Govern

Subcategory	About	Suggested Actions	Transparency and Documentation
Govern 1.1 Legal and regulatory requirements involving AI are understood, managed, and documented.	Like other types of AI, generative AI (GAI) systems may pose legal and regulatory risks related to each of the trustworthy characteristics and present new challenges. For example, GAI may introduce risks related to criminal activities, reporting, obscene content, data protection, data privacy, confidentiality or intellectual property ownership that broadly differ from risks of other types of AI. 	• Align GAI use with applicable data privacy laws and policies. • Define and communicate organizational access and use of GAI through management, legal and compliance functions. • Document existing or imminent legal requirements for GAI systems across relevant jurisdictions. • Disclose use of generative AI to users and establish related organizational policies. • Establish transparent acceptable use policies for GAI that address illegal use or applications of GAI. • Establish GAI policies limiting the use, publication, or distribution of licensed, patented, trademarked, copyrighted, or trade secret material according to commercial use, legal, and regulatory requirements. • Establish policies restricting the use of GAI in organizational activities in regulated dealings or in applications where compliance with applicable laws and regulations may be infeasible.  • Establish policies restricting the use of GAI to create child sexual abuse materials (CSAM) or other nonconsentual intimate imagery.	• Are GAI acceptable use policies transparent and accessible for all personnel? • Have AI actors documented applicable laws and regulations, including pending legislation, in the design or acquisition phase, and at a reasonable cadence after deployment? • Are organizational legal or compliance functions involvement in organizational GAI usage documented? • Have third-parties provided enough information to AI acquisition teams to enable legal and regulatory risk assessments? 

		• Report development of powerful foundation models in accordance with the Defense Production Act.	

Govern 1.2
 	
The characteristics of trustworthy AI are integrated into organizational policies, processes, and procedures.
	Transparent policies, procedures and processes that are applied to other types of AI systems within an organization can be applied to generative AI (GAI) systems, including those related to:
	• Accessibility and reasonable accommodations.
	• AI actor credentials and qualifications.
	• Alignment to organizational values.
	• Auditing and assessment.
	• Change-management controls.
	• Commercial use.
	• Data provenance.
	• Data protection.
	• Data retention.
	• Defining key terms.
	• Decommissioning.
	• Discouraging anonymous use.
	• Education.
	• Establishing standards for model development and TEVV activities.
	• Impact assessments.
	• Incident response.
	• Monitoring.
	• Opt-outs.
	• Risk-based controls.
	• Risk mapping and measurement.
	• Scientific integrity and TEVV practices.
	• Stakeholder engagement.
	• Whistleblower protections.
	• Workforce diversity and interdisciplinarity in teams that interact with GAI.
	
	GAI may also give rise to novel risks for which organizations may require new risk management policies, procedures and processes (e.g,
		• Connect new GAI policies, procedures and processes to existing model, data and IT governance and to legal, compliance and risk functions.
		• Consider factors such as internal vs. external use, narrow vs. broad application scope, fine-tuning and training data sources (i.e., grounding) when defining risk-based controls.
		• Define acceptable use policies for GAI systems deployed by, used by, and used within the organization.
		• Update existing policies, procedures and processes to control risks specific to GAI, such as:
		  ○ Abuse and related threats to information integrity (e.g., generation of phishing emails or malware).
		  ○ Accelerated procurement schedules and third-party dependencies.
		  ○ Ad-hoc, and unauthorized data collection and web-scraping.
		  ○ Algorithmic aversion, automation complacency and overreliance on GAI processes and content.
		  ○ Anthropomorphization of GAI in organizational practices or use.
		  ○ Complex data protection requirements (e.g., countermeasures for prompt injection).
			• Are GAI policies, procedures and processes aligned with the Trustworthiness Characteristics?
			• Are GAI policies, procedures and processes transparent for all AI actors?
			• Do GAI documented policies, procedures and processes address risks relating to algorithmic aversion, anthropomorphization, automation complacency, data protection, data provenance, data retention, emotional entanglement, harms in physical environments, information integrity, intellectual property infringement, insufficient transparency, model collapse, offensive outputs, procurement, third-parties, undisclosed use, unforeseen outcomes, web-scraping, or workforce displacement?
			• Do documented policies define and differentiate human roles and responsibilities in decision making and overseeing GAI systems?
			• Do documented GAI policies reflect interdisciplinary perspectives about GAI risks?
			• Do documented GAI policies, procedures and processes address data protection for decommissioned systems?
			• Do documented policies or procedures address

