**Comment [DK1]:** To learn how to fill in this document see:

**Video Tutorial** "How to Write ISO 27001 Procedure for Corrective and Preventive Action"
http://www.iso27001standard.com/video-tutorials

[organization logo]

**Comment [DK2]:** All fields in this document marked by square brackets [ ] must be filled in.

[organization name]

# PROCEDURE FOR CORRECTIVE ACTION

| | |
|---|---|
| Code: | |
| Version: | |
| Date of version: | |
| Created by: | |
| Approved by: | |
| Confidentiality level: | |

**Comment [DK3]:** The document coding system should be in line with the organization's existing system for document coding; in case such a system is not in place, this line may be deleted.

## Change history

| Date | Version | Created by | Description of change |
|---|---|---|---|
| 01/10/2013 | 0.1 | Dejan Kosutic | Basic document outline |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

## Table of contents

## 1. Purpose, scope and users

The purpose of this procedure is to describe all activities related to the initiation, implementation and keeping of records of corrections, as well as corrective actions.

This procedure is applied to all activities implemented in the Information Security Management System (ISMS) [Business Continuity Management System (BCMS)].

Users of this document are all employees of [organization name].

**Comment [DK4]:** This is to be inserted instead of the ISMS in case the procedure refers exclusively to business continuity management.

## 2. Reference documents

- ISO/IEC 27001 standard, clause 10.1
- ISO 22301 standard, clause 10.1
- BS 25999-2 standard, clause 6.1
- Information Security Policy
- Business Continuity Policy
- Internal audit procedure
- Incident management procedure

**Comment [DK5]:** Delete if the procedure refers only to business continuity management

**Comment [DK6]:** Delete if you are not implementing business continuity

**Comment [DK7]:** Delete if the procedure refers only to business continuity management

**Comment [DK8]:** Delete if you are not implementing business continuity

**Comment [DK9]:** If the documentation is written only for business continuity, replace with Incident Response Plan

## 3. Corrections and corrective actions

### 3.1. Nonconformities and corrections

A nonconformity is any failure to meet the requirements of the standards, [illegible] the ISMS. Nonconformities can be identified during an internal or [illegible] during normal business operations or on any other occasion.

**Comment [DK10]:** Or BCMS

An employee who notices a nonconformity must take immediate action to control it, contain it and [illegible] who must make a correction.

### 3.2. Corrective actions

Said responsible person must evaluate the need to eliminate the cause of nonconformity and [illegible]. The main difference is that corrective actions [illegible] whereas the correction focuses only on [illegible].

Corrective action may be initiated by any employee or (where appropriate) client, supplier or [illegible] document, process or arrangement within the ISMS.

**Comment [DK11]:** or BCMS

### 3.3. Implementation of corrective actions

Corrective action is implemented in the following way:

| *Step* | *Person responsible for implementation* |
|---|---|
| 1. Reviewing the nonconformity | Anyone with a role in the ISMS |
| 2. Determining the cause of nonconformity | Person responsible for the area where the nonconformity has been identified |
| 3. Identify if similar nonconformity already exists | Person responsible for the area where the nonconformity has been identified |
| 4. Evaluating the need for action to eliminate the nonconformity | Person responsible for the area where the nonconformity has been identified |
| 5. Determining the actions needed to eliminate the causes of nonconformity and to ensure that nonconformities do not recur | Person responsible for the area where the nonconformity has been identified |
| 6. Implementation of planned actions | Person in charge of implementation, appointed by the person responsible |
| 7. Reviewing whether the action taken resulted in the elimination of causes of nonconformity | [job title] |
| 8. Informing all persons concerned that corrective action has been implemented | Person in charge of implementation, appointed by the person responsible |
| 9. Making changes to the ISMS, if necessary | Person who is in charge of coordinating the ISMS |

Each of the above steps must be recorded in the corrective action form.

**Comment [DK12]:** or BCMS

**Comment [DK13]:** One person may be appointed for all corrective actions (for example Security Officer/Manager) or the person responsible may be authorized to appoint such a person each time new corrective action is initiated.

Implementation of actions against nonconformities identified during internal audit is usually reviewed by the internal auditor.

**Comment [DK14]:** or BCMS

**Comment [DK15]:** E.g. Security Officer or Business Continuity Coordinator

**Comment [DK16]:** or BCMS

**Comment [DK17]:** You can also use e.g. Help Desk application or any other system which uses tickets/cases to resolve certain problems.

## 4. Managing records kept on the basis of this document

| Record name | Storage location | Person responsible for storage | Control for record protection | Retention time |
|---|---|---|---|---|
| Corrective action form | [name of filing folder, in which cabinet] [intranet folder | [job title] | After all data has been recorded, any new additions or editing must be disabled | 3 years |

**Comment [DK18]:** If records are kept in paper form

| | | | | |
|---|---|---|---|---|
| | name] | | | |

Comment [DK19]: If records are kept in electronic form

Comment [DK20]: If you use an application, then specify the application name

## 5. Validity and document management

This document is valid as of [date].

The owner of this document is [job title], who must [illegible] at least once a year.

Comment [DK21]: This is only a recommendation; adjust frequency as appropriate

When evaluating the effectiveness and adequacy of this document, the following criteria need to be considered:

- number of [illegible]
- number of [illegible]
- number of corrective actions taken without having been recorded in a designated form

## 6. Appendices

Comment [DK22]: Delete this section if you are using an application

Appendix – Corrective Action Form

[job title]
[name]

_____
[signature]

Comment [DK23]: Only necessary if the Procedure for Document and Record Control prescribes that paper documents must be signed