Nonconformity and Corrective Actions Procedure (2025-26)

Version 1.0

Document Information:

Document Name	Nonconformity and Corrective Actions
Document Owner	H.O. BCM Team
Document Version number	1.0
Document Version Date	
Prepared By	H.O. BCM Team
Reviewed By	Head-O&FRMD
Approved By	IT Strategy Committee (ITSC)

Change Log/Revision History:

Sr. No.	Version No.	Approval Date	Description of Change	Reviewed By	Approved By

Table of Contents

1. Introduction

<<Client Name>> will continuously strive to improve the effectiveness of the Business Continuity Management System (BCMS). For this improvement, <<Client Name>> will utilize the defined ORM & OR policy, Business Continuity objectives, audit results, analysis of monitored events, corrections and corrective actions and their timescales, and management review.

To summarize, following scenarios would result into corrections and corrective actions:

- Non-conformities/ observations received after third party audits.
- Post information security incident reports.
- Post BCMS exercises reports.
- Results from performance evaluation and measurement of effectiveness of controls.
- Non-conformities/ observations received from Internal Audit.
- Action points from Management Reviews.

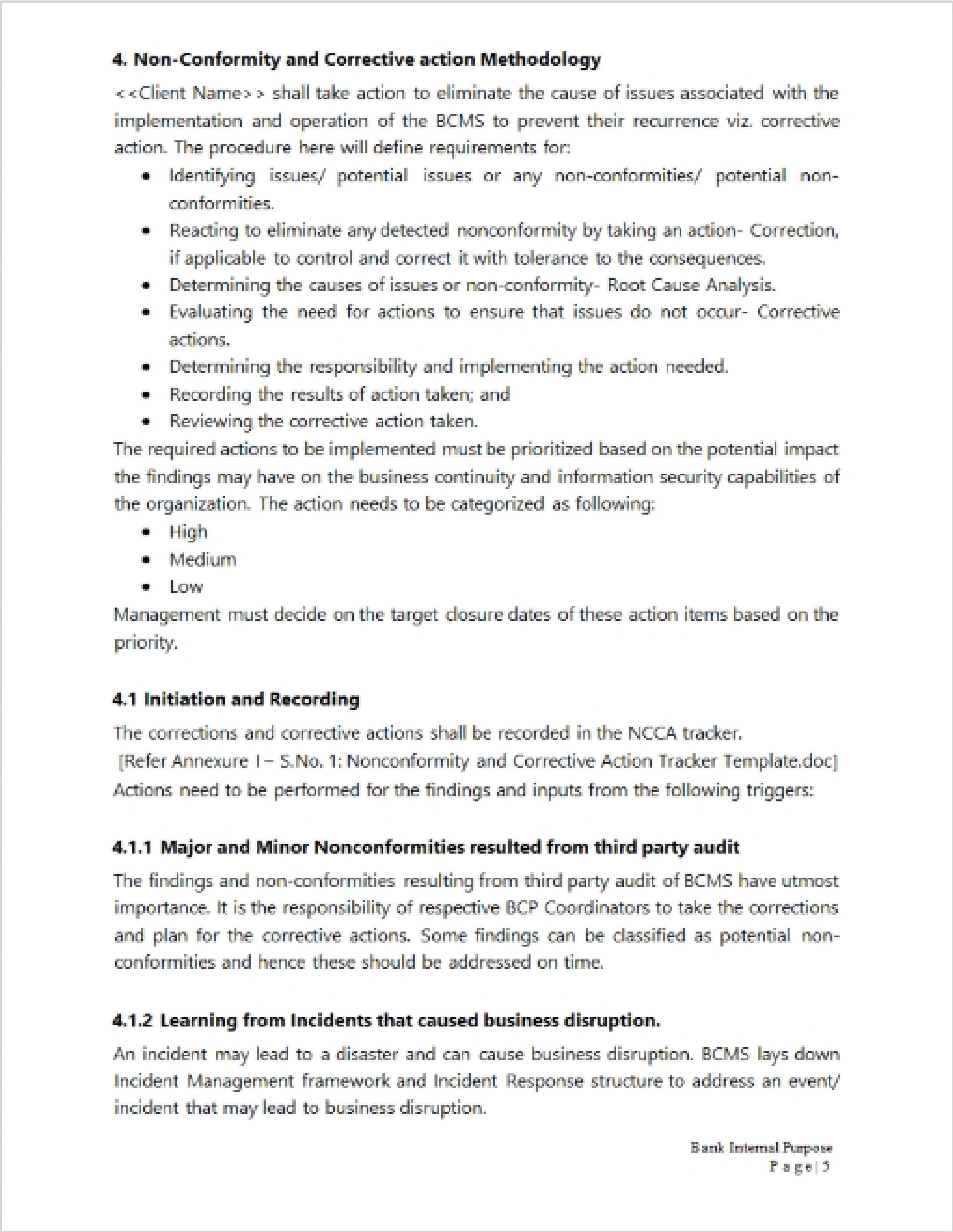
2. Scope

This procedure applies to all business units, departments, support functions, and critical third-party service providers that are part of the Bank's in-scope Business Continuity Management System (BCMS). It covers:

