GROUP TWO

PROJECT REPORT

ON

SECURITY ARCHITECTURE FOR AN SME USING NIST CSF

BY

EZEOGO DENIS – INT25013

NATHAN MBUZI – INT250139

IBITOYE MAYOKUN – INT250051

JOHN OLUBUSUYI OGUN – INT250186

ARIELLE – MILAN TCHALIEU NGMOSI – INT250391

AUGUST, 2025.

Team Roles and Responsibilities

RISK AND ASSET ANALYSIS FOR SME CYBERSECURITY ARCHITECTURE LEAD

EZEOGO DENIS – INT25013

CYBERSECURITY ARCHITECTURE (DESIGN AND NETWORK) LEAD

NATHAN MBUZI – INT250139

FRAMEWORK AND CONTROLS FOR AN SME LEAD

JOHN OLUBUSUYI OGUN – INT250186

REPORT COMPILATION LEAD

IBITOYE MAYOKUN – INT250051

PRESENTATION & GIT HUB REPOSITORY UPLOAD LEAD

ARIELLE – MILAN TCHALIEU NGMOSI – INT250391

RISK AND ASSET ANALYSIS FOR SME CYBERSECURITY ARCHITECTURE

1.0 SME and Industry Definition

We are simulating a small-to-medium enterprise (SME) operating in the financial services sector, specifically a microfinance institution. This business provides savings accounts, micro-loans, mobile banking, and financial advisory services to individuals and small businesses. As a financial service provider, the SME handles sensitive personal and financial data, which makes cybersecurity a top priority.

1.1 Digital Assets and Technology Functions

The company's operations heavily rely on digital infrastructure. Key digital assets include:

- Core banking software
- Customer Relationship Management (CRM) system
- Mobile and online banking platforms
- Employee workstations and company-owned mobile devices
- Internal network (LAN/WAN) and cloud storage
- Financial databases and transaction records
- Email communication systems
- Website and social media accounts

1.2 Critical Cybersecurity Outcomes

Using the NIST Cybersecurity Framework, the outcomes most important to the business include:

- Protecting customer financial data (Protect Function)
- Ensuring availability of online and mobile banking services (Respond & Recover Functions)
- Early detection of intrusions or data breaches (Detect Function)
- Maintaining compliance with financial data regulations (Identify & Protect Functions)
- Quick response and recovery from cybersecurity incidents (Respond & Recover Functions)

1.3 Potential Attacks and Impact

Possible cyberattacks include:

- Phishing attacks targeting employees to steal login credentials

- Ransomware attacks that encrypt financial data and disrupt services
- Insider threats leading to unauthorized access or data leaks
- Distributed Denial-of-Service (DDoS) attacks on the mobile banking platform
- Malware infections on employee systems

Impact of such incidents could range from temporary disruption of services and financial losses to legal penalties and loss of customer trust.

1.4 Legal Compliance and Obligations

The SME must comply with:

- Nigeria Data Protection Act (NDPA) and Central Bank of Nigeria (CBN) cybersecurity guidelines
- Payment Card Industry Data Security Standard (PCI DSS)
- International Financial Reporting Standards (IFRS)
- Any relevant anti-money laundering (AML) and data privacy laws applicable to its services

Failure to comply could result in regulatory sanctions, reputational damage, and significant financial penalties.

Table1.1: Risk Register

Asset	Threat	Vulnerability	Likelihood	Impact	Risk Level
Customer Database	Data breach	Weak access control	High	High	Critical
Online Banking Platform	DDoS attack	Lack of traffic filtering	Medium	High	High
Employee Emails	Phishing	Untrained users	High	Medium	High
Workstations	Malware	Outdated antivirus	Medium	Medium	Medium
Mobile App	Unauthorized access	Weak API security	Low	High	Medium

CYBERSECURITY ARCHITECTURE

2.0 Network Design & Infrastructure Security

2.0.1 Executive Summary

This section presents the **technical network design and security architecture** for the SME (a microfinance institution). The architecture is designed with **layered security**, segmentation, and defense-in-depth strategies to protect digital assets and ensure resilience against cyber threats such as **phishing, DDoS, ransomware, and insider threats**. The setup is aligned with best practices from **NIST CSF** and **ISO/IEC 27001** standards.

