NIST CSF Risk Assessment – Financial Services Organization

Executive summary:

Organization: Dizzy Financial Solutions Ltd(fictional)

Industry: Financial Services

Framework: NIST Cybersecurity Framework

This risk assessment was conducted to evaluate Dizzy financial Solutions Ltd cybersecurity posture and identify risks that could impact the confidentiality, integrity, and availability of critical systems and customer data.

The assessment focused on key business assets, identified major cyber threats and vulnerabilities, evaluated inherent risks, and mapped existing and recommended controls to the NIST CSF. The objective was to provide management with clear, actionable insights to reduce cyber risk and improve governance and compliance maturity for Dizzy Financial Solutions Ltd.

Key Findings -

High risk exposure related to customer data protection due to lack of multi-factor authentication.

Insufficient logging and monitoring capabilities affecting fraud detection and incident response.

Moderate governance gaps in access control management and risk monitoring.

Overall Risk Posture - Medium–High

Recommendation - Immediate prioritization of identity security controls, logging enhancements, and formalized risk governance.

Risk Assessment Scope:

In Scope -

Customer Database (PII)

Loan Management Application

Cloud Storage Environment

Employee Laptops

Out of Scope -

Physical security

Third-party vendor infrastructure

Assessment Objectives -

Identify cybersecurity risks

Evaluate control effectiveness

Align risks with business impact

Recommend mitigation strategies

Asset Inventory and classification:

Asset	**Business Owner**	**Data Type**	**Criticality**
Customer Database	IT	PII & Financial Data	High
Loan Management App	Operations	Financial Transactions	High
Cloud Storage	IT	Internal Documents	Medium
Employee Laptops	HR	Mixed	Medium

Risk Register:

Risk ID	Asset	Threat	Vulnerability	Likelihood	Impact	Risk Rating
R-01	Customer Database	Data Breach	No MFA	High	High	Critical
R-02	Loan Management App	Fraud	Weak Audit Logging	Medium	High	High
R-03	Cloud Storage	Data Leakage	Misconfigured Permissions	Medium	Medium	Medium

Control Mapping (NIST CSF):

Risk ID	Control	NIST function
R-01	Implement MFA for privileged access	Protect
R-02	Enable centralized logging & alerts	Detect
R-03	Periodic access reviews	Identify

Risk Heat Map:

Critical risks were identified in systems handling customer PII, primarily due to weak authentication mechanisms. Medium risks exist within cloud configurations and endpoint usage, requiring improved governance and monitoring.

Conclusion:

This assessment highlights the importance of strengthening identity management and detection capabilities. Addressing the identified risks will significantly reduce exposure to cyber incidents and regulatory non-compliance.