

Operational Planning And Control

# 1. Introduction

**1.1 Purpose**

The purpose of this document is to outline the operational planning and control processes required to meet the information security requirements of ABC-FinTech. These processes are designed to ensure that all security controls and actions are implemented and managed effectively.

**1.2 Scope**

This document applies to all processes, departments, and personnel within ABC-FinTech that are involved in the Information Security Management System (ISMS). It also includes controls for outsourced processes that have an impact on information security.

# 2. Operational Planning and Control Process

**2.1 Planning and Implementing Information Security Processes**

ABC-FinTech plans, implements, and controls processes to meet the following information security requirements:

* Ensuring the confidentiality, integrity, and availability (CIA) of information assets.
* Complying with ISO 27001:2022 standards and other regulatory requirements.
* Managing risks identified in the risk assessment.
* Achieving the information security objectives as outlined in the **Information Security Objectives** document.

**2.2 Documented Information for Process Control**

ABC-FinTech retains the necessary documented information for each process to ensure that they have been carried out as planned. This includes:

* Process flow diagrams.
* Audit logs.
* Change management records.
* Security incident response logs.

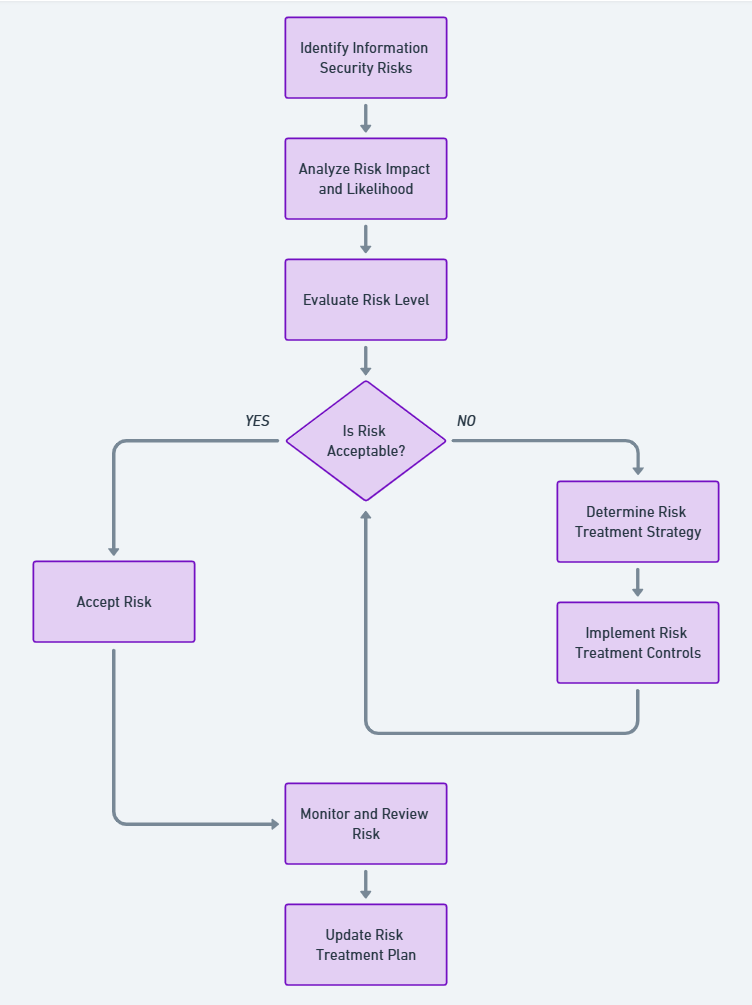
**2.3 Controlling Changes and Mitigating Adverse Effects**

ABC-FinTech ensures that all changes to information security processes are planned and controlled. Unintended changes are reviewed, and appropriate actions are taken to mitigate any negative impacts on the ISMS.

