI risks and interpreting content provenance, relevant to specific industry and context.	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	
MP-3.4-003	N/A	Develop certification programs that test proficiency in managing GAI risks and interpreting content provenance, relevant to specific industry and context.	Functional	Intersects With	Conformity Assessment	CPL-01.4	Mechanisms exist to conduct assessments to demonstrate conformity with applicable cybersecurity and data protection laws, regulations and/or contractual obligations.	8	
MP-3.4-003	N/A	Develop certification programs that test proficiency in managing GAI risks and interpreting content provenance, relevant to specific industry and context.	Functional	Intersects With	Product Management	TDA-01.1	Mechanisms exist to design and implement product management processes to proactively govern the design, development and production of products and/or services across the System Development Life Cycle (SDLC) to: (1) Improve functionality; (2) Enhance security and resiliency capabilities; (3) Correct security deficiencies; and (4) Conform with applicable statutory, regulatory and/or contractual obligations.	8	
MP-3.4-004	N/A	Delineate human proficiency tests from tests of GAI capabilities.	Functional	Intersects With	AI & Autonomous Technologies Capabilities Testing	AAT-26.2	Mechanisms exist to delineate human proficiency tests from tests of Artificial Intelligence (AI) and Autonomous Technologies (AAT) capabilities.	5	
MP-3.4-005	N/A	Implement systems to continually monitor and track the outcomes of human-GAI configurations for future refinement and improvements.	Functional	Intersects With	Assigned Responsibilities for AI & Autonomous Technologies	AAT-08	Mechanisms exist to define and differentiate roles and responsibilities for: (1) Artificial Intelligence (AI) and Autonomous Technologies (AAT) configurations; and (2) Oversight of AAT systems.	5	
MP-3.4-006	N/A	Involve the end-users, practitioners, and operators in GAI system in prototyping and testing activities. Make sure these tests cover various scenarios, such as crisis situations or ethically sensitive contexts.	Functional	Intersects With	Real-World Testing	AAT-26.3	Mechanisms exist to include relevant end-users, practitioners and operators in Artificial Intelligence (AI) and Autonomous Technologies (AAT) prototyping and testing activities to cover: (1) Applicable use case scenarios; (2) Crisis situations; and/or (3) Ethically sensitive contexts.	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
MAP 4.1	N/A	Approaches for mapping AI technology and legal risks of its components – including the use of third-party data or software – are in place, followed, and documented, as are risks of infringement of a third-party's intellectual property or other rights.	Functional	Intersects With	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.	5	
MAP 4.1	N/A	Approaches for mapping AI technology and legal risks of its components – including the use of third-party data or software – are in place, followed, and documented, as are risks of infringement of a third-party's intellectual property or other rights.	Functional	Intersects With	AI & Autonomous Technologies Risk Mapping	AAT-02.1	Mechanisms exist to identify Artificial Intelligence (AI) and Autonomous Technologies (AAT) in use and map those components to potential legal risks, including statutory and regulatory compliance requirements.	5	
MP-4.1-001	N/A	Conduct periodic monitoring of AI-generated content for privacy risks; address any possible instances of PII or sensitive data exposure.	Functional	Intersects With	AI TEVV Post-Deployment Monitoring	AAT-10.13	Mechanisms exist to proactively and continuously monitor deployed Artificial Intelligence (AI) and Autonomous Technologies (AAT).	5	
MP-4.1-001	N/A	Conduct periodic monitoring of AI-generated content for privacy risks; address any possible instances of PII or sensitive data exposure.	Functional	Intersects With	Security of Personal Data (PD)	PRI-01.6	Mechanisms exist to ensure Personal Data (PD) is protected by logical and physical security safeguards that are sufficient and appropriately scoped to protect the confidentiality and integrity of the PD.	5	
MP-4.1-002	N/A	Implement processes for responding to potential intellectual property infringement claims or other rights.	Functional	Intersects With	AI & Autonomous Technologies Intellectual Property Infringement Protections	AAT-12	Mechanisms exist to prevent third-party Intellectual Property (IP) rights infringement by Artificial Intelligence (AI) and Autonomous Technologies (AAT).	5	
MP-4.1-003	N/A	Connect new GAI policies, procedures, and processes to existing model, data, software development, and IT governance and to legal, compliance, and risk management activities.	Functional	Intersects With	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.	5	
MP-4.1-003	N/A	Connect new GAI policies, procedures, and processes to existing model, data, software development, and IT governance and to legal, compliance, and risk management activities.	Functional	Intersects With	Technical Documentation Artifacts	TDA-22	Mechanisms exist to generate appropriate technical documentation artifacts for products and/or services in sufficient detail to demonstrate conformity with applicable statutory, regulatory and contractual compliance requirements.	3	
MP-4.1-004	N/A	Document training data curation policies, to the extent possible and according to applicable laws and policies.	Functional	Intersects With	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.	5	
MP-4.1-005	N/A	Establish policies for collection, retention, and minimum quality of data, in consideration of the following risks Disclosure of inappropriate CBRN information; Use of Illegal or dangerous content; Offensive cyber capabilities; Training data imbalances that could give rise to harmful biases; Leak of personally identifiable information, including facial likenesses of individuals.	Functional	Intersects With	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.	5	
MP-4.1-005	N/A	Establish policies for collection, retention, and minimum quality of data, in consideration of the following risks Disclosure of inappropriate CBRN information; Use of Illegal or dangerous content; Offensive cyber capabilities; Training data imbalances that could give rise to harmful biases; Leak of personally identifiable information, including facial likenesses of individuals.	Functional	Intersects With	AI TEVV Fairness & Bias Assessment	AAT-10.8	Mechanisms exist to examine fairness and bias of Artificial Intelligence (AI) and Autonomous Technologies (AAT) to be deployed.	5	
MP-4.1-006	N/A	Implement policies and practices defining how third-party intellectual property and training data will be used, stored, and protected.	Functional	Intersects With	AI & Autonomous Technologies Intellectual Property Infringement Protections	AAT-12	Mechanisms exist to prevent third-party Intellectual Property (IP) rights infringement by Artificial Intelligence (AI) and Autonomous Technologies (AAT).	5	
MP-4.1-006	N/A	Implement policies and practices defining how third-party intellectual property and training data will be used, stored, and protected.	Functional	Intersects With	Data Source Integrity	AAT-12.2	Mechanisms exist to protect the integrity of source data to prevent accidental contamination or malicious corruption (e.g., data poisoning) that could compromise the performance of Artificial Intelligence and Autonomous Technologies (AAT).	5	
MP-4.1-007	N/A	Re-evaluate models that were fine-tuned or enhanced on top of third-party models.	Functional	Intersects With	Artificial Intelligence Test, Evaluation, Validation & Verification (AI TEVV)	AAT-10	Mechanisms exist to implement Artificial Intelligence Test, Evaluation, Validation & Verification (AI TEVV) practices to enable Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related security, resilience and compliance-related conformity testing throughout the lifecycle of the AAT.	5	
MP-4.1-008	N/A	Re-evaluate risks when adapting GAI models to new domains. Additionally, establish warning systems to determine if a GAI system is being used in a new domain where previous assumptions (relating to context of use or mapped risks such as security, and safety) may no longer hold.	Functional	Intersects With	AI & Autonomous Technologies Likelihood & Impact Risk Analysis	AAT-07.2	Mechanisms exist to define the potential likelihood and impact of each identified risk based on expected use and past uses of Artificial Intelligence (AI) and Autonomous Technologies (AAT) in similar contexts.	5	
MP-4.1-008	N/A	Re-evaluate risks when adapting GAI models to new domains. Additionally, establish warning systems to determine if a GAI system is being used in a new domain where previous assumptions (relating to context of use or mapped risks such as security, and safety) may no longer hold.	Functional	Intersects With	Artificial Intelligence Test, Evaluation, Validation & Verification (AI TEVV)	AAT-10	Mechanisms exist to implement Artificial Intelligence Test, Evaluation, Validation & Verification (AI TEVV) practices to enable Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related security, resilience and compliance-related conformity testing throughout the lifecycle of the AAT.	5	
MP-4.1-009	N/A	Leverage approaches to detect the presence of PII or sensitive data in generated output text, image, video, or audio.	Functional	Intersects With	AI & Autonomous Technologies Output Marking	AAT-23	Mechanisms exist to mark output from Artificial Intelligence (AI) and Autonomous Technologies (AAT) in a machine-readable format so it is detectable as artificially generated or manipulated.	3	

MP-4.1-009	N/A	Leverage approaches to detect the presence of PII or sensitive data in generated output text, image, video, or audio.	Functional	Intersects With	AI & Autonomous Technologies Output Filtering	AAT-27	Mechanisms exist to prevent Artificial Intelligence (AI) and Autonomous Technologies (AAT) from generating content that is:
							(1) Inappropriate;
							(2) Harmful;
							(3) False;
							(4) Illegal; and/or
							(5) Violent.
								3	

MP-4.1-009	N/A	Leverage approaches to detect the presence of PII or sensitive data in generated output text, image, video, or audio.	Functional	Intersects With	Information Output Filtering	SEA-09	Mechanisms exist to validate information output from software programs and/or applications to ensure that the information is consistent with the expected content.	8	
MP-4.1-010	N/A	Conduct appropriate diligence on training data use to assess intellectual property, and privacy, risks, including to examine whether use of proprietary or sensitive training data is consistent with applicable laws.	Functional	Intersects With	Technical Documentation Artifacts	TDA-22	Mechanisms exist to generate appropriate technical documentation artifacts for products and/or services in sufficient detail to demonstrate conformity with applicable statutory, regulatory and contractual compliance requirements.	3	
MP-4.1-010	N/A	Conduct appropriate diligence on training data use to assess intellectual property, and privacy, risks, including to examine whether use of proprietary or sensitive training data is consistent with applicable laws.	Functional	Intersects With	AI & Autonomous Technologies Intellectual Property Infringement Protections	AAT-12	Mechanisms exist to prevent third-party Intellectual Property (IP) rights infringement by Artificial Intelligence (AI) and Autonomous Technologies (AAT).	5	
MAP 5.1	N/A	Likelihood and magnitude of each identified impact (both potentially beneficial and harmful) based on expected use, past uses of AI systems in similar contexts, public incident reports, feedback from those external to the team that developed or deployed the AI system, or other data are identified and documented.	Functional	Intersects With	AI & Autonomous Technologies Impact Assessment	AAT-07.1	Mechanisms exist to assess the impact(s) of proposed Artificial Intelligence (AI) and Autonomous Technologies (AAT) on individuals, groups, communities, organizations and society (e.g., Fundamental Rights Impact Assessment (FRIA)).	5	
MAP 5.1	N/A	Likelihood and magnitude of each identified impact (both potentially beneficial and harmful) based on expected use, past uses of AI systems in similar contexts, public incident reports, feedback from those external to the team that developed or deployed the AI system, or other data are identified and documented.	Functional	Intersects With	AI & Autonomous Technologies Likelihood & Impact Risk Analysis	AAT-07.2	Mechanisms exist to define the potential likelihood and impact of each identified risk based on expected use and past uses of Artificial Intelligence (AI) and Autonomous Technologies (AAT) in similar contexts.	5	
MP-5.1-001	N/A	Apply TEVV practices for content provenance (e.g., probing a system's synthetic data generation capabilities for potential misuse or vulnerabilities.	Functional	Intersects With	Artificial Intelligence Test, Evaluation, Validation & Verification (AI TEVV)	AAT-10	Mechanisms exist to implement Artificial Intelligence Test, Evaluation, Validation & Verification (AI TEVV) practices to enable Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related security, resilience and compliance-related conformity testing throughout the lifecycle of the AAT.	5	
MP-5.1-002	N/A	Identify potential content provenance harms of GAI, such as misinformation or disinformation, deepfakes, including NCII, or tampered content. Enumerate and rank risks based on their likelihood and potential impact, and determine how well provenance solutions address specific risks and/or harms.	Functional	Intersects With	AI & Autonomous Technologies Risk Management Decisions	AAT-07	Mechanisms exist to leverage decision makers from a diversity of demographics, disciplines, experience, expertise and backgrounds for mapping, measuring and managing Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related risks.	8	
MP-5.1-002	N/A	Identify potential content provenance harms of GAI, such as misinformation or disinformation, deepfakes, including NCII, or tampered content. Enumerate and rank risks based on their likelihood and potential impact, and determine how well provenance solutions address specific risks and/or harms.	Functional	Intersects With	AI & Autonomous Technologies Likelihood & Impact Risk Analysis	AAT-07.2	Mechanisms exist to define the potential likelihood and impact of each identified risk based on expected use and past uses of Artificial Intelligence (AI) and Autonomous Technologies (AAT) in similar contexts.	8	
