



State of Indiana Standard: AI Readiness Assessment Methodology

Version: 1.0 (5/29/2025)

Contents

1	Purpose	2
2	Applicability.....	2
3	Revision History.....	2
4	Ownership	2
5	Definitions	2
6	Procedure.....	3
6.1	Executive Summary	3
6.2	NIST AI RMF Readiness Review Methodology	3
6.3	Core Trustworthiness Dimensions	4
6.3.1	Validity & Reliability	4
6.3.2	Safety & Resilience	4
6.3.3	Security	5
6.3.4	Accountability & Governance	5
6.3.5	Transparency & Explainability	5
6.3.6	Fairness & Non-discrimination	6
6.3.7	Privacy & Data Governance	6
6.4	Practical Considerations	7
6.4.1	Vendor Documentation Review	7
6.4.2	Cross-functional Consultation	7
6.4.3	Contextual Considerations	7
6.4.4	Risk-Based Prioritization	7
6.5	Conclusion	8
7	References.....	8



State of Indiana Standard: AI Readiness Assessment Methodology

Version: 1.0 (5/29/2025)

1 Purpose

This standard is intended to provide transparency into the methodology that MPH utilizes when reviewing AI Readiness Assessments.

2 Applicability

This standard shall apply to all AI Systems, excepting and to the extent those are governed by conflicting provisions in State or Federal law. For the sake of clarity, it applies to AI Systems including, but not limited to, those that are open source, those developed by a State Agency, those developed by a third party, those purchased as commercial off-the-shelf solutions, and combinations thereof.

3 Revision History

Version	Date	Name	Revision Description	Supersedes
1.0	5/29/2025	C. Schilling J. Stark	Initial version	n/a

4 Ownership

Please direct questions and concerns to the following owner(s) of this Procedure:

1. Indiana Management Performance Hub Data Governance team.

5 Definitions

Terms used but not defined herein are established in the Policy (see Section 7 References).

1. "FedRAMP" The Federal Risk and Authorization Management Program (FedRAMP) is a governmentwide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.
2. "GovRAMP" is a registered 501(C)(6) nonprofit membership organization that serves governments and provides services such as a standard method of verifying cloud security, security requirements based on NIST, a security framework, and continuous monitoring.
3. "Data" means Government Information and Personal Information, collectively, as set forth in IC 4-3-26-7 and IC 4-1-6-1(2), respectively.
4. "AI System" means an engineered or machine-based system that can, for a given set of objectives, generate outputs such as predictions, recommendations, or decisions influencing real or virtual environments. AI Systems are designed to operate with varying levels of autonomy.
5. "NIST" means the National Institute of Standards and Technology established by 15 U.S.C. §272.
6. "NIST AI RMF" means the AI Risk Management Framework 1.0 (NIST AI 100-1), adopted January 2023.
7. "OCDO" means the Office of the Chief Data Officer established by IC 4-3-26-9
8. "State Agency" has the meaning set forth in IC 4-3-26-2.
9. "Procedure" means this State of Indiana Standard: AI Readiness Assessment Methodology.
10. "Policy" means the State of Indiana Policy: Artificial Intelligence.



State of Indiana Standard: AI Readiness Assessment Methodology

Version: 1.0 (5/29/2025)

11. “Process” means any operation or set of operations performed, whether by manual or automated means, on Data or on sets of Data, such as the collection, use, storage, disclosure, analysis, deletion, or modification of Data.

6 Procedure

6.1 Executive Summary

“It is the joint responsibility of all AI actors to determine whether AI technology is an appropriate or necessary tool for a given context or purpose, and how to use it responsibly.” – NIST AI 100-1 (AI RMF 1.0)

To ensure the responsible and effective integration of artificial intelligence across State Agencies, it is imperative to establish a thorough assessment process. To accomplish this, the NIST AI Risk Management Framework (NIST AI RMF) provides a structured methodology for assessing AI systems that have been submitted for use by a State Agency.

By focusing on the NIST AI RMF considerations for Trustworthy AI, this framework provides the Management Performance Hub (MPH) with a structured yet flexible approach to evaluating AI systems. Balancing a detailed assessment with practical agency needs ensures that MPH approves AI systems that not only improve government efficiency but are trustworthy systems that can be ethically leveraged.

6.2 NIST AI RMF Readiness Review Methodology



Fig. 1. NIST AI 100-1 (AI RMF 1.0) – Characteristics of trustworthy AI systems

For any AI product or system, this methodology requires thorough examination and research of vendor documentation and critical analysis of how the system’s trustworthiness characteristics align with State of Indiana policy requirements.

