[organization logo]

[organization name]

**INTERNAL AUDIT PROCEDURE**

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

**Change history**

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Version** | **Created by** | **Description of change** |
| YYYY-MM-DD | 0.1 | Dejan Kosutic | Basic document outline |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Table of contents**

[1. Purpose, scope and users 3](#_Toc415655444)

[2. Reference documents 3](#_Toc415655445)

[3. Internal audit 3](#_Toc415655446)

[3.1. Purpose of internal audit 3](#_Toc415655447)

[3.2. Internal audit planning 3](#_Toc415655448)

[3.3. Appointing internal auditors 4](#_Toc415655449)

[3.4. Conducting individual internal audits 4](#_Toc415655450)

[4. Managing records kept on the basis of this document 4](#_Toc415655451)

[5. Validity and document management 5](#_Toc415655452)

[6. Appendices 5](#_Toc415655453)

# Purpose, scope and users

The purpose of this procedure is to describe all audit-related activities – writing the audit program, selecting an auditor, conducting individual audits and reporting.

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

Users of this document are [members of top management] of [organization name], as well as internal auditors.

# Reference documents

* ISO/IEC 27001 standard, clause 9.2
* ISO 22301 standard, clause 9.2
* BS 25999-2 standard, clause 5.1
* Information Security Management System Policy
* Business Continuity Management Policy
* Procedure for Corrective and Preventive Action

# Internal audit

## Purpose of internal audit

The purpose of internal audit is to determine whether procedures, controls, processes, arrangements and other activities within the ISMS [BCMS] are in line with ISO 27001 and ISO 22301/BS 25999-2 standards, applicable regulations, and the organization's internal documentation, whether they are effectively implemented and maintained and whether they meet policy requirements and set objectives.

## Internal audit planning

[job title] approves an annual program for internal audits, written as outlined in the form in Appendix 1.

One or more internal audits should be conducted in the course of one year, ensuring cumulative coverage of the entire ISMS [BCMS] scope. Internal audits are planned based on risk assessment, as well as results of previous audits; they are usually conducted before management review.

The Annual Internal Audit Program has to contain the following information about each individual internal audit:

* period of the audit (specifying dates, or month in which the audit is planned)
* scope of the audit (departments, processes, clauses of the standard, etc.)
* audit criteria (standards, legislation and regulations, internal documentation, corporate standards, and/or contractual obligations)
* auditing methods (review of documentation, interviews with employees, review of records, review of information systems, etc.)
* who will be conducting the audit (if there is more than one auditor, specify the audit team leader)

Conducted audits must be recorded in the Annual Internal Audit Program.

## Appointing internal auditors

[job title] shall appoint internal auditors.

An internal auditor may be someone from the organization or a person outside the organization. Criteria for appointing internal auditors are:

* knowledge of ISO/IEC 27001 and ISO 22301/BS 25999-2 standards
* familiarity with management system auditing techniques
* knowledge of how information and communication technologies function to the extent that he/she is familiar with the purpose of individual systems as well as the impacts on security processes and/or on business continuity

Internal auditors must be selected in such a way as to ensure objectivity and impartiality, i.e. to avoid conflict of interest, because auditors are not allowed to audit their own work.

It is recommended that internal auditors complete a course for internal auditors according to ISO/IEC 27001.

## Conducting individual internal audits

Persons responsible for individual internal audits are identified in the Annual Internal Audit Program. If an audit is conducted by a team consisting of several auditors, the person responsible for the audit is the one identified as Audit Team Leader.

The following must be taken into consideration during an internal audit:

* criteria laid down in the Annual Internal Audit Program
* results of previous internal or external audits
* results of risk assessment, controls implementation, business impact analysis, etc.
* Internal audit checklist – see Appendix 3

The following must be documented as internal audit results:

* Internal Audit Report – it must be sent to [job title]
* possible corrective actions must be documented in the Corrective Action Form, as required by the Procedure for Corrective Action

# Managing records kept on the basis of this document

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Record name | Storage location | Person responsible for storage | Controls for record protection | Retention time |
| Annual Internal Audit Program (in electronic form) | [job title]'s computer | [job title] | Only [job title] and the internal auditor have the right to make entries into and changes to the Annual Internal Audit program. | Programs are stored for a period of 3 years |
| Internal Audit Report (in electronic form) | Internal auditor's and [job title]'s computers | Internal auditor | Reports are stored in read-only versions | Reports are stored for a period of 3 years |
| Internal Audit Checklist (filled form during the internal audit) | Internal auditor's computer | Internal auditor | The checklist is stored in read-only version | The checklist is stored for a period of 3 years |

Only [job title] can grant other employees the right to access the Annual Internal Audit Program, the Internal Audit Report and the Internal Audit Checklist.

# Validity and document management

This document is valid as of [date].

The owner of this document is [job title], who must check and, if necessary, update the document at least once a year.

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

* number of corrective actions identified during the audit
* number of corrective actions identified during the certification audit conducted after the internal audit
* whether the internal audit frequency is in line with the Annual Internal Audit Program

# Appendices

* Appendix 1 – Annual Internal Audit Program
* Appendix 2 – Internal Audit Report
* Appendix 3 – Internal Audit Checklist

[job title]

[name]

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

[signature]