Cybersecurity ASSESSMENT

SECURITY MANAGEMENT

Prepared by
Bikal Magar

TABLE OF CONTENTS

CYBERSECURITY ASSESSMENT SUMMARY – NEPAL DIGITAL BANK LTD. (NDBL)

1. EXECUTIVE SUMMARY

The organization demonstrates partial implementation of cybersecurity practices across all CSF 2.0 functions, including **Govern (GV)**. Key weaknesses include absence of multi-factor authentication (MFA), unpatched legacy systems, flat network architecture, incomplete asset inventories, missing formal incident response and recovery plans, and inadequate governance over roles, responsibilities, and supply chain risk. While basic controls such as firewalls, endpoint protection, and logging exist, coverage and effectiveness are inconsistent. High-risk areas include identity and access management, supply chain security, and incident recovery. Overall maturity ranges from **partial (ad hoc)** to **defined (risk-informed)** across functions, with immediate attention required on high-priority risks.

2. INTRODUCTION

Nepal Digital Bank Ltd. (NDBL) conducted a comprehensive cybersecurity capability assessment aligned with NIST Cybersecurity Framework (CSF) 2.0, referencing the structure, methodology, and interpretive guidelines reflected in the CSF implementation model.

The goal of this assessment is to:

- Evaluate current cybersecurity posture
- Identify strengths, weaknesses, and maturity gaps
- Align cybersecurity practices with regulatory expectations (Including NRB guidelines)
- Support strategic planning and risk-informed improvement initiatives

The assessment covers all six cores of CSF Functions, evaluating each Category and Subcategory as Not Implemented, Partially Implemented, Largely Implemented, or Fully Implemented.

3. METHODOLOGY

The assessment uses **NIST CSF 2.0**, covering the updated functions:

1. **Govern (GV)** — Leadership, policies, roles, and supply chain governance.
2. **Identify (ID)** — Asset and risk identification.
3. **Protect (PR)** — Safeguarding systems and data.
4. **Detect (DE)** — Monitoring for anomalies and potential incidents.
5. **Respond (RS)** — Action during incidents.
6. **Recover (RC)** — Restoration and continuity after incidents.

Controls were scored on a **0–3 maturity scale**:

- 0 — Not Implemented
- 1 — Partially Implemented / Ad hoc
- 2 — Defined / Risk-informed
- 3 — Managed / Adaptive

Assessment sources: asset inventories, documentation, technical review, vulnerability scanning, and interviews with IT/security personnel.

4. DETAILED EVALUTAION OF CSF CATEGORIES

The following table shows the assessment results for all CSF categories grouped by their function, with an implementation score (0-3) and relevant observations or examples from the organization's environment:

Function	Current Profile	Description
Govern (GV)	1	NDBL has a basic understanding of its business mission and stakeholder expectations, especially regarding secure digital banking, regulatory compliance, and customer trust. The bank follows key NRB directives, SWIFT CSP requirements, and internal policies for general operational compliance. However, it has not fully implemented a structured cybersecurity risk management strategy

		that aligns these missions and expectations into actionable processes. Dependencies such as reliance on third-party vendors, cloud infrastructure, and national payment systems are not formally documented or risk assessed. Regulatory and contractual requirements are understood at a high level but not consistently translated into policies, technical controls, or monitoring mechanisms. Overall, the bank has foundational awareness but lacks a comprehensive governance structure that integrates cybersecurity into business strategy, vendor management, and day-to-day decision making.
Identify (ID)	1	The Identify Function at NDBL demonstrates basic awareness but lacks maturity and completeness. Asset records are incomplete, risk assessments are informal, and improvement processes are not fully institutionalized. To achieve NRB and international best-practice assessment, supplier evaluation procedures, and a structured continuous improvement framework.
Protect (PR)	1	The Protect Function at NDBL is partially implemented and operational lacks depth, consistency, and strong governance. Identity access controls are weak, employee training is insufficient, patching and configuration management are irregular, and key resilience mechanisms are not fully mature. Significant improvements are needed to meet NRB directives, reduce exploitable vulnerabilities, and build stronger protection against both internal and external threats.
Detect (DE)	1	NDBL's overall DETECT function is partially implemented, with basic monitoring and alerting capabilities in place but lacking the depth and integration needed for mature threat detection. The bank monitors networks, systems, and physical environments remain limited. Event analysis is mostly manual, with minimal use of threat intelligence and inconsistent correlation across different log sources. While the bank can identify anomalies. It does not yet have fully structured processes for analyzing impacts, correlating multi-source