- Business processes identified as critical in the BIA.
- Recovery strategies for personnel, facilities, technology, information, and third-party dependencies.
- Selection and documentation of recovery solutions for inclusion in Business Continuity Plans (BCPs).
- Integration of recovery strategies into crisis management and disaster recovery planning.

3. Objective

The objective of this procedure is to improve effectiveness of business continuity planning within <<Client Name>> and to achieve continual improvement in the existing BCMS. This procedure defines the methodology to undertake corrective actions. Any corrective action taken shall be appropriate to the magnitude of the problems and commensurate with the ORM & OR policy and objectives.



4. Non-Conformity and Corrective action Methodology

<<Client Name>> shall take action to eliminate the cause of issues associated with the implementation and operation of the BCMS to prevent their recurrence viz. corrective action. The procedure here will define requirements for:

- Identifying issues/ potential issues or any non-conformities/ potential non-conformities.
- Reacting to eliminate any detected nonconformity by taking an action- Correction, if applicable to control and correct it with tolerance to the consequences.
- Determining the causes of issues or non-conformity- Root Cause Analysis.
- Evaluating the need for actions to ensure that issues do not occur- Corrective actions.
- Determining the responsibility and implementing the action needed.
- Recording the results of action taken; and
- Reviewing the corrective action taken.

The required actions to be implemented must be prioritized based on the potential impact the findings may have on the business continuity and information security capabilities of the organization. The action needs to be categorized as following:

- High
- Medium
- Low

Management must decide on the target closure dates of these action items based on the priority.

4.1 Initiation and Recording

The corrections and corrective actions shall be recorded in the NCCA tracker.
[Refer Annexure I – S.No. 1: Nonconformity and Corrective Action Tracker Template.doc]
Actions need to be performed for the findings and inputs from the following triggers:

4.1.1 Major and Minor Nonconformities resulted from third party audit

The findings and non-conformities resulting from third party audit of BCMS have utmost importance. It is the responsibility of respective BCP Coordinators to take the corrections and plan for the corrective actions. Some findings can be classified as potential non-conformities and hence these should be addressed on time.

4.1.2 Learning from Incidents that caused business disruption.

An incident may lead to a disaster and can cause business disruption. BCMS lays down Incident Management framework and Incident Response structure to address an event/ incident that may lead to business disruption.

An incident may lead to unavailability of following basic blocks/ components, which supports continuity of business:

- People
- Technology
- Site
- Vendor/Suppliers

And unavailability of the above may result in business disruption.

The functional plans encompassing Incident Response and Business Continuity framework define the steps to follow in the event of an incident. Post incident, a thorough analysis of the incident management is done for assessing, what may have gone wrong (Root Cause Analysis) and required corrective actions and corrections that need to be taken or implemented. The required actions shall be recorded and monitored by the respective owner of the incident and shall become an input to the procedure.

4.1.3 Findings from BCMS Testing and Exercises

The BCM arrangements need to be tested and exercised at the defined intervals. One of the triggers to non-conformity and corrective action tracker is the findings obtained from the results of the exercises conducted and analyzed by the BCM team for following types of BCM exercises:

- BCP walkthrough testing.
- BCP Process Recovery Testing.
- All employee Call Tree Testing; and
- Site Recovery Testing.

4.1.4 Training and Awareness Effectiveness Results

Role based trainings and awareness programs are developed and implemented. The training and awareness programs are monitored by L& D, H.R. Team. The training progress is apprised by the H.O. BCM team to ORMC on a periodic basis.

One of the triggers to non-conformity and corrective action tracker is the findings obtained on the effectiveness of BCMS training programs.

4.1.5 Results and Findings from Performance Evaluation

A Performance Evaluation and measurement of effectiveness of controls is conducted to assess the effectiveness of the BCMS arrangements at the organization respectively. This helps in determining whether performance metrics defined are met or not. This review helps in identifying the required action items to be taken, to ensure that necessary changes/ gaps are incorporated to the BCMS arrangements as part of continual improvement of the organization. These action items become the input for correction and corrective actions required to be taken.

