**📑 Risk Assessment Report**

**Organization:** ABC Bank Ltd.  
**Project Title:** ISO/IEC 27001:2022 Certification Program  
**Version:** 1.0  
**Date:** [Insert Date]  
**Owner:** ISMS Lead

**1. Purpose**

The purpose of this report is to document the risk assessment conducted as part of the ISMS implementation for ABC Bank Ltd., in line with ISO/IEC 27001:2022 Clause 6.1.2 and ISO/IEC 27005:2018 guidelines.

**2. Methodology**

**Risk Assessment Steps:**

1. **Asset Identification:** Identify critical information assets supporting banking operations.
2. **Threat Identification:** Identify potential threats that could exploit vulnerabilities.
3. **Vulnerability Identification:** Identify weaknesses in processes, people, technology.
4. **Risk Analysis:** Estimate risk likelihood and impact.
5. **Risk Evaluation:** Prioritize risks against the bank’s risk acceptance criteria.
6. **Risk Treatment:** Recommend risk treatment options (separate document).

**Risk Evaluation Scale:**

* **Likelihood:**
  + 1 = Rare
  + 2 = Unlikely
  + 3 = Possible
  + 4 = Likely
  + 5 = Almost Certain
* **Impact (on CIA – Confidentiality, Integrity, Availability):**
  + 1 = Insignificant
  + 2 = Minor
  + 3 = Moderate
  + 4 = Major
  + 5 = Severe

**Risk Rating Formula:**  
Risk Score = Likelihood × Impact

**Risk Levels:**

* Low = 1–6
* Medium = 7–12
* High = 13–19
* Critical = 20–25

**3. Risk Assessment Criteria**

* **Scope:** Core Banking System, Internet/Mobile Banking, ATM Switch, Data Center, IT Security Operations.
* **Risk Acceptance Criteria:**
  + All **critical risks (20–25)** must be treated immediately.
  + **High risks (13–19)** require management-approved treatment plan.
  + **Medium risks (7–12)** can be reduced or accepted based on business justification.
  + **Low risks (1–6)** can be accepted with minimal monitoring.

**4. Risk Register (Sample Extract)**

| **Asset** | **Threat** | **Vulnerability** | **Likelihood** | **Impact** | **Risk Score** | **Risk Level** | **Remarks** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Core Banking System (CBS) | Cyber-attack (malware/ransomware) | Unpatched legacy modules | 4 | 5 | 20 | **Critical** | Requires immediate patch mgmt & EDR solution |
| Internet Banking Portal | Phishing attack | Lack of user awareness | 5 | 4 | 20 | **Critical** | Requires MFA + awareness campaigns |
| Mobile Banking App | Data leakage | Weak API security | 3 | 5 | 15 | **High** | Implement API gateway + code review |
| ATM Switch | Fraudulent transactions | Inadequate monitoring | 3 | 4 | 12 | **Medium** | Enhance transaction anomaly detection |
| Data Center | Power outage | Lack of UPS redundancy | 2 | 4 | 8 | **Medium** | Upgrade backup power system |
| Employee HR Data | Insider threat | Excessive access rights | 3 | 4 | 12 | **Medium** | Role-based access controls needed |
| Vendor Cloud Services | Data breach at vendor | No SLA-based security clause | 3 | 5 | 15 | **High** | Strengthen vendor contracts, periodic audits |
| SOC Operations | Missed threat detection | Overreliance on manual logs | 2 | 5 | 10 | **Medium** | Expand SIEM use cases, automation |

**5. Risk Heat Map**

| **Impact ↓ / Likelihood →** | **1 Rare** | **2 Unlikely** | **3 Possible** | **4 Likely** | **5 Almost Certain** |
| --- | --- | --- | --- | --- | --- |
| 5 Severe | M | H | H | **C** | **C** |
| 4 Major | M | M | H | H | **C** |
| 3 Moderate | L | M | M | H | H |
| 2 Minor | L | L | M | M | M |
| 1 Insignificant | L | L | L | M | M |

C = Critical, H = High, M = Medium, L = Low

**6. Key Findings**

* **Critical Risks:** Core banking unpatched modules, phishing risk in online banking.
* **High Risks:** Vendor cloud data breach, API weaknesses in mobile banking.
* **Medium Risks:** ATM fraud, insider threat, SOC detection gaps.
* **Low Risks:** None significant.

**7. Recommendations**

* Immediate patching of legacy CBS modules and implementation of advanced endpoint protection.
* Enforce MFA for all customer-facing portals; run quarterly phishing simulations.
* Strengthen vendor SLAs with explicit security clauses and audit rights.
* Implement API gateway for mobile apps with regular penetration testing.
* Automate SOC detection rules for faster incident response.

**8. Conclusion**

The assessment identified **2 critical, 2 high, and 4 medium risks** across banking operations. Immediate attention is required for CBS and online banking.