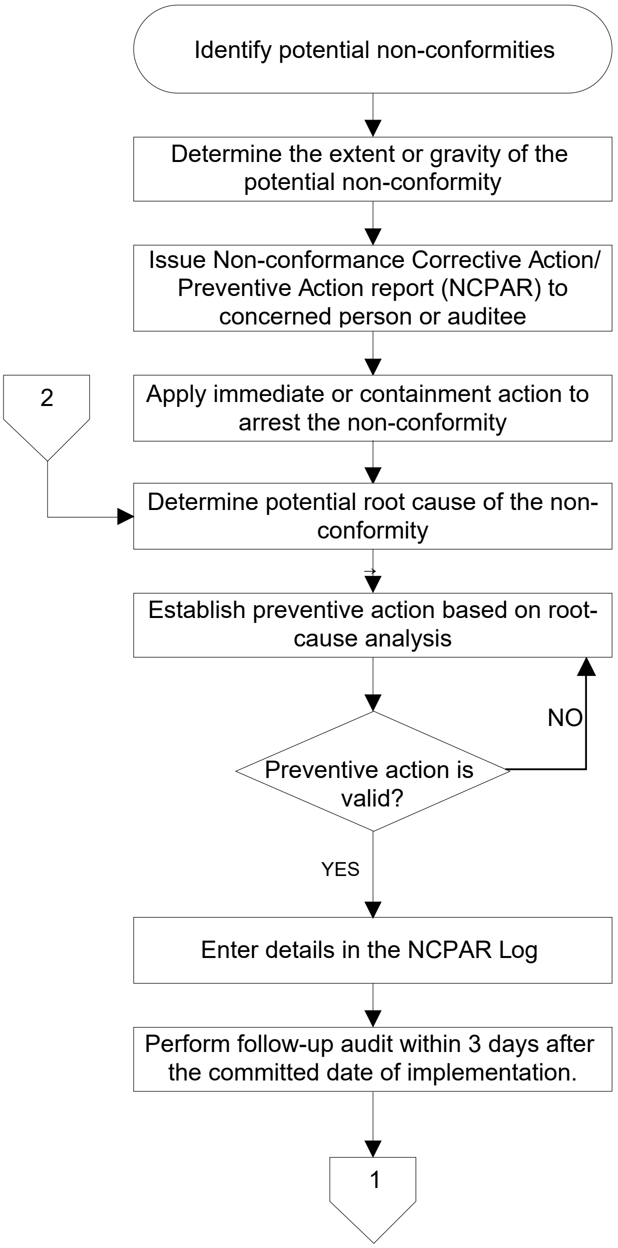
ISO 27K TOOLKIT	Document Title PREVENTIVE ACTION PROCEDURE		Document Ref No ISO27K-PAP	
	Original Author: RAHUL CHUGH	Approved by	Revision Stat 0	Page/Total 1/2

Purpose	The purpose of this procedure is to have a defined method in applying preventive actions to eliminate the cause of potential non-conformities on the established information security management system (ISMS).
Scope	This procedure covers the collection of data on potential non-conformities, analysis of the potential root causes of nonconformities and action planning to prevent occurrence of non-conformities.

