**📑 Gap 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 Gap Assessment Report is to evaluate ABC Bank Ltd.’s current information security practices against ISO/IEC 27001:2022 requirements and Annex A controls, to identify areas of compliance and gaps requiring remediation.

**2. Methodology**

* Reviewed existing **policies, procedures, and controls**.
* Conducted **stakeholder interviews** with IT, security, compliance, and HR teams.
* Mapped practices against **ISO 27001 clauses (4–10)** and **Annex A controls (93 controls in 2022 version, grouped under 4 themes: Organizational, People, Physical, Technological)**.
* Rated compliance maturity on a **5-level scale**:
  + 1 = Not Implemented
  + 2 = Partially Implemented
  + 3 = Implemented but Informal
  + 4 = Implemented and Formalized
  + 5 = Best Practice

**3. Summary of Findings**

* **Strengths:** Strong SOC operations, existing DLP & SIEM, established incident response, RBI compliance alignment.
* **Weaknesses:** Lack of formal ISMS policy, incomplete risk assessment framework, limited supplier risk management, inconsistent employee awareness training.
* **Opportunities:** Align risk management with ISO 27005, formalize SoA, expand vendor security contracts.
* **Threats:** Legacy core banking system vulnerabilities, phishing/social engineering threats, regulatory penalties for non-compliance.

**4. Clause-wise Gap Assessment (ISO 27001:2022 Clauses 4–10)**

| **Clause** | **Requirement** | **Current Status** | **Gap Identified** | **Maturity** |
| --- | --- | --- | --- | --- |
| 4 – Context of Org | Define internal/external context, scope, stakeholders | Draft prepared but not formally approved | Needs formal sign-off | 2 |
| 5 – Leadership | Information Security Policy, Roles & Responsibilities | CISO exists, but no ISMS policy | Policy needs approval, communication | 2 |
| 6 – Planning | Risk assessment, treatment, objectives | RBI risk assessment followed, but not ISO-aligned | Need ISO 27005-aligned RA, RTP | 2 |
| 7 – Support | Competence, awareness, communication, resources | Security awareness ad-hoc; training limited | Need formal training plan, budget | 2 |
| 8 – Operation | Implement risk treatment, change mgmt, supplier controls | No formal supplier security checks | Vendor risk framework required | 2 |
| 9 – Performance Eval | Monitoring, internal audit, management review | Monitoring exists (SOC), but no ISMS audit | Internal ISMS audit framework needed | 2 |
| 10 – Improvement | Nonconformity, corrective actions | Incident mgmt. strong, but no ISMS improvement loop | Add NC/CAPA system for ISMS | 2 |

**5. Annex A Control Gap Highlights**

**Theme 1 – Organizational Controls (A.5):**

* **A.5.7 Threat Intelligence:** SOC collects threat feeds → ✅ in place.
* **A.5.20 Supplier Relationships:** No supplier security review process → ❌ GAP.
* **A.5.32 Logging:** Logs maintained but retention inconsistent → 🔶 Partial.

**Theme 2 – People Controls (A.6):**

* **A.6.3 Awareness, Education, Training:** Awareness sessions ad-hoc → ❌ GAP.
* **A.6.7 Disciplinary Process:** HR has misconduct policies → ✅ in place.

**Theme 3 – Physical Controls (A.7):**

* **A.7.4 Physical Security Perimeter:** DC & DR sites secure → ✅ in place.
* **A.7.10 Equipment Maintenance:** Legacy ATMs not updated regularly → ❌ GAP.

**Theme 4 – Technological Controls (A.8):**

* **A.8.9 Configuration Management:** No formal baseline → ❌ GAP.
* **A.8.10 Malware Protection:** Endpoint protection deployed → ✅ in place.
* **A.8.16 Monitoring Activities:** SIEM & SOC operational → ✅ strong.

**6. Gap Summary & Recommendations**

* **Policies & Governance:** Draft ISMS policy, SoA, roles → must be approved.
* **Risk Management:** Conduct ISO 27005-aligned risk assessment & risk treatment.
* **Supplier Security:** Implement vendor due diligence & SLA-based control requirements.
* **Training & Awareness:** Launch mandatory training for all employees.
* **Internal Audit:** Establish audit framework & nonconformity handling.
* **Legacy Systems:** Upgrade ATM systems, ensure patching.

**7. Next Steps**

* Management approval of context, scope, and ISMS policy.
* Formal risk assessment and treatment plan.
* Establish internal audit program.
* Prepare for certification body readiness assessment (Stage 1).