

Evidence Of Nonconformities Identified And Corrective Actions Arising

# 1. Introduction

**1.1 Purpose**

This document provides evidence of nonconformities identified within ABC-FinTech’s Information Security Management System (ISMS) and the corrective actions taken to address these nonconformities. It outlines how the organization reacts to nonconformities, evaluates the causes, implements corrective actions, and reviews their effectiveness.

**1.2 Scope**

This document applies to all nonconformities related to the ISMS within ABC-FinTech. It covers nonconformities arising from internal audits, incidents, or other security-related activities, as well as the corrective actions taken to prevent recurrence.

# 2. Nonconformities and Corrective Actions Summary

**2.1 Nonconformity Identification Process**

When a nonconformity is identified, the following steps are followed:

1. Immediate actions are taken to **control and correct** the issue.
2. The causes of the nonconformity are reviewed, and appropriate corrective actions are planned to prevent recurrence.
3. If necessary, changes to the ISMS are implemented.
4. The effectiveness of the corrective action is reviewed and documented.

# 3. Nonconformities and Corrective Actions

**3.1 Nonconformity 1: Incident Reporting Delay**

|  |  |
| --- | --- |
| Nonconformity Details | Description |
| ID | NC-001 |
| Date Identified | December 10, 2023 |
| Source | Q4 2023 ISMS Internal Audit |
| Nonconformity | Security incident was reported 2 days late, outside the SLA timeframe. |
| Affected Area | Incident Response (A.16), IT Security Team |

**Corrective Actions for NC-001**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Action | Description | Responsible Party | Target Date | Status |
| Immediate Control and Correction | Incident was escalated and contained upon identification. Communication bottleneck addressed. | IT Security Manager | December 12, 2023 | Completed |
| Cause Evaluation | Root cause identified: delay in internal reporting process due to communication gap between SOC and IT. | Lead Auditor, SOC Manager | December 15, 2023 | Completed |
| Corrective Action | Incident reporting procedure updated, and communication channel established for urgent incidents. | IT Security Manager | January 15, 2024 | In Progress |
| Effectiveness Review | Review incident response times and conduct simulation drills to test new procedures. | IT Security Manager | March 2024 | Planned |

**Effectiveness Review**

* **Planned Review Date**: March 2024
* **Expected Outcome**: Incident reporting delays should be eliminated, with all incidents reported within the SLA timeframe.

**3.2 Nonconformity 2: Vendor Compliance Delays**

|  |  |
| --- | --- |
| Nonconformity Details | Description |
| ID | NC-002 |
| Date Identified | October 25, 2023 |
| Source | Vendor Management Review (Q4 2023) |
| Nonconformity | 10% of third-party vendors failed to submit their annual security compliance reports on time. |
| Affected Area | Vendor Management (A.15) |

**Corrective Actions for NC-002**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Action | Description | Responsible Party | Target Date | Status |
| Immediate Control and Correction | Vendors were contacted to submit overdue compliance reports. | Vendor Management Lead | November 5, 2023 | Completed |
| Cause Evaluation | Root cause: lack of follow-up reminders and tracking mechanisms for vendor compliance deadlines. | Lead Auditor, Vendor Lead | November 10, 2023 | Completed |
| Corrective Action | Develop a vendor compliance tracking system and implement automated reminders for vendors. | Vendor Management Lead | February 1, 2024 | In Progress |
| Effectiveness Review | Review vendor compliance rates after implementation of the tracking system. | Vendor Management Lead | April 2024 | Planned |

**Effectiveness Review**

* **Planned Review Date**: April 2024
* **Expected Outcome**: 100% vendor compliance with no delayed reports by Q2 2024.

**3.3 Nonconformity 3: Access Control Review Frequency**

|  |  |
| --- | --- |
| Nonconformity Details | Description |
| ID | NC-003 |
| Date Identified | July 15, 2023 |
| Source | Q3 2023 ISMS Internal Audit |
| Nonconformity | Access control reviews were performed bi-annually instead of the required quarterly schedule. |
| Affected Area | Access Control (A.9), IT Security Team |

**Corrective Actions for NC-003**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Action | Description | Responsible Party | Target Date | Status |
| Immediate Control and Correction | Conducted an unscheduled access control review and no violations were identified. | IT Security Manager | July 20, 2023 | Completed |
| Cause Evaluation | Cause: misunderstanding of the required frequency for access reviews. | Lead Auditor | August 1, 2023 | Completed |
| Corrective Action | IT security policy updated to clearly define quarterly review frequency. | IT Security Manager | September 1, 2023 | Completed |
| Effectiveness Review | Review audit logs in Q4 2023 to verify that quarterly reviews are being performed as scheduled. | Lead Auditor | December 2023 | Completed |

**Effectiveness Review**

* **Review Outcome**: All quarterly reviews for Q4 2023 were performed on time. No further nonconformities related to access control reviews were found.

# 4. Summary of Corrective Action Effectiveness

|  |  |  |  |
| --- | --- | --- | --- |
| Nonconformity | Corrective Action Status | Effectiveness Review Date | Expected Outcome |
| NC-001: Incident Reporting Delay | In Progress | March 2024 | Eliminate delays in incident reporting. |
| NC-002: Vendor Compliance Delays | In Progress | April 2024 | 100% vendor compliance with timely reporting. |
| NC-003: Access Control Review Frequency | Completed | December 2023 | Quarterly reviews conducted on schedule. |

# 5. Documentation and Retention

ABC-FinTech retains documented evidence of nonconformities and corrective actions, including:

* **Nonconformity Logs**: Maintained for 5 years.
* **Corrective Action Plans**: Retained for 3 years after the action is completed.
* **Effectiveness Reviews**: Retained for 3 years post-review.

# 6. Conclusion

ABC-FinTech’s ISMS corrective action process ensures that nonconformities are promptly addressed, and appropriate corrective actions are implemented to prevent recurrence. The organization continuously monitors the effectiveness of these actions to maintain compliance with ISO 27001:2022.

**Approved by:**

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