Crosswalk Between BSA Framework to Build Trust in AI and NIST AI Risk Management Framework

BSA FRAMEWORK			NIST AI RISK MANAGEMENT FRAMEWORK
GOVERNANCE			
Governance Framework	**Policies and Processes**	**Objectives:** Integrate AI risk management into broader risk management functions.	**Sec. 1.2.4:** Organizational Integration and Management of Risk: AI risk management should be integrated and incorporated into broader enterprise risk management strategies and processes. Treating AI risks along with other critical risks, such as cybersecurity and privacy, will yield a more integrated outcome and organizational efficiencies.
		Processes: Establish processes for identifying risks, assessing the materiality of those risks, and mitigating risks at each stage of the AI lifecycle.	**Govern 1:** Policies, processes, procedures, and practices across the organization related to the mapping, measuring, and managing of AI risks are in place, transparent, and implemented effectively. **Govern 4.3:** Organizational practices are in place to enable AI testing, identification of incidents, and information sharing. **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. **Measure 3:** Mechanisms for tracking identified AI risks over time are in place. **Manage 3:** AI risks and benefits from third-party entities are managed.
		Evaluation Mechanisms: Establish mechanisms, such as metrics and benchmarks, that the organization will use to evaluate whether policies and procedures are being carried out as specified.	**Govern 1.5:** Ongoing monitoring and periodic review of the risk management process and its outcomes are planned and organizational roles and responsibilities clearly defined, including determining the frequency of periodic review.
		Periodic Review: Organizations should periodically review and update their AI governance framework so it remains fit-for-purpose and capable of addressing the evolving landscape of risk.	**Govern 1.5:** Ongoing monitoring and periodic review of the risk management process and its outcomes are planned and organizational roles and responsibilities clearly defined, including determining the frequency of periodic review.
		Executive Oversight: Governance framework should be backed by executive oversight, including (1) approval of governance policies, (2) active role in overseeing product development lifecycle, and (3) accountability for go/no-go decisions for high-risk systems.	**Govern 2.3:** Executive leadership of the organization takes responsibility for decisions about risks associated with AI system development and deployment.

BSA FRAMEWORK			NIST AI RISK MANAGEMENT FRAMEWORK
GOVERNANCE *(continued)*			
Governance Framework	**Personnel, Roles, and Responsibilities**	**Independence:** Personnel should be structured in a manner that facilitates separate layers of independent review. For example, risk management responsibilities may be split between a product development team, a compliance team, and a governance team.	**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. **Measure 1.3:** 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.
		Competence, Resourcing, and Influence: Provide adequate training and resources for personnel to fulfill their governance functions and ensure that personnel are empowered to address and/or escalate risks.	**Govern 2.2:** The organization's personnel and partners receive AI risk management training to enable them to perform their duties and responsibilities consistent with related policies, procedures, and agreements.
		Diversity: Establish team with diverse perspectives and lived experiences, and include traditionally underrepresented perspectives throughout the lifecycle of the AI design and development process. Where diversity is lacking on internal team, consult with external stakeholders as appropriate.	**Govern 3.1:** Decision-making related to mapping, measuring, and managing AI risks throughout the lifecycle is informed by a diverse team (e.g., diversity of demographics, disciplines, experience, expertise, and backgrounds). **Map 1.2:** 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. **Measure 1.3:** 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. **Measure 4.1:** Measurement approaches for identifying AI risks are connected to deployment context(s) and informed through consultation with domain experts and other end users. Approaches are documented. **Measure 4.2:** 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. **Measure 4.3:** Measurable performance improvements or declines based on consultations with relevant AI actors, including affected communities, and field data about context-relevant risks and trustworthiness characteristics are identified and documented.