	grounding, strong meta prompts, citation of generated content). 	○ Consumption and proliferation of overly homogenized generated content (to minimize potential, model collapse). ○ Denigration, stereotypes, violence, toxicity, obscene, or otherwise objectionable outputs. ○ Displacement of workers due to reliance on GAI tasks and outputs. ○ Emotional entanglement of users with GAI systems. ○ Human roles and responsibilities in decision making and overseeing AI systems. ○ Human interactions with and sense-making of GAI content. ○ Intellectual property infringement. ○ Insufficient transparency into system mechanisms and training data. ○ Potential harm to ecosystems or in physical environments. ○ Unauthorized external sharing of generated content. ○ Undisclosed deployment of GAI for users, advertising and marketing, or other purposes.	monitoring for highly variable performance characteristics of GAI systems? ● Have documented AI system risk levels been updated to reflect the highly variable performance characteristics of GAI systems? ● Have documented data retention policies been updated to address GAI system input and outputs? ● Have any new documented GAI policies, procedures and processes been communicated to compliance, legal, risk and other oversight functions? ● Have documented training materials for AI Actors received training on GAI policies, procedures and processes? 
Govern 1.3 Processes and procedures are in place to determine the needed level of risk management activities based on the organization's risk tolerance.	Organizational risk tolerances enable standardized and efficient oversight of organizational GAI systems. Organizations' existing risk levels may be serviceable for generative AI (GAI) systems, or organizations may need to revise or update AI system risk levels to address GAI risks. Organizations may restrict any artificial	● Consider the following, or similar, factors when updating or defining risk tiers for GAI: ○ Abuses and risks to information integrity. ○ Cadence of vendor releases and updates. ○ Complex data protection requirements. ○ Dependencies between GAI and other IT or data systems.	● Are human review processes documented, clear, and actionable? ● Are GAI systems aligned with the Trustworthiness Characteristics? ● Do reporting processes for the public, board or senior management include GAI impacts on the organization, consumers, the public or the physical environment?

	intelligence (AI) applications that cause harm, exceed stated risk tolerances, or that conflict with organizational values.	○ Harm in physical environments. ○ Human review of GAI system outputs. ○ Legal or regulatory requirements. ○ Presentation of obscene, objectionable, toxic, invalid or untruthful output. ○ Psychological impacts to humans (e.g, anthropomorphization, algorithmic aversion, emotional entanglement). ○ Immediate and long term impacts. ○ Internal vs. external use. ○ Unreliable decision making capabilities. ○ Validity, adaptability and variability of GAI system performance over time. ● Define acceptable uses for GAI systems, where some applications may be restricted. ● Maintain an updated hierarchy of identified and expected risks connected to contexts of GAI use. ● Increase cadence for internal audits to address any unanticipated changes in GAI technologies or applications. ● Reevaluate organizational risk tolerances to account for broad GAI risks, including: ○ Immature 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.	● How are go/no-go decision processes documented for GAI systems across risk levels? ● How is alignment of GAI systems with organizational risk tolerances documented for high-risk systems? ● How is alignment of GAI systems with organizational values documented across risk levels? ● What updates are required for GAI system documentation across risk levels?

		• Revise and update existing risk levels to account for GAI risks, potentially including specialized risk levels for GAI systems that address risks such as model collapse and algorithmic monoculture. • Tie expected GAI behavior to trustworthy characteristics.	
Govern 1.6 Mechanisms are in place to inventory AI systems and are resourced according to organizational risk priorities.	An inventory of AI systems is a standard risk control that enables organizations to track AI risks in the aggregate and provides an organized repository to store relevant information for individual systems. The level of information inventoried for AI systems is expected to be commensurate to the system's sophistication and risk. Generative AI (GAI) systems may be inventoried like other types of AI systems, models, or quantitative tools but may also require special consideration and treatment. For example, GAI system training and evaluation data may be unknown, GAI capabilities may be embedded in general purpose software applications, GAI systems may operate on licensed or copyrighted works, or GAI systems may be fine-tuned for broadly varying applications.	• Adjust inventory requirements to match the risk level of GAI systems. • In addition to general model, governance and risk information, consider the following items in GAI system inventory entries: ○ Acceptable use policies and policy exceptions. ○ Application. ○ Assumptions and limitations of use, including enumeration of restricted uses. ○ Business or model owners. ○ Challenges for explainability, interpretability, or transparency. ○ Change management, maintenance, and monitoring plans. ○ Connections or dependencies between other systems. ○ Consent information and notices. ○ Data provenance information (e.g., source, signatures, versioning, watermarks). ○ Designation of in-house or third party development. ○ Designation of risk level. ○ Disclosure information or notices.	• Are acceptable uses, risk levels, and policy exceptions tracked in the AI system inventory? • Are the limitations and acceptable uses of GAI communicated to end users? • Do documented organizational AI policies and procedures address inventories for GAI systems? • Do organizational policies and procedures address varying inventory and documentation requirements for AI systems commensurate to a system's sophistication and risk profile. • Does the organizational AI system inventory have an owner? • How are third-party GAI systems accounted for and documented in the inventory? • Will GAI systems embedded in general purpose software be inventoried like other AI systems?

