Background

Who we are

The core problem being solved by the Ardent research and development team includes the significant risks and challenges associated with the development, deployment, and management of AI tools.

As AI becomes more pervasive in various critical sectors, from defense, national security, intelligence communities, public safety, disaster response, healthcare, and finance the potential consequences of untrustworthy or irresponsible AI use become more pronounced.

We deliver solutions for customers grounded in the following sociotechnical principles:

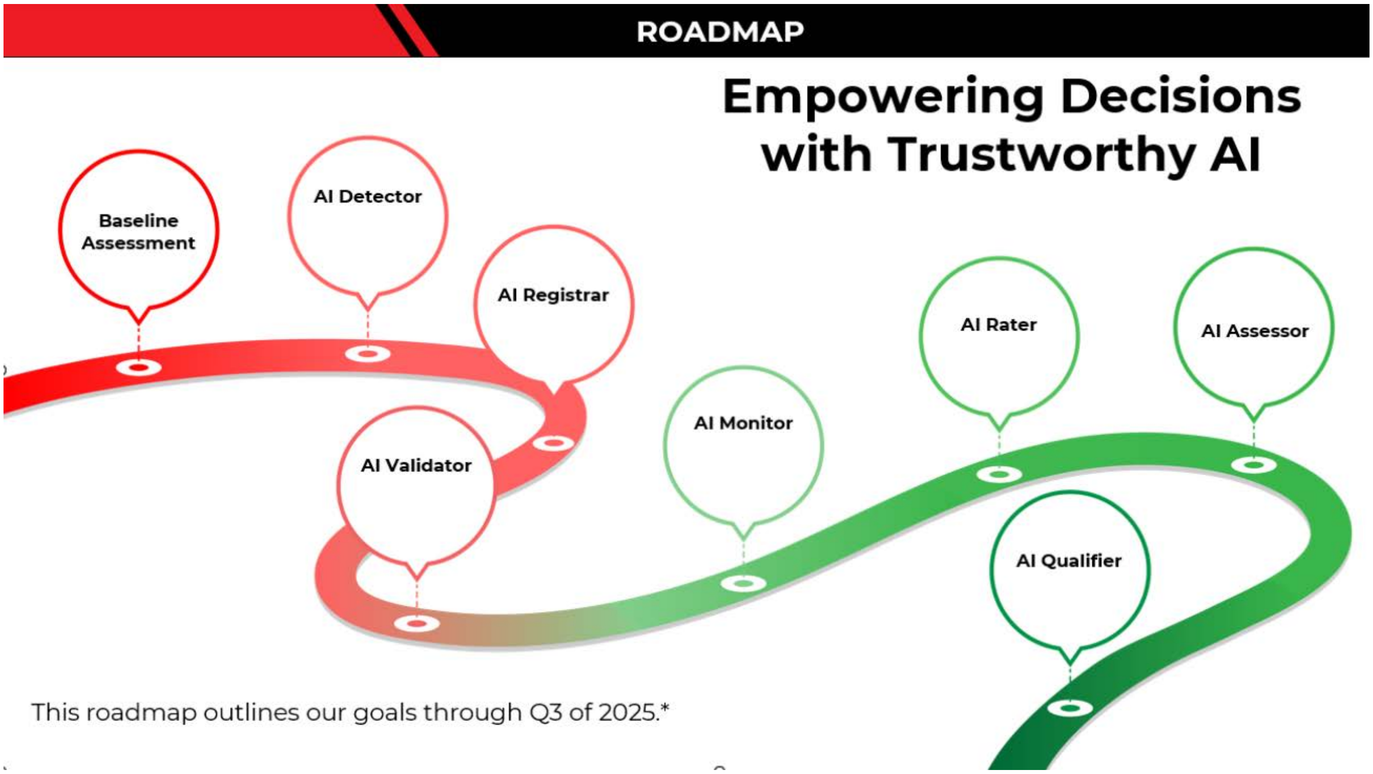
- Safe, Trustworthy, and Secure AI: Build trust and confidence to set standards and safeguards for AI solutions and detects biases, monitors performance, and provides a score for overall trust.
- Transparency & Human-AI collaboration: Provide clear explanation of the use of AI Solutions. Enhance human decision making and the importance of human in the loop feedback.
- Data Privacy and Security: Ensure robust security measures and compliance with data protection regulations. Act as a trustworthy steward of sensitive information used by AI solutions.
- Automation and Zero Trust: Automation that supports scalability, which makes it easier to handle large volumes of processes while continuously monitoring and analyzing threats to support zero trust principles.
- API Integration and Plugins: Enable organizations to tailor the software to their specific needs, promoting innovation and the development of new features. The result is a more integrated and cohesive technology ecosystem.
- Platform Agnostic: Operate on various operating systems and environments. Reduces dependency on specific vendors and allows easy adaptation to future technological change.
- Infrastructure as Code for Deployment: Enable consistent and version-controlled deployments. Reduces time to market and streamlines infrastructure management and fosters collaboration.

