

Information Security Risk Treatment

# 1. Introduction

**1.1 Purpose**

The purpose of this document is to define and apply an Information Security Risk Treatment process that addresses risks identified during the Information Security Risk Assessment. It includes selecting appropriate risk treatment options, determining necessary controls, developing a Statement of Applicability (SoA), and formulating a Risk Treatment Plan in alignment with ISO 27001:2022 standards.

**1.2 Scope**

This process applies to all information assets, systems, processes, and personnel within ABC-FinTech that fall under the scope of the ISMS. The objective is to mitigate risks to confidentiality, integrity, and availability of information by implementing controls from Annex A of ISO 27001:2022.

# 2. Information Security Risk Treatment Process

**2.1 Selecting Risk Treatment Options**

Based on the outcomes of the risk assessment, the following options are selected for each identified risk:

* **Avoidance:** Discontinue activities that introduce unacceptable risks.
* **Mitigation:** Apply security controls to reduce the risk to an acceptable level.
* **Transfer:** Transfer risk to external parties (e.g., via insurance).
* **Acceptance:** Accept the residual risk if it falls within acceptable limits.

**2.2 Determining Necessary Controls**

For each risk treatment option, necessary controls are identified. Controls are mapped directly from **Annex A of ISO/IEC 27001:2022**, ensuring they are adequate and no necessary controls are overlooked.

**2.3 Producing a Statement of Applicability (SoA)**

The **Statement of Applicability (SoA)** contains:

* Controls selected from **Annex A** of ISO/IEC 27001:2022.
* Justification for the inclusion of each control.
* Status of implementation (implemented or not).
* Justification for the exclusion of any controls.

**2.4 Formulating the Risk Treatment Plan**

The Risk Treatment Plan outlines the actions required to implement selected controls, allocate resources, and define timelines.

**2.5 Approval and Residual Risk Acceptance**

Risk owners review and approve the Risk Treatment Plan and accept residual risks once the treatment options and controls are applied. Documented approval ensures accountability.

# 3. Statement of Applicability (SoA)

The **Statement of Applicability** provides a mapping of relevant controls from **Annex A of ISO/IEC 27001:2022** to the identified risks, including justifications for inclusion or exclusion. Below is a summary:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Control Reference  (ISO 27001) | Control Description | Applicable Risks Addressed | Implemented | Justification for Inclusion |
| 5.1 | Policies for Information Security | All Risks (Governance) | Yes | Policies provide a framework for security governance. |
| 5.7 | Threat Intelligence | Cyber Attacks, Insider Threats | Yes | Necessary for identifying emerging threats. |
| 5.2 | Information Security Roles and Responsibilities | Governance-Related Risks | Yes | Ensures clear assignment of security responsibilities. |
| 6.1 | Screening | Insider Threats | Yes | Mitigates insider threats via background checks. |
| 5.9 | Inventory of Information Assets | Data Breaches, Data Loss | Yes | Asset management ensures proper data protection. |
| 5.15 | Access Control | Data Breaches, Unauthorized Access | Yes | Protects against unauthorized access to data. |
| 8.24 | Cryptography | Data Breaches, Data Loss | Yes | Ensures data confidentiality and integrity. |
| 8.8 | Technical Vulnerability Management | System Failures, Data Loss | Yes | Ensures vulnerabilities are managed appropriately. |
| 5.24 | Information Security Incident Management | Cyber Attacks, Data Breaches | Yes | Ensures effective response to security incidents. |
| 5.31 | Legal, statutory, regulatory and contractual requirements | Regulatory Non-Compliance | Yes | Ensures compliance with applicable laws. |

**Exclusion of Controls**

Some controls may not be applicable based on the organization's context. Justifications for any excluded controls are documented.

# 4. Risk Treatment Plan

The **Risk Treatment Plan** details the actions needed to address each risk, who is responsible, and the timeline for implementation. It is regularly updated to reflect changes in risk status and control effectiveness.

**4.1 Risk Treatment Actions**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Risk | Treatment Strategy | Control Measures (ISO 27001 Annex A) | Responsible Party | Target Date | Status |
| Cyber Attacks | Mitigation | 5.7, 5.15, 5.24 (Threat intelligence, Access control, Incident management) | IT Security Team | Q2 2024 | In Progress |
| Data Breaches | Mitigation | 5.9, 5.15, 8.24 (Asset management, Access control, Cryptography) | Data Protection Officer (DPO) | Q1 2024 | Completed |
| Insider Threats | Mitigation | 6.1, 5.2 (Screening, Roles & responsibilities) | HR Manager | Q3 2024 | Planned |
| Third-Party Risks | Mitigation | 5.19, A.5.20 (Supplier management, Agreements) | Vendor Management Lead | Q2 2024 | In Progress |
| Data Loss | Mitigation | 8.24, 8.8 (Cryptography, Vulnerability management) | Database Administrator | Q1 2024 | Completed |
| Unauthorized Transactions | Mitigation | 5.15, 8.24 (Access control, Cryptography) | Fraud Prevention Manager | Q2 2024 | In Progress |
| System Failures | Mitigation | 8.8 (Technical Vulnerability Management) | IT Operations Manager | Q4 2024 | Planned |
| Regulatory Non-Compliance | Mitigation | 5.31 (Compliance management) | Compliance Manager | Ongoing | Ongoing |

# 5. Approval and Acceptance

**5.1 Risk Owner Approval**

Risk owners review and approve the Risk Treatment Plan. Approval indicates that they accept the residual risks after applying the appropriate controls.

**5.2 Approval Signatures**

| **Risk Owner** | **Role** | **Signature** | **Date** |
| --- | --- | --- | --- |
| Chief Information Security Officer (CISO) | CISO | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_ |
| Data Protection Officer (DPO) | DPO | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_ |
| Human Resources Manager | HR Manager | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_ |
| Vendor Management Lead | Vendor Management Lead | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_ |
| Database Administrator | Database Administrator | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_ |
| Fraud Prevention Manager | Fraud Prevention Manager | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_ |
| IT Operations Manager | IT Operations Manager | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_ |
| Compliance Manager | Compliance Manager | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_ |

# 6. Documentation and Monitoring

**6.1 Documented Information**

The organization will retain documented information about the entire risk treatment process, including:

* Risk assessment results.
* Selected controls.
* Risk Treatment Plan.
* Statement of Applicability.
* Approvals.

**6.2 Monitoring and Review**

The effectiveness of risk treatments will be reviewed at regular intervals through audits, incident reports, and performance evaluations. Residual risks will be reassessed to ensure they remain within acceptable limits.

**Approved by:**

**CEO, ABC-FinTech**  
**Date: 14 Jan 2024**