State of North Carolina

Artificial Intelligence Impact Assessment (AIA)

Department of Information Technology
Office of Privacy and Data Protection

Document Information

Revision History

Date	Version	New or Revised Requirement	Description	Author
2/02/2026	1.0	New	Assessment Creation	Office of Privacy and Data Protection

Document Details

Department Name	Office of Privacy and Data Protection
Owner	Martha K. Wewer
Title	Artificial Intelligence Impact Assessment
Publication Date	February 2, 2026
Version	1.0

AIA Risk Scoring Rubric & Instructional Guide

Purpose

This assessment is designed to assist North Carolina agencies evaluate the risks associated with the use of Artificial Intelligence (AI) systems, the North Carolina Responsible Use of AI Framework and complies with the Governor's Executive Order on AI. Agencies must use this document to assess and manage risk associated with the specific use of AI before deployment and on a continuing basis once AI is deployed. This template is provided as a standardized method for evaluating the risk of AI systems used by North Carolina agencies, based on governance, oversight, model capabilities, data protection, performance, security, and access controls and provides transparency and documentation of the agency's due diligence.

Instructions:

1. **Complete All Sections**
   Respond to each question across the four (4) sections:
   - Governance & Accountability (to be completed by Agency Privacy/Security Liaison)
   - System and Data Mapping
   - Testing and Evaluation
   - Mitigation and Monitoring
2. **Provide Supporting Documentation**
   Where applicable, attach or reference relevant policies, procedures, audit reports, training materials, or system documentation.
3. **Be Specific and Transparent**
   Clearly describe processes, safeguards, and oversight mechanisms. If a question does not apply, indicate "Not Applicable" and explain why.
4. **Collaborate Across Teams**
   Engage privacy, security, legal, and technical teams to ensure comprehensive and accurate responses.
5. **Prepare for Scoring**
   After completing the questionnaire, please submit this document to privacy@nc.gov. OPDP will review using the scoring rubric to assess the overall risk level of the AI system. This will inform the documented risk level and any required mitigations or training.
6. **Questions?** Contact the Office of Privacy and Data Protection at **privacy@nc.gov**

Risk Categories & Scoring Dimensions

Each section of the AIA form will be scored across **three dimensions**:

Dimension	Description
Impact Level (FIPS 199)	Assesses potential impact on confidentiality, integrity, and availability.
Data Sensitivity	Evaluates the type and sensitivity of data processed (e.g., PII, PHI, confidential).
Use Case Criticality	Measures how critical the AI system is to public services, safety, or decision-making.

Risk Level Matrix

Impact Level	Data Sensitivity	Use Case Criticality	Overall Risk Level
High	High	High	**High**
Moderate	Moderate	Moderate	**Moderate**
Low	Low	Low	**Low**
Mixed	Highest of any	Highest of any	**Highest Applies**

Note: If any one dimension is rated **High**, the overall risk level is **High**.

Scoring Rubric

Each section of the OPDP AIA form will be scored using the following:

Section 1: Governance & Accountability
Score 0–3: No documentation or unclear ownership
Score 4–6: Partial documentation, roles mostly identified
Score 7–10: Clear governance, roles, and accountability defined

Section 2: System and Data Mapping
Score 0–3: Lack of clear purpose or use case; no data inventory
Score 4–6: Partially outlined purposes, inventories and data sources mostly identified
Score 7–10: Documented purposes, identified data types and sources clearly articulated

Section 3: Testing and Evaluation
Score 0–3: No PTA/PIA, no fairness, bias or rights and safety information
Score 4–6: Some information articulated, limited transparency
Score 7–10: Full lifecycle evaluation, bias mitigation, transparency

Section 4: Mitigation and Monitoring
Score 0–3: No performance metrics or monitoring, no data protection plan
Score 4–6: Some metrics, limited monitoring, no clear mitigation strategy
Score 7–10: Continuous monitoring, clear and attached mitigation strategy

Final Risk Rating & Decision Matrix

Total Score	Risk Level	Approval Decision
0–20	High	Not Approved
21–35	Moderate	Approved with Mitigations
36–50	Low	Approved

Safeguard Identification Scale

Level	Description
Not Identified	No safeguards reviewed
Partially Identified	Some safeguards noted
Mostly Identified	Most safeguards in place
Fully Identified	All safeguards documented
Not Applicable	No safeguards needed for use case

Training Required: If risk level is Moderate or High, additional AI literacy training may be required.