What we’re developing

We are building a comprehensive set of tools to manage, monitor, refine and certify AI models across different aspects such as bias, data drift, transparency, and security vulnerabilities.

Ardent delivers solutions to clients across the public sector and private sector. As we build AI safety tools and talk to customers, we are keenly aware that organizations operate at various maturity levels when it comes to adoption of AI Safety practices. This is why the first step of Ardent’s process is to conduct **baseline assessments** with our customers to assess their role in the AI ecosystem, their current maturity level, and identify areas where our toolkit can bridge operational gaps and help advance the maturity level of the organization.

Ardent believes in leveraging strategies from our baseline assessment process to improve the Voluntary Reporting Template (VRT). This will help identify the respondent’s current AI practices and tailor the form as needed to mitigate unnecessary reporting burdens.



ROADMAP

Empowering Decisions with Trustworthy AI

Baseline Assessment

AI Detector

AI Registrar

AI Validator

AI Monitor

AI Rater

AI Qualifier

AI Assessor

This roadmap outlines our goals through Q3 of 2025.*

VRT (Voluntary Reporting Template) Development Strategy Proposal

Goals

1. Administer the VRT(s) in such a way that minimizes the burden for the respondent (e.g. question quantity, phrasing, relevancy)
2. Effectively assess adoption of the NIST AI 600-1 across a wide variety of AI Actors with varying maturity levels

Strategy*

1. **Pre-processing:** Convert the NIST AI 600-1 action list into a database and augment with relevant information to streamline dynamic survey question generation
2. **Baseline assessment:** Assess the organization's AI Actor Role(s) and AI Maturity Level(s) to identify high-relevancy questions
3. **Tailored assessment:** Filter action list and present tailored set of questions to effectively assess NIST AI 600-1 adoption