BSA FRAMEWORK			NIST AI RISK MANAGEMENT FRAMEWORK
PROJECT CONCEPTION			
Impact Assessment	**Identify and Document Objectives and Assumptions**	Document the intent and purpose of the system.	**Map 1.1:** Intended purposes, potentially beneficial uses, context-specific laws, norms and expectations, and prospective settings in which the AI system will be deployed are understood and documented. Considerations include: the specific set or types of users along with their expectations; potential positive and negative impacts of system uses to individuals, communities, organizations, society, and the planet; assumptions and related limitations about AI system purposes, uses, and risks across the development or product AI lifecycle; and related TEVV and system metrics. **Map 3:** AI capabilities, targeted usage, goals, and expected benefits and costs compared with appropriate benchmarks are understood.
		Clearly define the model's intended effects.	**Map 1.1:** Intended purposes, potentially beneficial uses, context-specific laws, norms and expectations, and prospective settings in which the AI system will be deployed are understood and documented. Considerations include: the specific set or types of users along with their expectations; potential positive and negative impacts of system uses to individuals, communities, organizations, society, and the planet; assumptions and related limitations about AI system purposes, uses, and risks across the development or product AI lifecycle; and related TEVV and system metrics. **Map 2.1:** The specific tasks and methods used to implement the tasks that the AI system will support are defined (e.g., classifiers, generative models, recommenders). **Map 3.3:** Targeted application scope is specified and documented based on the system's capability, established context, and AI system categorization.
		Clearly define intended use cases and context in which the system will be deployed.	**Map 1.1:** Intended purposes, potentially beneficial uses, context-specific laws, norms and expectations, and prospective settings in which the AI system will be deployed are understood and documented. Considerations include: the specific set or types of users along with their expectations; potential positive and negative impacts of system uses to individuals, communities, organizations, society, and the planet; assumptions and related limitations about AI system purposes, uses, and risks across the development or product AI lifecycle; and related TEVV and system metrics. **Map 1.4:** The business value or context of business use has been clearly defined or—in the case of assessing existing AI systems—re-evaluated.
	Select and Document Metrics for Evaluating Fairness	Identify "fairness" metrics that will be used as a baseline for assessing bias in the AI system.	**Measure 1:** Appropriate methods and metrics are identified and applied.
	Document Stakeholder Impacts	Identify stakeholder groups that may be impacted by the system.	**Map 5:** Impacts to individuals, groups, communities, organizations, and society are characterized.

BSA FRAMEWORK			NIST AI RISK MANAGEMENT FRAMEWORK
PROJECT CONCEPTION *(continued)*			
Impact Assessment	**Document Stakeholder Impacts** *(continued)*	For each stakeholder group, document the potential benefits and potential adverse impacts, considering both the intended uses and reasonably foreseeable misuses of the system.	**Map 1.1:** Intended purposes, potentially beneficial uses, context-specific laws, norms and expectations, and prospective settings in which the AI system will be deployed are understood and documented. Considerations include: the specific set or types of users along with their expectations; potential positive and negative impacts of system uses to individuals, communities, organizations, society, and the planet; assumptions and related limitations about AI system purposes, uses, and risks across the development or product AI lifecycle; and related TEVV and system metrics. **Map 5.1:** 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. **Map 5.3:** 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.
		Assess whether the nature of the system makes it prone to potential bias-related harms based on user demographics.	**Measure 2:** AI systems are evaluated for trustworthy characteristics. **Measure 2.3:** AI system performance or assurance criteria are measured qualitatively or quantitatively and demonstrated for conditions similar to deployment setting(s). Measures are documented. **Measure 2.4:** The functionality and behavior of the AI system and its components—as identified in the MAP function—are monitored when in production. **Measure 2.5:** 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. **Measure 2.8:** Risks associated with transparency and accountability—as identified in the MAP function—are examined and documented. **Measure 2.9:** 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. **Measure 2.11:** Fairness and bias—as identified in the MAP function—are evaluated and results are documented.
	Document Risk Mitigations	If risk of bias is present, document efforts to mitigate risks.	**Manage 1:** AI risks based on assessments and other analytical output from the MAP and MEASURE functions are prioritized, responded to, and managed. **Manage 1.3:** 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.

BSA FRAMEWORK			NIST AI RISK MANAGEMENT FRAMEWORK
PROJECT CONCEPTION *(continued)*			
Impact Assessment	**Document Risk Mitigations** *(continued)*	Document how identified risks and potential harms of each risk will be measured and how the effectiveness of mitigation strategies will be evaluated.	**Measure 1:** Appropriate methods and metrics are identified and applied. **Measure 1.1:** 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. **Measure 1.2:** Appropriateness of AI metrics and effectiveness of existing controls are regularly assessed and updated, including reports of errors and potential impacts on affected communities. **Measure 4:** Feedback about efficacy of measurement is gathered and assessed.
		If risk of bias is present, document efforts to mitigate risk.	**Manage 1:** AI risks based on assessments and other analytical output from the MAP and MEASURE functions are prioritized, responded to, and managed. **Manage 1.3:** 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.
		If risks are unmitigated, document why the risk was deemed acceptable.	**Manage 1.4:** Negative residual risks (defined as the sum of all unmitigated risks) to both downstream acquirers of AI systems and end users are documented.
Risk Mitigation Best Practices	**Independence and Diversity**	Seek feedback from a diverse set of stakeholders to inform the impact assessment.	**Govern 3.1:** Decision-making related to mapping, measuring, and managing AI risks throughout the lifecycle is informed by a diverse team (e.g., diversity of demographics, disciplines, experience, expertise, and backgrounds). **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. **Map 1.2:** 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. **Measure 1.3:** 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. **Measure 4.1:** Measurement approaches for identifying AI risks are connected to deployment context(s) and informed through consultation with domain experts and other end users. Approaches are documented. **Measure 4.2:** 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. **Measure 4.3:** Measurable performance improvements or declines based on consultations with relevant AI actors, including affected communities, and field data about context-relevant risks and trustworthiness characteristics are identified and documented.