2.1 Network Diagram Overview

The network is logically divided into **three main zones**:

1. External Zone (Public-Facing):

Internet users (clients, customers), API Gateway, Web Application Firewall (WAF), Load Balancer, TLS/SSL encrypted access.

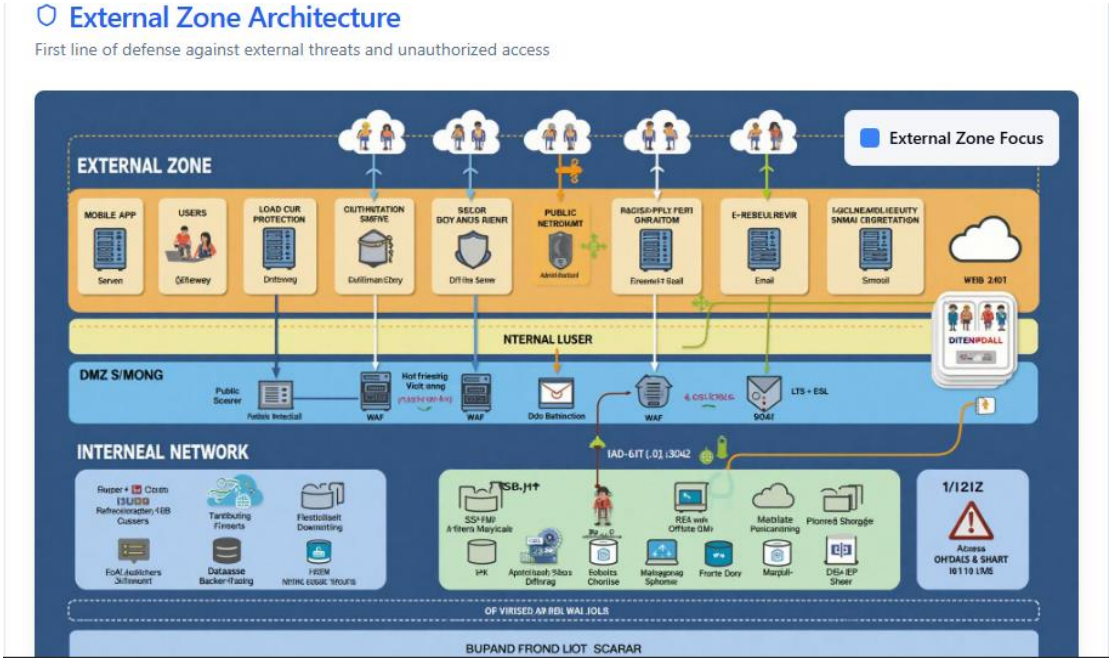

Fig: 2.1: External Zone 1

Fig 2.2: External Zone 2

Fig 2.3: External Zone 3

2. DMZ (Demilitarized Zone):

Public web and mobile banking servers, Reverse proxy server, Email gateway, DDoS protection layer, Limited and filtered access to internal services.

