PROCINCTUS SECURITY CONSULTING 

AI Risk Assessment Template

(Insert your small left-aligned logo here, then place the title block to the right in Word.)

Executive Summary

Provide a concise overview of the system, its purpose, and the scope of this assessment. Summarize key risks, impacts, and recommended actions.

System Overview

System Name: System Owner: Business Purpose: AI/ML Components Used: Data Sources and Data Flows: Third-Party Integrations:

AI Functionality Description

Describe how AI is used within the system, including:

- Model type (LLM, classifier, recommender, etc.)
- Training data sources
- Inference workflow
- Automation level
- Decision-making role (advisory, automated, high-impact)

Data Classification & Sensitivity

Identify all data processed by the AI system:

- Public
- Internal
- Confidential
- Regulated (HIPAA, PCI, GDPR, etc.)
- Personal Identifiable Information (PII)
- Sensitive Personal Data

Include:

- Data retention
- Data minimization
- Data lineage
- Data access controls

Threat Modeling

Evaluate risks across the AI lifecycle:

1. Data Risks

- Poisoning
- Leakage
- Unauthorized access

2. Model Risks

- Model inversion
- Membership inference
- Adversarial inputs
- Model theft

3. Operational Risks

- Misuse
- Drift
- Hallucinations
- Over-reliance

4. Business Risks

- Compliance violations
- Reputational harm
- Financial impact

Risk Analysis

For each identified risk:

- Risk ID

- Description
- Likelihood (Low / Medium / High)
- Impact (Low / Medium / High)
- Risk Score
- Mitigation Strategy
- Residual Risk

Security Controls

Document implemented and planned controls:

- Access control
- Encryption
- Monitoring & logging
- Model governance
- Data validation
- Human-in-the-loop review
- Incident response procedures

Compliance & Policy Alignment

Assess alignment with:

- NIST AI RMF
- ISO 42001
- SOC 2
- GDPR / CCPA
- Internal corporate policies

Testing & Validation

- Model accuracy testing
- Bias and fairness evaluation
- Red-team testing
- Adversarial testing
- Performance and drift monitoring

Final Recommendations

Summarize required actions, timelines, and responsible parties.

Approvals

Prepared By:

Reviewed By:

Approved By: Date: