

Fraud-to-Control Gap Analysis in a Banking environment

Executive Summary:

This project seeks to assess the common banking fraud scenarios faced by Dizzy Financial Solutions Ltd(fictional) and evaluate the effectiveness of existing controls. The analysis seeks to identify control gaps and recommend remediation actions aligned with globally recognized frameworks such as NIST CSF and COSO.

Fraud Scenarios Assessed:

1. Account Takeover
2. Insider Fraud
3. Identity Fraud

Existing Controls Assessment:

Fraud Type	Existing Control	Effectiveness
Account Takeover	Password Policy	Weak
Insider Fraud	Background Checks	Moderate
Identity Fraud	Manual Reviews	Weak

Control Gap Analysis:

Fraud Type	Control Gap	Risk Impact
Account Takeover	No MFA	High
Insider Fraud	No user activity monitoring	High
Identity Fraud	No automated detection	Medium

Framework Mapping:

Gap	Recommended Control	Framework
Weak Authentication	MFA	NIST PR.AC
Poor detection	SIEM and Monitoring logs	NIST DE.CM
Manual Reviews	Automated Analytics software	COSO

Recommendations and Prioritization:

High priority –

Implementation of MFA for customer and staff member access to employees and customer portals/web/app.

Deployment of a centralized logging and monitoring system for fraud detection.

Medium priority –

Automation of identity verification processes and enhancement of transaction monitoring rules and triggers.

Conclusion:

The analysis completed signifies the importance of aligning fraud prevention efforts with cybersecurity and governance controls. Addressing the identified gaps will significantly reduce financial losses and regulatory risks for Dizzy Financial Solutions Ltd.