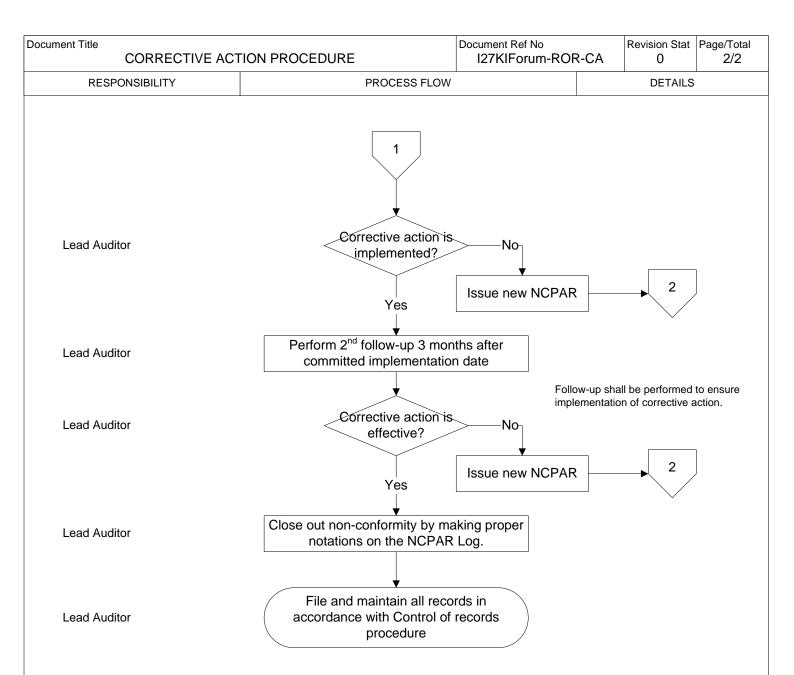
Document Title Document Ref No 150 CORRECTIVE ACTION PROCEDURE 127KIForum-ROR-CA Prepared and reviewed by **Revision Stat** Page/Total Approved by 27001 Richard O. Regalado 0 1/2 security The purpose of this procedure is to have a defined method in applying corrective actions to eliminate the cause of non-conformities Purpose on the established information security management system (ISMS). This procedure covers the collection of data on non-conformities, analysis of the root cause of nonconformities and action planning Scope to prevent recurrence of problems. RESPONSIBILITY PROCESS FLOW **DETAILS** Non-conformities may be identified in any Auditor Identify non-conformities several ways. Refer to non-conformities Observer identification guide on page 2. There are cases wherein the observed or Determine the extent or gravity of the nondetected non-conformity is just the Auditor conformity "surface" of a much bigger or serious non-Observer conformity. Issue Non-conformance Corrective Action/ Refer to instructions on page 2 of NCPAR Preventive Action report (NCPAR) to for proper usage Auditor concerned person or auditee Observer Apply immediate or containment action to 2 arrest the non-conformity Auditee Auditee's management Root cause analysis tools such as the Determine root cause of the non-conformity why-why analysis and Ishikawa diagram shall be used to identify root causes of Auditee the non-conformity. Auditee's management Corrective actions shall be applied in a Establish corrective action based on rootholistic manner with efforts done to cause analysis ensure applicability on other areas or processes. No For corrective action to be valid, it Corrective action is Lead Auditor shall ensure "non-recurrence" of the Auditor valid? non-conformity. Yes Lead Auditor shall monitor NCPAR Log Lead Auditor Enter details in the NCPAR Log on a weekly basis to verify "open" nonconformities and ensure timeliness of follow-up audits. Follow-up shall be performed to ensure Perform follow-up audit within 3 days after Lead Auditor implementation of corrective action. the committed date of implementation. REVISION HISTORY **Revision Details** No Effectivity Date 2007 09 20 0 Initial issue 1 2

This work is copyright © 2007, **Richard O. Regalado and ISO27k implementers' forum**, some rights reserved. It is licensed under the Creative Commons Attribution-Noncommercial-Share Alike 3.0 License. You are welcome to reproduce, circulate, use and create derivative works from this provided that (a) it is not sold or incorporated into a commercial product, (b) it is properly attributed to the ISO27k implementers' forum www.ISO27001security.com), and (c) derivative works are shared under the same terms as this.).



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)