

The Decisions Regarding Risk Treatment

# 1. Introduction

**1.1 Purpose**

This document provides an overview of the decisions made regarding the treatment of identified information security risks at ABC-FinTech. The decisions are based on the risk assessment results and are in line with the organization’s Information Security Management System (ISMS) and ISO 27001:2022 standards.

**1.2 Scope**

This document applies to all risks identified during the recent information security risk assessment and outlines the actions taken to mitigate, avoid, transfer, or accept the risks, as well as any decisions related to their treatment.

# 2. Scenario: Implementation of Risk Treatment Plan

Following the results of the risk assessment, ABC-FinTech’s Information Security Steering Committee held a meeting to review the high-priority risks. This scenario details the decisions made regarding the risk treatment for three key risks: **Cyber Attacks (R001)**, **Data Breaches (R002)**, and **Third-Party Vendor Risks (R004)**.

**2.1 Risk R001: Cyber Attacks**

* **Risk Description:** ABC-FinTech’s public-facing web applications and network infrastructure are at high risk of cyberattacks, including Distributed Denial of Service (DDoS) attacks and phishing campaigns.
* **Risk Level:** High
* **Treatment Option Chosen:** Mitigation
* **Decision Rationale:** Given the critical nature of ABC-FinTech’s public-facing services, the risk of cyberattacks requires mitigation through enhanced defenses.

**Actions Taken:**

* **Implement Threat Intelligence Solutions (5.7):** The IT Security Team was tasked with implementing an advanced threat intelligence system to detect potential attacks early. This includes monitoring dark web forums and external sources for signs of emerging threats.
  + **Decision:** Allocate budget and resources for implementing a third-party threat intelligence platform.
  + **Responsible Party:** CISO
  + **Target Date:** Q2 2024
* **Upgrade Firewall and IDS/IPS Systems (8.20):** The current network defenses were deemed insufficient to prevent large-scale DDoS attacks and targeted phishing attempts. As a result, the firewall and Intrusion Detection/Prevention Systems (IDS/IPS) were upgraded.
  + **Decision:** Purchase and deploy a next-generation firewall solution, and upgrade the IDS/IPS systems.
  + **Responsible Party:** IT Security Team
  + **Target Date:** Q1 2024
* **Employee Phishing Simulation (6.3):** To address phishing risks, a phishing simulation program was approved to train employees on how to detect and report phishing attempts.
  + **Decision:** Conduct quarterly phishing tests for all employees to measure their awareness and response to phishing emails.
  + **Responsible Party:** HR, IT Security Team
  + **Target Date:** Ongoing

**2.2 Risk R002: Data Breaches Due to Insufficient Encryption**

* **Risk Description:** Insufficient encryption practices were identified, exposing customer data stored in databases and in transit over the network.
* **Risk Level:** High
* **Treatment Option Chosen:** Mitigation
* **Decision Rationale:** Data breaches are a significant concern for ABC-FinTech due to the sensitivity of financial data. Encryption is a critical control to ensure data confidentiality and integrity.

**Actions Taken:**

* **Implement AES-256 Encryption (8.24):** ABC-FinTech decided to standardize AES-256 encryption for all sensitive customer data, both at rest in databases and in transit across the network.
  + **Decision:** Roll out AES-256 encryption for customer databases, and upgrade SSL/TLS protocols for data in transit.
  + **Responsible Party:** Data Protection Officer (DPO), Database Administrator
  + **Target Date:** Q1 2024 (Completed)
* **Encryption Key Management (8.24):** A key management system was introduced to ensure that encryption keys are stored, rotated, and managed securely.
  + **Decision:** Deploy a centralized key management solution to automate key lifecycle management.
  + **Responsible Party:** Database Administrator
  + **Target Date:** Q1 2024 (Completed)
* **Regular Encryption Audits (5.36):** To ensure compliance with the new encryption standards, quarterly audits of encryption practices were introduced.
  + **Decision:** Conduct encryption audits and report compliance levels to senior management.
  + **Responsible Party:** Data Protection Officer (DPO)
  + **Target Date:** Quarterly (Ongoing)

**2.3 Risk R004: Third-Party Vendor Risks**

* **Risk Description:** ABC-FinTech relies on several third-party vendors, including a payment processing provider. These vendors pose a risk if their security practices are inadequate, potentially exposing ABC-FinTech to data breaches or service interruptions.
* **Risk Level:** High
* **Treatment Option Chosen:** Mitigation
* **Decision Rationale:** Since outsourcing processes are critical to the business, it is essential to manage third-party risks through rigorous security assessments and contractual agreements.

**Actions Taken:**

* **Vendor Security Assessments (5.21):** ABC-FinTech decided to conduct comprehensive security assessments for all third-party vendors, focusing on compliance with ISO 27001 and PCI DSS.
  + **Decision:** Establish a formal vendor assessment program and require third-party vendors to undergo annual security audits.
  + **Responsible Party:** Vendor Management Lead
  + **Target Date:** Q2 2024 (In Progress)
* **Contractual Security Requirements (5.20):** All contracts with third-party vendors were revised to include specific security requirements, including encryption, incident reporting, and regular audits.
  + **Decision:** Update contracts with all vendors to include mandatory security requirements and clauses for breach notification.
  + **Responsible Party:** Legal Team, Vendor Management Lead
  + **Target Date:** Q2 2024 (In Progress)
* **Continuous Vendor Monitoring (8.16):** A continuous monitoring system was introduced to track the performance and compliance of third-party vendors, including real-time alerts for security incidents.
  + **Decision:** Implement a vendor monitoring platform to track vendor performance against security metrics.
  + **Responsible Party:** Vendor Management Lead
  + **Target Date:** Q3 2024 (Planned)

# 3. Monitoring and Review of Risk Treatment

To ensure that the risk treatments remain effective, the following monitoring and review mechanisms are in place:

|  |  |  |  |
| --- | --- | --- | --- |
| Risk ID | Monitoring Method | Frequency | Responsible Party |
| R001 | Continuous network and threat monitoring | Daily | IT Security Team |
| R002 | Regular encryption audits | Quarterly | Data Protection Officer (DPO) |
| R004 | Vendor security audits | Bi-annually | Vendor Management Lead |

**3.1 Continuous Improvement**

Risk treatment plans will be reviewed quarterly to ensure that they remain aligned with the evolving threat landscape. If new risks emerge or existing treatments are found to be inadequate, the Information Security Steering Committee will take immediate action to update the treatment plans.

# 4. Documentation and Evidence of Risk Treatment

ABC-FinTech retains documented information related to the risk treatment decisions, including:

* Records of risk assessments and the decision-making process.
* Documentation of controls implemented for each risk.
* Monitoring logs and audit reports for tracking the effectiveness of risk treatments.

# 5. Conclusion

The Information Security Steering Committee has reviewed the risk assessment results and implemented appropriate risk treatment actions. The treatments for **Cyber Attacks (R001)**, **Data Breaches (R002)**, and **Third-Party Vendor Risks (R004)** have been initiated and are either completed or in progress. Continuous monitoring and regular reviews will ensure that these treatments remain effective in protecting ABC-FinTech’s information assets.

**Approved by:**

**CEO, ABC-FinTech**  
**Date: 17 Jan 2024**