

Other ISMS-related Necessary Documents

# 1. Introduction

**1.1 Purpose**

This document identifies and describes additional ISMS-related documents that ABC-FinTech has determined are necessary for the effective management of its Information Security Management System (ISMS). These documents ensure that all critical aspects of information security, including industry-specific and organizational requirements, are adequately covered.

**1.2 Scope**

This document applies to all departments, functions, and processes within ABC-FinTech that are part of the ISMS. The additional documentation outlined herein complements the required ISO 27001 documentation and is deemed critical to the security, compliance, and effectiveness of ABC-FinTech's information security operations.

# 2. Additional ISMS-related Documents

**2.1 FinTech-Specific Compliance Documentation**

Due to the nature of ABC-FinTech’s business, several compliance requirements extend beyond ISO 27001. These documents are critical for ensuring the security of financial services and protection of customer data:

* **PCI DSS Compliance Documentation:** ABC-FinTech is required to comply with the Payment Card Industry Data Security Standard (PCI DSS) to secure payment transactions. This documentation includes PCI audit reports, network segmentation diagrams, and vulnerability scans.
* **GDPR Data Protection Documentation:** Given the organization’s exposure to European customers, GDPR compliance is mandatory. This includes data protection impact assessments (DPIAs), records of data processing activities, and privacy notices.

**2.2 Business Continuity and Disaster Recovery Plans**

Ensuring continuous operations and recovering from disasters quickly is essential for FinTech organizations. Additional documentation related to business continuity and disaster recovery includes:

* **Business Continuity Plan (BCP):** Documents how ABC-FinTech will maintain critical services during unforeseen events, such as cyberattacks or natural disasters.
* **Disaster Recovery Plan (DRP):** Details the steps necessary to recover information systems, databases, and infrastructure after a major incident. This is aligned with ISO 27001 Annex A.17 (Information Security Continuity).

**2.3 Cloud Security and Vendor Risk Management**

Given ABC-FinTech’s reliance on cloud infrastructure and third-party vendors, additional documentation is required to manage risks associated with external services:

* **Cloud Security Policy:** Defines specific security requirements and controls for cloud-hosted systems, including encryption, access controls, and monitoring. It is aligned with ISO 27001 Annex A.12 (Operations Security) and Annex A.15 (Supplier Relationships).
* **Vendor Risk Management Policy:** Ensures that all third-party vendors are compliant with ABC-FinTech’s security requirements, including regular security assessments and audits of key suppliers.

**2.4 Security Incident Response Procedures**

Effective incident management requires detailed documentation to guide responses to security breaches and other information security incidents:

* **Incident Response Plan (IRP):** Provides detailed procedures for detecting, reporting, responding to, and recovering from security incidents. It includes roles and responsibilities, escalation procedures, and communication plans.
* **Security Incident Logs and Records:** Documented records of all security incidents, including detailed logs, timelines, and actions taken. These documents are essential for incident reviews and audits, ensuring continual improvement of the ISMS.

**2.5 Data Encryption Standards**

Given the highly sensitive nature of financial transactions and customer data, additional documentation related to encryption practices is required:

* **Data Encryption Policy:** Specifies encryption standards, key management practices, and requirements for encrypting sensitive data at rest and in transit.
* **Cryptographic Key Management Documentation:** Provides detailed procedures for managing cryptographic keys, including creation, distribution, rotation, and deactivation. This is crucial for maintaining the confidentiality and integrity of encrypted data.

**2.6 Access Control and User Management**

Effective control over who has access to ABC-FinTech’s systems and data is crucial. In addition to the standard access control policies, the following documents are deemed necessary:

* **Role-Based Access Control (RBAC) Matrix:** Documents the access rights and permissions assigned to various roles within the organization, ensuring that only authorized personnel can access sensitive information.
* **Privileged Access Management (PAM) Policy:** Ensures that privileged accounts are managed securely, with stringent monitoring, auditing, and control measures in place.

**2.7 Cybersecurity Awareness and Training Programs**

To maintain a robust security posture, regular employee training and awareness programs are critical:

* **Security Awareness Program Documentation:** Outlines the structure and content of security awareness training provided to employees, including timelines, topics covered, and results from employee testing.
* **Employee Training Records:** Maintains a record of employees’ participation in mandatory security training, ensuring compliance with security policies and regulatory requirements.

# 3. Justification for Additional Documentation

ABC-FinTech has deemed the above documentation necessary for the following reasons:

* **Industry-Specific Requirements:** As a FinTech organization, ABC-FinTech must comply with financial industry-specific standards (e.g., PCI DSS) that require additional documentation.
* **Regulatory Compliance:** To ensure compliance with GDPR, PCI DSS, and other applicable regulations, additional documentation is required to demonstrate adherence to data protection and security standards.
* **Risk Management:** Documents such as the Vendor Risk Management Policy and Cloud Security Policy are necessary to manage risks associated with outsourcing and cloud services, which are integral to ABC-FinTech’s operations.
* **Incident Response and Business Continuity:** Detailed incident response and disaster recovery documentation is critical for minimizing the impact of security incidents and ensuring continuity of critical business functions.

# 4. Retention of Documented Information

ABC-FinTech ensures that all additional ISMS-related documents are retained and updated as necessary. The retention periods for these documents are as follows:

* **PCI DSS and GDPR Compliance Documentation:** Retained for a minimum of 6 years to align with regulatory requirements.
* **Business Continuity and Disaster Recovery Plans:** Reviewed and updated annually or after major incidents.
* **Security Incident Response Procedures:** Retained for at least 3 years to support audit and review processes.
* **Encryption Standards and Access Control Documents:** Updated as necessary to reflect changes in technology or policy and retained for the life of the ISMS.

# 5. Monitoring and Review

**5.1 Regular Reviews**

All additional ISMS-related documents are subject to annual review by the Information Security Steering Committee to ensure they remain relevant and effective. The review process ensures that any regulatory changes, technological advancements, or business needs are reflected in the documents.

**5.2 Continuous Improvement**

Feedback from internal audits, security incidents, and employee training will be used to continually improve the effectiveness of the ISMS, including the refinement of additional documentation as needed.

**Approved by:**

**CEO, ABC-FinTech**  
**Date: 18 Jan 2024**