BSA FRAMEWORK			NIST AI RISK MANAGEMENT FRAMEWORK
	PROJECT CONCEPTION *(continued)*		
Risk Mitigation Best Practices	**Transparent Documentation**	Share impact assessment documentation with personnel working on later stages of the AI pipeline so that risks and potential unintended impacts can be monitored throughout the development process.	**Govern 4.2:** 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. **Measure 1.3:** 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.
	Accountability and Governance	Ensure that senior leadership has been adequately briefed on potential high-risk AI systems.	**Govern 2.3:** Executive leadership of the organization takes responsibility for decisions about risks associated with AI system development and deployment.
	DATA ACQUISITION		
Impact Assessment	**Maintain Records of Data Provenance**	Maintain sufficient records to enable "recreation" of the data used to train the AI model, verify that its results are reproducible, and monitor for material updates to data sources.	**Govern 4.2:** 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. **Manage 3.2:** Pre-trained models which are used for development are monitored as part of AI system regular monitoring and maintenance.
	Examine Data for Potential Biases	Scrutinize data for historical biases.	**Map 2.3:** 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.
		Evaluate "representativeness" of the data.	**Map 2.3:** 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.
		Scrutinize data labeling methodology.	**Map 2.3:** 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.
	Document Risk Mitigations	Document whether and how data was augmented, manipulated, or re-balanced to mitigate bias.	**Map 2.3:** 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.
Risk Mitigation Best Practices	**Independence and Diversity**	To facilitate robust interrogation of the datasets, data review teams should include personnel that are diverse in terms of their subject matter expertise and lived experiences.	**Govern 3.1:** Decision-making related to mapping, measuring, and managing AI risks throughout the lifecycle is informed by a diverse team (e.g., diversity of demographics, disciplines, experience, expertise, and backgrounds). **Map 1.2:** 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. **Measure 1.3:** 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.

	BSA FRAMEWORK		NIST AI RISK MANAGEMENT FRAMEWORK
	DATA ACQUISITION *(continued)*		
Risk Mitigation Best Practices	**Re-Balancing Unrepresentative Data**	Consider re-balancing with additional data.	**Map 2.3:** 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. **Measure 2.11:** Fairness and bias—as identified in the MAP function—are evaluated and results are documented.
		Consider re-balancing with synthetic data.	**Map 2.3:** 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. **Measure 2.11:** Fairness and bias—as identified in the MAP function—are evaluated and results are documented.
	Data Labeling	Establish objective and scalable labeling guidelines.	**Map 2.3:** 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.
	Accountability and Governance	Integrate data labeling processes into a comprehensive data strategy.	**Map 2.3:** 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.
	DATA PREPARATION AND MODEL DEFINITION		
Impact Assessment	**Document Feature Selection and Engineering Processes**	Document rationale for choices made during the feature selection and engineering processes and evaluate their impact on model performance.	**Govern 1:** Policies, processes, procedures, and practices across the organization related to the mapping, measuring, and managing of AI risks are in place, transparent, and implemented effectively.
		Document potential correlation between selected features and sensitive demographic attributes.	**Measure 2.11:** Fairness and bias—as identified in the MAP function—are evaluated and results are documented.
	Document Model Selection Process	Document rationale for the selected modeling approach.	**Govern 1.4:** The risk management process and its outcomes are established through transparent policies, procedures, and other controls based on organizational risk priorities. **Map 2.1:** The specific tasks and methods used to implement the tasks that the AI system will support are defined (e.g., classifiers, generative models, recommenders).
		Identify, document, and justify assumptions in the selected approach and potential resulting limitations.	**Govern 1.4:** The risk management process and its outcomes are established through transparent policies, procedures, and other controls based on organizational risk priorities. **Map 2.2:** 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.