MP-5.1-002	N/A	Identify potential content provenance harms of GAI, such as misinformation or disinformation, deepfakes, including NCII, or tampered content. Enumerate and rank risks based on their likelihood and potential impact, and determine how well provenance solutions address specific risks and/or harms.	Functional	Intersects With	Data Source Identification	AAT-12.1	Mechanisms exist to identify and document data sources utilized in the training and/or operation of Artificial Intelligence and Autonomous Technologies (AAT).	8	
MP-5.1-002	N/A	Identify potential content provenance harms of GAI, such as misinformation or disinformation, deepfakes, including NCII, or tampered content. Enumerate and rank risks based on their likelihood and potential impact, and determine how well provenance solutions address specific risks and/or harms.	Functional	Intersects With	Data Source Lineage & Origin Disclosure	AAT-12.3	Mechanisms exist to ensure Artificial Intelligence and Autonomous Technologies (AAT) publicly disclose information with sufficient detail to assess: (1) Content lineage; and (2) The origin of data used by the AAT.	3	

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)
MP-5.1-002	N/A	Identify potential content provenance harms of GAI, such as misinformation or disinformation, deepfakes, including NCII, or tampered content. Enumerate and rank risks based on their likelihood and potential impact, and determine how well provenance solutions address specific risks and/or harms.	Functional	Intersects With	AI TEVV Benchmarking Content Provenance	AAT-10.17	Mechanisms exist to benchmark the verifiable lineage and origin of content used by Artificial Intelligence (AI) and Autonomous Technologies (AAT) according to industry -recognized standards.	3	
MP-5.1-003	N/A	Consider disclosing use of GAI to end users in relevant contexts, while considering the objective of disclosure, the context of use, the likelihood and magnitude of the risk posed, the audience of the disclosure, as well as the frequency of the disclosures.	Functional	Intersects With	AI & Autonomous Technologies Use Notification To Employees	AAT-22.7	Mechanisms exist to ensure employees, including workers' representatives, are informed about Artificial Intelligence (AI) and Autonomous Technologies (AAT) deployments, prior to the use of the AAT in a production environment.	8	
MP-5.1-003	N/A	Consider disclosing use of GAI to end users in relevant contexts, while considering the objective of disclosure, the context of use, the likelihood and magnitude of the risk posed, the audience of the disclosure, as well as the frequency of the disclosures.	Functional	Intersects With	AI & Autonomous Technologies Use Notification To Users	AAT-22.8	Mechanisms exist to ensure Artificial Intelligence (AI) and Autonomous Technologies (AAT) that make decisions, or assist in making decisions, inform the people in a clear manner that they are: (1) Utilizing an AAT solution; and (2) Expected to validate the output for relevance and accuracy.	8	
MP-5.1-004	N/A	Prioritize GAI structured public feedback processes based on risk assessment estimates.	Functional	Intersects With	Robust Stakeholder Engagement for AI & Autonomous Technologies	AAT-11	Mechanisms exist to compel ongoing engagement with relevant Artificial Intelligence (AI) and Autonomous Technologies (AAT) stakeholders to encourage feedback about positive, negative and unanticipated impacts.	5	
MP-5.1-004	N/A	Prioritize GAI structured public feedback processes based on risk assessment estimates.	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.	5	
MP-5.1-005	N/A	Conduct adversarial role-playing exercises, GAI red-teaming, or chaos testing to identify anomalous or unforeseen failure modes.	Functional	Intersects With	Red Team Exercises	VPM-10	Mechanisms exist to utilize "red team" exercises to simulate attempts by adversaries to compromise systems and applications in accordance with organization-defined rules of engagement.	5	
MP-5.1-006	N/A	Profile threats and negative impacts arising from GAI systems interacting with, manipulating, or generating content, and outlining known and potential vulnerabilities and the likelihood of their occurrence.	Functional	Intersects With	AI & Autonomous Technologies Likelihood & Impact Risk Analysis	AAT-07.2	Mechanisms exist to define the potential likelihood and impact of each identified risk based on expected use and past uses of Artificial Intelligence (AI) and Autonomous Technologies (AAT) in similar contexts.	5	
MAP 5.2	N/A	Practices and personnel for supporting regular engagement with relevant AI Actors and integrating feedback about positive, negative, and unanticipated impacts are in place and documented.	Functional	Intersects With	Robust Stakeholder Engagement for AI & Autonomous Technologies	AAT-11	Mechanisms exist to compel ongoing engagement with relevant Artificial Intelligence (AI) and Autonomous Technologies (AAT) stakeholders to encourage feedback about positive, negative and unanticipated impacts.	5	
MP-5.2-001	N/A	Determine context-based measures to identify if new impacts are present due to the GAI system, including regular engagements with downstream AI Actors to identify and quantify new contexts of unanticipated impacts of GAI systems.	Functional	Intersects With	AI & Autonomous Technologies Impact Assessment	AAT-07.1	Mechanisms exist to assess the impact(s) of proposed Artificial Intelligence (AI) and Autonomous Technologies (AAT) on individuals, groups, communities, organizations and society (e.g., Fundamental Rights Impact Assessment (FRIA)).	5	
MP-5.2-001	N/A	Determine context-based measures to identify if new impacts are present due to the GAI system, including regular engagements with downstream AI Actors to identify and quantify new contexts of unanticipated impacts of GAI systems.	Functional	Intersects With	AI & Autonomous Technologies Risk Tracking Approaches	AAT-18	Mechanisms exist to track Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related risks are difficult to assess using currently available measurement techniques or where metrics are not yet available.	5	
MP-5.2-001	N/A	Determine context-based measures to identify if new impacts are present due to the GAI system, including regular engagements with downstream AI Actors to identify and quantify new contexts of unanticipated impacts of GAI systems.	Functional	Intersects With	AI & Autonomous Technologies Likelihood & Impact Risk Analysis	AAT-07.2	Mechanisms exist to define the potential likelihood and impact of each identified risk based on expected use and past uses of Artificial Intelligence (AI) and Autonomous Technologies (AAT) in similar contexts.	5	
MP-5.2-002	N/A	Plan regular engagements with AI Actors responsible for inputs to GAI systems, including third-party data and algorithms, to review and evaluate unanticipated impacts.	Functional	Intersects With	Robust Stakeholder Engagement for AI & Autonomous Technologies	AAT-11	Mechanisms exist to compel ongoing engagement with relevant Artificial Intelligence (AI) and Autonomous Technologies (AAT) stakeholders to encourage feedback about positive, negative and unanticipated impacts.	5	
MP-5.2-002	N/A	Plan regular engagements with AI Actors responsible for inputs to GAI systems, including third-party data and algorithms, to review and evaluate unanticipated impacts.	Functional	Intersects With	AI & Autonomous Technologies Impact Assessment	AAT-07.1	Mechanisms exist to assess the impact(s) of proposed Artificial Intelligence (AI) and Autonomous Technologies (AAT) on individuals, groups, communities, organizations and society (e.g., Fundamental Rights Impact Assessment (FRIA)).	5	
MEASURE 1.1	N/A	Approaches and metrics for measurement of AI risks enumerated during the MAP function are selected for implementation starting with the most significant AI risks. The risks or trustworthiness characteristics that will not – or cannot – be measured are properly documented.	Functional	Intersects With	AI & Autonomous Technologies Risk Management Decisions	AAT-07	Mechanisms exist to leverage decision makers from a diversity of demographics, disciplines, experience, expertise and backgrounds for mapping, measuring and managing Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related risks.	5	
MEASURE 1.1	N/A	Approaches and metrics for measurement of AI risks enumerated during the MAP function are selected for implementation starting with the most significant AI risks. The risks or trustworthiness characteristics that will not – or cannot – be measured are properly documented.	Functional	Intersects With	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.	5	
MS-1.1-001	N/A	Employ methods to trace the origin and modifications of digital content.	Functional	Intersects With	Digital Content Modification Logging	AAT-12.4	Mechanisms exist to ensure Artificial Intelligence and Autonomous Technologies (AAT): (1) Enable auditing of content modifications; and (2) Generate event logs for content-related changes.	5	
MS-1.1-002	N/A	Integrate tools designed to analyze content provenance and detect data anomalies, verify the authenticity of digital signatures, and identify patterns associated with misinformation or manipulation.	Functional	Intersects With	AI TEVV Benchmarking Content Provenance	AAT-10.17	Mechanisms exist to benchmark the verifiable lineage and origin of content used by Artificial Intelligence (AI) and Autonomous Technologies (AAT) according to industry -recognized standards.	5	
MS-1.1-002	N/A	Integrate tools designed to analyze content provenance and detect data anomalies, verify the authenticity of digital signatures, and identify patterns associated with misinformation or manipulation.	Functional	Intersects With	Real World Testing of AI & Autonomous Technologies	AAT-24	Mechanisms exist to obtain consent from the subjects of testing Artificial Intelligence (AI) and Autonomous Technologies (AAT): (1) Prior to their participation in such testing; and (2) After their having been provided with clear and concise information regarding the testing.	5	
MS-1.1-002	N/A	Integrate tools designed to analyze content provenance and detect data anomalies, verify the authenticity of digital signatures, and identify patterns associated with misinformation or manipulation.	Functional	Intersects With	Anomalous Behavior	MON-16	Mechanisms exist to detect and respond to anomalous behavior that could indicate account compromise or other malicious activities.	8	
MS-1.1-003	N/A	Disaggregate evaluation metrics by demographic factors to identify any discrepancies in how content provenance mechanisms work across diverse populations.	Functional	Intersects With	AI TEVV Tools	AAT-10.2	Mechanisms exist to document test sets, metrics and details about the tools used during Artificial Intelligence Test, Evaluation, Validation & Verification (AI TEVV) practices.	5	
MS-1.1-004	N/A	Develop a suite of metrics to evaluate structured public feedback exercises informed by representative AI Actors.	Functional	Subset Of	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.	5	
MS-1.1-005	N/A	Evaluate novel methods and technologies for the measurement of GAI-related risks including in content provenance, offensive cyber, and CBRN, while maintaining the models' ability to produce valid, reliable, and factually accurate outputs.	Functional	Intersects With	Novel Risk Assessment Methods & Technologies	AAT-17.4	Mechanisms exist to utilize novel methods and technologies for the measurement of Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related risks to evaluate, if applicable: (1) Content provenance; (2) Offensive cyber capabilities; (3) Chemical, Biological, Radiological or Nuclear (CBRN) weapons; and/or (4) Other dangerous materials or agents.	5	
MS-1.1-006	N/A	Implement continuous monitoring of GAI system impacts to identify whether GAI outputs are equitable across various sub-populations. Seek active and direct feedback from affected communities via structured feedback mechanisms or red- teaming to monitor and improve outputs.	Functional	Intersects With	AI TEVV Post-Deployment Monitoring	AAT-10.13	Mechanisms exist to proactively and continuously monitor deployed Artificial Intelligence (AI) and Autonomous Technologies (AAT).	5	
MS-1.1-006	N/A	Implement continuous monitoring of GAI system impacts to identify whether GAI outputs are equitable across various sub-populations. Seek active and direct feedback from affected communities via structured feedback mechanisms or red- teaming to monitor and improve outputs.	Functional	Intersects With	Robust Stakeholder Engagement for AI & Autonomous Technologies	AAT-11	Mechanisms exist to compel ongoing engagement with relevant Artificial Intelligence (AI) and Autonomous Technologies (AAT) stakeholders to encourage feedback about positive, negative and unanticipated impacts.	5	
MS-1.1-007	N/A	Evaluate the quality and integrity of data used in training and the provenance of AI-generated content, for example by employing techniques like chaos engineering and seeking stakeholder feedback.	Functional	Intersects With	Robust Stakeholder Engagement for AI & Autonomous Technologies	AAT-11	Mechanisms exist to compel ongoing engagement with relevant Artificial Intelligence (AI) and Autonomous Technologies (AAT) stakeholders to encourage feedback about positive, negative and unanticipated impacts.	5	
MS-1.1-007	N/A	Evaluate the quality and integrity of data used in training and the provenance of AI-generated content, for example by employing techniques like chaos engineering and seeking stakeholder feedback.	Functional	Intersects With	Data Source Integrity	AAT-12.2	Mechanisms exist to protect the integrity of source data to prevent accidental contamination or malicious corruption (e.g., data poisoning) that could compromise the performance of Artificial Intelligence and Autonomous Technologies (AAT).	5	
MS-1.1-008	N/A	Define use cases, contexts of use, capabilities, and negative impacts where structured human feedback exercises, e.g., GAI red-teaming, would be most beneficial for GAI risk measurement and management based on the context of use.	Functional	Intersects With	Robust Stakeholder Engagement for AI & Autonomous Technologies	AAT-11	Mechanisms exist to compel ongoing engagement with relevant Artificial Intelligence (AI) and Autonomous Technologies (AAT) stakeholders to encourage feedback about positive, negative and unanticipated impacts.	5	