4.1.6 Non-conformities received after Internal Audits

Internal audits are carried out to identify the non-conformities in the BCMS in reference to the requirement of the BCMS standard (ISO 22301:2019). Internal audits are planned and scheduled by Internal Audit Team as per internal audit program calendar. The findings and non-conformities recorded as result of Internal Audits will be required to take certain corrections to address the observation and corrective actions to ensure these observations do not get repeated in future. The respective corrections and corrective actions shall be tracked and monitored till closure.

4.1.7 Action items from Management Review of BCMS

Top management for <<Client Name>> shall review the organization's BCMS Procedure at least once a year or whenever significant changes occur across Bank to ensure its continuing suitability, adequacy and effectiveness of the BCMS.

This management review shall include assessing opportunities for improvement and the need for changes to the BCMS, including the Business Continuity Management Policy and Objectives and Information security Management Policy and Objectives.

The results of the reviews shall be clearly documented and become the input for non-conformity and corrective action process.

4.1.8 Near Misses

All the security related issues which are identified before these can turn into incidents shall be categorized as "near misses". These near misses shall also be covered as inputs to NCCA tracker.

4.2 Execution

- The H.O. BCM team shall review the non-conformity/ actions identified as result of triggers.
- The BCP Coordinator shall investigate and determine the root causes(s) of the non-conformance, incidents, weakness, and modifications needed for BCMS policy and business continuity, Information security documents and document these as part of the NCCA action log.
- [Refer Annexure I – S. No. 1: Nonconformity and Corrective Action Form Template]
- The BCP Coordinator shall evolve a plan for their independent function to eliminate the root cause(s) of the non-conformance, incident taking into consideration the

magnitude of the problem and the risk involved and document the plan mentioning the target completion date.

- The BCP Coordinator shall implement the correction/ corrective action needed for his/ her independent function. The accountability for implementation of plan for correction/ corrective actions for all functions would lie with HO BCM team
- HO BCM team shall also take into consideration the results of the risk assessment and the business impact analysis. e.g., the risk assessment results into identification of threat leads to identification of corrective actions to be taken to ensure that the measures have been taken to prevent the damage that could occur due to the occurrence of the threats.
- The BCP Coordinator shall maintain records of correction/ corrective action with the root cause analysis.
- HO BCM team at <<Client Name>> shall review the corrective action once in a quarter for <<Client Name>>; and
- HO BCM team shall also identify any changes to the risk assessment and plan for correction/ corrective actions.

4.3 Review by Management

Status of corrections and corrective actions would be reviewed by the HO BCM team during their respective management reviews.

5. Roles and Responsibility

Sr. No.	Activity	Owner
1	Review of non-conformity, actions, observations derived for their own function out of third-party audits, incidents, after testing/ exercises, post internal audits and management reviews	BCP Coordinator with onward submission to Dept Head
2	Preparation and implementation of corrections and corrective actions plan for their independent function. Any correction or corrective action taken shall be appropriate to the magnitude of the problems and commensurate with the information security and business continuity policy and objectives	BCP Coordinator with onward submission to Dept Head
3	Collation of corrections and corrective actions plan for Bank	H.O. BCM team
4	Maintain records of corrections and corrective action with the root cause analysis at Bank	H.O. BCM team
5	Review the corrections/ corrective actions (during internal audits, self-assessments, and management reviews)	H.O. BCM team
6	Accountability for complete implementation of corrections and corrective actions as per plan for Bank	Department Head and functional head of respective function with reporting to Chief Risk Officer through Heda-O&FRM/H.O. BCM Team
7	Review the results of enterprise-wide corrections and corrective actions during the meetings of BCMS	ORMC

6. Continual Improvement

The Non-Conformity and Corrective action procedure helps an organization to identify areas and scope for improvement of the overall BCMS.

It is important for the stability and growth of an organization to showcase continual improvement by developing plans to identify the prospective improvements to the BCMS on periodic basis and action items to implement necessary BCM arrangements Controls in the organization.

The Corrective Action shall enable the management to identify areas of improvement and mechanism to monitor the implementation of the required action items.

Regular and effective review of the following key elements facilitate in ensuring continual improvement to the BCMS:

- Information Security and Business continuity policy and objectives.

- Audit results.
- Analysis of monitored events.
- Corrective actions; and
- Management reviews.

Management shall periodically review the BCMS arrangements take necessary decisions to showcase the continual improvement in the management system.

7. Annexure

- NCCA Tracker

NCCA Tracker.xlsx