# 3. Process Diagrams

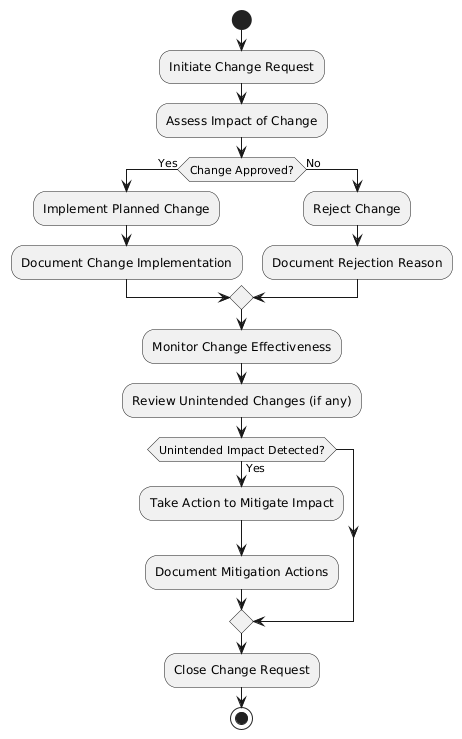
**3.1 Process 1: Risk Management and Control Process**

The following diagram outlines the steps involved in the risk management process, from risk identification to treatment and monitoring.



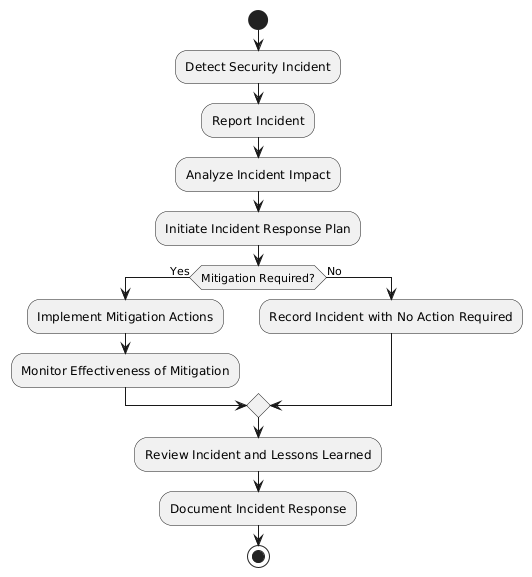
**3.2 Process 2: Change Management Process**

The following diagram outlines the steps to manage and control changes to security processes or infrastructure, including reviewing unintended changes.



**3.3 Process 3: Incident Response and Mitigation Process**

The following diagram describes the steps for managing security incidents, from detection to mitigation and review.



# 4. Controlling Outsourced Processes

**4.1 Identifying Outsourced Processes**

ABC-FinTech identifies and documents all outsourced processes that impact the ISMS. These include:

* Cloud service providers.
* Payment processing vendors.
* Third-party security monitoring services.

**4.2 Controlling Outsourced Processes**

ABC-FinTech ensures that outsourced processes are controlled by:

* Incorporating security requirements into contracts with vendors.
* Conducting regular security audits of third-party providers.
* Requiring compliance with relevant security standards (e.g., ISO 27001, PCI DSS).

# 5. Monitoring and Review

**5.1 Regular Reviews**

All information security processes are reviewed regularly to ensure that they are being carried out as planned. This includes:

* Monthly internal audits.
* Quarterly reviews of risk management and change management processes.
* Annual review of incident response procedures.

**5.2 Documentation and Evidence**

ABC-FinTech maintains the following documentation as evidence of effective process implementation:

* Change management logs.
* Security incident reports.
* Risk management records.
* Vendor audit reports.

# 6. Conclusion

This document defines the operational planning and control processes needed to meet ABC-FinTech’s information security requirements. By following these processes and retaining documented information, ABC-FinTech ensures that its ISMS is effective and compliant with ISO 27001:2022 standards.

**Approved by:**

**CEO, ABC-FinTech**  
**Date: 19 Jan 2024**