MS-1.1-008	N/A	Define use cases, contexts of use, capabilities, and negative impacts where structured human feedback exercises, e.g., GAI red-teaming, would be most beneficial for GAI risk measurement and management based on the context of use.	Functional	Intersects With	Real-World Testing	AAT-26.3	Mechanisms exist to include relevant end-users, practitioners and operators in Artificial Intelligence (AI) and Autonomous Technologies (AAT) prototyping and testing activities to cover: (1) Applicable use case scenarios; (2) Crisis situations; and/or (3) Ethically sensitive contexts.	8	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
MS-1.1-008	N/A	Define use cases, contexts of use, capabilities, and negative impacts where structured human feedback exercises, e.g., GAI red-teaming, would be most beneficial for GAI risk measurement and management based on the context of use.	Functional	Subset Of	Product Management	TDA-01.1	Mechanisms exist to design and implement product management processes to proactively govern the design, development and production of products and/or services across the System Development Life Cycle (SDLC) to: (1) Improve functionality; (2) Enhance security and resiliency capabilities; (3) Correct security deficiencies; and (4) Conform with applicable statutory, regulatory and/or contractual obligations.	10	
MS-1.1-008	N/A	Define use cases, contexts of use, capabilities, and negative impacts where structured human feedback exercises, e.g., GAI red-teaming, would be most beneficial for GAI risk measurement and management based on the context of use.	Functional	Intersects With	Product Conformity Governance	TDA-21	Mechanisms exist to ensure developed products and/or services conform to applicable statutory and regulatory requirements, based on the product's and/or service's: (1) Use case(s); and (2) Geographic markets.	8	
MS-1.1-008	N/A	Define use cases, contexts of use, capabilities, and negative impacts where structured human feedback exercises, e.g., GAI red-teaming, would be most beneficial for GAI risk measurement and management based on the context of use.	Functional	Intersects With	Red Team Exercises	VPM-10	Mechanisms exist to utilize "red team" exercises to simulate attempts by adversaries to compromise systems and applications in accordance with organization-defined rules of engagement.	3	
MS-1.1-009	N/A	Track and document risks or opportunities related to all GAI risks that cannot be measured quantitatively, including explanations as to why some risks cannot be measured (e.g., due to technological limitations, resource constraints, or trustworthy considerations). Include unmeasured risks in marginal risks.	Functional	Intersects With	Unmeasurable AI & Autonomous Technologies Risks	AAT-16.3	Mechanisms exist to identify and document unmeasurable risks or trustworthiness characteristics.	5	
MEASURE 1.3	N/A	Internal experts who did not serve as front-line developers for the system and/or independent assessors are involved in regular assessments and updates. Domain experts, users, AI Actors external to the team that developed or deployed the AI system, and affected communities are consulted in support of assessments as necessary per organizational risk tolerance.	Functional	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	
MS-1.3-001	N/A	Define relevant groups of interest (e.g., demographic groups, subject matter experts, experience with GAI technology) within the context of use as part of plans for gathering structured public feedback.	Functional	Intersects With	Robust Stakeholder Engagement for AI & Autonomous Technologies	AAT-11	Mechanisms exist to compel ongoing engagement with relevant Artificial Intelligence (AI) and Autonomous Technologies (AAT) stakeholders to encourage feedback about positive, negative and unanticipated impacts.	5	
MS-1.3-002	N/A	Engage in internal and external evaluations, GAI red-teaming, impact assessments, or other structured human feedback exercises in consultation with representative AI Actors with expertise and familiarity in the context of use, and/or who are representative of the populations associated with the context of use.	Functional	Intersects With	AI & Autonomous Technologies Impact Assessment	AAT-07.1	Mechanisms exist to assess the impact(s) of proposed Artificial Intelligence (AI) and Autonomous Technologies (AAT) on individuals, groups, communities, organizations and society (e.g., Fundamental Rights Impact Assessment (FRIA)).	5	
MS-1.3-002	N/A	Engage in internal and external evaluations, GAI red-teaming, impact assessments, or other structured human feedback exercises in consultation with representative AI Actors with expertise and familiarity in the context of use, and/or who are representative of the populations associated with the context of use.	Functional	Subset Of	Artificial Intelligence Test, Evaluation, Validation & Verification (AI TEVV)	AAT-10	Mechanisms exist to implement Artificial Intelligence Test, Evaluation, Validation & Verification (AI TEVV) practices to enable Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related security, resilience and compliance-related conformity testing throughout the lifecycle of the AAT.	10	
MS-1.3-002	N/A	Engage in internal and external evaluations, GAI red-teaming, impact assessments, or other structured human feedback exercises in consultation with representative AI Actors with expertise and familiarity in the context of use, and/or who are representative of the populations associated with the context of use.	Functional	Intersects With	Robust Stakeholder Engagement for AI & Autonomous Technologies	AAT-11	Mechanisms exist to compel ongoing engagement with relevant Artificial Intelligence (AI) and Autonomous Technologies (AAT) stakeholders to encourage feedback about positive, negative and unanticipated impacts.	8	
MS-1.3-002	N/A	Engage in internal and external evaluations, GAI red-teaming, impact assessments, or other structured human feedback exercises in consultation with representative AI Actors with expertise and familiarity in the context of use, and/or who are representative of the populations associated with the context of use.	Functional	Intersects With	Red Team Exercises	VPM-10	Mechanisms exist to utilize "red team" exercises to simulate attempts by adversaries to compromise systems and applications in accordance with organization-defined rules of engagement.	3	
MS-1.3-003	N/A	Verify those conducting structured human feedback exercises are not directly involved in system development tasks for the same GAI model.	Functional	Subset Of	Separation of Duties (SoD)	HRS-11	Mechanisms exist to implement and maintain Separation of Duties (SoD) to prevent potential inappropriate activity without collusion.	10	
MEASURE 2.2	N/A	Evaluations involving human subjects meet applicable requirements (including human subject protection) and are representative of the relevant population.	Functional	Intersects With	AI & Autonomous Technologies Human Subject Protections	AAT-17.1	Mechanisms exist to protect human subjects from harm.	3	
MS-2.2-001	N/A	Assess and manage statistical biases related to GAI content provenance through techniques such as re-sampling, re-weighting, or adversarial training.	Functional	Subset Of	AI & Autonomous Technologies Fairness & Bias	AAT-06	Mechanisms exist to prevent Artificial Intelligence (AI) and Autonomous Technologies (AAT) from unfairly identifying, profiling and/or statistically singling out a segmented population defined by race, religion, gender identity, national origin, religion, disability or any other politically-charged identifier.	10	
MS-2.2-001	N/A	Assess and manage statistical biases related to GAI content provenance through techniques such as re-sampling, re-weighting, or adversarial training.	Functional	Intersects With	AI TEVV Fairness & Bias Assessment	AAT-10.8	Mechanisms exist to examine fairness and bias of Artificial Intelligence (AI) and Autonomous Technologies (AAT) to be deployed.	8	
MS-2.2-001	N/A	Assess and manage statistical biases related to GAI content provenance through techniques such as re-sampling, re-weighting, or adversarial training.	Functional	Intersects With	Data Source Identification	AAT-12.1	Mechanisms exist to identify and document data sources utilized in the training and/or operation of Artificial Intelligence and Autonomous Technologies (AAT).	5	
MS-2.2-002	N/A	Document how content provenance data is tracked and how that data interacts with privacy and security. ConsiderAnonymizing data to protect the privacy of human subjects; Leveraging privacy output filters; Removing any personally identifiable information (PII) to prevent potential harm or misuse.	Functional	Intersects With	Data Source Identification	AAT-12.1	Mechanisms exist to identify and document data sources utilized in the training and/or operation of Artificial Intelligence and Autonomous Technologies (AAT).	5	
MS-2.2-002	N/A	Document how content provenance data is tracked and how that data interacts with privacy and security. ConsiderAnonymizing data to protect the privacy of human subjects; Leveraging privacy output filters; Removing any personally identifiable information (PII) to prevent potential harm or misuse.	Functional	Intersects With	Real World Testing of AI & Autonomous Technologies	AAT-24	Mechanisms exist to obtain consent from the subjects of testing Artificial Intelligence (AI) and Autonomous Technologies (AAT): (1) Prior to their participation in such testing; and (2) After their having been provided with clear and concise information regarding the testing.	5	
MS-2.2-002	N/A	Document how content provenance data is tracked and how that data interacts with privacy and security. ConsiderAnonymizing data to protect the privacy of human subjects; Leveraging privacy output filters; Removing any personally identifiable information (PII) to prevent potential harm or misuse.	Functional	Intersects With	De-Identification (Anonymization)	DCH-23	Mechanisms exist to anonymize data by removing Personal Data (PD) from datasets.	5	
MS-2.2-003	N/A	Provide human subjects with options to withdraw participation or revoke theirconsent for present or future use of their data in GAI applications.	Functional	Intersects With	Revoke Consent	PRI-03.4	Mechanisms exist to allow data subjects to revoke consent to collect, receive, process, store, transmit, update and/or share their Personal Data (PD).	5	
MS-2.2-004	N/A	Use techniques such as anonymization, differential privacy or other privacy-enhancing technologies to minimize the risks associated with linking AI-generated content back to individual human subjects.	Functional	Intersects With	De-Identification (Anonymization)	DCH-23	Mechanisms exist to anonymize data by removing Personal Data (PD) from datasets.	5	
MEASURE 2.3	N/A	AI system performance or assurance criteria are measured qualitatively or quantitatively and demonstrated for conditions similar to deployment setting(s). Measures are documented.	Functional	Intersects With	AI & Autonomous Technologies Implementation Documentation	AAT-20.2	Mechanisms exist to ensure Artificial Intelligence (AI) and Autonomous Technologies (AAT) include clear and concise documentation that is relevant, accessible and comprehensible to personnel implementing and maintaining the AAT that, at a minimum, provides: (1) Contact details of the provider; (2) Characteristics, capabilities and limitations of performance of the AAT; (3) Errata from the AAT's initial conformity assessment; (4) Details necessary to interpret the outputs of the AAT; (5) Human oversight measures necessary to facilitate the interpretation of the outputs of the AAT; (6) Computational and hardware resources needed to operate the AAT; (7) Projected useable lifetime of the AAT; and (8) A description of the mechanisms included within the AAT system to properly collect, store and interpret event logs.	5	
MS-2.3-001	N/A	Consider baseline model performance on suites of benchmarks when selecting a model for fine tuning or enhancement with retrieval-augmented generation.	Functional	Intersects With	System Hardening Through Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for technology platforms that are consistent with industry-accepted system hardening standards.	5	
MS-2.3-002	N/A	Evaluate claims of model capabilities using empirically validated methods.	Functional	Intersects With	AI TEVV Empirically Validated Methods	AAT-10.16	Mechanisms exist to evaluate claims of Artificial Intelligence (AI) and Autonomous Technologies (AAT) model capabilities using empirically validated methods.	10	
MS-2.3-003	N/A	Share results of pre-deployment testing with relevant GAI Actors, such as those with system release approval authority.	Functional	Intersects With	AI TEVV Reporting	AAT-10.15	Mechanisms exist to report the status and results of Artificial Intelligence Test, Evaluation, Validation & Verification (AI TEVV) to relevant stakeholders, including governing bodies, as required.	8	
MS-2.3-004	N/A	Utilize a purpose-built testing environment such as NIST Dioptra to empirically evaluate GAI trustworthy characteristics.	Functional	Subset Of	Secure Development Environments	TDA-07	Mechanisms exist to maintain a segmented development network to ensure a secure development environment.	10	
MEASURE 2.5	N/A	The AI system to be deployed is demonstrated to be valid and reliable. Limitations of the generalizability beyond the conditions under which the technology was developed are documented.	Functional	Intersects With	AI TEVV Trustworthiness Demonstration	AAT-10.3	Mechanisms exist to demonstrate the Artificial Intelligence (AI) and Autonomous Technologies (AAT) to be deployed is valid, reliable and operate as intended based on approved designs.	5	
MS-2.5-001	N/A	Avoid extrapolating GAI system performance or capabilities from narrow, non- systematic, and anecdotal assessments.	Functional	Intersects With	AI TEVV Empirically Validated Methods	AAT-10.16	Mechanisms exist to evaluate claims of Artificial Intelligence (AI) and Autonomous Technologies (AAT) model capabilities using empirically validated methods.	3	

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)

MS-2.5-002	N/A	Document the extent to which human domain knowledge is employed to improve GAI system performance, via, e.g., RLHF, fine-tuning, retrieval-augmented generation, content moderation, business rules.	Functional	Intersects With	AI & Autonomous Technologies Human Domain Knowledge Reliance	AAT-20.3	Mechanisms exist to document the extent to which human domain knowledge is employed to improve Artificial Intelligence (AI) and Autonomous Technologies (AAT) performance including:
							(1) Reinforcement Learning from Human Feedback (RLHF);
							(2) Fine-tuning;
							(3) Retrieval- augmented generation;
							(4) Content moderation; and
							(5) Business rules.
