NIST Cybersecurity Framework (CSF) And Implementation Plan

Company: X Bank

Prepared by: Elizabeth P. A. Onyango

Date: 20/4/2025.

Table of Contents

Executive Summary

This implementation plan outlines how X Bank adopts the NIST Cybersecurity Framework (CSF) to enhance its cybersecurity posture. The goal is to align the organization's security practices with industry standards, reduce cyber risks, and improve incident readiness.

Organization Overview

X Bank is a mid-sized fintech company specializing in online banking solutions. The organization manages critical systems such as a web app, customer databases, internal networks, and payment systems.

Risk Assessment Overview

Based on initial risk assessments, critical-priority risk includes lack of user awareness training; high-priority risks include data breaches, DDoS attacks, ransomware, malware infections among others. These risks are documented in detail in the risk register attached in the appendix.

NIST CSF Overview

The NIST Cybersecurity Framework consists of five core functions: Identify, Protect, Detect, Respond, and Recover. These guide the development of policies and controls tailored to X Bank's operations.

Function-Based Controls

1. Identify
    - Asset management approach
    - Risk assessment methods
    - Governance practices
2. Protect
    - Access control measures
    - Acceptable use policies
    - Data protection techniques
    - Staff awareness programs
3. Detect
    - Monitoring tools used
    - Event detection mechanisms
    - Alert and escalation strategy
4. Respond
    - Incident response planning
    - Communication plans
    - Forensic analysis methods
5. Recover
    - Backup and restore process
    - Lessons learned documentation
    - Disaster recovery and business continuity strategies

Policies Summary

This section summarizes key policies such as:

- Asset Management Policy
- Access Control Policy
- Acceptable Use Policy
- Security Awareness & Training Policy
- Incident Response Policy
- Backup & Recovery Policy
- Business Continuity Policy

Full policy versions are available in the Appendix.

Implementation Timeline

Phase	Timeline	Task	Responsible Party	Notes
Phase 1 - Planning	Month 1	Conduct NIST CSF gap analysis	CISO/ Security Lead	Use self-assessment or external audit
Phase 2 – Governance Setup	Month 2	Define cybersecurity roles and policies	HR + IT + Compliance	Includes Acceptable Use, BCP, etc.
Phase 3 – Inventory & Risk	Month 3	Complete asset inventory & risk register	IT department	Match to ID.AM category
Phase 4 – Control Implementation	Month 4 - 6	Implement basic controls (access, backups, MFA, etc.)	IT + Security Operations	Covers Protect function
Phase 5 – Awareness & Training	Month 5	Launch security awareness training	HR + IT	Include phishing simulation
Phase 6 – IP Planning	Month 6	Develop and test incident response plan	Security Operations	Align with Respond function
Phase 7 – Monitoring & SIEM	Month 7	Deploy SIEM, log monitoring tools	SOC Team	Begin continuous monitoring
Phase 8 – Business Continuity	Month 8	Finalize and test BC & DR plans	IT + Operations	Backup validation, failover testing
Phase 9 – Review & Audit	Month 9	Conduct internal audit & gap reassessment	Internal Audit	Compare against initial results
Phase 10 - Optimization	Month 10+	Refine policies, update controls	Security Steering Committee	Ongoing improvement

Review and Maintenance

The implementation plan will be reviewed annually. Metrics and ownership of tasks are documented to ensure continuous improvement and successful measurement.

Appendices

Appendix A: Supporting Documents

Document Title	Description	Format	Location/ Reference
NIST CSF Policies Document	Contains all security policies: Asset Management, Access Control, AUP, Security Awareness, IR, Backup & Recovery, BCP	PDF	Attached: NIST CSF Policies Document
Risk Register	Lists key assets, threats, vulnerabilities, impact, and associated risk levels	Excel	Attached: Risk Register
NIST CSF Control Mapping Sheet	Maps each CSF Function to subcategories, controls, and implementation status	Excel	Attached: NIST CSF Control Mapping Sheet