		○ Incident response plans. ○ Known issues reported from internal bug tracking or external information sharing resources (e.g., AI incident database, AVID, CVE, or OECD incident monitor). ○ Human oversight roles and responsibilities. ○ Special rights and considerations for intellectual property, licensed works, or personal, privileged, proprietary or sensitive data. ○ Time frame for valid deployment, including date of last risk assessment. ○ Underlying foundation models, versions of underlying models, and access modes. ○ Updated hierarchy of identified and expected risks connected to contexts of use. ● Define any inventory exemptions for GAI systems embedded into application software in organizational policies. ● Enumerate organizational GAI systems for incorporation into an AI system inventory. ● Inventory recently decommissioned systems, systems with imminent deployment plans, and operational systems. ● Update policy definitions for AI systems, models, qualitative tools or similar to address generative AI systems.	

Govern 1.7
 	
Processes and procedures are in place for decommissioning and phasing out of AI systems safely and in a manner that does not increase risks or decrease the organization's trustworthiness
	GAI systems may require decommissioning due to operational expense, poor or unexpected system performance, user requests for data deletion, abuse of system for purposes such as disinformation propagation, or unauthorized publication of obscene or protected material. Compared to other AI systems, aspects or applications of generative AI (GAI) may complicate decommissioning. Contributing causes for decommissioning may include negative impacts to humans or the environment. Humans may develop emotional or other dependencies on GAI systems. After decommission, impacted community members may require recourse and redress and systems may require additional data protection and data privacy controls.
	
	The decommission of GAI systems may take many forms, and require quick action in the case of incident response. Since sudden termination or drastic changes in GAI services may decrease trust and increase risk, decommissioning should be iterative, staged, involve rollover or fallback processes, and can necessitate substantial data retention. Organizations can incrementally update systems prior to decommissioning by updating blocklists and hardening content moderation, session limits, and rate-limiting). As with other AI systems,
		• Update existing policies (e.g., enterprise record retention policies) or establish new policies for the decommissioning of GAI systems.
		• Allocate time and resources for staged decommissioning to avoid service disruptions.
		• Consider the following factors when decommissioning GAI systems:
		  ○ Clear versioning of decommissioned and replacement systems.
		  ○ Contractual, legal, or regulatory requirements.
		  ○ Data 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.
		  ○ Digital and physical artifacts.
		  ○ Recourse mechanisms for impacted users or communities.
		  ○ Termination of related cloud or vendor services.
		  ○ Users' emotional entanglement with GAI functions.
		• Communicate decommissioning and support plans to AI actors and users through various channels and maintain communication and associated training protocols.
		• Implement data security and privacy controls for
			• Are migration and decommissioning plans addressed in the design phase of GAI systems?
			• Are steps for containing decommissioned AI systems (i.e., severing from all other computer, data, or information systems) recorded in model documentation or incident response plans?
			• Do incident response plans include information such as data retention requirements, AI actor contacts, and ongoing recourse requirements?
			• Have data retention requirements for GAI system inputs and outputs been cataloged in system documentation?
			• Have relevant third-party resources, vendors, or personnel been recorded in system documentation?
			• Have AI Actors with the organizational authority and capability to complete decommissioning been recorded in system documentation?
			• Will recourse mechanisms for impacted users or communities be available after decommissioning?

