## **Summary of Key Findings**

**DISCLAIMER: All mentions of the bank’s actual name have been intentionally redacted or generalized due to operational security concerns.**

**Organization:** Local Bank  
**Assessment Date:** 2/23/25  
**Location:** Aino Maina  
**Assessor:** Jabbar Yaqub

This document summarizes the findings of a basic cybersecurity risk assessment conducted for **Local Bank** on 2/23/25. The assessment focused on key operational areas including access control, data protection, physical security, network security, incident response, employee awareness, and regulatory compliance. The checklist was tailored for small- to medium-sized financial institutions operating in **Aino Maina, Afghanistan** to identify practical gaps in cybersecurity hygiene.

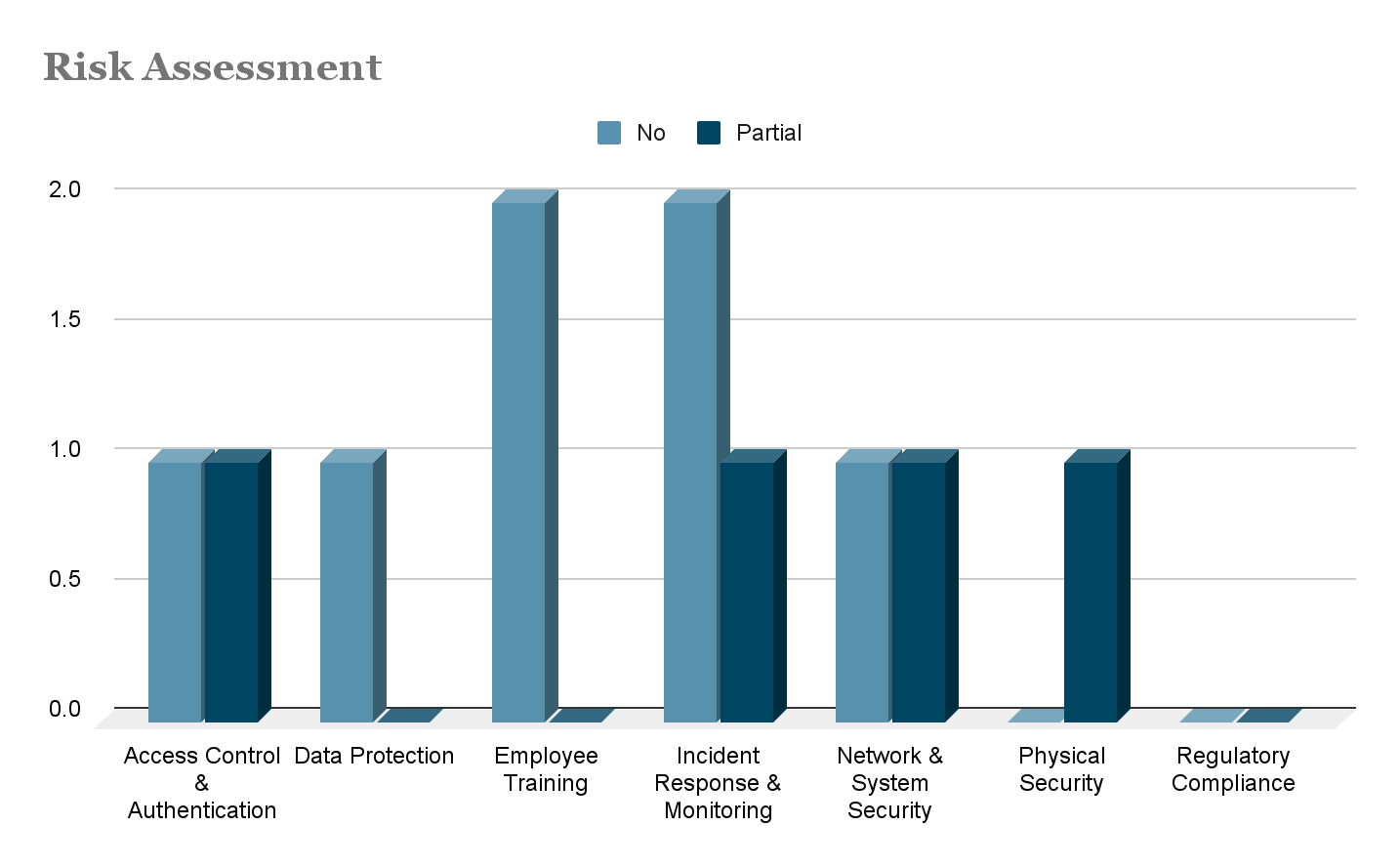
The goal was to provide a simple yet effective self-evaluation tool to highlight potential vulnerabilities and areas requiring improvement. Each item in the checklist was marked as **Yes**, **No**, or **Partial**, based on current practices observed or reported by the organization. Visualizations for the data were created to better understand current their risk posture

