**ISMS Project Initiation Document (PID)**

**Organization:** ABC Bank Ltd.  
**Project Title:** ISO/IEC 27001:2022 Certification Program  
**Version:** 1.0  
**Date:** 21/9/2025

**Owner:** ISMS Program Manager

**1. Executive Summary**

ABC Bank Ltd., a mid-sized banking organization, intends to achieve ISO/IEC 27001:2022 certification within 12 months. This initiative aligns with the bank’s strategic objectives of:

* Strengthening its cybersecurity and information security posture,
* Meeting increasing regulatory expectations (RBI Cybersecurity Framework, PCI DSS, DPDP Act), and
* Enhancing customer trust in its digital banking platforms.

The ISMS will be rolled out in a **phased approach** covering governance, risk management, control implementation, and certification.

**2. Project Objectives**

* Establish a compliant ISMS framework aligned with ISO/IEC 27001:2022.
* Conduct gap assessment and risk assessment across banking operations.
* Implement risk treatment plans and required security controls.
* Train employees and enhance security awareness.
* Achieve successful Stage 1 and Stage 2 ISO 27001 certification audits.

**3. Project Scope**

**In-Scope (Core Operations):**

* Core Banking System (CBS)
* Internet & Mobile Banking Platforms
* Data Center (Primary & DR site)
* ATM Switch and related infrastructure
* IT Operations & Security Functions
* HR, Legal, and Compliance (where handling sensitive information)

**Out-of-Scope:**

* Marketing functions
* Branch interior facilities (except those handling IT or customer data)

**Scope Boundary:** ISMS is limited to India operations for Phase 1; global expansion may follow post-certification.

**4. Business Case**

* **Regulatory Pressure:** RBI mandates stronger cybersecurity practices for banks.
* **Customer Trust:** High-profile breaches in banking have eroded confidence; certification provides reassurance.
* **Competitive Advantage:** Certification enhances market reputation, particularly against fintech competitors.
* **Risk Reduction:** Systematic identification and treatment of risks will reduce chances of fraud, data leakage, and outages.

**5. Project Deliverables**

* ISMS Project Initiation Document (this doc)
* Context of the Organization document
* Gap Assessment Report
* Risk Assessment & Risk Treatment Plan
* Statement of Applicability (SoA)
* ISMS Policy, Procedures, and Control Documentation
* Internal Audit Reports
* Non-Conformity Reports & Corrective Action Plans
* Management Review Meeting Minutes
* Stage 1 & Stage 2 Audit Preparation Packages

**6. Project Organization & Governance**

**Steering Committee (Strategic Oversight):**

* Chief Information Officer (Chair)
* Chief Information Security Officer (CISO)
* Chief Operating Officer
* Head of Compliance

**ISMS Project Team (Operational Execution):**

* Project Manager (ISMS Lead)
* IT Infrastructure Lead
* IT Security Lead
* HR Manager
* Legal Counsel
* Risk & Compliance Analyst

**Roles & Responsibilities:**

* **CISO:** Overall accountability for ISMS.
* **Project Manager:** Day-to-day coordination and status reporting.
* **Functional Leads:** Implement controls in respective areas.
* **Internal Audit Lead:** Ensure audit readiness.

**7. Project Approach**

* **Phase 1 – Initiation (Month 1):** Form ISMS team, finalize scope, approve project plan.
* **Phase 2 – Gap Assessment (Months 2-3):** Assess compliance with ISO 27001 requirements.
* **Phase 3 – Risk Management (Months 4-5):** Identify, evaluate, and treat risks.
* **Phase 4 – Implementation (Months 6-9):** Implement policies, procedures, and technical controls.
* **Phase 5 – Internal Audit & Review (Months 10-11):** Perform internal audit, address non-conformities, conduct management review.
* **Phase 6 – Certification (Month 12):** Undergo Stage 1 and Stage 2 audits with certification body.

**8. Timeline (High-Level)**

| **Phase** | **Duration** | **Key Milestones** |
| --- | --- | --- |
| Initiation | 1 month | Project kickoff, governance established |
| Gap Assessment | 2 months | Gap report delivered |
| Risk Assessment | 2 months | Risk register approved |
| Implementation | 4 months | Policies, controls, training rolled out |
| Internal Audit & Review | 2 months | Internal audit, MR meeting |
| Certification | 1 month | Stage 1 & 2 audits completed |

**9. Resources & Budget**

* **Estimated Budget:** ₹1.2 Crore (~$150K)
* **Breakdown:**
  + Consultancy & Certification Fees – 25%
  + Training & Awareness – 15%
  + Tools & Technology (SIEM, DLP, IAM) – 40%
  + Internal Staff Effort – 20%

**10. Risks & Dependencies**

**Risks:**

* Staff resistance to new policies.
* Legacy system compatibility issues.
* Tight timelines may cause resource strain.

**Dependencies:**

* Support from top management.
* Timely budget approvals.
* Availability of certification body slots.

**11. Success Criteria**

* ISMS implemented across defined scope.
* All critical risks addressed or accepted by management.
* No major non-conformities in certification audits.
* ISO/IEC 27001 certificate awarded within project timeline.

**12. Approval**

**Approved By:**

* CIO (Steering Committee Chair) -
* CISO -
* COO -
* Head of Compliance -