	GAI artifacts may require preservation due to forensic or regulatory investigations, data retention requirements, backtesting, or benchmarking. Retrospective reviews may be undertaken subsequent to system decommissioning as part of broader continual improvement efforts. Organizations may also consider sharing information about incidents or decommissioning processes through incident or vulnerability databases, or through appropriate GAI community channels.	stored decommissioned systems.	
Govern 3.2 Policies and procedures are in place to define and differentiate roles and responsibilities for human-AI configurations and oversight of AI systems.	Generative AI systems demonstrate extreme heterogeneity in output and AI generated output can be perceived and acted upon by humans in broadly varying ways. GAI opportunities, risks and long-term performance characteristics are also not currently well understood. For these reasons - and others - generative AI (GAI) may require different levels of oversight from AI actors or different human-AI configurations to support effective risk management. Organizational use of GAI systems may require additional human review, tracking and documentation and associated board and management oversight. GAI technology can produce output in multiple modalities and present many classes of user interfaces. This leads to a broader set of AI actors	• Adjust roles for AI actors across different components and life cycle stages of large or complex GAI systems. • Establish processes to include and empower interdisciplinary team member perspectives along the AI lifecycle. • Evaluate AI actor teams in consideration of credentials, demographic representation, interdisciplinary diversity, and professional qualifications. • Bolster oversight of GAI systems with independent audits or assessments, or by the application of authoritative external standards. • Consider adjustment of organizational roles for the following: ○ AI actor, user, and community feedback relating to GAI systems.	• Are organizational structures that enable accountability and independent oversight documented in AI policies? • Are documented processes in place for forming interdisciplinary organizational teams to support structured human feedback mechanisms? • Are chains of command and lines of communication for AI actors documented and transparent? • Do acceptable use policies or other organizational policies establish guidance for appropriate human-AI configurations across various GAI modalities and interfaces? • Is the acceptable use policy for GAI documented, transparent, and communicated to AI actors and those that

	interacting with GAI systems for widely differing applications and contexts of use, including data labeling and preparation, development of GAI models, content moderation, code generation and review, text generation and editing, image and video generation, summarization, search, and chat. These activities can take place within organizational settings or in the public domain. Establishing acceptable use policies and guidance for the use of GAI in formal human-AI teaming settings as well as different levels of human-AI configurations can decrease risks arising from misuse, abuse, repurpose, and misalignment between systems and users. The development and use of structured human feedback mechanisms can also increase the effectiveness of risk management efforts. The effective capture, analysis and integration of user feedback requires human-centered design protocols and domain expertise in fields such as human-AI interaction, cognitive science, human factors engineering, and the social sciences.	○ Audit, validation, and red-teaming of GAI systems. ○ GAI content moderation. ○ Data documentation, labeling, preprocessing and tagging. ○ Decommissioning GAI systems. ○ Decreasing risks of emotional entanglement between users and GAI systems. ○ Discouraging anonymous use of GAI systems. ○ Enhancing explainability of GAI systems. ○ GAI system development and engineering. ○ Increased accessibility of GAI tools, interfaces, and systems. ○ Incident response and containment. ○ Overseeing relevant AI actors and digital entities, including management of security credentials and communication between AI entities. ○ Training GAI users within an organization about GAI fundamentals and risks. ● Define acceptable use policies for the various categories of GAI interfaces, modalities, and human-AI configurations. ● Establish policies to empower accountable executives to oversee GAI system adoption, use, and decommissioning. ● Establish policies for user feedback	interact with GAI systems?

		mechanisms in GAI systems.	

Govern 5.1
 	
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.
	Capabilities, risks, opportunities, and performance characteristics of GAI systems are typically less well-understood than those of more established types of AI. AI actors may have limited visibility and awareness of - or lack the necessary skills and resources to fulsomely address - GAI system risks and impacts across AI lifecycle phases and deployment contexts. The diverse ways and contexts in which GAI systems may be used and repurposed further complicates the systematic solicitation and incorporation of feedback from individuals and communities external to the organization. Individuals and communities may also be impacted by GAI use or content, even if they are not direct users of the technology.
	
