

ISMS Internal Audit

# 1. Introduction

**1.1 Purpose**

This document outlines the internal audit program for ABC-FinTech’s Information Security Management System (ISMS). It is designed to ensure the ISMS conforms to the organization's own requirements, ISO 27001:2022 standards, and is effectively implemented and maintained. The document also provides a summary of the results from recent audits.

**1.2 Scope**

The internal audit program applies to all information security processes and controls within the scope of ABC-FinTech's ISMS, covering all relevant departments, systems, and personnel.

# 2. ISMS Internal Audit Program

**2.1 Audit Program Overview**

The ISMS internal audit program is established to:

* Verify conformity to ABC-FinTech's information security policies and procedures.
* Ensure compliance with ISO 27001:2022 requirements.
* Assess the effectiveness of controls in achieving the organization’s information security objectives.

**2.2 Audit Frequency**

Internal audits are conducted:

* **Annually:** Full ISMS audit covering all key processes and controls.
* **Quarterly:** Focused audits on high-risk areas (e.g., third-party risk management, access control).
* **Event-Triggered Audits:** In response to significant incidents, system changes, or non-conformities detected in prior audits.

**2.3 Audit Methods**

Audits are performed using a combination of:

* **Document Reviews:** Review of policies, procedures, and documented information to ensure compliance.
* **Interviews:** Discussions with relevant personnel to verify awareness and understanding of ISMS controls.
* **On-Site Inspections:** Physical verification of security controls (e.g., access controls, data center security).
* **System Testing:** Penetration testing and vulnerability scans to verify the effectiveness of technical controls.

**2.4 Audit Planning**

Audit planning considers:

* The **importance** of the processes to the ISMS (e.g., higher frequency of audits for high-risk processes like vendor management or incident response).
* The **results of previous audits**, prioritizing areas with non-conformities or improvement opportunities.

**2.5 Audit Responsibilities**

* **Audit Team:** Composed of internal auditors trained in ISO 27001:2022 and information security best practices. To ensure impartiality, auditors do not audit processes for which they are responsible.
* **Lead Auditor:** Coordinates the audit, ensures objectivity, and oversees the reporting of results.
* **Relevant Departments:** Cooperate with the audit team, provide necessary documentation, and participate in interviews.

**2.6 Audit Criteria and Scope**

The audit criteria include:

* **ABC-FinTech’s ISMS Requirements:** Internal policies, procedures, and security controls.
* **ISO 27001:2022 Requirements:** Compliance with the standard’s Annex A controls and overall ISMS structure.

The **scope** of each audit varies:

* **Full ISMS Audit:** Covers all processes, controls, and departments.
* **Focused Audits:** Address specific areas, such as data encryption, incident response, or vendor management.

**2.7 Selection of Auditors**

Auditors are selected based on their expertise, independence, and familiarity with the ISO 27001 standard. They are trained in internal auditing practices to ensure impartiality and objectivity.

# 3. ISMS Internal Audit Results

**3.1 Recent Audit Overview (Annual Full ISMS Audit - Q4 2023)**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Audit Area | Criteria | Auditor(s) | Summary of Findings | Non-Conformities/Observations |
| Access Control (5.25) | Access control policies, logs, RBAC | Jane Doe, Lead Auditor | Access controls are effective; multi-factor authentication in place. | Observation: Improve frequency of access reviews. |
| Data Encryption (8.24) | Encryption policies, key management | John Smith, Auditor | AES-256 encryption for sensitive data is implemented and audited. | No major non-conformities. |
| Incident Response (5.26) | Incident response procedures | Lisa Adams, Auditor | Incident response plans are updated; response time is within SLA. | Non-conformity: Delayed reporting of a minor incident. |
| Third-Party Risk Management (5.19) | Vendor security assessments | Michael Brown, Auditor | Most vendors have undergone security audits; contracts updated. | Observation: 10% of vendors have delayed security compliance reports. |
| Physical Security (7.4) | Data center security, physical access | Jane Doe, Lead Auditor | Physical access controls are enforced; CCTV and alarm systems functional. | No major non-conformities. |

# 3.2 Summary of Findings

1. **Access Control (5.25)**:
   * **Observation**: While the overall access control mechanism is robust, the audit revealed that access reviews are not conducted as frequently as recommended. The frequency of these reviews will be increased to quarterly instead of bi-annually to ensure up-to-date records.
2. **Data Encryption (8.24)**:
   * **Compliance**: Full compliance with AES-256 encryption standards for sensitive data. Encryption key management was audited and found to be secure.
   * **No Non-Conformities Identified.**
3. **Incident Response (5.26)**:
   * **Non-Conformity**: A minor security incident was reported 2 days beyond the SLA timeframe. Root cause analysis indicates that a procedural bottleneck caused the delay. Corrective actions have been initiated to streamline incident reporting.
4. **Third-Party Risk Management (5.19)**:
   * **Observation**: 10% of third-party vendors have delayed submitting their annual security compliance reports. The Vendor Management team has been advised to improve follow-up and communication with vendors to ensure timely submission.
5. **Physical Security (7.4)**:
   * **Compliance**: Physical security controls, such as badge-based access control and CCTV monitoring at the data center, are functioning as expected.
   * **No Non-Conformities Identified.**

# 4. Audit Actions and Corrective Measures

**4.1 Non-Conformities and Corrective Actions**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Non-Conformity | Corrective Action | Responsible Party | Target Date | Status |
| Incident reporting delay (5.26) | Streamline incident reporting procedures and improve communication. | IT Security Manager | Q1 2024 | In Progress |

**4.2 Observations and Improvement Opportunities**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Observation | Improvement Action | Responsible Party | Target Date | Status |
| Frequency of access reviews (5.25) | Increase frequency of access control reviews from bi-annual to quarterly. | IT Security Team | Q1 2024 | Planned |
| Vendor compliance reports (5.19) | Strengthen follow-up with vendors to ensure timely compliance reporting. | Vendor Management Lead | Q2 2024 | Planned |

# 5. Reporting and Documentation

**5.1 Audit Reports**

* All audit results are documented and reported to the **Information Security Steering Committee** (ISSC) and relevant department heads for review and action.
* The **Lead Auditor** is responsible for compiling the audit reports, including non-conformities, observations, and corrective actions.

**5.2 Audit Evidence and Record Retention**

ABC-FinTech retains the following documented information as evidence of the ISMS internal audit program:

* **Audit Schedules and Plans:** Retained for 5 years to track audit frequencies and areas of focus.
* **Audit Reports:** Detailed reports of each audit, including findings, non-conformities, and corrective actions, are retained for 5 years.
* **Corrective Action Logs:** Logs of corrective actions taken in response to non-conformities are retained for 3 years after the action has been completed.

# 6. Monitoring and Review of the Audit Program

The ISMS internal audit program is reviewed annually by the **Information Security Steering Committee** to:

* Ensure audit frequencies are appropriate based on the criticality of processes and the results of prior audits.
* Verify that the audit methods and procedures remain effective.
* Make any necessary updates to the audit program based on changes in the organization’s ISMS or risk landscape.

# 7. Conclusion

The internal audit program for ABC-FinTech’s ISMS ensures compliance with both internal requirements and ISO 27001:2022 standards. The results of the recent audit indicate that the ISMS is effectively implemented and maintained, with minor improvements needed in access review frequency and third-party vendor reporting.

**Approved by:**

**CEO, ABC-FinTech**  
**Date: 24 Jan 2024**