BSA FRAMEWORK			NIST AI RISK MANAGEMENT FRAMEWORK
DATA PREPARATION AND MODEL DEFINITION *(continued)*			
Risk Mitigation Best Practices	**Feature Selection**	Examine for biased proxy features.	**Measure 2.11:** Fairness and bias—as identified in the MAP function—are evaluated and results are documented.
		Scrutinize features that correlate to sensitive attributes.	**Measure 2.11:** Fairness and bias—as identified in the MAP function—are evaluated and results are documented.
	Independence and Diversity	Seek feedback from diverse stakeholders with domain-specific expertise.	**Govern 3.1:** Decision-making related to mapping, measuring, and managing AI risks throughout the lifecycle is informed by a diverse team (e.g., diversity of demographics, disciplines, experience, expertise, and backgrounds). **Map 1.2:** 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. **Measure 1.3:** 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. **Measure 4.1:** Measurement approaches for identifying AI risks are connected to deployment context(s) and informed through consultation with domain experts and other end users. Approaches are documented. **Measure 4.2:** 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. **Measure 4.3:** Measurable performance improvements or declines based on consultations with relevant AI actors, including affected communities, and field data about context-relevant risks and trustworthiness characteristics are identified and documented.
	Model Selection	Avoid inscrutable models in circumstances where both the risk and potential impact of bias are high.	No equivalent category

BSA FRAMEWORK			NIST AI RISK MANAGEMENT FRAMEWORK
VALIDATING, TESTING, AND REVISING THE MODEL			
Impact Assessment	**Document Validation Processes**	Document how the system (and individual components) will be validated to evaluate whether it is performing consistent with the design objectives and intended deployment scenarios.	**Measure 1:** Appropriate methods and metrics are identified and applied. **Measure 2.3:** AI system performance or assurance criteria are measured qualitatively or quantitatively and demonstrated for conditions similar to deployment setting(s). Measures are documented. **Measure 2.4:** The functionality and behavior of the AI system and its components—as identified in the MAP function—are monitored when in production. **Measure 2.5:** 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. **Measure 2.9:** 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. **Measure 2.13:** Effectiveness of the employed TEVV metrics and processes in the MEASURE function are evaluated and documented.
		Document re-validation processes	**Manage 2.2:** Mechanisms are in place and applied to sustain the value of deployed AI systems. **Manage 2.3:** Procedures are followed to respond to and recover from a previously unknown risk when it is identified.
	Document Testing Processes	Test the system for bias by evaluating and documenting model performance.	**Measure 2.11:** Fairness and bias—as identified in the MAP function—are evaluated and results are documented.
		Document how testing was performed, which fairness metrics were evaluated, and why those measures were selected.	**Measure 2.1:** Test sets, metrics, and details about the tools used during TEVV are documented. **Measure 2.11:** Fairness and bias—as identified in the MAP function—are evaluated and results are documented.
		Document model interventions.	**Manage 1.3:** 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. **Manage 2.3:** Procedures are followed to respond to and recover from a previously unknown risk when it is identified. **Manage 2.4:** 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.

	BSA FRAMEWORK		NIST AI RISK MANAGEMENT FRAMEWORK
	VALIDATING, TESTING, AND REVISING THE MODEL *(continued)*		
Risk Mitigation Best Practices	**Model Interventions**	Evaluate potential model refinements to address bias surfaced during testing.	**Manage 1.3:** 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. **Manage 2.3:** Procedures are followed to respond to and recover from a previously unknown risk when it is identified. **Manage 2.4:** 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.
	Independence and Diversity	Validation and testing documentation should be reviewed by personnel who were not involved in the system's development.	**Measure 1.3:** 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.
	PREPARING FOR DEPLOYMENT AND USE		
Impact Assessment	**Document Lines of Responsibility**	Define and document who is responsible for the system's outputs and the outcomes they may lead to, including details about how a system's decisions can be reviewed if necessary.	**Govern 1.5:** Ongoing monitoring and periodic review of the risk management process and its outcomes are planned and organizational roles and responsibilities clearly defined, including determining the frequency of periodic review. **Govern 2.1:** 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.
		Establish management plans for responding to potential incidents or reports of system errors.	**Manage 2.3:** Procedures are followed to respond to and recover from a previously unknown risk when it is identified. **Manage 2.4:** 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. **Manage 4:** Risk treatments, including response and recovery, and communication plans for the identified and measured AI risks are documented and monitored regularly. **Manage 4.1:** 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.
	Document Processes for Monitoring Data	Document what processes and metrics will be used to evaluate whether production data (i.e., input data the system encounters during deployment) differs materially from training data.	**Manage 4.1:** 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. **Measure 4.2:** 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.