		data, or formally declaring incidents based on standardized criteria. As a result, NDBL can detect potential issues, but its ability to identify early indicators of compromise and understand the true scope of threats remains incomplete and in need of improvement.
Respond (RS)	1	NDBL has basic incident response capability, but it remains partially implemented. An incident response plan exists, and the bank can coordinate with third parties once an incident is declared, but declaration criteria, escalation paths, and prioritization are not consistently applied. Incident analysis is performed, though evidence collection and preservation processes are still weak. Internal communication occurs, but external regulatory reporting is not always timely or complete. Containment and eradication actions are carried out, but they rely on manual steps and lack standardized playbooks. Overall, NDBL can respond to incidents but needs stronger documentation, consistent procedures, and better communication to improve response maturity.
Recovery (RC)	0	NDBL's recovery capabilities are **minimally developed**, making this the weakest CSF function. While the bank has basic backup systems and can restore operations after incidents, recovery actions are not consistently prioritized, tested, or documented. Backup integrity checks are irregular, and restored systems are not always validated thoroughly before returning to service. Communication during recovery is limited—internal updates are inconsistent, and external or public updates are rarely issued. Criteria for formally ending recovery efforts are unclear, leading to ad-hoc closure of incidents. Overall, NDBL can recover from disruptions, but the recovery process lacks structure, formal testing, verification steps, and coordinated communication, resulting in low maturity.

5. GAP ANALYSIS AND PRIORITIZED REOMMENDATIONS

Based on the detailed results above, the assessment identified several critical gaps in the organization's cybersecurity controls. This section highlights the most significant gaps, their implications, and recommended actions to address them. The gaps are prioritized by risk level (impact and likelihood), with an understanding that the organization intends to mitigate high risks as a priority (consistent with its risk posture).

1. **No formal Incident Response Plan – Very High Risk:** NDBL lacks a documented, tested, and approved Incident Response Plan. Incident handling is reactive and uncoordinated.
   Risk Impact: Delays in detection, containment, and recovery can lead to longer outages, financial losses, and regulatory penalties.
   Recommendation: Develop an IRP aligned with NIST CSF and NRB guidelines, define roles, create runbooks, and perform annual IR drills.

2. **Lack of Multi-Factor Authentication (MFA) – Very High Risk:** NDBL has not implemented MFA across core banking systems, administrative accounts, or internal applications. Password-only authentication remains the default method for most users.
   Risk Impact: Credential theft through phishing or brute-force attacks can lead to unauthorized access, fraudulent transactions, manipulation of customer accounts, or full system compromise.
   Recommendation: Deploy MFA for VPN, email, core banking, SWIFT systems, privileged accounts, and all remote access endpoints.

3. **Weak Network Segmentation – Very High Risk:** The internal network is largely flat, with limited segmentation between branches, internal systems, and sensitive environments.
   Risk Impact: Once inside the network, attackers can move laterally to compromise ATMs, core banking systems, or SWIFT infrastructure.
   Recommendation: Implement VLAN-based segmentation, isolate critical systems, and enforce 'Zero Trust' access rules.

4. **Outdated Firewall and ISP signatures – High Risk:** Firewall and IPS signature updates are irregular, leaving the perimeter security controls outdated.

Risk Impact: New malware, botnet traffic, and zero-day exploits may bypass detection, increasing exposure to intrusion and data breaches. **Recommendation:** Apply automated signature updates, enforce weekly patch cycles, and enable real-time threat feeds

5. **Lack of continuous vulnerability Scanning – High Risk:** NDBL does not operate an automated vulnerability assessment system. Scans are infrequent and largely manual. **Risk Impact:** Unpatched vulnerabilities may remain undetected for months, exposing critical systems to exploits.
   Recommendation: Deploy a vulnerability scanner (Nessus, Qualys, OpenVAS) and perform weekly scans with monthly remediation tracking.