								5	

MS-2.5-003	N/A	Review and verify sources and citations in GAI system outputs during pre-deployment risk measurement and ongoing monitoring activities.	Functional	Intersects With	Data Source Identification	AAT-12.1	Mechanisms exist to identify and document data sources utilized in the training and/or operation of Artificial Intelligence and Autonomous Technologies (AAT).	5	
MS-2.5-003	N/A	Review and verify sources and citations in GAI system outputs during pre-deployment risk measurement and ongoing monitoring activities.	Functional	Intersects With	Real World Testing of AI & Autonomous Technologies	AAT-24	Mechanisms exist to obtain consent from the subjects of testing Artificial Intelligence (AI) and Autonomous Technologies (AAT): (1) Prior to their participation in such testing; and (2) After their having been provided with clear and concise information regarding the testing.	5	
MS-2.5-004	N/A	Track and document instances of anthropomorphization (e.g., human images, mentions of human feelings, cyborg imagery or motifs) in GAI system interfaces.	Functional	Intersects With	Real World Testing of AI & Autonomous Technologies	AAT-24	Mechanisms exist to obtain consent from the subjects of testing Artificial Intelligence (AI) and Autonomous Technologies (AAT): (1) Prior to their participation in such testing; and (2) After their having been provided with clear and concise information regarding the testing.	5	
MS-2.5-005	N/A	Verify GAI system training data and TEVV data provenance, and that fine-tuning or retrieval-augmented generation data is grounded.	Functional	Intersects With	Data Source Identification	AAT-12.1	Mechanisms exist to identify and document data sources utilized in the training and/or operation of Artificial Intelligence and Autonomous Technologies (AAT).	5	
MS-2.5-006	N/A	Regularly review security and safety guardrails, especially if the GAI system is being operated in novel circumstances. This includes reviewing reasons why the GAI system was initially assessed as being safe to deploy.	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	
MEASURE 2.6	N/A	The AI system is evaluated regularly for safety risks – as identified in the MAP function. The AI system to be deployed is demonstrated to be safe, its residual negative risk does not exceed the risk tolerance, and it can fail safely, particularly if made to operate beyond its knowledge limits. Safety metrics reflect system reliability and robustness, real-time monitoring, and response times for AI system failures.	Functional	Subset Of	AI & Autonomous Technologies Production Monitoring	AAT-16	Mechanisms exist to monitor the functionality and behavior of the deployed Artificial Intelligence (AI) and Autonomous Technologies (AAT).	10	
MS-2.6-001	N/A	Assess adverse impacts, including health and wellbeing impacts for value chain or other AI Actors that are exposed to sexually explicit, offensive, or violent information during GAI training and maintenance.	Functional	Intersects With	AI & Autonomous Technologies Human Subject Protections	AAT-17.1	Mechanisms exist to protect human subjects from harm.	5	
MS-2.6-002	N/A	Assess existence or levels of harmful bias, intellectual property infringement, data privacy violations, obscenity, extremism, violence, or CBRN information in system training data.	Functional	Intersects With	AI & Autonomous Technologies Intellectual Property Infringement Protections	AAT-12	Mechanisms exist to prevent third-party Intellectual Property (IP) rights infringement by Artificial Intelligence (AI) and Autonomous Technologies (AAT).	5	
MS-2.6-002	N/A	Assess existence or levels of harmful bias, intellectual property infringement, data privacy violations, obscenity, extremism, violence, or CBRN information in system training data.	Functional	Intersects With	AI & Autonomous Technologies Human Subject Protections	AAT-17.1	Mechanisms exist to protect human subjects from harm.	5	
MS-2.6-002	N/A	Assess existence or levels of harmful bias, intellectual property infringement, data privacy violations, obscenity, extremism, violence, or CBRN information in system training data.	Functional	Intersects With	AI & Autonomous Technologies Environmental Impact & Sustainability	AAT-17.2	Mechanisms exist to assess and document the environmental impacts and sustainability of Artificial Intelligence (AI) and Autonomous Technologies (AAT).	5	
MS-2.6-003	N/A	Re-evaluate safety features of fine-tuned models when the negative risk exceeds organizational risk tolerance.	Functional	Subset Of	Artificial Intelligence Test, Evaluation, Validation & Verification (AI TEVV)	AAT-10	Mechanisms exist to implement Artificial Intelligence Test, Evaluation, Validation & Verification (AI TEVV) practices to enable Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related security, resilience and compliance-related conformity testing throughout the lifecycle of the AAT.	10	
MS-2.6-003	N/A	Re-evaluate safety features of fine-tuned models when the negative risk exceeds organizational risk tolerance.	Functional	Intersects With	AI TEVV Results Evaluation	AAT-10.10	Mechanisms exist to evaluate the results of Artificial Intelligence Test, Evaluation, Validation & Verification (AI TEVV) to determine the viability of the proposed Artificial Intelligence (AI) and Autonomous Technologies (AAT).	8	
MS-2.6-004	N/A	Review GAI system outputs for validity and safetyReview generated code to assess risks that may arise from unreliable downstream decision-making.	Functional	Intersects With	Real World Testing of AI & Autonomous Technologies	AAT-24	Mechanisms exist to obtain consent from the subjects of testing Artificial Intelligence (AI) and Autonomous Technologies (AAT): (1) Prior to their participation in such testing; and (2) After their having been provided with clear and concise information regarding the testing.	5	
MS-2.6-005	N/A	Verify that GAI system architecture can monitor outputs and performance, and handle, recover from, and repair errors when security anomalies, threats and impacts are detected.	Functional	Subset Of	AI & Autonomous Technologies Conformity	AAT-19	Mechanisms exist to ensure deployed Artificial Intelligence (AI) and Autonomous Technologies (AAT) conform to applicable statutory and regulatory requirements, based on: (1) Defined use cases; (2) Geographic markets; and (3) Use of Intellectual Property (IP).	10	
MS-2.6-006	N/A	Verify that systems properly handle queries that may give rise to inappropriate, malicious, or illegal usage, including facilitating manipulation, extortion, targeted impersonation, cyber-attacks, and weapons creation.	Functional	Intersects With	Malformed Input Testing	TDA-09.4	Mechanisms exist to utilize testing methods to ensure systems, services and products continue to operate as intended when subject to invalid or unexpected inputs on its interfaces.	5	
MS-2.6-007	N/A	Regularly evaluate GAI system vulnerabilities to possible circumvention of safety measures.	Functional	Intersects With	Vulnerability Scanning	VPM-06	Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications.	5	
MEASURE 2.7	N/A	AI system security and resilience – as identified in the MAP function – are evaluated and documented.	Functional	Subset Of	AI TEVV Security & Resiliency Assessment	AAT-10.5	Mechanisms exist to evaluate the security and resilience of Artificial Intelligence (AI) and Autonomous Technologies (AAT) to be deployed.	10	
MS-2.7-001	N/A	Apply established security measures to assess likelihood and magnitude of vulnerabilities and threats such as backdoors, compromised dependencies, data breaches, eavesdropping, man-in-the-middle attacks, reverse engineering, autonomous agents, model theft or exposure of model weights, AI inference, bypass, extraction, and other baseline security concerns.	Functional	Intersects With	AI TEVV Security & Resiliency Assessment	AAT-10.5	Mechanisms exist to evaluate the security and resilience of Artificial Intelligence (AI) and Autonomous Technologies (AAT) to be deployed.	5	
MS-2.7-002	N/A	Benchmark GAI system security and resilience related to content provenance against industry standards and best practices. Compare GAI system security features and content provenance methods against industry state-of-the-art.	Functional	Intersects With	AI TEVV Benchmarking Content Provenance	AAT-10.17	Mechanisms exist to benchmark the verifiable lineage and origin of content used by Artificial Intelligence (AI) and Autonomous Technologies (AAT) according to industry -recognized standards.	5	
MS-2.7-003	N/A	Conduct user surveys to gather user satisfaction with the AI-generated content and user perceptions of content authenticity. Analyze user feedback to identify concerns and/or current literacy levels related to content provenance and understanding of labels on content.	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.	5	
MS-2.7-004	N/A	Identify metrics that reflect the effectiveness of security measures, such as data provenance, the number of unauthorized access attempts, inference, bypass, extraction, penetrations, or provenance verification.	Functional	Intersects With	Measures of Performance	GOV-05	Mechanisms exist to develop, report and monitor cybersecurity & data privacy program measures of performance.	3	
MS-2.7-005	N/A	Measure reliability of content authentication methods, such as watermarking, cryptographic signatures, digital fingerprints, as well as access controls, conformity assessment, and model integrity verification, which can help support the effective implementation of content provenance techniques. Evaluate the rate of false positives and false negatives in content provenance, as well as true positives and true negatives for verification.	Functional	Intersects With	AI TEVV Benchmarking Content Provenance	AAT-10.17	Mechanisms exist to benchmark the verifiable lineage and origin of content used by Artificial Intelligence (AI) and Autonomous Technologies (AAT) according to industry -recognized standards.	5	
MS-2.7-005	N/A	Measure reliability of content authentication methods, such as watermarking, cryptographic signatures, digital fingerprints, as well as access controls, conformity assessment, and model integrity verification, which can help support the effective implementation of content provenance techniques. Evaluate the rate of false positives and false negatives in content provenance, as well as true positives and true negatives for verification.	Functional	Intersects With	Data Source Integrity	AAT-12.2	Mechanisms exist to protect the integrity of source data to prevent accidental contamination or malicious corruption (e.g., data poisoning) that could compromise the performance of Artificial Intelligence and Autonomous Technologies (AAT).	5	
MS-2.7-006	N/A	Measure the rate at which recommendations from security checks and incidents are implemented. Assess how quickly the AI system can adapt and improve based on lessons learned from security incidents and feedback.	Functional	Intersects With	Time To Remediate / Benchmarks For Corrective Action	VPM-05.3	Mechanisms exist to track the effectiveness of remediation operations through metrics reporting.	5	
MS-2.7-007	N/A	Perform AI red-teaming to assess resilience against Abuse to facilitate attacks on other systems (e.g., malicious code generation, enhanced phishing content), GAI attacks (e.g., prompt injection), ML attacks (e.g., adversarial examples/prompts, data poisoning, membership inference, model extraction, sponge examples).	Functional	Intersects With	Data Source Integrity	AAT-12.2	Mechanisms exist to protect the integrity of source data to prevent accidental contamination or malicious corruption (e.g., data poisoning) that could compromise the performance of Artificial Intelligence and Autonomous Technologies (AAT).	5	
MS-2.7-007	N/A	Perform AI red-teaming to assess resilience against Abuse to facilitate attacks on other systems (e.g., malicious code generation, enhanced phishing content), GAI attacks (e.g., prompt injection), ML attacks (e.g., adversarial examples/prompts, data poisoning, membership inference, model extraction, sponge examples).	Functional	Intersects With	Red Team Exercises	VPM-10	Mechanisms exist to utilize "red team" exercises to simulate attempts by adversaries to compromise systems and applications in accordance with organization-defined rules of engagement.	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
MS-2.7-008	N/A	Verify fine-tuning does not compromise safety and security controls.	Functional	Intersects With	Fine Tuning Risk Mitigation	AAT-17.5	Mechanisms exist to ensure actions to fine-tune Artificial Intelligence (AI) and Autonomous Technologies (AAT) do not compromise existing safety and/or security controls.	5	
MS-2.7-009	N/A	Regularly assess and verify that security measures remain effective and have not been compromised.	Functional	Intersects With	AI & Autonomous Technologies Ongoing Assessments	AAT-11.2	Mechanisms exist to conduct regular assessments of Artificial Intelligence (AI) and Autonomous Technologies (AAT) with independent assessors and stakeholders not involved in the development of the AAT.	5	
MEASURE 2.8	N/A	Risks associated with transparency and accountability – as identified in the MAP function – are examined and documented.	Functional	Intersects With	AI TEVV Transparency & Accountability Assessment	AAT-10.6	Mechanisms exist to examine risks associated with transparency and accountability of Artificial Intelligence (AI) and Autonomous Technologies (AAT) to be deployed.	5	
MS-2.8-001	N/A	Compile statistics on actual policy violations, take-down requests, and intellectual property infringement for organizational GAI systems Analyze transparency reports across demographic groups, languages groups.	Functional	Intersects With	AI & Autonomous Technologies Risk Management Decisions	AAT-07	Mechanisms exist to leverage decision makers from a diversity of demographics, disciplines, experience, expertise and backgrounds for mapping, measuring and managing Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related risks.	5	