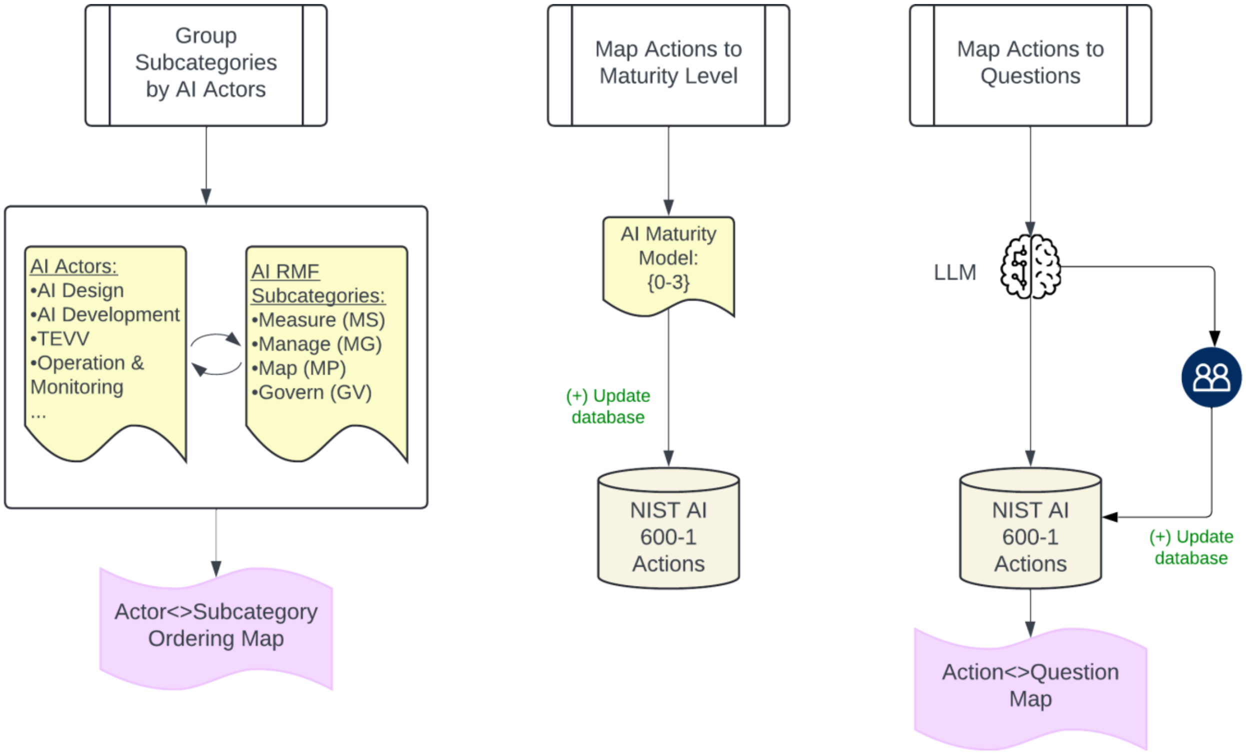
*Note: Below steps represent a suggested strategy with recommendations. Elements (e.g. survey questions) should be modified / tailored further based on the needs determined by NIST, and not used directly as is.

Pre-Processing

Recommendation: As the NIST AI 600-1 document evolves, pre-processing steps may need to be performed again, and database should be updated.

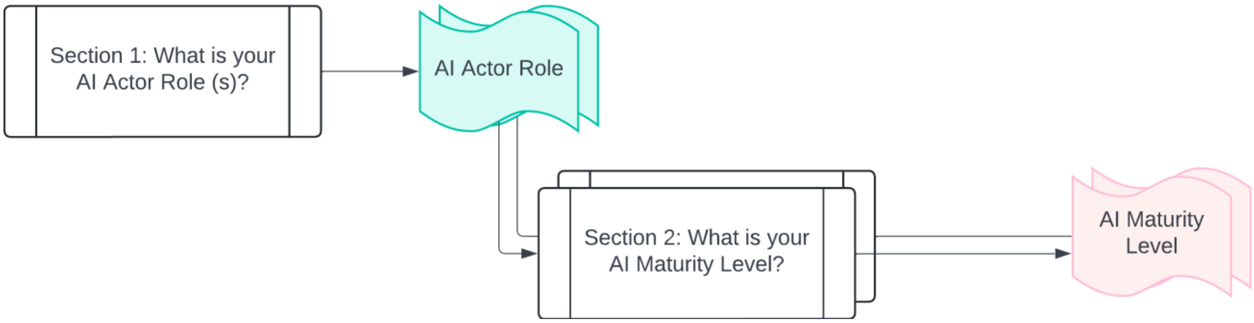
These steps can be performed during a pre-processing phase in order to support dynamic generation of survey questions based on an organization's responses to the baseline assessment.

1. ***Group subcategories by AI Actors*** by parsing through the NIST AI 600-1 document and developing a mapping between AI Actor Role and the most relevant ordering scheme. See Appendix B.
2. ***Map Actions to Maturity Level***. See Appendix A.
3. ***Map Actions to Questions*** using a human-in-the-loop any time a generative AI system is responsible for delivering final output (i.e. survey questions).