	Laddering up structured human feedback to understand societal risks and impacts is complex and a topic of inquiry. To address such challenges, organizations can design policies, procedures, and processes that incentivize and prioritize structured feedback from the many AI actors and community members that may be impacted by GAI systems.
		• Allocate time and resources for outreach, feedback, and recourse processes.
		• Establish processes to bolster and foster internal AI actor culture in alignment with organizational principles and norms and to empower exploration of GAI limitations beyond development settings
		• Enstate processes to enhance transparency across the lifecycle to:
		  ○ Improve AI actors' ability to explore and evaluate GAI capabilities and limitations.
		  ○ Capture external feedback about experiences using GAI technology.
		• Establish the following GAI-specific policies and procedures:
		  ○ Continuous improvement processes for increasing explainability and mitigating other risks.
		  ○ Impact assessments.
		  ○ Incentives for internal AI actors to provide feedback and conduct independent risk management activities.
		  ○ Independent management and reporting structures for AI actors engaged in model and system audit, validation, and oversight.
		  ○ TEVV processes for the effectiveness of feedback mechanisms employing participation rates, resolution time, or
			• Are AI actor credentials, curriculum vitae, resumes or other background information documented and cataloged?
			• Are mechanisms in place to document and review internal team perspectives about organizational culture?
			• Are plans for incentivized internal and external feedback solicitation activities documented?
			• Is the process by which internal and external feedback is incorporated into GAI system development or maintenance clearly documented in organizational policies or procedures, or in relevant model or system documentation?
			• Is the process to appeal, override, or otherwise seek recourse, for harmful GAI system outcomes documented and transparent?

		similar measurements. ○ Empowered cross-functional AI actor teams that exhibit demographic and interdisciplinary diversity. ○ Ownership of feedback and recourse processes. ○ Privacy harms related to large scale or ad-hoc data collection. ○ Recourse mechanisms for harmful data and GAI impacts. ○ Societal impact and harms related to unpredictable GAI capabilities and human perceptions about performance. ○ Structured internal feedback mechanisms throughout the AI lifecycle, e.g., bug reporting, code reviews, formal validation processes, hackathons, internal audit, legal and compliance review, red-teaming. ○ Structured external engagement mechanisms throughout the AI lifecycle, e.g., participatory engagement, citizen juries, user testing, focus groups, audits, assessments, bug bounties, meetings and conferences, hackathons, interest or user groups, product management, public surveys, social media outreach, red-teaming, user research, and A/B testing.	

		○ User feedback mechanisms in GAI user interfaces. ○ Whistleblower protections for AI Actors. ● Disclose interactions with GAI systems to users prior to interactive activities. ● Provide thorough instructions for GAI system users that address feedback or recourse mechanisms. ● Standardize user feedback about GAI system behavior, risks and limitations for efficient adjudication and incorporation.	
Govern 6.1 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.	With the potential and complexity of generative AI (GAI) technologies, organizations may look to acquire, embed, incorporate, procure, or use open source or proprietary third-party GAI systems or generated data. Organizations may also seek advice or assistance about these topics from third-party service providers. Organizations should apply standard or existing risk controls and processes to proprietary or open source GAI technologies, data, and third-party service providers (e.g., acquisition and procurement due diligence, requests for software bills of materials (SBOMs), application of service level agreements (SLAs), statement on standards for attestation engagement (SSAE) reports, conducting background checks, and consideration of sanctioned entity lists). GAI opportunities and	● Define and communicate organizational roles and responsibilities for GAI acquisition, human resources, procurement, and talent management processes in policies and procedures. ● Establish approved GAI technology and service provider lists. ● 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 policies to: ○ Address robotic process automation (RPA), software-as-a-service (SAAS), and other solutions that may rely on embedded GAI technologies. ○ Address ongoing audits, assessments, and alerting, dynamic risk assessments, and real-time reporting tools for monitoring	● Are vendor or service provider assessments documented and standardized? ● Are open source tools addressed in GAI risk management policies, procedures, and documentation? ● Are roles and responsibilities for acquiring and procuring GAI resources documented and with requirements available across the organization? ● Are roles and responsibilities for human resources and talent management for third-party GAI providers documented and available across the organization? ● Do vendor or service provider assessments address GAI risks such as intellectual property infringement? ● Do third-party service providers document their use of GAI, including models or data embedded in standard productivity