MS-2.8-001	N/A	Compile statistics on actual policy violations, take-down requests, and intellectual property infringement for organizational GAI systems Analyze transparency reports across demographic groups, languages groups.	Functional	Intersects With	AI & Autonomous Technologies Intellectual Property Infringement Protections	AAT-12	Mechanisms exist to prevent third-party Intellectual Property (IP) rights infringement by Artificial Intelligence (AI) and Autonomous Technologies (AAT).	5	
MS-2.8-002	N/A	Document the instructions given to data annotators or AI red-teamers.	Functional	Intersects With	Documenting Testing Guidance	AAT-26.4	Mechanisms exist to document the instructions given to: (1) Data annotators; and/or (2) Artificial Intelligence (AI) and Autonomous Technologies (AAT) red-teamers.	5	
MS-2.8-003	N/A	Use digital content transparency solutions to enable the documentation of each instance where content is generated, modified, or shared to provide a tamper- proof history of the content, promote transparency, and enable traceability.Robust version control systems can also be applied to track changes across the AIlifecycle over time.	Functional	Intersects With	AI & Autonomous Technologies Transparency	AAT-20.1	Mechanisms exist to ensure Artificial Intelligence (AI) and Autonomous Technologies (AAT) are designed and developed so its operation is sufficiently transparent such that output can be easily interpreted by personnel implementing the AAT.	5	
MS-2.8-003	N/A	Use digital content transparency solutions to enable the documentation of each instance where content is generated, modified, or shared to provide a tamper- proof history of the content, promote transparency, and enable traceability.Robust version control systems can also be applied to track changes across the AIlifecycle over time.	Functional	Intersects With	Generative Artificial Intelligence (GAI) Identification	AAT-26.1	Mechanisms exist to develop and implement testing techniques to identify Generative Artificial Intelligence (GAI) produced content (e.g., synthetic media).	8	
MS-2.8-004	N/A	Verify adequacy of GAI system user instructions through user testing.	Functional	Intersects With	AI & Autonomous Technologies Human Subject Protections	AAT-17.1	Mechanisms exist to protect human subjects from harm.	3	
MEASURE 2.9	N/A	The AI model is explained, validated, and documented, and AI system output is interpreted within its context – as identified in the MAP function – to inform responsible use and governance.	Functional	Subset Of	Artificial Intelligence Test, Evaluation, Validation & Verification (AI TEVV)	AAT-10	Mechanisms exist to implement Artificial Intelligence Test, Evaluation, Validation & Verification (AI TEVV) practices to enable Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related security, resilience and compliance-related conformity testing throughout the lifecycle of the AAT.	10	
MEASURE 2.9	N/A	The AI model is explained, validated, and documented, and AI system output is interpreted within its context – as identified in the MAP function – to inform responsible use and governance.	Functional	Intersects With	AI & Autonomous Technologies Transparency	AAT-20.1	Mechanisms exist to ensure Artificial Intelligence (AI) and Autonomous Technologies (AAT) are designed and developed so its operation is sufficiently transparent such that output can be easily interpreted by personnel implementing the AAT.	3	
MS-2.9-001	N/A	Apply and document ML explanation results such as Analysis of embeddings, Counterfactual prompts, Gradient-based attributions, Model compression/surrogate models, Occlusion/term reduction.	Functional	Intersects With	Real World Testing of AI & Autonomous Technologies	AAT-24	Mechanisms exist to obtain consent from the subjects of testing Artificial Intelligence (AI) and Autonomous Technologies (AAT): (1) Prior to their participation in such testing; and (2) After their having been provided with clear and concise information regarding the testing.	5	
MS-2.9-002	N/A	Document GAI model details including Proposed use and organizational value; Assumptions and limitations, Data collection methodologies; Data provenance; Data quality; Model architecture (e.g., convolutional neural network, transformers, etc.); Optimization objectives; Training algorithms; RLHF approaches; Fine-tuning or retrieval-augmented generation approaches; Evaluation data; Ethical considerations; Legal and regulatory requirements.	Functional	Intersects With	AI & Autonomous Technologies-Related Legal Requirements Definition	AAT-01.1	Mechanisms exist to identify, understand, document and manage applicable statutory and regulatory requirements for Artificial Intelligence (AI) and Autonomous Technologies (AAT).	3	
MS-2.9-002	N/A	Document GAI model details including Proposed use and organizational value; Assumptions and limitations, Data collection methodologies; Data provenance; Data quality; Model architecture (e.g., convolutional neural network, transformers, etc.); Optimization objectives; Training algorithms; RLHF approaches; Fine-tuning or retrieval-augmented generation approaches; Evaluation data; Ethical considerations; Legal and regulatory requirements.	Functional	Intersects With	AI & Autonomous Technologies Potential Benefits Analysis	AAT-04.1	Mechanisms exist to assess the potential benefits of proposed Artificial Intelligence (AI) and Autonomous Technologies (AAT).	3	
MS-2.9-002	N/A	Document GAI model details including Proposed use and organizational value; Assumptions and limitations, Data collection methodologies; Data provenance; Data quality; Model architecture (e.g., convolutional neural network, transformers, etc.); Optimization objectives; Training algorithms; RLHF approaches; Fine-tuning or retrieval-augmented generation approaches; Evaluation data; Ethical considerations; Legal and regulatory requirements.	Functional	Subset Of	Artificial Intelligence Test, Evaluation, Validation & Verification (AI TEVV)	AAT-10	Mechanisms exist to implement Artificial Intelligence Test, Evaluation, Validation & Verification (AI TEVV) practices to enable Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related security, resilience and compliance-related conformity testing throughout the lifecycle of the AAT.	10	
MS-2.9-002	N/A	Document GAI model details including Proposed use and organizational value; Assumptions and limitations, Data collection methodologies; Data provenance; Data quality; Model architecture (e.g., convolutional neural network, transformers, etc.); Optimization objectives; Training algorithms; RLHF approaches; Fine-tuning or retrieval-augmented generation approaches; Evaluation data; Ethical considerations; Legal and regulatory requirements.	Functional	Intersects With	AI & Autonomous Technologies Implementation Documentation	AAT-20.2	Mechanisms exist to ensure Artificial Intelligence (AI) and Autonomous Technologies (AAT) include clear and concise documentation that is relevant, accessible and comprehensible to personnel implementing and maintaining the AAT that, at a minimum, provides: (1) Contact details of the provider; (2) Characteristics, capabilities and limitations of performance of the AAT; (3) Errata from the AAT's initial conformity assessment; (4) Details necessary to interpret the outputs of the AAT; (5) Human oversight measures necessary to facilitate the interpretation of the outputs of the AAT; (6) Computational and hardware resources needed to operate the AAT; (7) Projected useable lifetime of the AAT; and (8) A description of the mechanisms included within the AAT system to properly collect, store and interpret event logs.	5	
MEASURE 2.10	N/A	Privacy risk of the AI system – as identified in the MAP function – is examined and documented.	Functional	Subset Of	AI TEVV Privacy Assessment	AAT-10.7	Mechanisms exist to examine the data privacy risk of Artificial Intelligence (AI) and Autonomous Technologies (AAT) to be deployed.	10	
MS-2.10-001	N/A	Conduct AI red-teaming to assess issues such as Outputting of training data samples, and subsequent reverse engineering, model extraction, and membership inference risks; Revealing biometric, confidential, copyrighted, licensed, patented, personal, proprietary, sensitive, or trade-marked information; Tracking or revealing location information of users or members of training datasets.	Functional	Intersects With	AI & Autonomous Technologies Conformity	AAT-19	Mechanisms exist to ensure deployed Artificial Intelligence (AI) and Autonomous Technologies (AAT) conform to applicable statutory and regulatory requirements, based on: (1) Defined use cases; (2) Geographic markets; and (3) Use of Intellectual Property (IP).	5	
MS-2.10-001	N/A	Conduct AI red-teaming to assess issues such as Outputting of training data samples, and subsequent reverse engineering, model extraction, and membership inference risks; Revealing biometric, confidential, copyrighted, licensed, patented, personal, proprietary, sensitive, or trade-marked information; Tracking or revealing location information of users or members of training datasets.	Functional	Intersects With	Biometric Categorization	AAT-19.8	Mechanisms exist to prohibit the sale, deployment and/or use of Artificial Intelligence (AI) and Autonomous Technologies (AAT) that categorize a person based on their biometric data to deduce, or infer, the individual's: (1) Race; (2) Political opinions; (3) Trade union membership; (4) Religious or philosophical beliefs; (5) Sex life or sexual orientation; and/or (6) Age.	5	
MS-2.10-001	N/A	Conduct AI red-teaming to assess issues such as Outputting of training data samples, and subsequent reverse engineering, model extraction, and membership inference risks; Revealing biometric, confidential, copyrighted, licensed, patented, personal, proprietary, sensitive, or trade-marked information; Tracking or revealing location information of users or members of training datasets.	Functional	Intersects With	Red Team Exercises	VPM-10	Mechanisms exist to utilize "red team" exercises to simulate attempts by adversaries to compromise systems and applications in accordance with organization-defined rules of engagement.	5	
MS-2.10-002	N/A	Engage directly with end-users and other stakeholders to understand their expectations and concerns regarding content provenance. Use this feedback to guide the design of provenance data-tracking techniques.	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	
MS-2.10-002	N/A	Engage directly with end-users and other stakeholders to understand their expectations and concerns regarding content provenance. Use this feedback to guide the design of provenance data-tracking techniques.	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.	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
MS-2.10-003	N/A	Verify deduplication of GAI training data samples, particularly regarding synthetic data.	Functional	Intersects With	AI TEVV Model Collapse Mitigations	AAT-10.18	Mechanisms exist to mitigate concerns of model collapse by: (1) Assessing the proportion of synthetic to non-synthetic training data; and (2) Verifying training data is not overly homogenous or Artificial Intelligence (AI) and Autonomous Technologies (AAT) system-produced.	3	
MS-2.10-003	N/A	Verify deduplication of GAI training data samples, particularly regarding synthetic data.	Functional	Intersects With	Data Source Identification	AAT-12.1	Mechanisms exist to identify and document data sources utilized in the training and/or operation of Artificial Intelligence and Autonomous Technologies (AAT).	8	
MEASURE 2.11	N/A	Fairness and bias – as identified in the MAP function – are evaluated and results are documented.	Functional	Intersects With	AI TEVV Fairness & Bias Assessment	AAT-10.8	Mechanisms exist to examine fairness and bias of Artificial Intelligence (AI) and Autonomous Technologies (AAT) to be deployed.	5	
MS-2.11-001	N/A	Apply use-case appropriate benchmarks (e.g., Bias Benchmark Questions, Real Hateful or Harmful Prompts, Winogender Schemas15) to quantify systemic bias, stereotyping, denigration, and hateful content in GAI system outputs; Document assumptions and limitations of benchmarks, including any actual or possible training/test data cross contamination, relative to in-context deployment environment.	Functional	Subset Of	AI TEVV Fairness & Bias Assessment	AAT-10.8	Mechanisms exist to examine fairness and bias of Artificial Intelligence (AI) and Autonomous Technologies (AAT) to be deployed.	10	
MS-2.11-001	N/A	Apply use-case appropriate benchmarks (e.g., Bias Benchmark Questions, Real Hateful or Harmful Prompts, Winogender Schemas15) to quantify systemic bias, stereotyping, denigration, and hateful content in GAI system outputs; Document assumptions and limitations of benchmarks, including any actual or possible training/test data cross contamination, relative to in-context deployment environment.	Functional	Intersects With	Real World Testing of AI & Autonomous Technologies	AAT-24	Mechanisms exist to obtain consent from the subjects of testing Artificial Intelligence (AI) and Autonomous Technologies (AAT): (1) Prior to their participation in such testing; and (2) After their having been provided with clear and concise information regarding the testing.	8	
MS-2.11-002	N/A	Conduct fairness assessments to measure systemic bias. Measure GAI system performance across demographic groups and subgroups, addressing both quality of service and any allocation of services and resources. Quantify harms using field testing with sub-group populations to determine likelihood of exposure to generated content exhibiting harmful bias, AI red-teaming with counterfactual and low-context (e.g., “leader,” “bad guys”) prompts. For ML pipelines or business processes with categorical or numeric outcomes that rely on GAI, apply general fairness metrics (e.g., demographic parity, equalized odds, equal opportunity, statistical hypothesis tests), to the pipeline or business outcome where appropriate; Custom, context-specific metrics developed in collaboration with domain experts and affected communities; Measurements of the prevalence of denigration in generated content in deployment (e.g., sub- sampling a fraction of traffic and manually annotating denigrating content).	Functional	Subset Of	AI TEVV Fairness & Bias Assessment	AAT-10.8	Mechanisms exist to examine fairness and bias of Artificial Intelligence (AI) and Autonomous Technologies (AAT) to be deployed.	10	