Baseline Assessment

Recommendation: Construct the baseline assessment such that it can be completed in under 10 minutes.


Section 1: What is your AI Actor Role (s)?
AI Actor Role
Section 2: What is your AI Maturity Level?
AI Maturity Level

Section 1: Which AI Actor are you?

The initial step is to determine the organization’s AI Actor role(s). This will help determine the organization’s adoption of NIST AI 600-1 particularly for sections most relevant to the organization’s AI activities.

Demographics	
1. Which role(s) does your organization primarily represent in the AI field? (Select all that apply)	• Data Scientist • AI Developer • Domain Expert • Governance/Compliance Officer • End User • Other (please specify)
2. In which industry does your organization primarily work in? (Select all that apply)	• Healthcare • Finance • Technology • Government • Education • Other (please specify)
3. What capabilities does your organization regularly have access to in order to perform AI work?	• Qualified Personnel • Sufficient team sizes • Data infrastructure • Technology Stack • Compliance/Policy Team

Task Engagement

4. Which of the following tasks does your organization frequently engage in? (Select all that apply)	• Articulating AI system concepts and objectives • Gathering and cleaning data • Building or training AI models • Piloting AI systems and ensuring compliance • Monitoring AI system performance • Evaluating user experience • Conducting impact assessments • Other (please specify)
5. How often does your organization collaborate with others in your field for AI-related tasks?	• Very frequently • Frequently • Occasionally • Rarely • Never

Focus Areas	
6. Which of the following areas are prioritized by your organization? (Select all that apply)	• Ethical use of AI • Technical performance • Compliance with regulations • User experience and accessibility • Monitoring and auditing AI systems • Addressing biases in AI outputs
7. What type of AI system does your organization typically work with?	• Decision support systems • Predictive analytics • Autonomous systems • Natural language processing • Other (please specify)

Responsibilities and Expertise	
8. What best describes your organization's primary responsibility? (Select one)	• Designing and planning AI systems • Developing and testing AI models • Deploying and integrating AI systems • Operating and monitoring AI systems • Evaluating and validating AI systems • Providing governance and oversight • Supporting users of AI systems

9. How would you rate your organization’s understanding of the ethical implications of AI?	• Very high • High • Moderate • Low • Very low

Perspectives and Challenges	
10. What challenges do you face in your role as an AI actor? (Select all that apply)	• Lack of clear regulations • Difficulty in ensuring data quality • Challenges in user acceptance and trust • Ethical dilemmas in AI deployment • Technical limitations of AI systems • Other (please specify)
11. What does your organization believe is the most critical factor for the successful deployment of AI systems?	• Robust governance structures • User engagement and feedback • Technical reliability and performance • Ongoing monitoring and assessment • Other (please specify)

Section 2: What is your AI Maturity Level?

After determining the organization’s AI Actor role(s), the organization should receive tailored questions that assess the AI Maturity Level for their given role(s).

AI Design	
1. How well-defined are the objectives and requirements for AI systems in your organization?	• Very clear and documented • Somewhat clear, but not fully documented • Unclear or not documented
2. How regularly do you involve stakeholders (e.g., domain experts, affected communities) in the design phase?	• Always • Often • Sometimes • Rarely • Never

AI Development

1. What is the process for selecting and validating models or algorithms in your organization?	- Formal and documented process - Informal but generally followed - No established process
2. How do you assess the socio-cultural implications of your AI models?	- Regular assessments are conducted - Occasional assessments are conducted - No assessments are conducted

AI Deployment	
1. How does your organization ensure compliance with legal and regulatory requirements during deployment?	- Formal compliance checks are in place - Informal checks are done - No compliance checks
2. How is user experience evaluated during the deployment phase?	- Comprehensive evaluations are conducted - Some evaluations are conducted - No evaluations are conducted

Operation and Monitoring	
1. How frequently does your organization monitor the performance and impacts of deployed AI systems?	- Continuously - Regularly (e.g., weekly, monthly) - Occasionally - Rarely - Never
2. What mechanisms are in place for reporting issues or incidents related to AI systems?	- Formal reporting mechanisms are established - Rudimentary reporting mechanisms are established - Informal reporting is encouraged - No reporting mechanisms are in place