	risks may bring new requirements for acquisition, human resources, or procurement risk controls and processes. For example, GAI may give rise to increased intellectual property, data privacy, or information security risks or risks stemming from a general lack of transparency. GAI may also be embedded in standard productivity software, used in third-party solutions or by expert service providers. Organizations may consider varying risk controls for foundation models, fine-tuned models, and embedded tools, enhanced intellectual property, data privacy, and security controls, augmented vendor or service assessments, and bolstering or establishing additional processes and controls for interacting with external GAI technologies or service providers.	third-party GAI risks. ○ Address accessibility, accommodations, or opt-outs in GAI vendor offerings. ○ Address commercial use of GAI outputs and secondary use of collected data by third parties. ○ Assess vendor risk controls for intellectual property infringements and data privacy. ○ Consider policy adjustments across GAI modeling libraries, tools and APIs, fine-tuned models, and embedded tools. ○ Establish ownership of GAI acquisition and procurement processes. ○ Include relevant organizational functions in evaluations of GAI third parties (e.g., legal, information technology (IT), security, privacy, fair lending). ○ Include instruction on intellectual property infringement and other third-party GAI risks in GAI training for AI actors. ○ Screen GAI vendors, open source or proprietary GAI tools, or GAI service providers against incident or vulnerability databases (e.g., AI incident database, AVID, OWASP top-10 for LLMs, and MITRE Att&ck ATLAS). ○ Screen open source or proprietary GAI training data or outputs against patents, copyrights,	tools? ● Do third-party GAI solutions include detailed instructions and documentation to accompany tools? Are any utilized open source tools well-documented? ● Do vendors and third parties present documentation addressing processes and outcomes for GAI risk mitigation?

		trademarks and trade secrets. ● Update GAI acceptable use policies to address proprietary and open source GAI technologies and data, and contractors, consultants, and other third party personnel. ● Update human resource and talent management standards to address acceptable use of generative AI. ● Update third-party contracts, service agreements, and warranties to address GAI risks. ○ Contracts, service agreements, and similar documents may include GAI-specific indemnity clauses, audit rights, dispute resolution mechanisms, and other risk controls.	
Govern 6.2 Contingency processes are in place to handle failures or incidents in third-party data or AI systems deemed to be high-risk.	Organizations may rely on third-party generative AI (GAI) data, productivity tools, models, open source software, or other systems for mission-related tasks. The high variability of GAI data and system applications allows for misuse, abuse, or failure, potentially exposing organizations to negative impacts and reputational harm. Organizations may use materiality, security or privacy risk assessments, or other frameworks to determine risk levels for third-party GAI technologies. To mitigate risks and negative impacts of third-party GAI data and systems, organizations can use contracts and warranties for third-party resources,	● Apply existing organizational risk management policies, procedures, and documentation processes to third-party GAI data and systems, including open source data and software. ● Document incidents involving third-party GAI data and systems, including open source data and software. ● Establish acceptable use policies that address third-party GAI data or systems deemed high-risk by organizational risk tolerance. ● Establish incident response plans for third-party GAI technologies deemed high-risk: ○ Align incident response plans with	● Do GAI acceptable use policies and other policy and procedure documents address third-party data and systems? ● Do GAI policies and procedures document incident response, redundancy, rollover and fallback for high-risk third-party systems? ● Do GAI vendor contracts undergo documented legal review? ● Does the organizational AI inventory include documentation of third-party GAI technologies deemed high-risk by organizational risk tolerance? ● Does third-party GAI system or data

	and establish and rehearse incident response protocols, including deployment of rollover or fallback technologies.	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. ● Establish policies and procedures to address rollover and fallback technologies for GAI data or systems deemed high-risk—rollover and fallback may include manual processing. ● Establish policies that address testing of rollover and fallback processes for GAI data or systems deemed high-risk ● Establish policies and procedures that address GAI data redundancy, including model weights and other system artifacts. ● Establish policies and procedures for continuous monitoring of third-party GAI systems in deployment. ● Identify and document high-risk third-party GAI technologies in organizational AI inventories, including open-source GAI software. ● Participate in AI incident disclosure programs (e.g., AI incident	documentation provided by vendors contain clear instructions for use, meaningful explanation of system mechanisms, and ample contact information?

		database, AVID, OECD AI Incidents Monitor). ● Review vendor contracts. ○ Avoid: ■ Arbitrary or capricious termination of critical GAI technologies or vendor services. ■ Non-standard terms that may amplify or defer liability in unexpected ways. ■ 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). ○ Request: ■ Notification and disclosure for serious incidents arising from third-party data and systems. ■ Service line agreements (SLAs) in vendor contracts that address incident response, response times, and availability of critical support. ● Review GAI vendor documentation for thorough instructions, meaningful transparency into data or system mechanisms, ample support and contact information, and alignment with organizational principles. ● Review GAI vendor release cadences and roadmaps for irregularities and alignment with	

		organizational principles.	