## **Risk Assessment and Response Data**

| **Category** | **Audit Question** | **Response** |
| --- | --- | --- |
| Access Control & Authentication | Are user accounts reviewed and deactivated upon employee departure? | Yes |
|  | Are multi-factor authentication (MFA) systems enforced for all internal banking systems? | No |
|  | Are privileged/admin accounts monitored and logged? | Partial |
| Data Protection | Is sensitive customer data encrypted at rest and in transit? | Yes |
|  | Are backups performed daily and stored securely off-site or on a secure cloud? | Yes |
|  | Is there a clear data classification policy in place? | No |
| Physical Security | Are server rooms locked, with restricted access and CCTV monitoring? | Yes |
|  | Are ATM and branch terminals physically secured and inspected regularly? | Partial |
|  | Are visitors to secure areas logged and escorted? | Yes |
| Network & System Security | Is there a firewall and intrusion detection/prevention system (IDS/IPS) in place? | Yes |
|  | Are core banking systems regularly patched and maintained? | Partial |
|  | Is USB/portable storage device access restricted or monitored? | No |
| Incident Response & Monitoring | Is there an incident response plan that staff are trained on? | No |
|  | Are system logs regularly reviewed for suspicious activity? | Partial |
|  | Has a cybersecurity incident simulation been conducted in the past 6 months? | No |
| Employee Training | Have all employees completed cybersecurity awareness training in the last 12 months? | No |
|  | Are phishing tests conducted regularly to assess employee awareness? | No |
| Regulatory Compliance | Are KYC and AML processes regularly reviewed for compliance gaps? | Yes |
|  | Are compliance reports submitted to *Da Afghanistan Bank* as required? | Yes |

## **Risk Assessment and Response Data Visualization**

| **Category** | **No** | **Partial** | **Yes** | **Total** | **Risk Level** |
| --- | --- | --- | --- | --- | --- |
| Access Control & Authentication | 1 | 1 | 1 | 3 | Medium |
| Data Protection | 1 | 0 | 2 | 3 | Low |
| Employee Training | 2 | 0 | 0 | 2 | High |
| Incident Response & Monitoring | 2 | 1 | 0 | 3 | Critical |
| Network & System Security | 1 | 1 | 1 | 3 | Medium |
| Physical Security | 0 | 1 | 2 | 3 | Low |
| Regulatory Compliance | 0 | 0 | 2 |  | None |



## **Comprehensive Risk Assessment Summary – Local Bank**

**Framework Alignment:** Based on the NIST CSF's five core functions — Identify, Protect, Detect, Respond, Recover — with considerations for Afghan-specific institutional requirements per NISA.

### **Access Control & Authentication**

**Findings:**

* **Multi-Factor Authentication (MFA)** is not enforced across all internal systems. This significantly elevates the risk of unauthorized access, especially in remote or high-privilege contexts.
* **Admin/privileged account activity** is only partially logged, creating gaps in auditability and making insider threat detection difficult.
* **User account deactivation** appears to be managed correctly upon employee departure, mitigating orphaned account risk.

**NIST Alignment:** Protect (PR.AC), Detect (DE.AE)  
 **NISA Relevance:** Strong identity access management and privileged account logging are high priorities.

### **Employee Training & Awareness**

**Findings:**

* **No cybersecurity awareness training** has been conducted within the past 12 months.
* **No phishing simulations** have been deployed, leaving staff untested and vulnerable to social engineering.