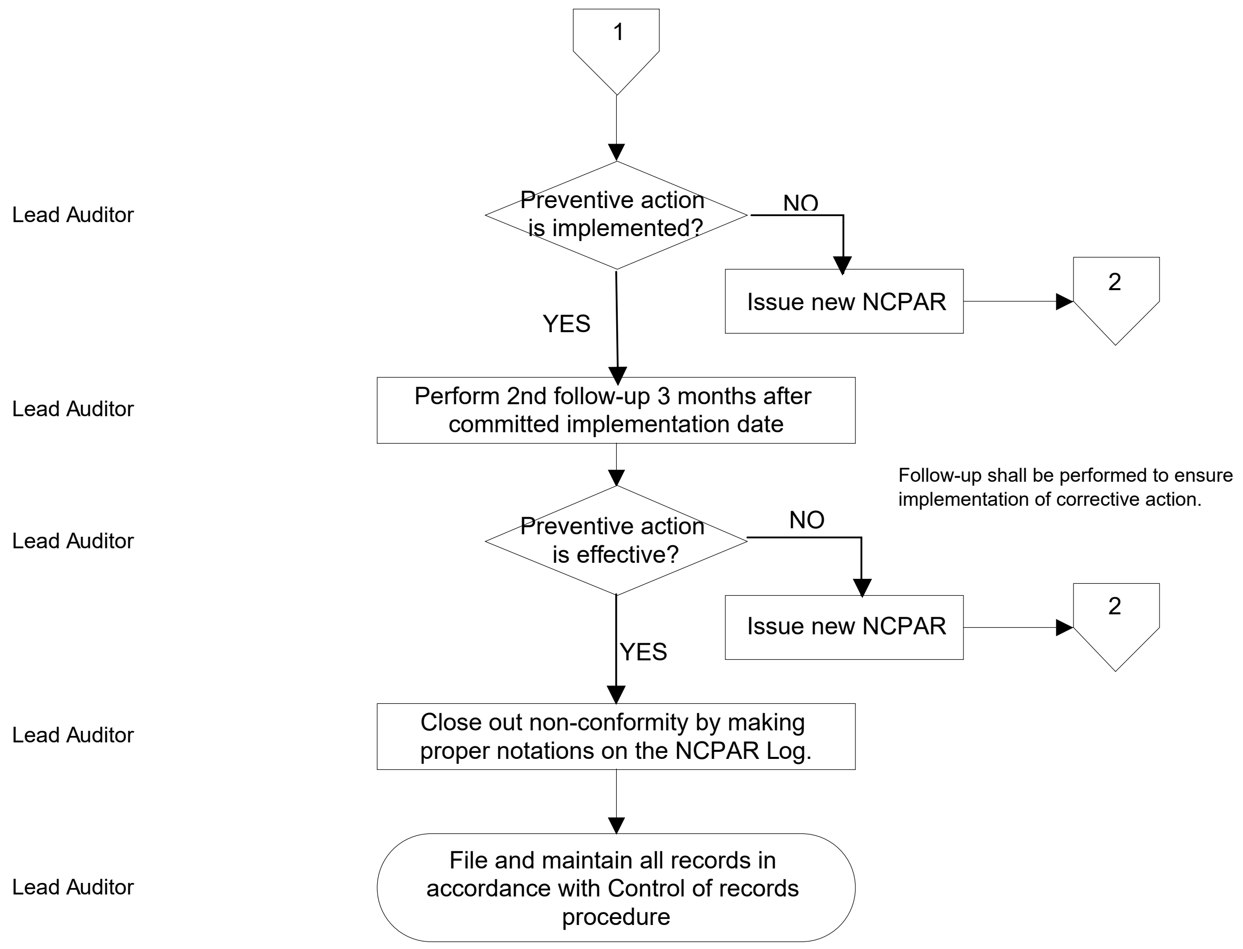


RESPONSIBILITY	PROCESS FLOW	DETAILS
Auditor Observer	Identify potential non-conformities	Potential non-conformities maybe in the form of findings during internal audits (improvement potentials), suspected information security weaknesses and suggestions by [company] staff.
Auditor Observer	Determine the extent or gravity of the potential non-conformity	
Auditor Observer	Issue Non-conformance Corrective Action/ Preventive Action report (NCPAR) to concerned person or auditee	Refer to instructions on page 2 of NCPAR for proper usage
Auditee Auditee's management	Apply immediate or containment action to arrest the non-conformity	
	2 → Determine potential root cause of the non-conformity	Root cause analysis tools such as the why-why analysis and Ishikawa diagram shall be used to identifv potential root
Auditee Auditee's management	Establish preventive action based on root-cause analysis	Preventive actions shall be applied in a holistic manner with efforts done to ensure applicability on other areas or processes.
Lead Auditor Auditor	Preventive action is valid? (NO → Establish preventive action; YES → next)	For preventive action to be valid, it shall ensure "non-occurrence" of the non-conformitv.
Lead Auditor	Enter details in the NCPAR Log	Lead Auditor shall monitor NCPAR Log on a weekly basis to verify "open" potential non-conformities and ensure timeliness of follow-up audits.
Lead Auditor	Perform follow-up audit within 3 days after the committed date of implementation.	Follow-up shall be performed to ensure implementation of preventive action.
	1	

REVISION HISTORY

No	Revision Details	Effectivity Date
0	Initial issue	2020 03 26
1		
2		

RESPONSIBILITY	PROCESS FLOW	DETAILS


1
Lead Auditor
Preventive action is implemented?
NO
Issue new NCPAR
2
YES
Lead Auditor
Perform 2nd follow-up 3 months after committed implementation date
Lead Auditor
Preventive action is effective?
NO
Issue new NCPAR
2
YES
Lead Auditor
Close out non-conformity by making proper notations on the NCPAR Log.
Lead Auditor
File and maintain all records in accordance with Control of records procedure

Follow-up shall be performed to ensure implementation of corrective action.

Instances where potential non-conformities may be identified

SITUATIONS	DESCRIPTION
As a result of internal audits	Observed improvement potentials are possible sources of preventive actions.
Identification of information security weaknesses	Weaknesses shall be issued appropriate preventive actions lest they become full-blown information security incidents.
Near-misses	Environmental and health and safety near-misses shall be issue corresponding preventive actions before they become accidents.