Cloud Risk Assessment - AWS Environment
Sample Project | No Real Data Used

Role: Cloud & AI Risk Analyst

Responsibilities:

- Risk identification and analysis
- Likelihood and impact assessment
- Development of mitigation recommendations
- Executive-level risk reporting

Date: December 2025
Version: 1.0

Overview

This assessment evaluates cybersecurity risks associated with a customer-facing web application hosted on Amazon Web Services (AWS). The objective is to identify key cloud-related risks, assess their potential impact, and recommend appropriate mitigation controls aligned with industry standards.

Scope

- AWS cloud environment
- Customer-facing web application
- Backend database storing personal data
- Identity and Access Management (IAM)

Methodology

The assessment was conducted using a risk-based approach aligned with **ISO/IEC 27005** and **NIST Cybersecurity Framework (CSF)**. Risks were identified through asset analysis, review of common cloud misconfiguration scenarios, and evaluation of shared responsibility between the cloud provider and the customer.

Key Assets

- Web application (customer portal)
- Database containing personal data (PII)
- IAM system managing user access

Risk Identification & Assessment

Risk	Description	Likelihood	Impact	Risk Level
Data Leakage	Misconfigured storage or lack of encryption	Medium	High	High
Unauthorized Access	Weak IAM controls or lack of MFA	Medium	High	High
Service Disruption	Insufficient monitoring and backups	Low	Medium	Medium

Shared Responsibility Model

AWS Responsibilities:

- Physical security
- Infrastructure availability

Customer Responsibilities:

- IAM configuration
- Data protection and encryption
- Logging and monitoring

Risk Treatment & Mitigation

- Encryption at rest and in transit
- Least privilege access and multi-factor authentication (MFA)
- Centralized logging, monitoring, and regular backups

Residual Risk

After implementing the recommended controls, residual risks are reduced to **Medium** and considered acceptable.

Executive Summary

Primary cloud risks are driven by IAM misconfiguration and potential data exposure. Applying standard cloud security controls significantly improves the organization's security posture and reduces overall risk.

Sources

- AWS Shared Responsibility Model
- AWS Well-Architected Framework
- NIST Cybersecurity Framework (CSF)
- ISO/IEC 27001 & 27005
- Cloud Security Alliance (CCM)