The review of these AI systems or products aims to identify potential risks before deployment while recognizing the business value that trustworthy AI can deliver. To do this, the methodology emphasizes seven overarching considerations for AI systems such as:

1. Validity & Reliability
2. Safety & Resilience
3. Security
4. Accountability & Governance



State of Indiana Standard: AI Readiness Assessment Methodology

Version: 1.0 (5/29/2025)

5. Transparency & Explainability
6. Fairness & Non-discrimination
7. Privacy & Data Governance

Throughout, additional practical considerations are evaluated such as:

- Vendor Documentation Review
- Cross-functional Consultation
- Contextual Considerations
- Risk-based Prioritization

After the evaluation, a final risk classification will be determined and sent to the appropriate party for either:

- [Low or Moderate]
 - Exception granted
 - Discretionary intervention
- [High]
 - Additional risk tiering
 - Further review of system or product
 - Exception granted or denial issued

6.3 Core Trustworthiness Dimensions

6.3.1 Validity & Reliability

This evaluation considers whether the AI system or product can consistently perform as intended with an appropriate level of accuracy. This evaluation consists of:

- Are performance claims backed by meaningful evidence?
- Has the system or product gone through testing for the specific use case?
- Are the performance metrics appropriate for the specific use case?

This focuses on the vendor's claims about system performance. Can they be independently verified or are the claims aspirational? Documentation of rigorous testing protocols and real-world use cases is paramount.

6.3.2 Safety & Resilience

This considers whether the proposed AI system or product has been designed with safety in mind. Additionally, consider stress testing through various forms (ex. red teaming). This evaluation includes:

- Has the vendor put time into appropriate guardrails that intentionally prevent harmful actions or outputs?
- How has the vendor mitigated the risk of adversarial inputs or manipulation attempts?



State of Indiana Standard: AI Readiness Assessment Methodology

Version: 1.0 (5/29/2025)

- Does the AI system or product have a human-in-the-loop approach? I.e. What mechanisms for human intervention when necessary.
- What does failure of the system look like?

The primary focus through this evaluation is whether the AI system is ethically sound, and if the appropriate guardrails have been considered. How much time has the vendor put into mitigating future risks for prior deployment?

6.3.3 Security

For any review of this type, a security assessment is critical to consider the data involved and how it's processed through the proposed AI system or product. This evaluation considers:

- Does the system implement appropriate access controls and authentication?
- Will the data being used properly be protected 'in-transit' & 'at-rest'?
- Security Certifications (GovRAMP, FedRAMP, etc.)
- Does the vendor address AI-specific vulnerabilities?
- What does the vendor's incident response look like?

Documentation from the vendor plays a key role in this evaluation. Detailed and transparent security documentation allows for a faster and more efficient evaluation. In turn, faster approval or exception granted.

6.3.4 Accountability & Governance

This evaluation considers whether the AI system or product provides governance mechanisms for oversight and accountability. Such as:

- Does the proposed AI system or product maintain audit trails of usage?
- Are the responsibilities clearly defined between the vendor and agency?
- Can governance controls be configured to match Management Performance Hub (MPH) and Indiana Office of Technology (IOT) policies?
- How does one identify and address potential issues?

Primarily, the focus for this evaluation is verifying whether the proposed AI system or product's governance mechanisms are clearly defined, and whether appropriate planning has been defined for accountability.

6.3.5 Transparency & Explainability

"Transparency for Explainability" – This evaluates the AI system or product's visibility into its operations. Verifying that, as an agency, we can gain deeper insight into the system's functionality to prove the trustworthiness of the proposed system or product:

- Is the documentation comprehensive and understandable?
- What are the known limitations of the system or product?
- Does the vendor allow the disclosure of their product's documentation?



State of Indiana Standard: AI Readiness Assessment Methodology

Version: 1.0 (5/29/2025)

- If not, do they provide demos for explainability to mitigate the risk of the lack of provided documentation?
- How does the system or product mitigate the risk to interpretability?
 - Do they provide a description or mechanism to why an AI system made a particular prediction or recommendation?

The focus here is on whether the vendor's transparency features are usable by the procurer and if they provide meaningful insights rather than superficial explanations.