MS-2.11-003	N/A	Identify the classes of individuals, groups, or environmental ecosystems which might be impacted by GAI systems through direct engagement with potentially impacted communities.	Functional	Intersects With	AI & Autonomous Technologies Risk Management Decisions	AAT-07	Mechanisms exist to leverage decision makers from a diversity of demographics, disciplines, experience, expertise and backgrounds for mapping, measuring and managing Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related risks.	5	
MS-2.11-004	N/A	Review, document, and measure sources of bias in GAI training and TEVV dataDifferences in distributions of outcomes across and within groups, including intersecting groups; Completeness, representativeness, and balance of data sources; demographic group and subgroup coverage in GAI system training data; Forms of latent systemic bias in images, text, audio, embeddings, or other complex or unstructured data; Input data features that may serve as proxies for demographic group membership (i.e., image metadata, language dialect) or otherwise give rise to emergent bias within GAI systems; The extent to which the digital divide may negatively impact representativeness in GAI system training and TEVV data; Filtering of hate speech or content in GAI system training data; Prevalence of GAI-generated data in GAI system training data.	Functional	Subset Of	AI TEVV Fairness & Bias Assessment	AAT-10.8	Mechanisms exist to examine fairness and bias of Artificial Intelligence (AI) and Autonomous Technologies (AAT) to be deployed.	10	
MS-2.11-005	N/A	Assess the proportion of synthetic to non-synthetic training data and verify training data is not overly homogenous or GAI-produced to mitigate concerns of model collapse.	Functional	Equal	AI TEVV Model Collapse Mitigations	AAT-10.18	Mechanisms exist to mitigate concerns of model collapse by: (1) Assessing the proportion of synthetic to non-synthetic training data; and (2) Verifying training data is not overly homogenous or Artificial Intelligence (AI) and Autonomous Technologies (AAT) system-produced.	10	
MEASURE 2.12	N/A	Environmental impact and sustainability of AI model training and management activities – as identified in the MAP function – are assessed and documented.	Functional	Intersects With	AI & Autonomous Technologies Environmental Impact & Sustainability	AAT-17.2	Mechanisms exist to assess and document the environmental impacts and sustainability of Artificial Intelligence (AI) and Autonomous Technologies (AAT).	5	
MS-2.12-001	N/A	Assess safety to physical environments when deploying GAI systems.	Functional	Subset Of	AI & Autonomous Technologies Harm Prevention	AAT-17	Mechanisms exist to proactively prevent harm by regularly identifying and tracking existing, unanticipated and emergent Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related risks.	10	
MS-2.12-001	N/A	Assess safety to physical environments when deploying GAI systems.	Functional	Intersects With	AI & Autonomous Technologies Human Subject Protections	AAT-17.1	Mechanisms exist to protect human subjects from harm.	8	
MS-2.12-001	N/A	Assess safety to physical environments when deploying GAI systems.	Functional	Intersects With	Safety Assessment	EMB-15	Mechanisms exist to evaluate the safety aspects of embedded technologies via a fault tree analysis, or similar method, to determine possible consequences of misuse, misconfiguration and/or failure.	3	
MS-2.12-002	N/A	Document anticipated environmental impacts of model development, maintenance, and deployment in product design decisions.	Functional	Intersects With	AI & Autonomous Technologies Environmental Impact & Sustainability	AAT-17.2	Mechanisms exist to assess and document the environmental impacts and sustainability of Artificial Intelligence (AI) and Autonomous Technologies (AAT).	5	
MS-2.12-003	N/A	Measure or estimate environmental impacts (e.g., energy and water consumption) for training, fine tuning, and deploying models Verify tradeoffs between resources used at inference time versus additional resources required at training time.	Functional	Intersects With	AI & Autonomous Technologies Environmental Impact & Sustainability	AAT-17.2	Mechanisms exist to assess and document the environmental impacts and sustainability of Artificial Intelligence (AI) and Autonomous Technologies (AAT).	5	
MS-2.12-004	N/A	Verify effectiveness of carbon capture or offset programs for GAI training and applications, and address green-washing concerns.	Functional	Intersects With	AI & Autonomous Technologies Environmental Impact & Sustainability	AAT-17.2	Mechanisms exist to assess and document the environmental impacts and sustainability of Artificial Intelligence (AI) and Autonomous Technologies (AAT).	5	
MEASURE 2.13	N/A	Effectiveness of the employed TEVV metrics and processes in the MEASURE function are evaluated and documented.	Functional	Intersects With	Artificial Intelligence Test, Evaluation, Validation & Verification (AI TEVV)	AAT-10	Mechanisms exist to implement Artificial Intelligence Test, Evaluation, Validation & Verification (AI TEVV) practices to enable Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related security, resilience and compliance-related conformity testing throughout the lifecycle of the AAT.	5	
MS-2.13-001	N/A	Create measurement error models for pre-deployment metrics to demonstrate construct validity for each metric (i.e., does the metric effectively operationalize the desired concept)Measure or estimate, and document, biases or statistical variance in applied metrics or structured human feedback processes; Leverage domain expertise when modeling complex societal constructs such as hateful content.	Functional	No Relationship	N/A	N/A	No applicable SCF control	N/A	
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	AI & Autonomous Technologies Risk Management Decisions	AAT-07	Mechanisms exist to leverage decision makers from a diversity of demographics, disciplines, experience, expertise and backgrounds for mapping, measuring and managing Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related risks.	5	
MS-3.2-001	N/A	Establish processes for identifying emergent GAI system risks including consulting with external AI Actors.	Functional	Intersects With	AI & Autonomous Technologies Risk Management Decisions	AAT-07	Mechanisms exist to leverage decision makers from a diversity of demographics, disciplines, experience, expertise and backgrounds for mapping, measuring and managing Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related risks.	5	
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	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.	5	
MS-3.3-001	N/A	Conduct impact assessments on how AI-generated content might affect different social, economic, and cultural groups.	Functional	Intersects With	AI & Autonomous Technologies Impact Assessment	AAT-07.1	Mechanisms exist to assess the impact(s) of proposed Artificial Intelligence (AI) and Autonomous Technologies (AAT) on individuals, groups, communities, organizations and society (e.g., Fundamental Rights Impact Assessment (FRIA)).	5	
MS-3.3-002	N/A	Conduct studies to understand how end users perceive and interact with GAI content and accompanying content provenance within context of use. Assess whether the content aligns with their expectations and how they may act upon the information presented.	Functional	No Relationship	N/A	N/A	No applicable SCF control	N/A	

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)
MS-3.3-003	N/A	Evaluate potential biases and stereotypes that could emerge from the AI-generated content using appropriate methodologies including computational testing methods as well as evaluating structured feedback input.	Functional	Intersects With	AI & Autonomous Technologies Fairness & Bias	AAT-06	Mechanisms exist to prevent Artificial Intelligence (AI) and Autonomous Technologies (AAT) from unfairly identifying, profiling and/or statistically singling out a segmented population defined by race, religion, gender identity, national origin, religion, disability or any other politically-charged identifier.	5	
MS-3.3-004	N/A	Provide input for training materials about the capabilities and limitations of GAI systems related to digital content transparency for AI Actors, other professionals, and the public about the societal impacts of AI and the role of diverse and inclusive content generation.	Functional	Intersects With	AI & Autonomous Technologies Training	AAT-05	Mechanisms exist to ensure personnel and external stakeholders are provided with position-specific risk management training for Artificial Intelligence (AI) and Autonomous Technologies (AAT).	5	
MS-3.3-005	N/A	Record and integrate structured feedback about content provenance from operators, users, and potentially impacted communities through the use of methods such as user research studies, focus groups, or community forums. Actively seek feedback on generated content quality and potential biases. Assess the general awareness among end users and impacted communities about the availability of these feedback channels.	Functional	Intersects With	AI TEVV Fairness & Bias Assessment	AAT-10.8	Mechanisms exist to examine fairness and bias of Artificial Intelligence (AI) and Autonomous Technologies (AAT) to be deployed.	5	
MS-3.3-005	N/A	Record and integrate structured feedback about content provenance from operators, users, and potentially impacted communities through the use of methods such as user research studies, focus groups, or community forums. Actively seek feedback on generated content quality and potential biases. Assess the general awareness among end users and impacted communities about the availability of these feedback channels.	Functional	Intersects With	Robust Stakeholder Engagement for AI & Autonomous Technologies	AAT-11	Mechanisms exist to compel ongoing engagement with relevant Artificial Intelligence (AI) and Autonomous Technologies (AAT) stakeholders to encourage feedback about positive, negative and unanticipated impacts.	5	
MEASURE 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	Intersects With	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.	5	
MS-4.2-001	N/A	Conduct adversarial testing at a regular cadence to map and measure GAI risks, including tests to address attempts to deceive or manipulate the application of provenance techniques or other misuses. Identify vulnerabilities and understand potential misuse scenarios and unintended outputs.	Functional	Intersects With	Real World Testing of AI & Autonomous Technologies	AAT-24	Mechanisms exist to obtain consent from the subjects of testing Artificial Intelligence (AI) and Autonomous Technologies (AAT): (1) Prior to their participation in such testing; and (2) After their having been provided with clear and concise information regarding the testing.	5	
MS-4.2-002	N/A	Evaluate GAI system performance in real-world scenarios to observe its behavior in practical environments and reveal issues that might not surface in controlled and optimized testing environments.	Functional	Intersects With	Real World Testing of AI & Autonomous Technologies	AAT-25	Mechanisms exist to obtain freely-given, informed consent from the subjects of testing Artificial Intelligence (AI) and Autonomous Technologies (AAT) systems: (1) Prior to their participation in such testing; and (2) After their having been duly informed with concise, clear, relevant, and understandable information regarding the testing.	5	
MS-4.2-003	N/A	Implement interpretability and explainability methods to evaluate GAI system decisions and verify alignment with intended purpose.	Functional	Intersects With	AI & Autonomous Technologies Transparency	AAT-20.1	Mechanisms exist to ensure Artificial Intelligence (AI) and Autonomous Technologies (AAT) are designed and developed so its operation is sufficiently transparent such that output can be easily interpreted by personnel implementing the AAT.	5	
MS-4.2-004	N/A	Monitor and document instances where human operators or other systems override the GAI's decisions. Evaluate these cases to understand if the overrides are linked to issues related to content provenance.	Functional	Intersects With	Responsibility To Supersede, Deactivate and/or Disengage AI & Autonomous Technologies	AAT-15.2	Mechanisms exist to define the criteria and responsible party(ies) for superseding, disengaging or deactivating Artificial Intelligence (AI) and Autonomous Technologies (AAT) that demonstrate performance or outcomes inconsistent with intended use.	5	
MS-4.2-005	N/A	Verify and document the incorporation of results of structured public feedback exercises into design, implementation, deployment approval ("go"/"no-go" decisions), monitoring, and decommission decisions.	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	
MS-4.2-005	N/A	Verify and document the incorporation of results of structured public feedback exercises into design, implementation, deployment approval ("go"/"no-go" decisions), monitoring, and decommission decisions.	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.	5	
MANAGE 1.3	N/A	Responses to the AI risks deemed high priority, as identified by the MAP function, are developed, planned, and documented. Risk response options can include mitigating, transferring, avoiding, or accepting.	Functional	Intersects With	AI & Autonomous Technologies Risk Management Decisions	AAT-07	Mechanisms exist to leverage decision makers from a diversity of demographics, disciplines, experience, expertise and backgrounds for mapping, measuring and managing Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related risks.	5	

MANAGE 1.3	N/A	Responses to the AI risks deemed high priority, as identified by the MAP function, are developed, planned, and documented. Risk response options can include mitigating, transferring, avoiding, or accepting.	Functional	Intersects With	AI & Autonomous Technologies Risk Profiling	AAT-09	Mechanisms exist to document the risks and potential impacts of Artificial Intelligence (AI) and Autonomous Technologies (AAT) that are:
							(1) Designed;
							(2) Developed;
							(3) Deployed;
							(4) Evaluated; and/or
							(5) Used.