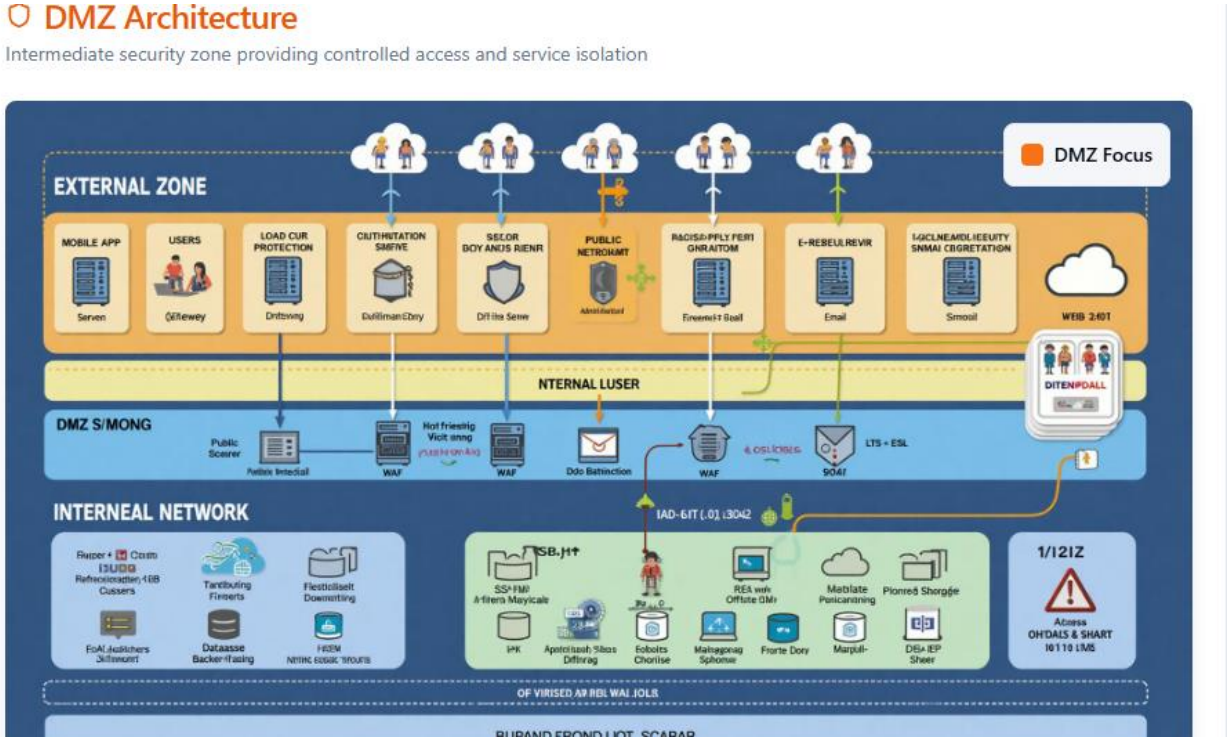

Fig 2.4: Demilitarized Zone 1

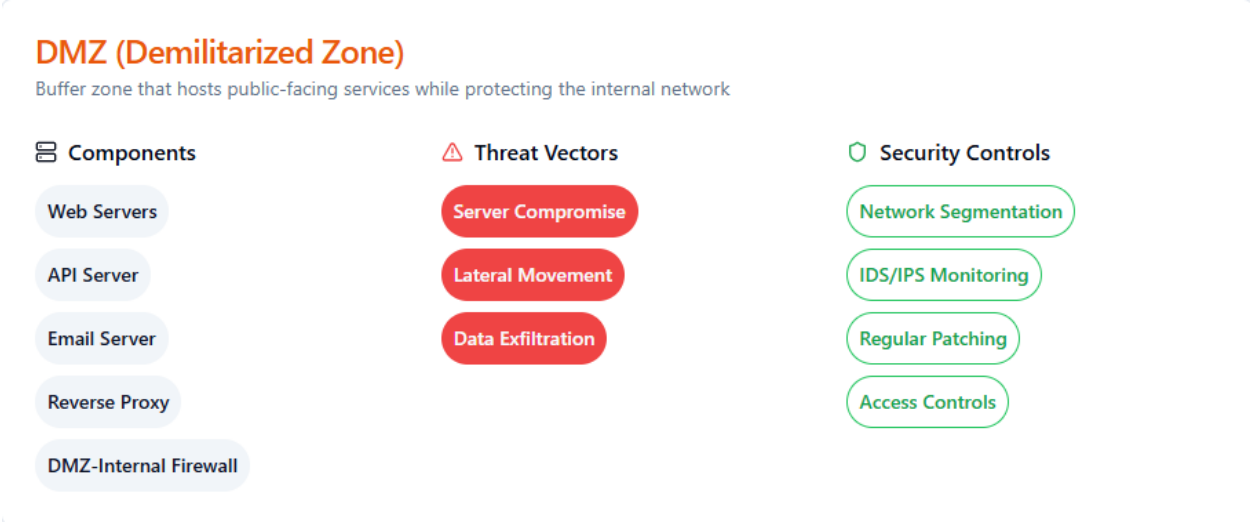

Fig 2.5: Demilitarized Zone 2

Network Segmentation

- Isolated VLAN for DMZ services
- Firewall rules between zones
- Limited access to internal network
- Service-specific security policies