6. **No Endpoint Detection and Response (EDR) – High Risk:** Endpoints rely only on legacy antivirus with no behavioural detection or real-time attack monitoring. **Risk Impact:** Malware, ransomware, and insider activity may remain undetected until significant damage occurs.
   Recommendation: Implement an EDR/XDR solution with alerting, isolation, and real-time threat visibility.

7. **Inadequate Log Collection & SIEM Coverage – High Risk:** SIEM currently receives limited logs and does not monitor ATM switches, SWIFT servers, or cloud workloads. **Risk Impact:** Critical events may go unnoticed, delaying incident detection and investigation.
   Recommendation: Expand SIEM integrations, enforce log forwarding from all critical assets, and implement basic correlation rules.

8. **48-Hour Backup Window Violating NRB Guidelines – Medium Risk:** Backups are performed every 48 hours, which fails to meet NRB's RPO expectations and modern banking standards.
   Risk Impact: A major incident may cause loss of up to 48 hours of financial data, leading to errors and compliance penalties.
   Recommendation: Shift to daily (or 12-hour) backups with offsite replication and automated backup integrity checks.

9. **No Cybersecurity Awareness Training – Medium Risk:** Staff do not receive regular security training, despite frequent phishing attempts and social engineering targeting branches.

   Risk Impact: Employees remain the weakest link, increasing the likelihood of phishing-driven breaches.

   Recommendation: Implement mandatory quarterly awareness training, phishing simulations, and role-based security training for high-risk units.

10. **Poor Access Control Hygiene – Medium Risk:** Shared passwords, privilege creep, and lack of quarterly access reviews persist across systems.

    Risk Impact: Unauthorized or excessive access can lead to insider threats, fraudulent activities, or data leakage.

    Recommendation: Enforce unique credentials, implement access review cycles, and adopt least-privilege policies with automated provisioning.

6. FINAL RECOMMENDATIONS FOR NRB COMPLIANCE – NDBL

1. Governance and Risk Management

- Establish a formal cybersecurity governance framework aligned with NRB directives and cyber resilience Guidelines (CRG).
- Define board-level oversight, roles, and responsibilities for cybersecurity and risk management.
- Implement a risk management strategy including asset classification risk appetite, vendor assessment, and regulatory compliance monitoring.

2. Identity and Access Management

- Implement Multi-Factor Authentication (MFA) for all users, administrators, and remote access.
- Enforce least privilege and separation of duties; regularly review access rights.
- Implement secure onboarding/offboarding processes to prevent dormant or unauthorized accounts.

3. Asset & Platform Security

- Maintain updated inventories of hardware, software, data, and services, including supplier-provided services.
- Ensure network segmentation between internal systems, branches, ATMs, and payment platforms.
- Apply patch management and secure configuration practices for all servers, endpoints, and network devices.
- Secure critical platforms such as SWIFT servers, core banking systems, and digital banking apps.

4. Monitoring & Detection

- Expand SIEM coverage to include ATMs, branch systems, SWIFT, and cloud environments.
- Implement Continuous monitoring and log analysis, integrating threat intelligence feeds.
- Correlate events from multiple sources to detect anomalies, unauthorized access, and potential breaches.

5. Incident Response & Recovery

- Develop a comprehensive Incident Response Plan including detection, analysis, containment, mitigation, and recovery.
- Establish recovery procedures with tested backups and integrity verification before restoration.
- Define communication protocols for internal teams, NRB reporting customers, and other stake holders.

6. Data Security

- Implement encryption for data-at-rest, in-transit, and in-use for sensitive financial and personal data.
- Regularly back up critical data, maintain integrity checks, and test recovery procedures.
- Establish secure software development practices for all digital platforms.

7. Awareness and Training

- Conduct regular cybersecurity awareness programs for all employees, focusing on phishing, social engineering, and secure handling of credentials.
- Provide role-specific training for IT, operations, and compliance staff.

8. Vendor & Third-Party Risk Management

- Assess critical suppliers and outsourced IT vendors for cybersecurity compliance and operational risk.
- Monitor third-party activities continuously and include them in incident response and monitoring.

9. Documentation and Compliance Reporting

- Maintain records of controls, audits, risk assessments, and incidents to demonstrate compliance with NRB directives.
- Conduct periodic internal audits and remediation tracking aligned with NRB inspections.