**Statement of Applicability (SoA)**

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

**1. Purpose**

This document states which Annex A controls (ISO/IEC 27001:2022, 93 controls) are applicable to ABC Bank Ltd.’s ISMS, the justification for inclusion/exclusion, and implementation status.

**2. Scope Reference**

* ISMS scope includes: **Core Banking System (CBS), Internet & Mobile Banking Platforms, ATM Switch, Data Center (DC), Disaster Recovery (DR), Security Operations Center (SOC), HR, Compliance, and Legal functions.**

**3. SoA Summary**

| **Control Domain** | **Control ID** | **Control Description** | **Status** | **Inclusion Justification** | **Implementation Evidence** |
| --- | --- | --- | --- | --- | --- |
| **A.5 Organizational Controls** | A.5.1 | ISMS Policy | Included | Mandatory for ISO framework | ISMS Policy v1.2 signed by CEO |
|  | A.5.7 | Threat Intelligence | Included | Required for cyber resilience | SOC TI subscription with FS-ISAC |
|  | A.5.20 | Supplier Security Mgmt | Included | Banking has 3rd-party cloud vendors | Vendor risk mgmt policy, SLA with AWS |
|  | A.5.23 | Supplier Agreements | Included | Required for legal compliance | Vendor agreements with data protection clauses |
|  | A.5.36 | Compliance with legal and contractual | Included | Banking requires RBI/PCI compliance | Compliance monitoring checklist |
| **A.6 People Controls** | A.6.3 | Security Awareness Training | Included | Human error is top threat vector | E-learning portal, HR records |
|  | A.6.7 | Disciplinary Process | Included | Required for insider risk | HR policy v3.1 |
| **A.7 Physical Controls** | A.7.4 | Physical Entry Controls | Included | DC/DR security is critical | Biometric access, CCTV logs |
|  | A.7.11 | Power Supply | Included | Business continuity requirement | UPS & generator maintenance logs |
| **A.8 Technological Controls** | A.8.9 | Configuration Mgmt | Included | CBS system requires hardening | Baseline config docs |
|  | A.8.15 | Vulnerability Mgmt | Included | Required to mitigate ransomware | VA/PT reports, patch logs |
|  | A.8.16 | Monitoring Activities | Included | SOC operations | SIEM monitoring dashboard |
|  | A.8.23 | Web Filtering | Excluded | Not relevant for isolated ATM switch | Justified via risk assessment |
|  | A.8.25 | Secure Coding | Included | In-house mobile app development | DevSecOps pipeline evidence |
|  | A.8.27 | Secure System Testing | Included | Banking app release cycles | Test reports in JIRA |
|  | A.8.32 | Logging | Included | Required for fraud investigation | SIEM log storage 1 year |
|  | A.8.35 | Malware Protection | Included | ATM & endpoints exposed | Antivirus, EDR solution reports |

**4. Control Exclusions Justification**

* **A.8.23 Web Filtering:** Excluded since ATM switch network is isolated, not exposed to internet browsing.
* **A.7.5 Working from Home Controls:** Excluded since all core banking ops must be done onsite (per RBI guidelines).
* **A.8.37 ICT Readiness for Business Continuity:** Covered under existing BCP framework outside ISMS scope.

**5. Approval**

* Approved by: CIO, CISO, ISMS Steering Committee
* Date: [Insert Date]