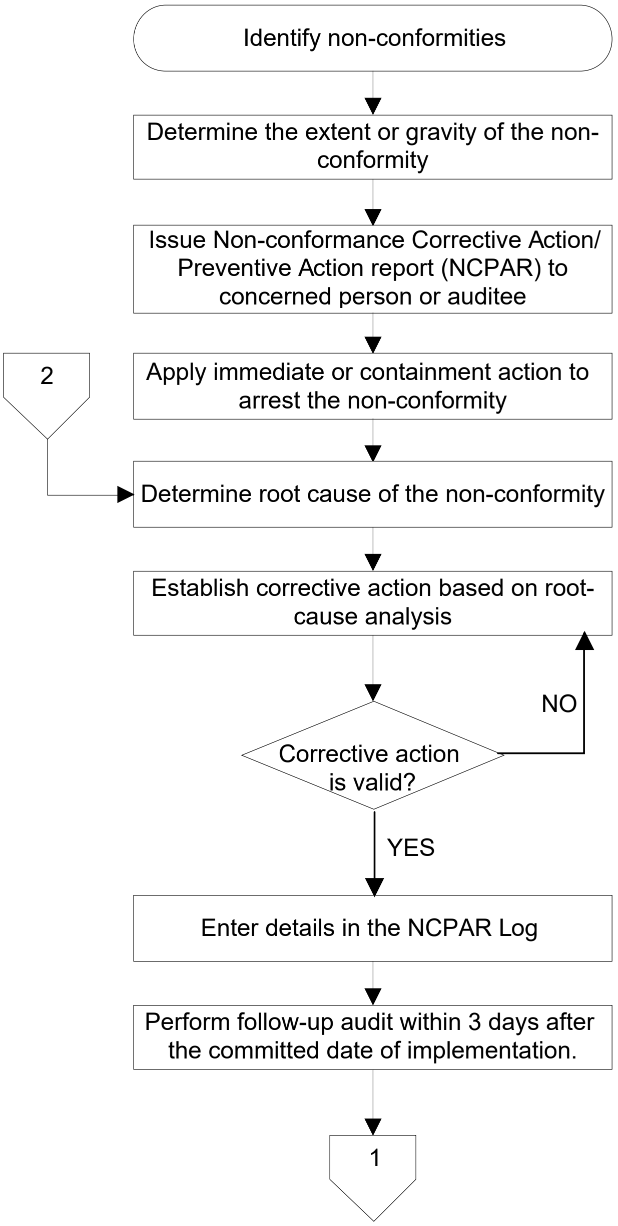
ISO 27K TOOLKIT	Document Title CORRECTIVE ACTION PROCEDURE		Document Ref No ISO27K-CAP	
	Original Author: Rahul Chugh	Approved by	Revision Stat 0	Page/Total 1/2