Monitoring & Detection

- Intrusion Detection System (IDS)
- Intrusion Prevention System (IPS)
- Real-time traffic analysis
- Anomaly detection and alerting

Fig 2.6: Demilitarized Zone 3

3. Internal Network:

Application Servers (Banking, CRM), Authentication Server (LDAP + MFA), Database Server (Encrypted storage), Admin Portal (RBAC enforced), Endpoint Protection Server (AV + EDR), Backup Server (Isolated + cloud sync)

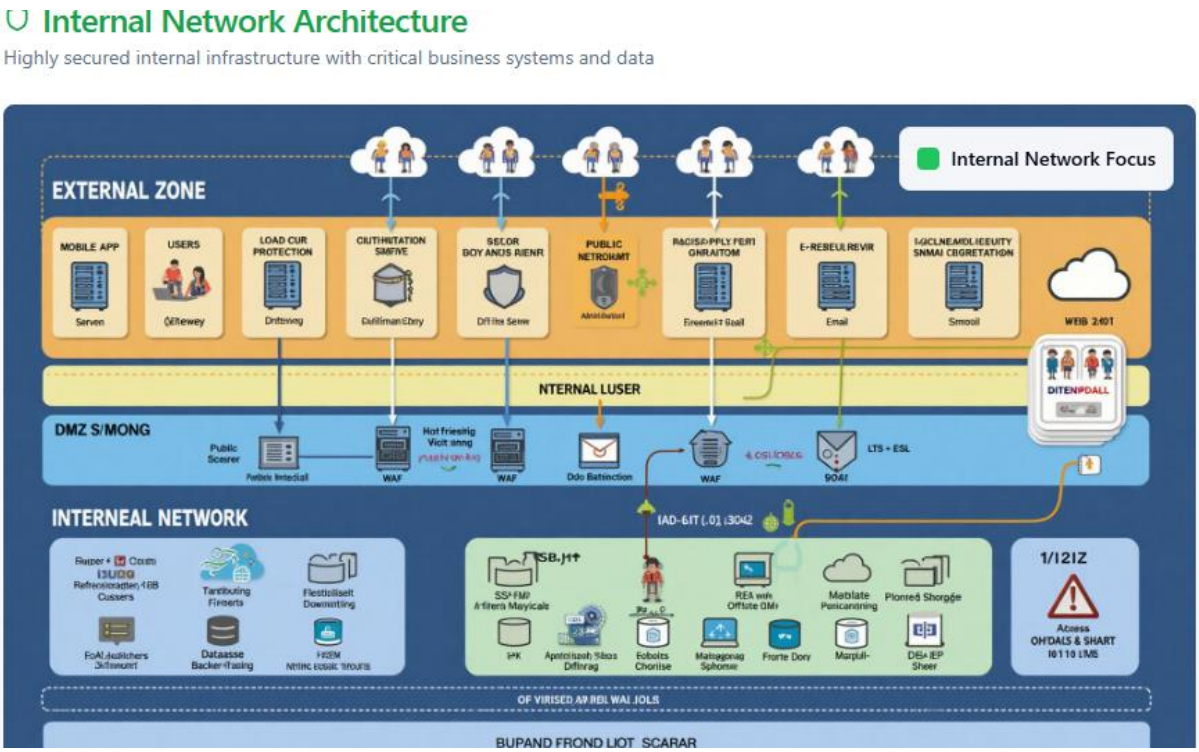

Fig 2.7: Internal Zone 1

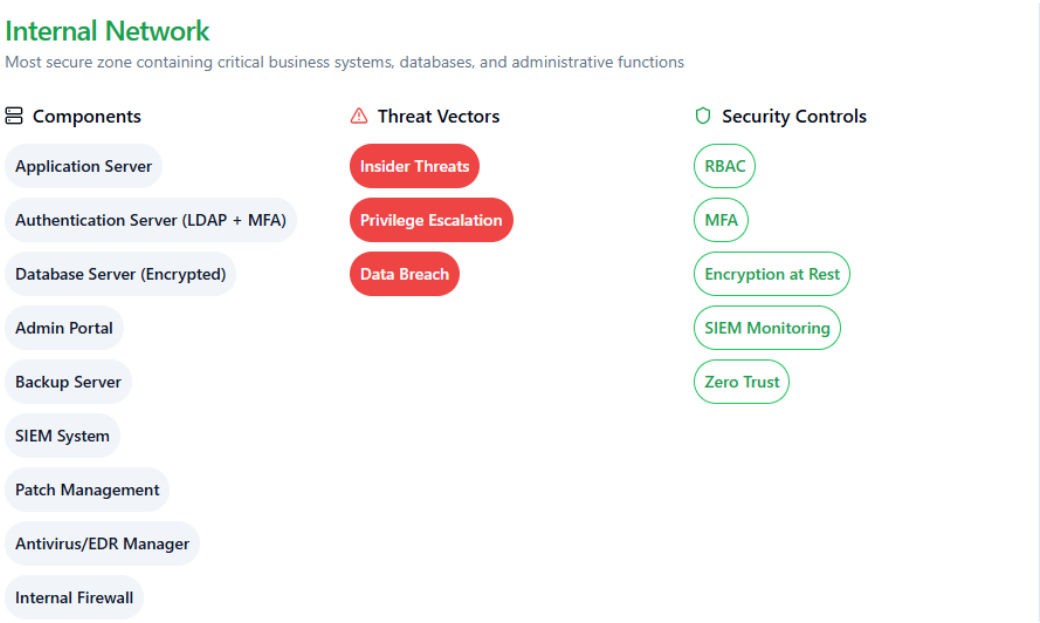

Fig 2.8: Internal Zone 2

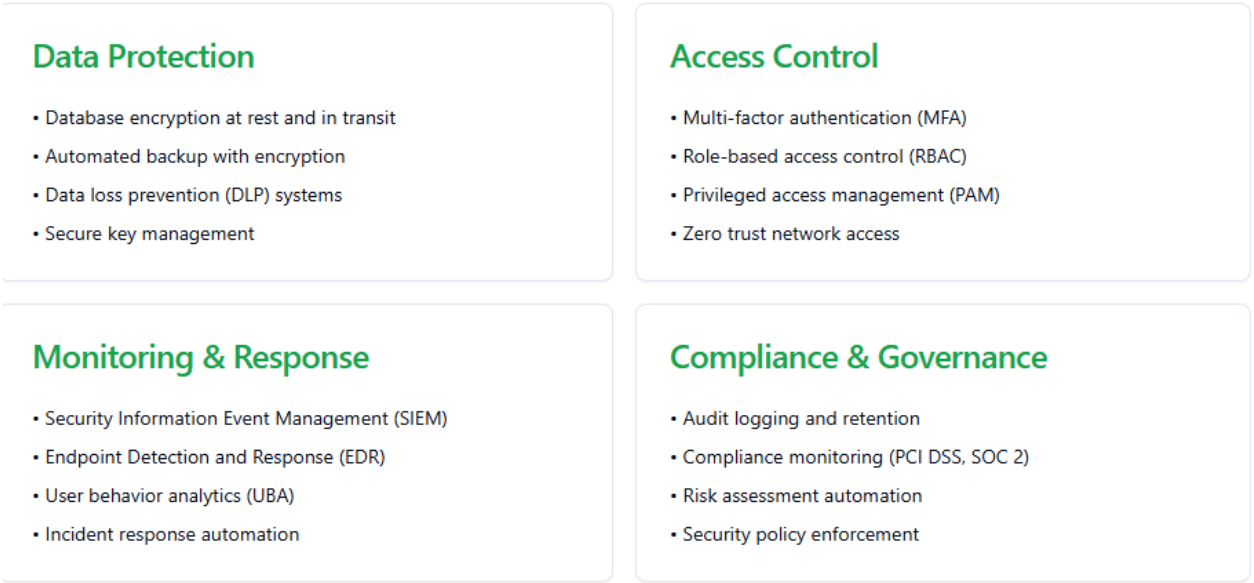

Fig 2.9: Internal Zone 3

2.2 Monitoring & SIEM

Secure access is enforced via **VPN** for employee/admin access, and all internal traffic is encrypted using **IPSec tunnels**. **Network segmentation** is applied using VLANs and internal firewalls.

