

Evidence Of The Monitoring And Measurement Of Information Security

# 1. Introduction

**1.1 Purpose**

This document outlines the processes and methods used by ABC-FinTech to monitor and measure the performance and effectiveness of its Information Security Management System (ISMS). It describes what is monitored, how it is monitored, and who is responsible for evaluating and analyzing the results, in alignment with ISO 27001:2022 standards.

**1.2 Scope**

This document applies to all relevant information security processes, controls, and personnel within ABC-FinTech. The monitoring and measurement activities focus on ensuring the continuous effectiveness of the ISMS and the achievement of information security objectives.

# 2. Monitoring and Measurement of Information Security

**2.1 What Needs to Be Monitored and Measured**

ABC-FinTech has identified the following information security processes, controls, and metrics for monitoring and measurement:

|  |  |  |
| --- | --- | --- |
| Monitoring Area | Objective | Key Metrics |
| Incident Response Performance | Measure response time and effectiveness in resolving security incidents. | Number of incidents, response time, severity |
| Data Encryption Compliance | Ensure that all sensitive data is encrypted at rest and in transit. | Percentage of data encrypted, encryption audits |
| Access Control Compliance | Ensure proper access control is in place for critical systems and data. | Number of access violations, unauthorized access |
| Vulnerability Management | Identify and remediate vulnerabilities in IT infrastructure. | Number of vulnerabilities identified and resolved, remediation time |
| Vendor Risk Management | Monitor and manage risks associated with third-party vendors. | Percentage of vendors compliant with security requirements, audit results |
| User Security Awareness | Assess the effectiveness of security awareness training programs. | Employee participation, test scores, phishing simulation results |

**2.2 Methods for Monitoring and Measurement**

The following methods are used to ensure accurate monitoring, measurement, and evaluation of the ISMS:

|  |  |  |
| --- | --- | --- |
| Monitoring Area | Method for Monitoring | Measurement Tools |
| Incident Response Performance | Incident tracking and analysis | Incident response logs, ticketing system |
| Data Encryption Compliance | Encryption audits and compliance checks | Encryption audit tools, log analysis |
| Access Control Compliance | Regular access reviews, monitoring of access control logs | Access control logs, IAM software |
| Vulnerability Management | Automated vulnerability scans, manual penetration testing | Vulnerability scanning tools, pen-testing reports |
| Vendor Risk Management | Regular vendor security audits and assessments | Vendor risk management platform |
| User Security Awareness | Phishing simulations, post-training assessments | Phishing test platform, survey tools |

**2.3 When Monitoring and Measurement Shall Be Performed**

|  |  |
| --- | --- |
| Monitoring Area | Frequency of Monitoring |
| Incident Response Performance | Monthly, with real-time monitoring for critical incidents |
| Data Encryption Compliance | Quarterly audits |
| Access Control Compliance | Quarterly access reviews |
| Vulnerability Management | Monthly scans, annual penetration tests |
| Vendor Risk Management | Bi-annual audits, continuous monitoring |
| User Security Awareness | Quarterly phishing simulations, post-training evaluations |

**2.4 Who Shall Monitor and Measure**

The following personnel and teams are responsible for monitoring and measuring the performance of the ISMS:

|  |  |
| --- | --- |
| Monitoring Area | Responsible Party |
| Incident Response Performance | SOC (Security Operations Center) Team |
| Data Encryption Compliance | Data Protection Officer (DPO), IT Security Team |
| Access Control Compliance | IT Security Team, Access Control Administrators |
| Vulnerability Management | IT Security Team |
| Vendor Risk Management | Vendor Management Lead |
| User Security Awareness | HR, IT Security Team |

