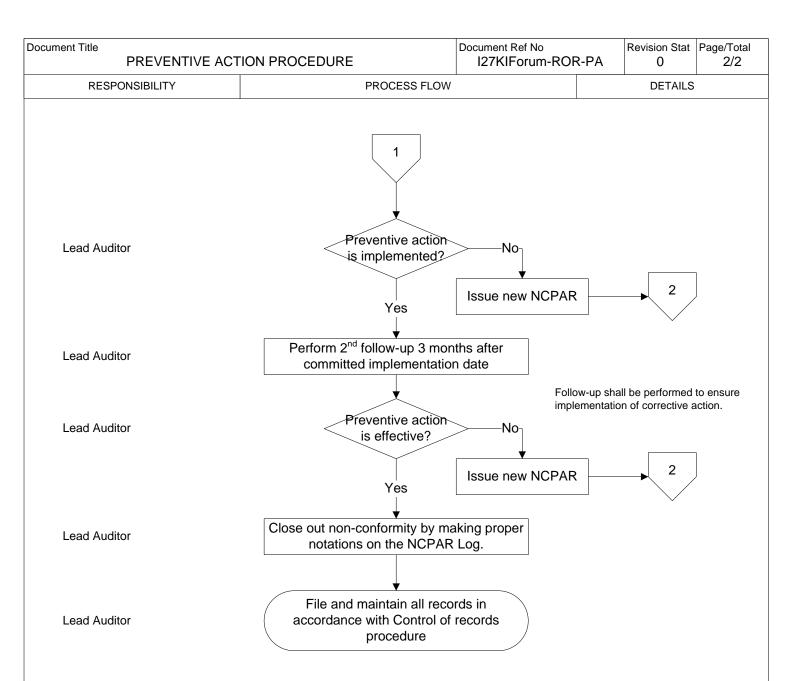
Document Title Document Ref No 150 PREVENTIVE ACTION PROCEDURE 127KIForum-ROR-PA Original Author: Approved by **Revision Stat** Page/Total 27001 Richard O. Regalado 0 1/2 security The purpose of this procedure is to have a defined method in applying preventive actions to eliminate the Purpose cause of potential non-conformities on the established information security management system (ISMS). This procedure covers the collection of data on potential non-conformities, analysis of the potential root Scope causes of nonconformities and action planning to prevent occurrence of non-conformities. RESPONSIBILITY PROCESS FLOW **DETAILS** Potential non-conformities maybe in the form of findings during internal audits Auditor Identify potential non-conformities (improvement potentials), suspected Observer information security weaknesses and suggestions by [company] staff. Determine the extent or gravity of the Auditor potential non-conformity Observer 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 potential root cause of the nonwhy-why analysis and Ishikawa diagram conformity shall be used to identify potential root causes of the non-conformity. Auditee Auditee's management Preventive actions shall be applied in a Establish preventive action based on rootholistic manner with efforts done to cause analysis ensure applicability on other areas or processes. No For preventive action to be valid, it Preventive action Lead Auditor shall ensure "non-occurrence" of the Auditor is 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" potential non-conformities 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 preventive action. the committed date of implementation. REVISION HISTORY **Revision Details** No Effectivity Date 2009 06 03 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 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.