Section 1 – Governance and Accountability

(To be completed by Agency Security or Privacy Liaison)

a. System Name/System ID:		
b. Version:		
c. Agency/Department:		
d. Desired Deployment Date:		
e. Privacy/Security Liaison:		
f. System Owner:		
g. Project Manager:		
h. Applicable Statutes Agency must comply with:		
i. Risk Tolerance Statement:		
j. Existing Contract or SLA in Place	Yes ☐	No☐
k. Oversight Body or Review Board Involved:		
l. AI feature can be enabled/disabled by user:	Yes ☐	No☐

Section 2 - System and Data Mapping

2a. System Purpose/Business Objective:

i. What other approaches to solving this problem were considered (if any) and why were they rejected?

ii. If the system will assist with or make decisions, which individuals/roles are currently responsible for making these decisions now informed by the system?

2b. Deployment Environment (Cloud/On-Prem/Hybrid):

2c Data Types Processed – please select one from the boxes and explain all the elements of the data:

PII ☐ PHI ☐ FTI ☐ Other ☐

2d. If identifiable data is being used will the data be de-identified before use:

Yes ☐ No☐

If yes: please include data protection plan in Section 4c.

2e. Data Sources and Provenance:

2f. Sensitive Data Categories (PII, PHI Images, Biometrics, FTI, CUI, etc.)

2g. Stakeholder Groups Affected: i. Are you providing notice to the individuals whose information is being collected if the information is identifiable? If so, please include the language here.

2h. Any potential or identified unintended uses? If so, how will you prevent those uses.

Section 3 - Testing and Evaluation

a. PTA Completed	Yes ☐	No☐
b. PIA Completed	Yes ☐	No☐
c. Rights Impacting and Safety Impacting	Yes ☐	No☐
d. Fairness Testing Conducted (Groups/Attributes Tested):		
e. Bias Mitigations Applied:		
f. Explainability Method (Ex. Model Card, SHAP, etc.):		
g. Transparency Limitations Identified:		

h. Safety Tests Conducted (Stress Adversarial, Drift):	
i. Reliability Metrics (Accuracy, FPR/FNR, Latency):	
j. Environmental Impact Estimate CO2e Compute Hours if known:	
k. Economic Impacts Identified (Costs, Workforce):	
l. PII Categorization on your approved PTA/PIA (Low, Medium, High)	Low ☐ Medium ☐ High ☐

Section 4 - Mitigation and Monitoring

a. Mitigation Actions Required (ex. Hallucinations, data leaks into unauthorized folders):	
b. Data protection plan: including but not limited to de-identification, anonymization, hashing, etc.	
c. Monitoring Plan (Metrics, Frequency):	
d. Incident Response Plan?	Yes ☐ No☐
e. Human in the Loop?	Yes ☐ No☐

f. Reassessment Trigger Conditions:	
g. Describe the process and frequency for software updates and patch management:	

Risk Rating and Mitigation Decisions

Score:	_____
Overall Risk Rating:	Low ☐ Medium ☐ High ☐
Decision:	☐Approved ☐Approved with Mitigations ☐Not Approved
Mitigations Required:	_____
Training required before using this system (for Medium or High):	Yes ☐ No☐
State Chief Privacy Officer Signature:	
Information Security Officer Signature:	
Privacy Liaison Officer Signature:	
Records Liaison Officer Signature:	
AI Impact Assessment Number:	
Date Reviewed:	