6.3.6 Fairness & Non-discrimination

This evaluation considers the vendor's due diligence in addressing issues such as harmful bias and discrimination. The vendor's risk management efforts are recognized by:

- Has the AI system or product been tested across diverse populations relevant to the proposed use case's context?
- What bias mitigation strategies have been implemented?
- Can governance parameters regarding fairness be configured to align with the State of Indiana ethical standards?
- Are there governance controls that can be enabled for monitoring bias?
- Does the vendor provide detailed documentation describing their risk management of NIST's identified bias categories?
 - Systemic
 - Computational and statistical
 - Human-cognitive

"Standards of fairness can be complex and difficult to define because perceptions of fairness differ among cultures and may shift depending on application. Organizations' risk management efforts will be enhanced by recognizing and considering these differences." - NIST AI 100-1 (AI RMF 1.0)

6.3.7 Privacy & Data Governance

This assesses whether the AI system or product has safeguards for privacy and appropriate implementation of data governance:

- Does the proposed AI system or product intentionally minimize data collection to what is absolutely necessary?
- Are there appropriate and obvious consent mechanisms in place?
- How are data subject rights supported?
- Are data flow and retention policies clearly defined, understood, and documented?
- How does the AI system or product maintain proper data quality standards?

Similarly to security certifications, any relevant privacy regulations, ex. HIPAA, etc., with proper documentation greatly assist in proving trustworthiness. Configurable privacy controls that enable the AI system or product to match State of Indiana policies assist with this evaluation as well.



State of Indiana Standard: AI Readiness Assessment Methodology

Version: 1.0 (5/29/2025)

6.4 Practical Considerations

6.4.1 Vendor Documentation Review

Throughout the evaluation, a comprehensive review of vendor-provided documentation is completed to specifically look for:

- Evidence-based claims besides marketing statements such as articles.
- Comprehensive disclosure of the AI system or product's limitations and constraints.
- Detailed technical specifications of features that prove trustworthiness.
- Data flow documentation and privacy indicators.
- (If any) - Third party validations or certifications.

The focus is not just that the documentation exists, but the quality and explainability of it. Transparency of the AI system or product's strengths and weaknesses go hand in hand.

6.4.2 Cross-functional Consultation

Recognizing the range of considerations for AI trustworthiness, individuals across domains assist with evaluation to accurately assess all aspects of the proposed AI system or product. Typical consultation consists of:

- Security specialists
- Legal counsel for compliance verification
- Technical staff such as communication between MPH & IOT
- Communication with the agency who submitted the AI system or product for domain-specific validation (IOT is also communicated with in these situations)

6.4.3 Contextual Considerations

Evaluation of AI trustworthiness specifically within the agency and organizational context consists of:

- How does the proposed AI system or product interact with existing systems?
- Is there already a previously procured system or product that has the same functionality?
- Can we effectively operate and govern this system with our resources?
- Does the AI system or product fall into compliance with MPH, IOT, or agency specific policies and obligations?

6.4.4 Risk-Based Prioritization

Priority considerations that may not carry equal weight on every proposed AI system or product consist of:

- The system's decision-making authority and autonomy
- Potential impact on individuals and stakeholder groups and mitigation measures
 - Harm to people
 - Harm to organization
 - Harm to ecosystem



State of Indiana Standard: AI Readiness Assessment Methodology

Version: 1.0 (5/29/2025)

- Sensitivity of the data being processed and used
- Regulatory requirements specific to the use case with the proposed AI system or product

The risk-based approach and scoring ensures that the higher-risk systems receive the appropriate scrutiny while fast-tracking lower/moderate-risk AI systems or products.

6.5 Conclusion

The AI Readiness Scoring Matrix Methodology framework establishes a comprehensive approach to evaluating AI system or product trustworthiness, based on Section 3 of the NIST AI Risk Management Framework. By considering the seven core trustworthiness dimensions, this methodology ensures systematic evaluation of AI systems against established standards. The emphasis on contextual evaluation, transparency behind cross-functional consultation, and risk-based prioritization provides due diligence for defensible approval decisions. Through consistent application of these trustworthiness considerations, MPH can confidently navigate AI adoption while ensuring that deployed AI systems align with state policy and governance standards that are essential for responsible AI implementation.

7 References

1. National Institute of Standards and Technology's AI Risk Management Framework (NIST AI RMF), <https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf>
2. State of Indiana AI Readiness Assessment, <https://in.accessgov.com/mph/Forms/Page/mph/in-state-ocdo-ai-questionnaire/0>
3. State of Indiana Artificial Intelligence Policy, <https://www.in.gov/mph/cdo/files/State-of-Indiana-Artificial-Intelligence-Policy.pdf>
4. State Agency Artificial Intelligence Systems Standard, <https://www.in.gov/mph/cdo/files/State-of-Indiana-State-Agency-AI-Systems-Standard.pdf>