	BSA FRAMEWORK		NIST AI RISK MANAGEMENT FRAMEWORK
	PREPARING FOR DEPLOYMENT AND USE *(continued)*		
Impact Assessment	**Document Processes for Monitoring Model Performance**	For static models, document how performance levels and classes of error will be monitored over time and benchmarks that will trigger review.	**Manage 3.2:** Pre-trained models which are used for development are monitored as part of AI system regular monitoring and maintenance. **Manage 4.1:** 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.
		For models that are intended to evolve over time, document how changes will be inventoried; if, when, and how versions will be captured and managed; and how performance levels will be monitored (e.g., cadence of scheduled reviews, performance indicators that may trigger out-of-cycle review).	**Manage 4.1:** 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.
	Document Audit and End-of-Life Processes	Document the cadence at which impact assessment evaluations will be audited to evaluate whether risk mitigation controls remain fit-for-purpose.	**Govern 1.5:** Ongoing monitoring and periodic review of the risk management process and its outcomes are planned and organizational roles and responsibilities clearly defined, including determining the frequency of periodic review.
		Document expected timeline that system support will be provided and processes for decommissioning system in event that it falls below reasonable performance thresholds.	**Govern 1.7:** 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. **Manage 4.1:** 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.
Risk Mitigation Best Practices	**Monitoring for Drift and Model Degradation**	Input data encountered during deployment can be evaluated against a statistical representation of the system's training data to evaluate the potential for data drift (i.e., material differences between the training data and deployment data that can degrade model performance).	**Measure 1.2:** Appropriateness of AI metrics and effectiveness of existing controls are regularly assessed and updated, including reports of errors and potential impacts on affected communities. **Manage 2.2:** Mechanisms are in place and applied to sustain the value of deployed AI systems. **Manage 4.2:** Measurable activities for continual improvements are integrated into AI system updates and include regular engagement with interested parties, including relevant AI actors.
	Product Features and User Interface	Integrate product and user interface features to mitigate risk of foreseeable unintended uses (e.g., interface that enforces human-in-the-loop requirements, alerts to notify when a system is being misused).	**Manage 1.4:** Negative residual risks (defined as the sum of all unmitigated risks) to both downstream acquirers of AI systems and end users are documented. **Manage 2.4:** 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. **Manage 4.1:** 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.

BSA FRAMEWORK			NIST AI RISK MANAGEMENT FRAMEWORK
PREPARING FOR DEPLOYMENT AND USE *(continued)*			
Risk Mitigation Best Practices	**System Documentation**	AI Developers should provide sufficient documentation regarding system capabilities, specifications, limitations, and intended uses to enable AI Deployers to perform independent impact assessment concerning deployment risks.	No equivalent category
		Consider incorporating terms into the End User License Agreement that set forth limitations designed to prevent foreseeable misuses (e.g., contractual obligations to ensure end user will comply with acceptable use policy).	No equivalent category
		Sales and marketing materials should be closely reviewed to ensure that they are consistent with the system's actual capabilities.	No equivalent category
	AI User Training	AI Deployers should provide training for AI Users regarding a system's capabilities and limitations, and how outputs should be evaluated and integrated into a workflow.	**Govern 2.2:** The organization's personnel and partners receive AI risk management training to enable them to perform their duties and responsibilities consistent with related policies, procedures, and agreements.
	Incident Response and Feedback Mechanisms	AI Deployers should maintain a feedback mechanism to enable AI Users and Affected Individuals (i.e., members of the public who may interact with the system) to report concerns about the operation of a system.	**Govern 5.2:** Mechanisms are established to enable the team that developed or deployed AI systems to regularly incorporate adjudicated feedback from relevant AI actors into system design and implementation. **Map 5.2:** 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. **Measure 3.3:** Feedback processes for end users and impacted communities to report problems and appeal system outcomes are established and integrated into AI system evaluation metrics. **Measure 4:** Feedback about efficacy of measurement is gathered and assessed. **Manage 4:** Risk treatments, including response and recovery, and communication plans for the identified and measured AI risks are documented and monitored regularly.