

Functional Area Summary | Risk at a Glance

For a summary view of the assessment, security program practices and mechanisms were correlated across twelve (12) functional areas, represented below with a rationalized risk summary to indicate the overall risk for a given area.

Risk Definitions

Risk Rating	Definition <i>(Aligned with NIST SP 800-30)</i>
Low	AI risk controls are in place and operating effectively. Minor opportunities for optimization or documentation may exist but pose no material risk. No immediate action required.
Moderate	AI risk controls are partially in place or inconsistently applied. Gaps should be addressed through planned remediation within normal business cycles.
High	A significant gap or insufficient control exists that could expose the organization to AI-enabled harm, regulatory noncompliance, or reputational damage. Prioritized corrective action is recommended.

Risk by Functional Area

Functional Area	Area Risk
AI Governance & Accountability	Moderate
AI Risk Management Framework	High
AI Model Inventory & Lifecycle	Moderate
Data Governance & Quality	Moderate
Trustworthiness & Bias Management	High
AI Security & Adversarial Robustness	High
Privacy & Data Protection for AI	Moderate
AI Transparency & Explainability	Moderate
Third-Party & AI Supply Chain Risk	High
AI Incident Response & Monitoring	Moderate
Human Oversight & AI Decision Controls	Moderate
AI Compliance & Regulatory Alignment	Moderate