Table 2.1: Technical Architecture Notes

Component	**Role**	**Security Features**
Firewall (NGFW)	Zone segmentation, packet filtering	App-layer rules, geo-blocking, IDS integration
WAF	Protects public web and API services	Blocks SQLi, XSS, command injection
Authentication Server	Verifies user/admin access	LDAP, MFA, session timeout
Antivirus/EDR	Secures endpoints	Behavioral analysis, real-time scanning
SIEM	Centralized logging and alerts	Detects anomalies, aggregates logs
Backups	Disaster recovery	Daily incremental + weekly full backups, offline storage
VPN	Secure remote access	AES-256 encrypted tunnels, role restrictions
Patch Management System	Keeps systems updated	Automated OS/app patches, vulnerability scan integration

Table 2.2: How the Setup Protects Against Risks

Risk (from Risk Register)	**Architecture Protection**
Phishing Attacks	MFA on all accounts, email filtering via gateway, login anomaly detection
Ransomware	Endpoint protection (EDR), secure file access controls, isolated backups

Risk (from Risk Register)	Architecture Protection
Insider Threat	Role-based access, access logging, least privilege enforcement, SIEM monitoring
DDoS Attacks	Load balancer with rate limiting, DDoS mitigation tools in DMZ, WAF
Malware on Workstations	AV/EDR installed on all devices, regular signature updates, web filtering
API Abuse / Unauthorized App Access	Token-based authentication, encrypted channels, WAF policies, regular API key rotation

2.3 Mitigation Strategy Summary

The entire setup follows a **Defense-in-Depth strategy**, ensuring that if one layer is breached, others continue to protect the system. Key strategic controls include:

Preventive Controls: Firewalls, WAF, MFA, antivirus, secure coding practices

Detective Controls: SIEM alerts, IDS, access logs, behavioral monitoring

Responsive Controls: Automated threat response rules, backup recovery, incident response procedures

By integrating these controls with **clear segmentation**, **encrypted communication**, and **centralized monitoring**, the system minimizes both **attack surface** and **blast radius** in case of compromise.

Table 2.3: Deliverables Summary

Item	Description
Network Diagram	Visual overview of security architecture
Architecture Notes	Explanation of each security layer/component
Risk Protection Mapping	How the design mitigates each identified risk
Strategy Overview	Prevent, detect, and respond layers detailed

RISKS & PREVENTION CONTROLS FOR AN SME (MICROFINANCE INSTITUTION)

Based on the NIST Cybersecurity Framework, aligned with ISO/IEC 27001

Below is a breakdown of realistic risks an MFI and the corresponding prevention controls which could be deployed - mapped to NIST CSF functions and ISO/IEC 27001:2022 Annex A controls.

3.1 **IDENTITY**:

Recognize who is responsible, what you own, and where you are exposed.

3.1.1 Risks:

- Endpoints that are not monitored (teller PCs, mobile tablets)
- Unauthorized fintech apps, or shadow IT
- Inadequate adherence to local MFI license regulations

3.1.2 Preventive Measures / Control

A. Keep an up-to-date asset inventory of cloud services, data repositories, software, and hardware.

- Asset Inventory - ISO 27001 A.8.1.1:

B. Conduct regular risk assessments with an emphasis on money-laundering and financial fraud.

- Risk assessment for information security, ISO 27001 A.6.1.2

C. Describe and record IT support, compliance officers, and data owners' roles and responsibilities

- Information security roles and responsibilities (ISO 27001 A.6.1.1)

3.2 **PROTECT**:

Build barriers to keep threats—and human error—out of your critical systems.

