**📑 2. Internal Audit Report**

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

**1. Purpose**

This document records the results of the internal ISMS audit, conducted to verify conformity with ISO/IEC 27001:2022 requirements prior to the certification audit.

**2. Audit Scope**

* ISMS covering CBS, Internet/Mobile Banking, ATM switch, DC/DR, SOC, HR, Legal, Compliance.
* Annex A controls (93 controls).

**3. Audit Method**

* Document review (policies, risk assessment, SoA, logs).
* Interviews with stakeholders (IT, HR, Compliance, SOC).
* Sampling of implemented controls.

**4. Audit Findings Summary**

| **Area** | **Strengths** | **Weaknesses** | **Conformance** |
| --- | --- | --- | --- |
| ISMS Policy & Scope | Scope defined, top management signed policy | Communication not complete to all branches | Partial |
| Risk Assessment | ISO 27005-aligned RA performed | Risk acceptance criteria not formally approved | Partial |
| Risk Treatment & SoA | RTP prepared, mapped to Annex A | SoA not signed by management | Partial |
| Supplier Security | Vendor list maintained | No periodic vendor audits | Non-conformity |
| Awareness & Training | SOC trained well | Bank-wide training inconsistent | Non-conformity |
| Incident Response | Strong SOC & IR playbooks | Limited business continuity exercises | Partial |
| Monitoring & Logging | SIEM in place | Log retention not uniform | Partial |

**5. Audit Conclusion**

* **Major Nonconformities:** 2 (Supplier security, Awareness training).
* **Minor Nonconformities:** 3 (SoA approval, risk acceptance criteria, log retention).
* **Observations:** BC/DR testing frequency, HR policy updates.

**6. Recommendations**

* Formalize risk acceptance process and SoA approval.
* Launch mandatory training for all employees.
* Enhance supplier risk management framework.
* Implement consistent log retention policy.
* Conduct full-scope BC/DR exercise annually.

**7. Auditor Sign-off**

Audited by: Internal Audit Lead  
Reviewed by: CISO  
Date: [Insert Date]