

Results Of Risk Assessments

# 1. Introduction

**1.1 Purpose**

The purpose of this document is to summarize the results of ABC-FinTech’s Information Security Risk Assessment. The assessment is performed to evaluate risks to the organization’s information security and determine appropriate measures for mitigating those risks. This document contains the results of risk assessments performed at planned intervals and after significant changes.

**1.2 Scope**

The risk assessment covers all relevant information assets, systems, processes, and personnel within the scope of the ISMS. It evaluates risks to the confidentiality, integrity, and availability (CIA) of information in accordance with the criteria defined in the **Risk Management Process**.

# 2. Overview of the Risk Assessment Process

The risk assessment process involved the following steps:

1. **Risk Identification:** Identification of threats and vulnerabilities affecting ABC-FinTech’s information assets.
2. **Risk Analysis:** Analysis of the likelihood and impact of identified risks.
3. **Risk Evaluation:** Classification of risks based on the organization’s risk criteria (low, medium, high).
4. **Risk Treatment:** Determination of appropriate measures to treat the risks, including acceptance, mitigation, transfer, or avoidance.

**2.1 Timing of Risk Assessments**

The risk assessment results documented here are based on:

* **Scheduled Assessment:** Performed every 6 months.
* **Change-triggered Assessment:** Conducted due to significant changes, including:
  + Implementation of new cloud infrastructure.
  + Onboarding of a third-party payment processor.
  + Introduction of a new data encryption standard.

# 3. Results of the Information Risk Assessment

**3.1 Risk Identification**

The following risks were identified during the most recent assessment:

|  |  |  |  |
| --- | --- | --- | --- |
| Risk ID | Risk Description | Affected Assets/Systems | Risk Owner |
| R001 | Cyber attacks (e.g., DDoS, phishing) | Public-facing web applications, network | CISO |
| R002 | Data breaches due to insufficient encryption | Customer databases | Data Protection Officer (DPO) |
| R003 | Insider threats (intentional or accidental data leakage) | HR and finance systems | HR Manager |
| R004 | Third-party vendor risks | Payment processing systems | Vendor Management Lead |
| R005 | System failure due to insufficient backup and redundancy | Database servers, critical IT infrastructure | IT Operations Manager |
| R006 | Regulatory non-compliance (GDPR and PCI DSS) | Customer and payment data | Compliance Manager |
| R007 | Fraudulent transactions through compromised credentials | Payment gateway | Fraud Prevention Manager |

**3.2 Risk Analysis**

For each identified risk, the likelihood and impact were assessed based on the defined risk criteria.

|  |  |  |  |
| --- | --- | --- | --- |
| Risk ID | Likelihood | Impact | Risk Level (Low/Medium/High) |
| R001 | High | High | High |
| R002 | Medium | High | High |
| R003 | Medium | Medium | Medium |
| R004 | Medium | High | High |
| R005 | Low | High | Medium |
| R006 | Low | High | Medium |
| R007 | High | High | High |

**3.3 Risk Evaluation**

Based on the risk analysis, the following risks were prioritized for treatment:

|  |  |  |  |
| --- | --- | --- | --- |
| Risk ID | Risk Level | Risk Treatment Option | Justification |
| R001 | High | Mitigation | High likelihood and impact require strong defenses. |
| R002 | High | Mitigation | Encryption is critical to protect sensitive data. |
| R003 | Medium | Mitigation | Insider threats are a moderate risk to information. |
| R004 | High | Mitigation | Vendor relationships need to be secured. |
| R005 | Medium | Mitigation | Backup and redundancy are crucial for system uptime. |
| R006 | Medium | Mitigation | Regulatory compliance is mandatory. |
| R007 | High | Mitigation | Fraud risks must be actively mitigated. |

# 4. Risk Treatment Actions

The following actions were taken to address the identified risks:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Risk ID | Treatment Strategy | Control Measures (ISO 27001 Annex A) | Responsible Party | Status |
| R001 | Mitigation | 5.7, 8.8 (Threat intelligence, Vulnerability management) | IT Security Team | In Progress |
| R002 | Mitigation | 8.24 (Data encryption) | Data Protection Officer (DPO) | Completed |
| R003 | Mitigation | 6.1 (Screening and background checks) | HR Manager | Planned |
| R004 | Mitigation | 5.20 (Supplier risk management) | Vendor Management Lead | In Progress |
| R005 | Mitigation | 8.13 (Backup and business continuity management) | IT Operations Manager | Planned |
| R006 | Mitigation | 5.36 (Regulatory compliance management) | Compliance Manager | Ongoing |
| R007 | Mitigation | 8.5 (Identity and access management) | Fraud Prevention Manager | In Progress |

# 5. Monitoring and Review

The following monitoring actions are being undertaken to ensure the effectiveness of the risk treatment measures:

**5.1 Monitoring Actions**

|  |  |  |  |
| --- | --- | --- | --- |
| 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) |
| R003 | Internal audit of HR security practices | Annually | HR Manager |
| R004 | Vendor security audits | Bi-annually | Vendor Management Lead |
| R005 | Backup recovery drills | Monthly | IT Operations Manager |
| R006 | Internal compliance audits | Quarterly | Compliance Manager |
| R007 | Fraud detection system logs | Real-time monitoring | Fraud Prevention Manager |

**5.2 Review Schedule**

* **Quarterly Reviews:** All risk treatments are reviewed quarterly by the Information Security Steering Committee.
* **Annual Audit:** An annual internal audit will be conducted to evaluate the overall effectiveness of the risk treatment plan.
* **Change-Triggered Reviews:** Any significant changes in infrastructure, processes, or vendor relationships will trigger an immediate reassessment of relevant risks.

# 6. Results Summary

The risk assessment identified **7 key risks**, with 5 classified as high risk and 2 as medium risk. Risk treatment plans have been implemented or are in progress for all identified risks. Continuous monitoring and periodic reviews are scheduled to ensure ongoing effectiveness.

* **Key Areas of Concern:** Cyber attacks (R001), Data breaches (R002), and Fraudulent transactions (R007) represent the highest risks due to their potential impact on ABC-FinTech’s operations and reputation.
* **Status of Risk Treatments:** Risk treatments are in various stages of implementation, with encryption measures for sensitive data (R002) already completed, and ongoing work for the remaining high-priority risks.
* **Monitoring and Auditing:** Ongoing monitoring and quarterly reviews will ensure that mitigation measures remain effective, with adjustments made as needed based on changes in the threat landscape.

# 7. Conclusion

This document summarizes the results of ABC-FinTech’s most recent Information Security Risk Assessment. By identifying and prioritizing risks, and implementing risk treatment plans, ABC-FinTech ensures that its information security practices are aligned with ISO 27001:2022 standards, minimizing the potential for significant security incidents.

**Approved by:**

**CEO, ABC-FinTech**  
**Date: 20 Jan 2024**