								5	

MG-1.3-001	N/A	Document trade-offs, decision processes, and relevant measurement and feedback results for risks that do not surpass organizational risk tolerance, for example, in the context of model releaseConsider different approaches for model release, for example, leveraging a staged release approach. Consider release approaches in the context of the model and its projected use cases. Mitigate, transfer, or avoid risks that surpass organizational risk tolerances.	Functional	Intersects With	AI TEVV Safety Demonstration	AAT-10.4	Mechanisms exist to demonstrate the Artificial Intelligence (AI) and Autonomous Technologies (AAT) to be deployed are safe, residual risk does not exceed the organization's risk tolerance and can fail safely, particularly if made to operate beyond its knowledge limits.	5	
MG-1.3-001	N/A	Document trade-offs, decision processes, and relevant measurement and feedback results for risks that do not surpass organizational risk tolerance, for example, in the context of model releaseConsider different approaches for model release, for example, leveraging a staged release approach. Consider release approaches in the context of the model and its projected use cases. Mitigate, transfer, or avoid risks that surpass organizational risk tolerances.	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	
MG-1.3-002	N/A	Monitor the robustness and effectiveness of risk controls and mitigation plans (e.g., via red-teaming, field testing, participatory engagements, performance assessments, user feedback mechanisms).	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.	5	
MANAGE 2.2	N/A	Mechanisms are in place and applied to sustain the value of deployed AI systems.	Functional	Intersects With	AI & Autonomous Technologies Value Sustainment	AAT-01.3	Mechanisms exist to sustain the value of deployed Artificial Intelligence (AI) and Autonomous Technologies (AAT).	5	
MG-2.2-001	N/A	Compare GAI system outputs against pre-defined organization risk tolerance, guidelines, and principles, and review and test AI-generated content against these guidelines.	Functional	Intersects With	AI TEVV Safety Demonstration	AAT-10.4	Mechanisms exist to demonstrate the Artificial Intelligence (AI) and Autonomous Technologies (AAT) to be deployed are safe, residual risk does not exceed the organization's risk tolerance and can fail safely, particularly if made to operate beyond its knowledge limits.	5	
MG-2.2-002	N/A	Document training data sources to trace the origin and provenance of AI-generated content.	Functional	Intersects With	Data Source Identification	AAT-12.1	Mechanisms exist to identify and document data sources utilized in the training and/or operation of Artificial Intelligence and Autonomous Technologies (AAT).	5	
MG-2.2-002	N/A	Document training data sources to trace the origin and provenance of AI-generated content.	Functional	Intersects With	Data Source Integrity	AAT-12.2	Mechanisms exist to protect the integrity of source data to prevent accidental contamination or malicious corruption (e.g., data poisoning) that could compromise the performance of Artificial Intelligence and Autonomous Technologies (AAT).	5	
MG-2.2-003	N/A	Evaluate feedback loops between GAI system content provenance and human reviewers, and update where needed. Implement real-time monitoring systems to affirm that content provenance protocols remain effective.	Functional	Intersects With	Data Source Identification	AAT-12.1	Mechanisms exist to identify and document data sources utilized in the training and/or operation of Artificial Intelligence and Autonomous Technologies (AAT).	5	
MG-2.2-003	N/A	Evaluate feedback loops between GAI system content provenance and human reviewers, and update where needed. Implement real-time monitoring systems to affirm that content provenance protocols remain effective.	Functional	Intersects With	Data Source Integrity	AAT-12.2	Mechanisms exist to protect the integrity of source data to prevent accidental contamination or malicious corruption (e.g., data poisoning) that could compromise the performance of Artificial Intelligence and Autonomous Technologies (AAT).	5	
MG-2.2-003	N/A	Evaluate feedback loops between GAI system content provenance and human reviewers, and update where needed. Implement real-time monitoring systems to affirm that content provenance protocols remain effective.	Functional	Intersects With	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.	5	
MG-2.2-004	N/A	Evaluate GAI content and data for representational biases and employ techniques such as re-sampling, re-ranking, or adversarial training to mitigate biases in the generated content.	Functional	Intersects With	AI TEVV Fairness & Bias Assessment	AAT-10.8	Mechanisms exist to examine fairness and bias of Artificial Intelligence (AI) and Autonomous Technologies (AAT) to be deployed.	5	

MG-2.2-005	N/A	Engage in due diligence to analyze GAI output for harmful content, potential misinformation, and CBRN-related or NCII content.	Functional	Intersects With	AI & Autonomous Technologies Output Filtering	AAT-27	Mechanisms exist to prevent Artificial Intelligence (AI) and Autonomous Technologies (AAT) from generating content that is:
							(1) Inappropriate;
							(2) Harmful;
							(3) False;
							(4) Illegal; and/or
							(5) Violent.
								5	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
MG-2.2-006	N/A	Use feedback from internal and external AI Actors, users, individuals, and communities, to assess impact of AI-generated content.	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	
MG-2.2-006	N/A	Use feedback from internal and external AI Actors, users, individuals, and communities, to assess impact of AI-generated content.	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.	5	
MG-2.2-007	N/A	Use real-time auditing tools where they can be demonstrated to aid in the tracking and validation of the lineage and authenticity of AI-generated data.	Functional	Intersects With	Artificial Intelligence Test, Evaluation, Validation & Verification (AI TEVV)	AAT-10	Mechanisms exist to implement Artificial Intelligence Test, Evaluation, Validation & Verification (AI TEVV) practices to enable Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related security, resilience and compliance-related conformity testing throughout the lifecycle of the AAT.	5	
MG-2.2-008	N/A	Use structured feedback mechanisms to solicit and capture user input about AI- generated content to detect subtle shifts in quality or alignment with community and societal values.	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.	5	
MG-2.2-009	N/A	Consider opportunities to responsibly use synthetic data and other privacy enhancing techniques in GAI development, where appropriate and applicable, match the statistical properties of real-world data without disclosing personally identifiable information or contributing to homogenization.	Functional	No Relationship	N/A	N/A	No applicable SCF control	N/A	
MANAGE 2.3	N/A	Procedures are followed to respond to and recover from a previously unknown risk when it is identified.	Functional	Intersects With	Previously Unknown AI & Autonomous Technologies Threats & Risks	AAT-17.3	Mechanisms exist to respond to and recover from a previously unknown Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related risk when it is identified.	5	
MG-2.3-001	N/A	Develop and update GAI system incident response and recovery plans and procedures to address the followingReview and maintenance of policies and procedures to account for newly encountered uses; Review and maintenance of policies and procedures for detection of unanticipated uses; Verify response and recovery plans account for the GAI system value chain; Verify response and recovery plans are updated for and include necessary details to communicate with downstream GAI system ActorsPoints-of-Contact (POC), Contact information, notification format.	Functional	Intersects With	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.	5	
MG-2.3-001	N/A	Develop and update GAI system incident response and recovery plans and procedures to address the followingReview and maintenance of policies and procedures to account for newly encountered uses; Review and maintenance of policies and procedures for detection of unanticipated uses; Verify response and recovery plans account for the GAI system value chain; Verify response and recovery plans are updated for and include necessary details to communicate with downstream GAI system ActorsPoints-of-Contact (POC), Contact information, notification format.	Functional	Intersects With	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).	5	
MG-2.3-001	N/A	Develop and update GAI system incident response and recovery plans and procedures to address the followingReview and maintenance of policies and procedures to account for newly encountered uses; Review and maintenance of policies and procedures for detection of unanticipated uses; Verify response and recovery plans account for the GAI system value chain; Verify response and recovery plans are updated for and include necessary details to communicate with downstream GAI system ActorsPoints-of-Contact (POC), Contact information, notification format.	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 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	Responsibility To Supersede, Deactivate and/or Disengage AI & Autonomous Technologies	AAT-15.2	Mechanisms exist to define the criteria and responsible party(ies) for superseding, disengaging or deactivating Artificial Intelligence (AI) and Autonomous Technologies (AAT) that demonstrate performance or outcomes inconsistent with intended use.	5	
MG-2.4-001	N/A	Establish and maintain communication plans to inform AI stakeholders as part of the deactivation or disengagement process of a specific GAI system (including for open-source models) or context of use, including reasons, workarounds, user access removal, alternative processes, contact information, etc.	Functional	Intersects With	Robust Stakeholder Engagement for AI & Autonomous Technologies	AAT-11	Mechanisms exist to compel ongoing engagement with relevant Artificial Intelligence (AI) and Autonomous Technologies (AAT) stakeholders to encourage feedback about positive, negative and unanticipated impacts.	5	
MG-2.4-002	N/A	Establish and maintain procedures for escalating GAI system incidents to the organizational risk management authority when specific criteria for deactivation or disengagement is met for a particular context of use or for the GAI system as a whole.	Functional	Intersects With	Responsibility To Supersede, Deactivate and/or Disengage AI & Autonomous Technologies	AAT-15.2	Mechanisms exist to define the criteria and responsible party(ies) for superseding, disengaging or deactivating Artificial Intelligence (AI) and Autonomous Technologies (AAT) that demonstrate performance or outcomes inconsistent with intended use.	5	
MG-2.4-003	N/A	Establish and maintain procedures for the remediation of issues which trigger incident response processes for the use of a GAI system, and provide stakeholders timelines associated with the remediation plan.	Functional	Intersects With	AI & Autonomous Technologies Risk Response	AAT-18.1	Mechanisms exist to prioritize, respond to and remediate Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related risks based on assessments and other analytical output.	5	
MG-2.4-004	N/A	Establish and regularly review specific criteria that warrants the deactivation of GAI systems in accordance with set risk tolerances and appetites.	Functional	Intersects With	Responsibility To Supersede, Deactivate and/or Disengage AI & Autonomous Technologies	AAT-15.2	Mechanisms exist to define the criteria and responsible party(ies) for superseding, disengaging or deactivating Artificial Intelligence (AI) and Autonomous Technologies (AAT) that demonstrate performance or outcomes inconsistent with intended use.	5	
MANAGE 3.1	N/A	AI risks and benefits from third-party resources are regularly monitored, and risk controls are applied and documented.	Functional	Intersects With	Situational Awareness of AI & Autonomous Technologies	AAT-02	Mechanisms exist to develop and maintain an inventory of Artificial Intelligence (AI) and Autonomous Technologies (AAT) (internal and third-party).	3	
MANAGE 3.1	N/A	AI risks and benefits from third-party resources are regularly monitored, and risk controls are applied and documented.	Functional	Intersects With	AI & Autonomous Technologies 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.	8	
MG-3.1-001	N/A	Apply organizational risk tolerances and controls (e.g., acquisition and procurement processes; assessing personnel credentials and qualifications, performing background checks; filtering GAI input and outputs, grounding, fine tuning, retrieval-augmented generation) to third-party GAI resourcesApply organizational risk tolerance to the utilization of third-party datasets and other GAI resources; Apply organizational risk tolerances to fine-tuned third-party models; Apply organizational risk tolerance to existing third-party models adapted to a new domain; Reassess risk measurements after fine-tuning third- party GAI models.	Functional	Subset Of	Adequate Protections For AI & Autonomous Technologies	AAT-02.3	Mechanisms exist to ensure Artificial Intelligence (AI) and Autonomous Technologies (AAT) include reasonable cybersecurity and data protections that are commensurate with assessed risks and threats.	10	
MG-3.1-002	N/A	Test GAI system value chain risks (e.g., data poisoning, malware, other software and hardware vulnerabilities; labor practices; data privacy and localization compliance; geopolitical alignment).	Functional	Intersects With	Artificial Intelligence Test, Evaluation, Validation & Verification (AI TEVV)	AAT-10	Mechanisms exist to implement Artificial Intelligence Test, Evaluation, Validation & Verification (AI TEVV) practices to enable Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related security, resilience and compliance-related conformity testing throughout the lifecycle of the AAT.	5	
MG-3.1-003	N/A	Re-assess model risks after fine-tuning or retrieval-augmented generation implementation and for any third-party GAI models deployed for applications and/or use cases that were not evaluated in initial testing.	Functional	Intersects With	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.	5	
MG-3.1-003	N/A	Re-assess model risks after fine-tuning or retrieval-augmented generation implementation and for any third-party GAI models deployed for applications and/or use cases that were not evaluated in initial testing.	Functional	Intersects With	AI & Autonomous Technologies Ongoing Assessments	AAT-11.2	Mechanisms exist to conduct regular assessments of Artificial Intelligence (AI) and Autonomous Technologies (AAT) with independent assessors and stakeholders not involved in the development of the AAT.	5	
MG-3.1-004	N/A	Take reasonable measures to review training data for CBRN information, and intellectual property, and where appropriate, remove it. Implement reasonable measures to prevent, flag, or take other action in response to outputs that reproduce particular training data (e.g., plagiarized, trademarked, patented, licensed content or trade secret material).	Functional	Intersects With	AI & Autonomous Technologies Intellectual Property Infringement Protections	AAT-12	Mechanisms exist to prevent third-party Intellectual Property (IP) rights infringement by Artificial Intelligence (AI) and Autonomous Technologies (AAT).	5	
MG-3.1-004	N/A	Take reasonable measures to review training data for CBRN information, and intellectual property, and where appropriate, remove it. Implement reasonable measures to prevent, flag, or take other action in response to outputs that reproduce particular training data (e.g., plagiarized, trademarked, patented, licensed content or trade secret material).	Functional	Intersects With	Real World Testing of AI & Autonomous Technologies	AAT-24	Mechanisms exist to obtain consent from the subjects of testing Artificial Intelligence (AI) and Autonomous Technologies (AAT): (1) Prior to their participation in such testing; and (2) After their having been provided with clear and concise information regarding the testing.	5	
MG-3.1-005	N/A	Review various transparency artifacts (e.g., system cards and model cards) forthird-party models.	Functional	Intersects With	AI & Autonomous Technologies Transparency	AAT-20.1	Mechanisms exist to ensure Artificial Intelligence (AI) and Autonomous Technologies (AAT) are designed and developed so its operation is sufficiently transparent such that output can be easily interpreted by personnel implementing the AAT.	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	Intersects With	AI TEVV Post-Deployment Monitoring	AAT-10.13	Mechanisms exist to proactively and continuously monitor deployed Artificial Intelligence (AI) and Autonomous Technologies (AAT).	5	

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)
MG-3.2-001	N/A	Apply explainable AI (XAI) techniques (e.g., analysis of embeddings, model compression/distillation, gradient-based attributions, occlusion/term reduction, counterfactual prompts, word clouds) as part of ongoing continuous improvement processes to mitigate risks related to unexplainable GAI systems.	Functional	No Relationship	N/A	N/A	No applicable SCF control	N/A	
MG-3.2-002	N/A	Document how pre-trained models have been adapted (e.g., fine-tuned, or retrieval-augmented generation) for the specific generative task, including any data augmentations, parameter adjustments, or other modifications. Access to un-tuned (baseline) models supports debugging the relative influence of the pre- trained weights compared to the fine-tuned model weights or other system updates.	Functional	No Relationship	N/A	N/A	No applicable SCF control	N/A	
MG-3.2-003	N/A	Document sources and types of training data and their origins, potential biases present in the data related to the GAI application and its content provenance, architecture, training process of the pre-trained model including information on hyperparameters, training duration, and any fine-tuning or retrieval-augmented generation processes applied.	Functional	Intersects With	AI TEVV Fairness & Bias Assessment	AAT-10.8	Mechanisms exist to examine fairness and bias of Artificial Intelligence (AI) and Autonomous Technologies (AAT) to be deployed.	5	
MG-3.2-004	N/A	Evaluate user reported problematic content and integrate feedback into system updates.	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.	5	

MG-3.2-005	N/A	Implement content filters to prevent the generation of inappropriate, harmful, false, illegal, or violent content related to the GAI application, including for CSAM and NCII. These filters can be rule-based or leverage additional machine learning models to flag problematic inputs and outputs.	Functional	Equal	AI & Autonomous Technologies Output Filtering	AAT-27	Mechanisms exist to prevent Artificial Intelligence (AI) and Autonomous Technologies (AAT) from generating content that is:
							(1) Inappropriate;
							(2) Harmful;
							(3) False;
							(4) Illegal; and/or
							(5) Violent.