3.2.1 Risks:

- Weak or reused passwords for teller and admin accounts
- Unpatched core banking, CRM, or operating system software
- Insider misconfigurations that expose consumer data

3.2.2 Prevention Controls linked to ISO IEC 27001

A. Implement multi-factor authentication (MFA) for all privileged and teller logins.

- Secure Log-On Procedures ISO 27001 A.9.4.2

B. Implement a disciplined patch management program for applications and operating systems.

- Management of technical vulnerabilities: ISO 27001 A.12.6.1

C. Encrypt consumer data both at rest (database) and in transit (TLS for mobile/online channels).

- Cryptographic Controls : ISO 27001 A.10.1.1

D. Segment networks (for example, isolate the teller VLAN from the corporate office).

- Network Controls ISO 27001 A.13.1.1

E. Conduct regular security awareness. Training in phishing, social engineering, and secure financial management.

- Information Security Awareness, Education, and Training ISO 27001 A.7.2.2

3.3 DETECT:

Detect harmful or unusual activity before it spreads.

3.3.1 Risks

- Fraudulent transaction patterns include excessive withdrawals and irregular loan disbursements.
- Malware hidden in teller machines or staff PCs.
- Unauthorized access attempts outside of office hours.

3.3.2 Prevention Controls

A. Enable centralized event logging for teller servers, VPN gateways, firewalls, and core banking systems.

- Event Logging: ISO 27001 A.12.4.1:

B. Deploy Endpoint Detection and Response (EDR) agents on all workstations and servers.

C. Implement rule-based alerts for transaction anomalies, such as cumulative daily limit breaches.

D. Schedule frequent vulnerability scans against web portals and corporate networks.

- Restrictions on Software Installation: ISO 27001 A.12.6.2:

3.4. RESPOND:

Have a clear plan for containing, analyzing, and resolving incidents.

3.4.1 Risks:

- Slow response to fraud detection leads to a greater financial impact.
- Uncoordinated internal/external messaging erodes customer trust.

3.4.2 Prevention Controls:

A. Maintain an incident response plan (IRP) that includes containment, eradication, recovery, and legal-regulatory notification.

- ISO 27001 A.16.1.5: Response to Information Security Incidents

B. Keep up to date. Contact List (IT Responders, Legal Counsel, Regulator Hotlines, Law Enforcement)

C. Runs quarterly, Tabletop Exercises that simulate data-Leak or loan fraud scenarios

3.5 RECOVER:

Quickly resume operations and fortify your defenses using the knowledge you've gained.

3.5.1 Risks

- Transactional data loss that is irreversible following hardware failure or ransomware
- Regulatory penalties for business continuity plans that haven't been tested

3.5.2 Preventive controls:

A. Automate Offsite/Cloud Encrypted Backups for Configuration Data, Databases, and Customer Records

B. Verify, examine, and test business continuity protocols in accordance with

- ISO 27001 A.17.1.3.

C. Establish Recovery Time Objectives (RTOs) for each system and use restore drills to confirm them.

D. Update IRP, close any gaps, and retrain employees by conducting post-incident reviews

Table 3.1: Summary Mapping Table

NIST CSF Function	**Sample Risks**	**Key Prevention Controls**	**ISO/IEC 27001 Controls**
Identify	Shadow IT, untracked devices	Asset inventory, risk assessment, role definitions	A.8.1.1, A.6.1.2, A.6.1.1
Protect	Weak passwords, unpatched banking apps, insider error	MFA, patch management, encryption, network segmentation, training	A.9.4.2, A.12.6.1, A.10.1.1, A.13.1.1, A.7.2.2
Detect	Fraudulent transactions, hidden malware	Logging, EDR, anomaly-based alerts, vulnerability scans	A.12.4.1, A.12.6.2
Respond	Delayed fraud response, poor breach communications	IR plan, contact roster, tabletop exercises	A.16.1.5
Recover	Data loss, untested continuity plans	Encrypted backups, RTO definitions, restore drills, post-mortems	A.17.1.3