**2.5 When Results Shall Be Analyzed and Evaluated**

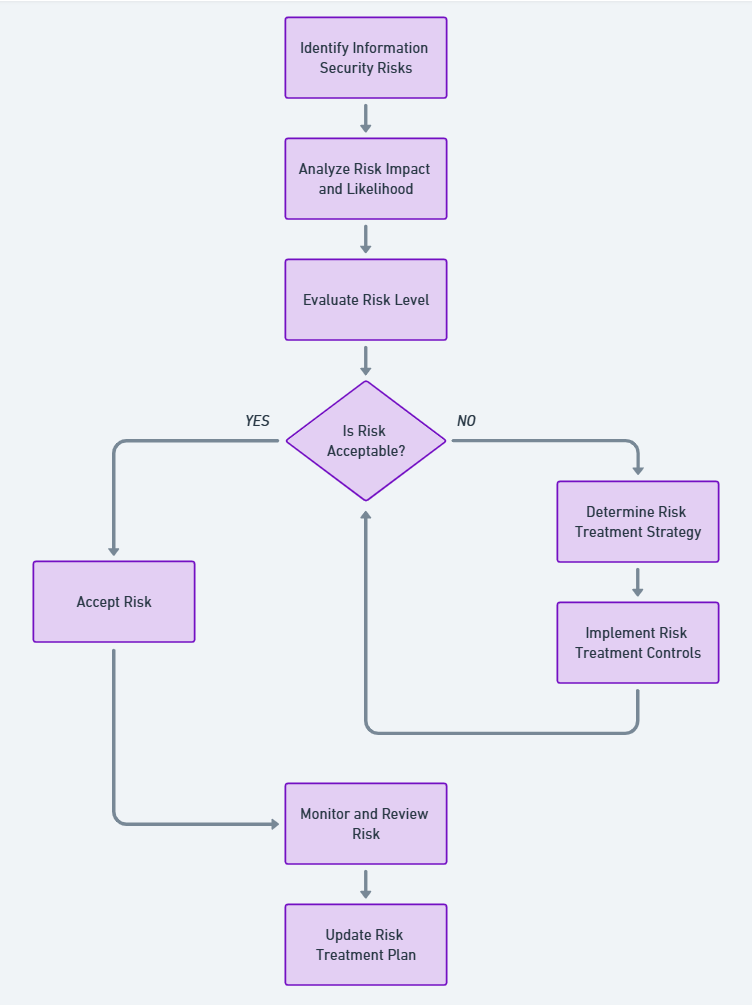
|  |  |
| --- | --- |
| Monitoring Area | When Results Are Analyzed |
| Incident Response Performance | Monthly, with real-time analysis for critical incidents |
| Data Encryption Compliance | Quarterly report to the Information Security Steering Committee |
| Access Control Compliance | Quarterly analysis of access logs and user reviews |
| Vulnerability Management | Monthly review of vulnerability scan results, annual pen-test analysis |
| Vendor Risk Management | Bi-annual review of vendor compliance status |
| User Security Awareness | Quarterly review of phishing simulation results and training effectiveness |

**2.6 Who Shall Analyze and Evaluate the Results**

|  |  |
| --- | --- |
| Monitoring Area | Responsible for Analysis and Evaluation |
| Incident Response Performance | SOC Manager, IT Security Manager |
| Data Encryption Compliance | Data Protection Officer (DPO), Chief Information Security Officer (CISO) |
| Access Control Compliance | IT Security Manager, CISO |
| Vulnerability Management | IT Security Manager, CISO |
| Vendor Risk Management | Vendor Management Lead, Risk & Compliance Manager |
| User Security Awareness | HR Manager, IT Security Manager |

# 3. Risk Management Process Diagram

The following diagram represents the **Risk Management Process**, which includes risk identification, treatment, monitoring, and review.



# 4. Evidence of Monitoring and Evaluation

**4.1 Incident Response Monitoring**

* **Monthly Incident Reports:** SOC logs and incident response performance are documented and reported to the CISO. The monthly incident reports include incident count, response times, and severity levels.
* **Critical Incident Analysis:** Any critical security incident undergoes real-time monitoring and immediate review, with a detailed report submitted to senior management.

**4.2 Data Encryption Compliance**

* **Quarterly Encryption Audits:** Encryption audits are performed by the DPO, and the results are presented to the Information Security Steering Committee. The audits track encryption coverage for all critical systems and identify any gaps in compliance.

**4.3 Vulnerability Management**

* **Vulnerability Scan Results:** Monthly vulnerability scans are conducted, and the results are documented. The IT Security Team analyzes scan results to identify high-risk vulnerabilities and prioritize remediation efforts.
* **Annual Penetration Testing Report:** The annual penetration test report is analyzed by the IT Security Manager and used to update the vulnerability management process.

**4.4 User Security Awareness**

* **Phishing Simulation Results:** The IT Security Team conducts quarterly phishing simulations and compiles the results in a report. Participation rates and test scores are analyzed to assess the effectiveness of training and adjust the awareness program accordingly.

# 5. Documentation and Record Retention

ABC-FinTech maintains the following documented information as evidence of monitoring and measurement activities:

* **Incident Logs:** SOC incident logs are retained for 3 years.
* **Encryption Audit Reports:** Quarterly audit reports are retained for 5 years.
* **Vulnerability Management Logs:** Vulnerability scan results and penetration test reports are retained for 3 years.
* **Vendor Risk Assessments:** Vendor audit reports are retained for the duration of the vendor contract plus 2 years.
* **User Security Awareness Records:** Training participation and phishing simulation results are retained for 5 years.

# 6. Conclusion

ABC-FinTech’s monitoring and measurement of information security processes ensure that the ISMS remains effective and aligned with the organization’s information security objectives. By using the outlined methods, personnel, and schedules, the organization continually assesses its security posture and adjusts controls as necessary to mitigate risks.

**Approved by:**

**CEO, ABC-FinTech**  
**Date: 22 Jan 2024**