

Evidence Of Top Management

Reviews Of The ISMS

# 1. Introduction

**1.1 Purpose**

This document provides evidence of the top management review of ABC-FinTech’s Information Security Management System (ISMS), conducted at planned intervals to ensure its continuing suitability, adequacy, and effectiveness.

**1.2 Scope**

This review applies to all departments, processes, and information security controls within the scope of ABC-FinTech’s ISMS, focusing on key areas including the status of previous actions, changes to internal and external factors, performance trends, risk assessments, and opportunities for continual improvement.

# 2. Management Review Summary

**2.1 Date of Review:**

* **Date:** February 15, 2024

**2.2 Attendees:**

|  |  |
| --- | --- |
| Role | Name |
| CEO | John Doe |
| CISO | Jane Smith |
| Head of IT | Michael Brown |
| Data Protection Officer (DPO) | Lisa Adams |
| HR Manager | Sarah Johnson |
| Vendor Management Lead | David Green |
| Lead Auditor | Paul Davis |

# 3. Review Agenda and Key Discussion Points

**3.1 Status of Actions from Previous Management Reviews**

|  |  |  |
| --- | --- | --- |
| Previous Action | Status | Outcome |
| Increase the frequency of access control reviews from bi-annual to quarterly. | Implemented as of October 2023 | No access control violations were identified in Q4 2023. |
| Streamline incident reporting procedures to prevent delays in reporting incidents. | In progress | Minor incident in Dec 2023 was reported late. Ongoing. |

**3.2 Changes in External and Internal Issues**

|  |  |
| --- | --- |
| Category | Details |
| External | **Regulatory Update (GDPR):** Changes in European data protection laws require updated vendor contracts.  **Cyber Threat Landscape:** Increase in ransomware attacks in the financial sector. |
| Internal | **System Upgrade:** Migration to a new cloud service provider. **New Vendors:** Several new third-party vendors onboarded. |

**3.3 Information Security Performance Feedback**

**3.3.1 Nonconformities and Corrective Actions**

|  |  |  |
| --- | --- | --- |
| Issue | Corrective Action | Status |
| Delayed incident reporting in Q4 2023 | Update incident reporting procedures to prevent future delays. | In Progress |

**3.3.2 Monitoring and Measurement Results**

|  |  |
| --- | --- |
| Monitoring Area | Result (Q4 2023) |
| Incident Response Performance | Average response time: 30 minutes (within SLA). |
| Data Encryption Compliance | 100% sensitive data encrypted at rest and in transit. |

**3.3.3 Audit Results**

The results of the **Q4 2023 internal audit** revealed no major nonconformities, but observations were made regarding vendor compliance with annual security reporting.

* **Vendor Reporting:** 10% of vendors did not submit their annual security compliance reports on time.

**3.3.4 Fulfillment of Information Security Objectives**

1. **Objective 1 (Reduce Cyber Attacks by 30%):** Achieved a 35% reduction in successful cyber attacks during Q4 2023 compared to Q4 2022.
2. **Objective 2 (Achieve 100% Encryption of Sensitive Data):** 100% compliance with encryption requirements has been maintained.

**3.4 Feedback from Interested Parties**

|  |  |
| --- | --- |
| Source | Feedback |
| Employees | 95% passed phishing simulation tests in Q4 2023. |
| Vendors | Some vendors facing challenges meeting new encryption requirements. |
| Customers | No customer complaints or data breaches reported in Q4 2023. |

**3.5 Results of Risk Assessment and Risk Treatment Status**

|  |  |
| --- | --- |
| Risk | Status |
| Cyber attacks on web applications | Mitigated through enhanced threat detection and firewall upgrades. |
| Delays in incident reporting | Corrective actions in progress. |
| Vendor security risks due to compliance delays | Follow-up actions initiated to improve vendor compliance reporting. |

**3.6 Opportunities for Continual Improvement**

|  |  |
| --- | --- |
| Improvement Opportunity | Action Plan |
| Incident Response Automation | Explore options for automated incident response tools. |
| Vendor Compliance Management | Strengthen follow-up mechanisms to ensure timely vendor compliance reporting. |
| Phishing Simulation Frequency | Increase phishing simulations to monthly to improve employee security awareness. |

# 4. Decisions and Actions from the Review

**4.1 Continual Improvement Opportunities**

|  |  |  |  |
| --- | --- | --- | --- |
| Improvement Area | Decision | Action Owner | Target Date |
| Incident Response Automation | Explore options for automated incident response. | IT Security Manager | Q2 2024 |
| Vendor Compliance Management | Develop vendor follow-up process for compliance. | Vendor Management Lead | Q1 2024 |
| Phishing Simulation Frequency Increase | Increase phishing simulations to monthly. | HR Manager | Q1 2024 |

**4.2 Changes to the ISMS**

|  |  |  |  |
| --- | --- | --- | --- |
| Change Area | Decision | Action Owner | Target Date |
| Vendor Security Policy | Amend policy to introduce stricter compliance deadlines for vendors. | Vendor Management Lead | Q1 2024 |
| Incident Reporting Procedures | Update procedures to prevent delays in incident reporting. | IT Security Manager | Q1 2024 |

**4.3 Approved Resources**

* **Budget for Incident Response Automation:** Approved a budget of $50,000 for evaluating and procuring an automated incident response system by Q2 2024.

# 5. Documentation and Retention

ABC-FinTech retains the following documentation as evidence of the management reviews:

* **Meeting Agenda and Minutes:** Retained for 5 years.
* **Action Plans and Follow-Up Reports:** Retained for 3 years or until actions are completed.
* **Audit Reports and Non-Conformity Logs:** Retained for 5 years.

# 6. Conclusion

The top management review of ABC-FinTech’s ISMS for Q4 2023 confirms the system's effectiveness and alignment with ISO 27001:2022 standards. Action plans have been created to address non-conformities and improve information security processes. The ISMS will be reviewed again in Q2 2024.

**Approved by:**

**CEO, ABC-FinTech**  
**Date: 27 Feb 2024**