**Implications:** The human attack surface is currently the most exposed part of the bank’s defense posture.

**NIST Alignment:** Protect (PR.AT), Respond (RS.IM)  
 **NISA Relevance:** Public and institutional awareness training is a national-level directive.

### **Incident Response & Recovery**

**Findings:**

* **No formal incident response (IR) plan** is in place.
* **No recent cyber incident simulations** have been conducted.
* **System logs are only partially reviewed**, missing early warning indicators of compromise.

**Implications:** The bank lacks preparedness to detect, respond to, and contain security incidents.

**NIST Alignment:** Respond (RS), Detect (DE.CM)  
**NISA Relevance:** Crisis handling and breach notification readiness are core responsibilities for critical financial infrastructure.

### **Data Protection & Classification**

**Findings:**

* **Encryption is properly implemented** at rest and in transit.
* **Backups are performed and stored securely.**
* **No data classification policy** exists to define levels of sensitivity or access rules for customer vs. internal data.

**Implications:** Without classification, sensitive data may not be consistently protected or audited.

**NIST Alignment:** Identify (ID.AM), Protect (PR.DS)  
 **NISA Relevance:** Handling of personally identifiable information (PII) and financial data requires clear labeling and handling procedures.

### **Network, Endpoint & Removable Media**

**Findings:**

* **Firewalls and IDS/IPS** systems are in place, supporting perimeter defense.
* **Patching of core banking systems** is only partially completed, creating an exploitable attack window.
* **USB device usage is unrestricted and unmonitored**, introducing risk of malware infection and data leakage.

**NIST Alignment:** Protect (PR.IP, PR.PT), Detect (DE.CM)  
 **NISA Relevance:** Device control and patch hygiene are foundational technical safeguards.

### **Physical Security**

**Findings:**

* **Server rooms are locked and monitored.**
* **ATM and terminal inspections are partially conducted**, indicating inconsistencies in physical controls.
* **Visitor logs and escort procedures** are being followed in secure areas.

**NIST Alignment:** Protect (PR.PH)  
**NISA Relevance:** Branch-level controls are expected for customer trust and system safety.

## **Strategic Recommendations**

1. **Implement Mandatory MFA**
   * Enforce MFA for all internal systems, especially privileged accounts and VPN access.
   * low-cost MFA tools compatible with limited bandwidth environments (e.g., DUO, FreeOTP, Microsoft Authenticator).
2. **Create and Train on an Incident Response Plan**
   * Draft a response plan with defined roles, procedures, and escalation paths.
   * Conduct tabletop and live-fire simulations every 6 months.
3. **Launch a Cybersecurity Awareness Program**
   * Schedule employee training with local-language materials.
   * Run quarterly phishing simulations tailored to local attack methods.
4. **Restrict and Monitor USB & Device Use**
   * Disable ports by default, allow usage only via documented exceptions.
   * Implement endpoint monitoring for device usage and data transfers.
5. **Formalize Data Classification Policy**
   * Define categories like Public, Internal, Confidential, and Customer-Sensitive.
   * Map security controls to each classification level.
6. **Standardize Patch Management & ATM Inspections**
   * Create a patch cycle (e.g., 30-day SLA for critical updates).
   * Centralize ATM inspection reporting to ensure auditability.

## **Overall Risk Rating: MODERATE to HIGH**

While foundational compliance tasks (e.g., KYC/AML, DAB reporting) are being met, significant security weaknesses remain in:

* Staff readiness
* Endpoint controls
* Detection and response maturity

These gaps expose the institution to risks from phishing, ransomware, insider abuse, and regulatory non-conformance.

**Remediation Timeline:**

* **High-priority controls (MFA, training, IR planning):** Within 30 days
* **Medium-priority controls (patching, USB controls):** Within 60–90 days

## **Final Notes**

The current cybersecurity posture of **Local** reflects a foundational stage of maturity. While certain protective measures (e.g., physical security, encryption, data backups) are commendable, the **lack of formal policy, monitoring, training, and response plans** poses notable risk. A structured roadmap, grounded in the NIST CSF, is recommended for scalable and cost-effective cybersecurity improvement.