AI Risk Assessment & Governance - Chatbot System

Sample Project | No Real Data Used

Role: AI Risk & Governance Analyst

Responsibilities:

- AI risk identification and classification
- Likelihood and impact assessment
- Regulatory impact analysis (EU AI Act)
- Definition of governance and oversight controls
- Executive-level risk documentation

Date: December 2025
Version: 1.0

AI System Description

The assessed system is an AI-powered customer support chatbot designed to answer user questions using internal company documentation.

Purpose

Improve customer support efficiency while ensuring responsible, secure, and compliant AI usage.

Methodology

AI risks were identified based on guidance from the EU AI Act, NIST AI Risk Management Framework, and OWASP Top 10 for LLM Applications. Risks were evaluated based on likelihood, potential impact, and regulatory considerations.

Sample Project | No Real Data Used

Key AI Risks

Risk	Description	Risk Level
Hallucinations	Generation of incorrect or misleading responses	High
Data Leakage	Exposure of sensitive data through prompts	High
Bias	Unequal or unfair responses	Medium

EU AI Act Classification

The system is classified as Limited Risk under the EU AI Act. Transparency and user awareness obligations apply.

Mitigation Measures

- Human oversight and response review
- Data filtering and input/output controls
- Regular testing and bias monitoring

Residual Risk

Residual AI risks remain Medium and require continuous monitoring and governance.

AI Governance Recommendations

- Establish an AI usage and governance policy
- Define accountability and human oversight roles
- Implement AI incident response and review procedures

Sources

- EU AI Act (high-level guidance)

Sample Project | No Real Data Used

- NIST AI Risk Management Framework
- OWASP Top 10 for LLM Applications
- Industry publications on responsible AI

Sample Project | No Real Data Used