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



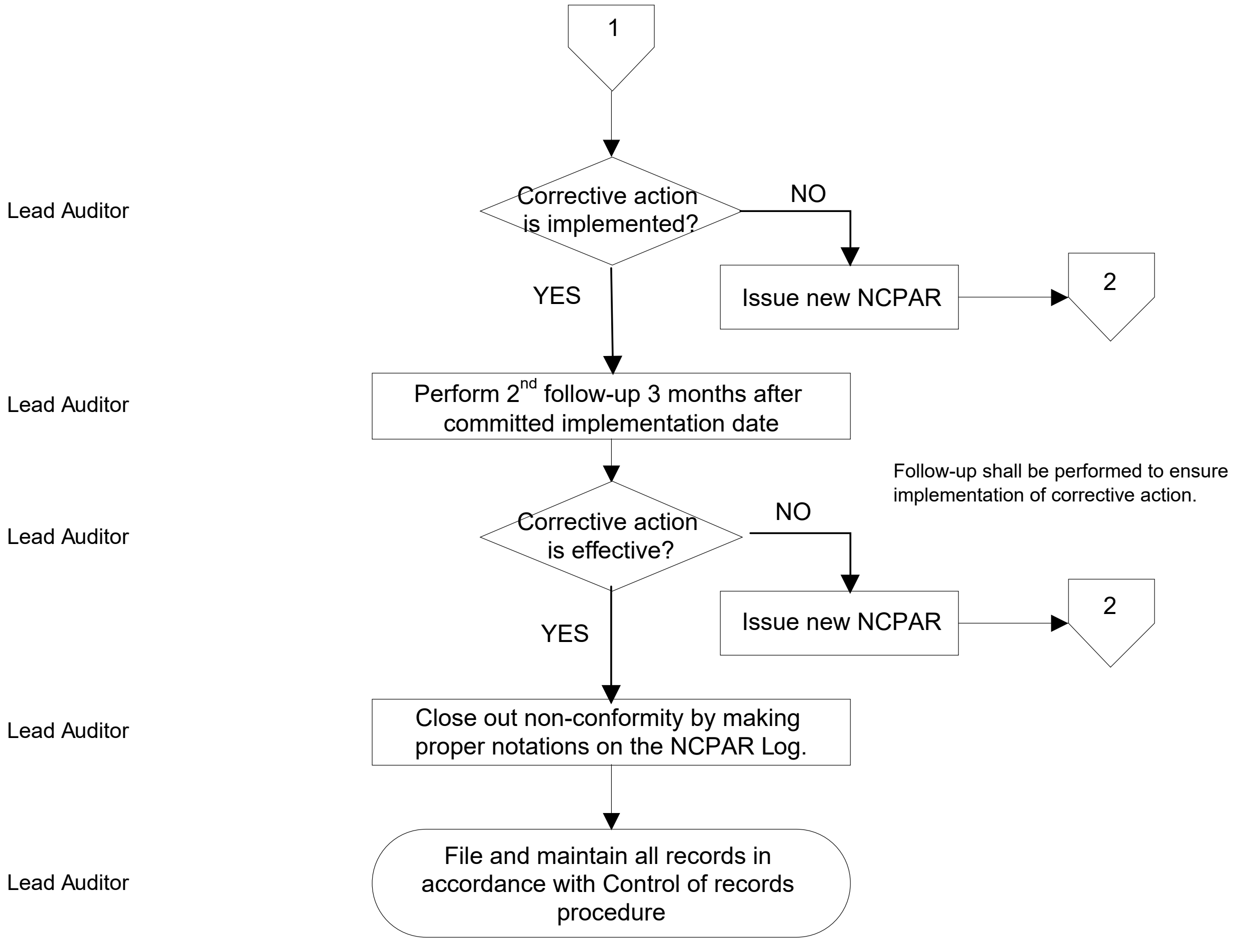
RESPONSIBILITY	PROCESS FLOW	DETAILS
Auditor Observer	Identify non-conformities	Non-conformities may be identified in any several ways. Refer to non-conformities identification guide on page 2.
Auditor Observer	Determine the extent or gravity of the non-conformity	There are cases wherein the observed or detected non-conformity is just the "surface" of a much bigger or serious 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	
	Determine root cause of the non-conformity	Root cause analysis tools such as the why-why analysis and Ishikawa diagram shall be used to identify root causes of the
Auditee Auditee's management	Establish corrective action based on root-cause analysis	Corrective actions shall be applied in a holistic manner with efforts done to ensure applicability on other areas or processes.
Lead Auditor Auditor	Corrective action is valid?	For corrective action to be valid, it shall ensure "non-recurrence" of the non-conformity.
Lead Auditor	Enter details in the NCPAR Log	Lead Auditor shall monitor NCPAR Log on a weekly basis to verify "open" 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 corrective action.

REVISION HISTORY

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

Document Title CORRECTIVE ACTION PROCEDURE	Document Ref No ISO27K-CAP	Revision Stat 0	Page/Total 2/2

RESPONSIBILITY	PROCESS FLOW	DETAILS


1
Lead Auditor
Corrective action is implemented?
NO
Issue new NCPAR
2
YES
Lead Auditor
Perform 2nd follow-up 3 months after committed implementation date
Follow-up shall be performed to ensure implementation of corrective action.
Lead Auditor
Corrective 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

Instances where non-conformities may be found

SITUATIONS	DESCRIPTION
As a result of internal ISMS audits	All observed non-conformities and observations shall merit corrective actions from the auditee and auditee's management.
Process non-conformity	Non-conformities related to process deviations. Examples would be: non-updating of virus definitions, non-monitoring of required logs, non-implementation of a security procedure. Process non-conformities may be raised outside the inernal audit activities by any staff who has observed the event.
Product non-conformity	A deviation or error on the output of a process thereby compromising integrity. Examples would be errors in coding that were uncovered by the customer, non-attainment of service level agreements. Product non-conformities may be raised outside the internal audit activities by any staff who has witnessed the non-conformity.
Customer complaints	Valid complaints coming from customers.
Information security incidents	Corrective action shall be established on all valid information security breaches after the remediation steps have been accomplished (Refer to IS Investigation form)