INTERNAL REVIEW DRAFT

AI Risk Assessment

Sample Company LLC

Prepared as a structured operating document for internal use, review, and controlled distribution.

Review this document after major operational, regulatory, or technology changes.

Version 1.0

DOCUMENT CONTROL

RECOMMENDED

PREPARED FOR Sample Company LLC	**DOCUMENT OWNER** Plan Owner
CLASSIFICATION Confidential	**DISTRIBUTION** Executive Leadership, Process Owners
GENERATED July 21, 2026	**NEXT REVIEW DATE** 2027-07-21
STATUS Internal Review Draft	**DOCUMENT VERSION** 1.0
TEMPLATE VERSION 1.0.0	**TARGET CONTROL LEVEL** Recommended
FRAMEWORKS Core baseline only	

Table of Contents

INFO: IMPORTANT NOTICE — READ BEFORE USE

This assessment was generated as a structured starting template from the information provided. It does not constitute legal, regulatory, or professional compliance advice, and it does not by itself establish or prove compliance with any framework or regulation. Specific obligations vary by jurisdiction, industry, and circumstance. Before adopting or relying on it, have this assessment reviewed by qualified legal counsel and the appropriate internal owners, and adapt it to your organization's actual environment.

Governance

Executive Summary

This AI Risk Assessment captures Sample Company LLC's AI use posture and risk profile, anchored on the NIST AI Risk Management Framework (AI RMF) MAP and MEASURE functions. The assessment covers 4 AI systems cataloged, six AI risk categories assessed under the MEASURE function, four MEASURE-function monitoring capabilities, and four AI-specific vendor risk dimensions. Sample Company LLC is a Technology-sector organization of approximately 50-100 employees operating across 1-3 business locations.

Residual AI risk profile: grade C. 2 categories are rated High, 3 Medium, 1 Low, and 0 Not Applicable. At this profile, two High-rated AI risks need active mitigation; this is the typical profile of an organization mid-program-build.

The High-rated categories are Accuracy and Hallucination Risk, and Privacy and Regulatory Risk; treatment actions for each are documented in the AI Risk Register and prioritized in the Risk Treatment Plan.

NIST AI RMF organizes risk management around four core functions: Govern (accountability and policy), Map (identify and categorize AI risks), Measure (assess and quantify risks), and Manage (prioritize and treat risks). This assessment focuses on MAP (the six risk categories surveyed below) and MEASURE (the monitoring and incident-tracking capabilities). The Govern function is documented in the AI Governance Policy; the Manage function is operationalized through the prioritized treatment plan in the final section of this assessment.

AI System Inventory

The inventory catalogs 4 AI systems in use across the organization. This inventory is the scope boundary for the rest of the assessment — risks identified below apply to these systems, and any AI tool not listed here is by definition shadow AI requiring sanction or removal.

AI System Inventory

SYSTEM	VENDOR	USE CASE	DEPLOYMENT	DATA TYPES PROCESSED
Customer support drafting assistant	Vendor A	Draft customer email responses	SaaS / vendor-hosted	Customer PII, Internal documents
Code generation copilot	Vendor B	Developer productivity	API integration	Source code, Internal documents
HR screening assistant	Vendor C	Resume summarization for recruiters	SaaS / vendor-hosted	Employee PII
Marketing content generator	Internal model team	Blog and social drafts	Self-hosted / on-prem	Public data only

2 of 4 cataloged AI systems process regulated or sensitive data (PII). These systems carry the highest privacy-risk concentration and warrant DPA / BAA review and DLP enforcement at the input boundary.

Risk Assessment

AI Data Flow Posture

AI data flow analysis evaluates four boundary controls: what data can enter AI tools, where AI vendors process and store that data, whether vendors use it for training, and whether AI outputs are reviewed before use. Together these define the organization's AI data exposure surface.

AI Data Flow Posture

CONTROL	STATUS
Input controls	Partial: guidelines exist but not enforced
Data residency	Partially: some vendors specify, others do not
Training-data opt-out	Some vendors
Output review	Sometimes: depends on use case

Guidelines on AI input exist but rely on employee compliance rather than technical enforcement; this is a frequent source of accidental data leakage.

Data residency is contractually defined for some vendors but not others; the gap should be closed through vendor renegotiation or replacement.

Some AI vendors have been opted out of training-data use, but coverage is incomplete; the remaining vendors may use organizational inputs to improve their models, which can leak data through future outputs.

Human review of AI outputs is conditional on use case; the per-use-case review threshold should be documented to avoid drift.

AI Risk Register (NIST AI RMF MAP)

The NIST AI RMF MAP function identifies AI-specific risks; the MEASURE function assesses and quantifies them. The six categories below reflect the failure modes most directly applicable to organizational AI deployment, each cross-referenced to the MEASURE subcategory under which it is evaluated. Each is rated High, Medium, Low, or Not Applicable based on the impact of a realized failure in this organization's context.

AI Risk Register (NIST AI RMF)

RISK CATEGORY	RATING	NIST AI RMF REFERENCE
Accuracy and Hallucination Risk	⚠ HIGH	NIST AI RMF MEASURE 2.5 (validity and reliability of the deployed AI system)
Bias and Discrimination Risk	◐ MEDIUM	NIST AI RMF MEASURE 2.11 (fairness and bias are evaluated and documented)
Privacy and Regulatory Risk	⚠ HIGH	NIST AI RMF MEASURE 2.10 (privacy risk of the AI system is examined and documented)
Security and Adversarial Attack Risk	◐ MEDIUM	NIST AI RMF MEASURE 2.7 (AI system security and resilience are evaluated and documented)