TEVV (Testing, Evaluation, Verification, and Validation)	
1. How often do you conduct verification and validation of AI systems throughout their lifecycle?	- Always - Often - Sometimes - Rarely

	• Never
2. What methods do you use to evaluate AI system performance?	• Quantitative methods • Qualitative methods • A mix of both • No specific methods

Human Factors and Impact Assessment	
1. How is user feedback incorporated into the design and development of AI systems?	• Regularly integrated • Occasionally integrated • Rarely or never integrated
2. How do you assess the social and ethical implications of AI systems?	• Comprehensive assessments are conducted • Some assessments are conducted • No assessments are conducted

Governance and Oversight	
1. What is the role of leadership in overseeing AI projects?	• Actively involved and engaged • Somewhat involved • Not involved
2. How does your organization manage AI-related risks?	• Formal risk management processes are in place • Informal processes are followed • No risk management processes exist

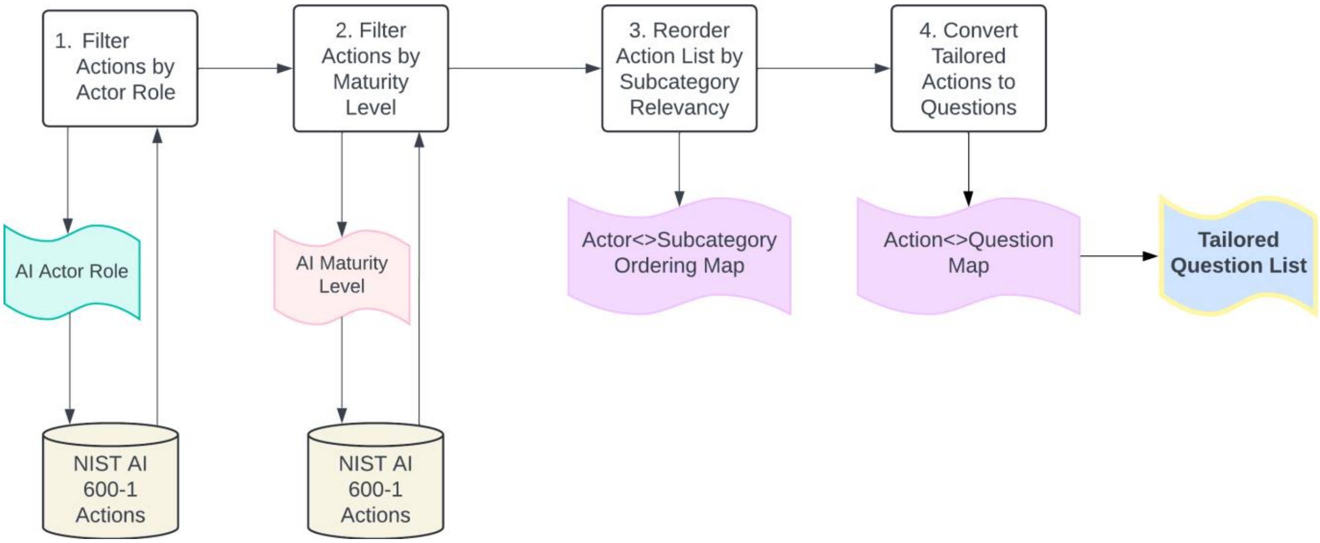
Tailored Assessment

Recommendation: Use a flexible survey tool to generate a dynamic list of questions based on respondents' actor role and maturity level.

Section 3: NIST Generative AI Profile (600-1) Voluntary Reporting

Now that AI Actor role(s) and AI Maturity Level(s) have been determined, the NIST AI 600-1 Actions can be subdivided by AI Actor Role {AR} and AI Maturity Level {ML} to ensure the respondent receives the most relevant questions related to Generative AI Profile adoption.

See the flow charts below describing how to generate a dynamic survey tailored to the respondent.


1. Filter Actions by Actor Role
2. Filter Actions by Maturity Level
3. Reorder Action List by Subcategory Relevancy
4. Convert Tailored Actions to Questions
AI Actor Role
AI Maturity Level
Actor<>Subcategory Ordering Map
Action<>Question Map
Tailored Question List
NIST AI 600-1 Actions
NIST AI 600-1 Actions

4. ***Filter*** all Actions that apply to the organization's AI Actor role(s)
5. Per AI Actor role, ***filter*** by Maturity Level
6. ***Reorder*** the actions by subcategory (i.e. MS, MG, MP, GV), based on the AI Actor Role mapping to most relevant ordering of subcategories. See Appendix B
7. ***Convert*** the list of tasks into questions that can be presented in survey form

Case Study: Ardent Management Consulting

Baseline Assessment

Section 1: Which AI Actor are you?

1. Which role(s) does your organization primarily represent in the AI field? (Select all that apply)
    a. [x] Other: AI Safety Assessments, Testing, and Monitoring
2. In which industry does your organization primarily work in?
    a. [x] Government
    b. [x] Technology
3. Which of the following tasks does your organization frequently engage in? (Select all that apply)
    a. [x] Monitoring AI system performance
    b. [x] Conducting impact assessments
4. How often does your organization collaborate with others in your field for AI-related tasks?
    a. [x] Occasionally
5. Which of the following areas are prioritized by your organization? (Select up to three)
    a. [x] Monitoring and auditing AI systems
    b. [x] Addressing biases in AI outputs
6. What type of AI system does your organization typically work with?
    a. [x] Decision Support Systems
7. What best describes your organization's primary responsibility? (Select one)
    a. [x] Evaluating and validating AI systems
8. How would you rate your understanding of the ethical implications of AI?
    a. [x] High
9. What challenges do you face in your role as an AI actor? (Select all that apply)
    a. [x] Lack of clear regulations
10. What does your organization believe is the most critical factor for the successful deployment of AI systems?
    a. [x] Ongoing monitoring and assessment

Potential Result: AI Actor Role(s) = TEVV, Operation and Monitoring

Section 2: What is your AI Maturity Level?

TEVV

1. How often do you conduct verification and validation of AI systems throughout their lifecycle?
    a. [x] Often
2. What methods do you use to evaluate AI system performance?
    a. [x] Quantitative

Operation & Monitoring

1. How frequently does your organization monitor the performance and impacts of deployed AI systems?
    a. [x] Occasionally
2. What mechanisms are in place for reporting issues or incidents related to AI systems?
    a. [x] Rudimentary reporting mechanisms are established

Potential Result: AI Maturity Level = {TEVV: 3}, {Operation and Monitoring: 2}

Tailored Assessment

1. Filter Actions by AI Actor Role(s} and Maturity Level
    a. $\text{Actions}_{\text{TEVV}}$ | Actor Role == TEVV && Maturity Level == 3
    b. $\text{Actions}_{\text{OM}}$ | Actor Role == Operation and Monitoring && Maturity Level == 2
2. Reorder Task List by Subcategory Relevancy
    a. $\text{Actions}_{\text{TEVV}}$ reordered by {MS, MP, GV, MG}. See Appendix B.
    b. $\text{Actions}_{\text{OM}}$ reordered by {MS, GV, MG, MP}
3. Convert Tailored Actions to Questions
    a. Actions = $\text{Actions}_{\text{TEVV}} \cup \text{Actions}_{\text{OM}}$
    b. Actions --> Questions
4. Present Tailored Questions List

Appendix A: Maturity Model

Recommendation: NIST, in collaboration with industry, should develop a standardized AI Maturity Model that can be used to assess an organization's AI readiness.

Determining a maturity model is not a simple task, but for the purposes of VRT development a quick prototype was generated. First, NIST's Cybersecurity Framework (CSF) 2.0 was considered to understand maturity model assessments.