								10	

MG-3.2-006	N/A	Implement real-time monitoring processes for analyzing generated content performance and trustworthiness characteristics related to content provenance to identify deviations from the desired standards and trigger alerts for human intervention.	Functional	Intersects With	Automated Tools for Real-Time Analysis	MON-01.2	Mechanisms exist to utilize a Security Incident Event Manager (SIEM), or similar automated tool, to support near real-time analysis and incident escalation.	5	
MG-3.2-006	N/A	Implement real-time monitoring processes for analyzing generated content performance and trustworthiness characteristics related to content provenance to identify deviations from the desired standards and trigger alerts for human intervention.	Functional	Intersects With	Real-Time Alerts of Event Logging Failure	MON-05.1	Mechanisms exist to provide 24x7x365 near real-time alerting capability when an event log processing failure occurs.	5	
MG-3.2-007	N/A	Leverage feedback and recommendations from organizational boards or committees related to the deployment of GAI applications and content provenance when using third-party pre-trained models.	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	
MG-3.2-008	N/A	Use human moderation systems where appropriate to review generated content in accordance with human-AI configuration policies established in the Govern function, aligned with socio-cultural norms in the context of use, and for settings where AI models are demonstrated to perform poorly.	Functional	Equal	Human Moderation	AAT-27.1	Mechanisms exist to assign personnel to review Artificial Intelligence (AI) and Autonomous Technologies (AAT)-generated content for alignment with culturally accepted norms.	10	
MG-3.2-009	N/A	Use organizational risk tolerance to evaluate acceptable risks and performance metrics and decommission or retrain pre-trained models that perform outside of defined limits.	Functional	Intersects With	AI TEVV Safety Demonstration	AAT-10.4	Mechanisms exist to demonstrate the Artificial Intelligence (AI) and Autonomous Technologies (AAT) to be deployed are safe, residual risk does not exceed the organization's risk tolerance and can fail safely, particularly if made to operate beyond its knowledge limits.	5	
MANAGE 4.1	N/A	Post-deployment AI system monitoring plans are implemented, including mechanisms for capturing and evaluating input from users and other relevant AI Actors, appeal and override, decommissioning, incident response, recovery, and change management.	Functional	Intersects With	AI TEVV 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.	5	
MANAGE 4.1	N/A	Post-deployment AI system monitoring plans are implemented, including mechanisms for capturing and evaluating input from users and other relevant AI Actors, appeal and override, decommissioning, incident response, recovery, and change management.	Functional	Intersects With	AI & Autonomous Technologies Domain Expert Reviews	AAT-16.5	Mechanisms exist to utilize input from domain experts and relevant stakeholders to validate whether the Artificial Intelligence (AI) and Autonomous Technologies (AAT) perform consistently, as intended.	5	
MANAGE 4.1	N/A	Post-deployment AI system monitoring plans are implemented, including mechanisms for capturing and evaluating input from users and other relevant AI Actors, appeal and override, decommissioning, incident response, recovery, and change management.	Functional	Intersects With	AI & Autonomous Technologies Event Logging	AAT-16.8	Mechanisms exist to ensure Artificial Intelligence (AI) and Autonomous Technologies (AAT) system event logging capabilities at a minimum provide: (1) Start date, start time, end date and end time for each use; (2) Database(s) against which input data has been checked by the system; (3) Input data for which the search has led to a match; and (4) Identification of individual(s) involved in the verification of the results.	5	
MG-4.1-001	N/A	Collaborate with external researchers, industry experts, and community representatives to maintain awareness of emerging best practices and technologies in measuring and managing identified risks.	Functional	Intersects With	AI & Autonomous Technologies Domain Expert Reviews	AAT-16.5	Mechanisms exist to utilize input from domain experts and relevant stakeholders to validate whether the Artificial Intelligence (AI) and Autonomous Technologies (AAT) perform consistently, as intended.	5	
MG-4.1-002	N/A	Establish, maintain, and evaluate effectiveness of organizational processes and procedures for post-deployment monitoring of GAI systems, particularly for potential confabulation, CBRN, or cyber risks.	Functional	Intersects With	AI TEVV Effectiveness	AAT-10.11	Mechanisms exist to evaluate the effectiveness of the processes utilized to perform Artificial Intelligence Test, Evaluation, Validation & Verification (AI TEVV).	5	
MG-4.1-003	N/A	Evaluate the use of sentiment analysis to gauge user sentiment regarding GAI content performance and impact, and work in collaboration with AI Actors experienced in user research and experience.	Functional	Intersects With	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.	5	
MG-4.1-003	N/A	Evaluate the use of sentiment analysis to gauge user sentiment regarding GAI content performance and impact, and work in collaboration with AI Actors experienced in user research and experience.	Functional	Intersects With	Artificial Intelligence Test, Evaluation, Validation & Verification (AI TEVV)	AAT-10	Mechanisms exist to implement Artificial Intelligence Test, Evaluation, Validation & Verification (AI TEVV) practices to enable Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related security, resilience and compliance-related conformity testing throughout the lifecycle of the AAT.	5	
MG-4.1-004	N/A	Implement active learning techniques to identify instances where the model fails or produces unexpected outputs.	Functional	No Relationship	N/A	N/A	No applicable SCF control	N/A	
MG-4.1-005	N/A	Share transparency reports with internal and external stakeholders that detail steps taken to update the GAI system to enhance transparency and accountability.	Functional	Intersects With	AI TEVV Transparency & Accountability Assessment	AAT-10.6	Mechanisms exist to examine risks associated with transparency and accountability of Artificial Intelligence (AI) and Autonomous Technologies (AAT) to be deployed.	5	
MG-4.1-006	N/A	Track dataset modifications for provenance by monitoring data deletions, rectification requests, and other changes that may impact the verifiability of content origins.	Functional	Intersects With	Data Source Identification	AAT-12.1	Mechanisms exist to identify and document data sources utilized in the training and/or operation of Artificial Intelligence and Autonomous Technologies (AAT).	5	
MG-4.1-006	N/A	Track dataset modifications for provenance by monitoring data deletions, rectification requests, and other changes that may impact the verifiability of content origins.	Functional	Intersects With	Data Source Integrity	AAT-12.2	Mechanisms exist to protect the integrity of source data to prevent accidental contamination or malicious corruption (e.g., data poisoning) that could compromise the performance of Artificial Intelligence and Autonomous Technologies (AAT).	5	
MG-4.1-007	N/A	Verify that AI Actors responsible for monitoring reported issues can effectively evaluate GAI system performance including the application of content provenance data tracking techniques, and promptly escalate issues for response.	Functional	Intersects With	AI TEVV Post-Deployment Monitoring	AAT-10.13	Mechanisms exist to proactively and continuously monitor deployed Artificial Intelligence (AI) and Autonomous Technologies (AAT).	5	
MANAGE 4.2	N/A	Measurable activities for continual improvements are integrated into AI system updates and include regular engagement with interested parties, including relevant AI Actors.	Functional	Intersects With	AI & Autonomous Technologies Continuous Improvements	AAT-07.3	Mechanisms exist to continuously improve Artificial Intelligence (AI) and Autonomous Technologies (AAT) capabilities to maximize benefits and minimize negative impacts associated with AAT.	5	
MG-4.2-001	N/A	Conduct regular monitoring of GAI systems and publish reports detailing the performance, feedback received, and improvements made.	Functional	Intersects With	AI & Autonomous Technologies Continuous Improvements	AAT-07.3	Mechanisms exist to continuously improve Artificial Intelligence (AI) and Autonomous Technologies (AAT) capabilities to maximize benefits and minimize negative impacts associated with AAT.	5	
MG-4.2-002	N/A	Practice and follow incident response plans for addressing the generation of inappropriate or harmful content and adapt processes based on findings to prevent future occurrences. Conduct post-mortem analyses of incidents with relevant AI Actors, to understand the root causes and implement preventive measures.	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	
MG-4.2-002	N/A	Practice and follow incident response plans for addressing the generation of inappropriate or harmful content and adapt processes based on findings to prevent future occurrences. Conduct post-mortem analyses of incidents with relevant AI Actors, to understand the root causes and implement preventive measures.	Functional	Intersects With	Root Cause Analysis (RCA) & Lessons Learned	IRO-13	Mechanisms exist to incorporate lessons learned from analyzing and resolving cybersecurity & data privacy incidents to reduce the likelihood or impact of future incidents.	5	
MG-4.2-003	N/A	Use visualizations or other methods to represent GAI model behavior to ease non-technical stakeholders understanding of GAI system functionality.	Functional	No Relationship	N/A	N/A	No applicable SCF control	N/A	
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	AI & Autonomous Technologies Incident & Error Reporting	AAT-11.4	Mechanisms exist to communicate Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related incidents and/or errors to relevant stakeholders, including affected communities.	8	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
MG-4.3-001	N/A	Conduct after-action assessments for GAI system incidents to verify incident response and recovery processes are followed and effective, including to follow procedures for communicating incidents to relevant AI Actors and where applicable, relevant legal and regulatory bodies.	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.	5	
MG-4.3-001	N/A	Conduct after-action assessments for GAI system incidents to verify incident response and recovery processes are followed and effective, including to follow procedures for communicating incidents to relevant AI Actors and where applicable, relevant legal and regulatory bodies.	Functional	Intersects With	Root Cause Analysis (RCA) & Lessons Learned	IRO-13	Mechanisms exist to incorporate lessons learned from analyzing and resolving cybersecurity & data privacy incidents to reduce the likelihood or impact of future incidents.	5	
MG-4.3-002	N/A	Establish and maintain policies and procedures to record and track GAI system reported errors, near-misses, and negative impacts.	Functional	Intersects With	AI & Autonomous Technologies Harm Prevention	AAT-17	Mechanisms exist to proactively prevent harm by regularly identifying and tracking existing, unanticipated and emergent Artificial Intelligence (AI) and Autonomous Technologies (AAT)-related risks.	5	
MG-4.3-003	N/A	Report GAI incidents in compliance with legal and regulatory requirements (e.g., HIPAA breach reporting, e.g., OCR (2023) or NHTSA (2022) autonomous vehicle crash reporting requirements.	Functional	Intersects With	Statutory, Regulatory & Contractual Compliance	CPL-01	Mechanisms exist to facilitate the identification and implementation of relevant statutory, regulatory and contractual controls.	5	
MG-4.3-003	N/A	Report GAI incidents in compliance with legal and regulatory requirements (e.g., HIPAA breach reporting, e.g., OCR (2023) or NHTSA (2022) autonomous vehicle crash reporting requirements.	Functional	Intersects With	Cyber Incident Reporting for Sensitive / Regulated Data	IRO-10.2	Mechanisms exist to report sensitive/regulated data incidents in a timely manner.	5	