Third-Party Vendor Risk Assessment

Problem Statement

Organizations rely on third-party vendors to deliver critical services, but vendors can introduce cybersecurity and compliance risks due to shared access to sensitive data. Without a structured vendor risk assessment process, organizations may be exposed to data breaches, regulatory violations, and operational disruptions. This project simulates a third-party risk assessment aligned with NIST CSF.

Scope & Assumptions

- Hypothetical SaaS payroll vendor
- Access to employee PII and financial data
- Vendor considered business-critical
- Assessment based on documentation and questionnaires

Methodology

Identified vendor data access and criticality, classified data sensitivity, assessed inherent risk, evaluated existing controls, assigned likelihood and impact ratings, calculated overall risk, and developed mitigation recommendations.

Key Findings

Vendor processes sensitive PII and financial data, provides a SOC 2 report, but has limited transparency into incident response testing and inconsistent MFA enforcement.

Recommendations

Require annual SOC 2 Type II review, enforce MFA for all users, establish incident notification SLAs, and conduct annual reassessments.

Outcome

Improved visibility into third-party risk, reduced likelihood of data exposure, and strengthened vendor governance.