# Enterprise Risk Register – Mock FinTech Organization

## 1. Project Overview

This project focuses on the creation of an enterprise information security risk register for a mock FinTech organization operating in a cloud-based environment. The objective was to identify, assess, and manage key operational, technical, and compliance-related risks using standard Governance, Risk, and Compliance (GRC) practices.

The risk register was designed to support structured risk prioritization, informed decision-making, and ongoing risk monitoring across security and business functions.

## 2. Mock Organization Background

Organization Type: FinTech / Digital Payments
Organization Size: Approximately 150 employees
IT Environment: Cloud-based infrastructure
Data Handled**:** Customer personal data, transaction metadata, and internal business information

Due to its reliance on cloud services and the handling of sensitive financial data, the organization faces elevated cybersecurity, operational, and regulatory risks. Implementing a structured risk register helps improve visibility into these risks and supports proactive risk treatment

## 3. Project Scope

**In Scope**

- Information security and operational risks
- Cloud infrastructure and identity management
- Third-party vendor risk
- Incident response and security operations
- Compliance documentation and data protection

**Out of Scope**

- Penetration testing and vulnerability exploitation
- Financial risk modelling
- Legal enforcement or regulatory filing activities

## 4. Risk Assessment Methodology

**Risk Identification**

Risks were identified through a review of the organization’s cloud environment, security processes, operational workflows, and compliance requirements.

**Risk Scoring Approach**

- **Likelihood** was rated on a scale of 1 (Low) to 5 (High)
- **Impact** was rated on a scale of 1 (Low) to 5 (High)
- **Risk Score** was calculated as *Likelihood* × *Impact*

**Risk States Tracked**

- **Pre-Mitigation (Inherent Risk):** Risk before any controls
- **Current Risk:** Risk after existing controls
- **Post-Mitigation (Residual Risk):** Expected risk after planned actions

This approach supports consistent risk comparison and prioritization.

## 5. Risk Register Summary

**Total Risks Identified:** 10

**Risk Categories Covered:**

a. Cloud security
b. Identity and access management
c. Third-party risk
d. Incident response readiness
e. Compliance and data protection

The risk register highlights cloud misconfiguration, access control weaknesses, and third-party dependencies as key risk themes requiring focused attention.

## 6. Risk Treatment and Governance

Each risk includes:

- Assigned risk owner
- Defined risk response (Mitigate, Transfer, or Accept)
- Documented mitigation actions
- Escalation level based on risk severity
- Review dates, progress, and historical progress tracking

This governance structure supports accountability and ongoing risk lifecycle management.

## 7. Outcomes and Key Learnings

Through this project, I gained practical exposure to:

- Enterprise risk assessment and scoring techniques
- Development of a structured risk register
- GRC documentation and governance practices
- Understanding how SOC, cloud security, and compliance risks intersect
- Tracking risk progress and historical actions over time

The project strengthened my understanding of how organizations manage cybersecurity risk in real-world environments.

## 8. Disclaimer

This project was developed using a fictional organization for learning and demonstration purposes only. No real organizational data was used.