Table 1: Cybersecurity Framework Tiers

Tier Level	Risk Management
1	There is limited awareness of cybersecurity risks at the organizational level.
2	There is an awareness of cybersecurity risks at the organizational level, but an organization-wide approach to managing cybersecurity risks has not been established.
3	There is an organization-wide approach to managing cybersecurity risks. Cybersecurity information is routinely shared throughout the organization.
4	The organization adapts its cybersecurity practices based on previous and current cybersecurity activities, including lessons learned and predictive indicators. Through a process of continuous improvement that incorporates advanced cybersecurity technologies and practices, the organization actively adapts to a changing technological landscape and responds in a timely and effective manner to evolving, sophisticated threats.

Loosely based on the Cybersecurity Capability Maturity Model, we constructed an AI Maturity Model which maps to an organization's AI readiness and implemented best practices.

Table 2: AI Maturity Model Tiers

Tier Level	Risk Management
1	There is limited awareness of AI risks at the organizational level.

	The organization implements AI risk management on an irregular, case-by-case basis. The organization may not have processes that enable AI policies and best practices to be shared within the organization. The organization is generally unaware of the AI risks associated with its suppliers and the products and services it acquires and uses.
2	There is an awareness of AI risks at the organizational level, but an organization-wide approach to managing AI risks has not been established. Consideration of AI risks in organizational objectives and programs may occur at some but not all levels of the organization. AI risk assessment of internal and third-party assets occurs but is not typically repeatable or reoccurring. AI policy and best practices are shared within the organization on an informal basis. The organization is aware of the AI risks associated with its suppliers and the products and services it acquires and uses, but it does not act consistently or formally in response to those risks.
3	There is an organization-wide approach to managing AI risks. Information related to artificial intelligence risk management policies, including safeguarding sensitive information, is routinely shared throughout the organization. Consistent methods are in place to respond effectively to changes in risk. Personnel possess the knowledge and

	skills to perform their appointed roles and responsibilities. The organization consistently and accurately monitors the AI risks of assets. Senior AI and non-AI executives communicate regularly regarding AI risks. Executives ensure that AI risks are considered through all lines of operation in the organization. The organization risk strategy is informed by the AI risks associated with its suppliers and the products and services it acquires and uses. Personnel formally act upon those risks through mechanisms such as written agreements to communicate baseline requirements, governance structures (e.g., risk councils), and policy implementation and monitoring. These actions are implemented consistently and as intended and are continuously monitored and reviewed.
4	The organization adapts its AI practices based on previous and current AI activities, including lessons learned and predictive indicators. Through a process of continuous improvement that incorporates emerging AI standards and best practices, the organization actively adapts to a changing technological landscape and responds in a timely and effective manner to evolving, sophisticated risks. The organization uses real-time or near real-time information to understand and consistently act upon the AI risks associated with its suppliers and the products and services it acquires and uses. AI policies and best practices are constantly shared throughout the organization and with authorized third parties.

Appendix B: AI RMF Subcategories

The AI RMF Subcategories are as follows:

- Measure (MS)
- Manage (MG)
- Map (MP)
- Govern (GV)

The NIST AI 600-1 document already groups AI Actors under each AI RMF Subcategory. We parsed the document and performed a one-time exercise to identify how AI actors are distributed across each RMF subcategory. See table below:

	GV	MP	MS	MG
AI Design	4	3	0	1
AI Development	2	3	3	1
AI Deployment	4	4	12	9
Operation and Monitoring	7	4	13	9
Test, Evaluation, Verification, and Validation (TEVV)	2	2	17	1
Human Factors	0	2	1	2
Domain Expert	0	3	12	2
AI Impact Assessment	1	2	10	2
Procurement	1	1	0	0
Governance and Oversight	8	1	0	2
Fairness and Bias	1	0	0	0
Affected Individuals and Communities	1	2	3	3
Third Party Entities	2	1	0	2
End Users	0	4	6	3

This table was used to generate AI<>Subcategory Ordering Map referenced in the pre-processing section,. e.g. ‘Operation and Monitoring’ AI Actor is mapped to a {MS, GV, MG, MP} ordering.