[Organization logo]

[Organization name]

Commented [270012]: All fields in this document marked by square brackets [ ] must be filled in.

INTERNAL AUDIT PROCEDURE

Commented [270013]: To learn more about this topic, read these articles:

- Dilemmas with ISO 27001 internal auditors https://advisera.com/27001academy/blog/2010/03/22/dilemmas-with-iso-27001-bs-25999-2-internal-auditors/
- How to prepare for an ISO 27001 internal audit https://advisera.com/27001academy/blog/2016/07/11/how-to-prepare-for-an-iso-27001-internal-audit/

Consider taking this free online training: ISO 27001 Internal Auditor Course https://training.advisera.com/course/iso-27001-internal-auditor-course/

Furthermore, take a look at this book: ISO Internal Audit: A Plain English Guide https://advisera.com/books/iso-internal-audit-plain-english-guide/

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

Commented [270014]: 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
	0.1	27001Academy	Basic document outline

Table of contents

1. 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.

Commented [270015]: This is to be inserted instead of the ISMS in case the procedure refers exclusively to business continuity management.

Commented [270016]: Top management body within the scope of ISMS/BCMS.

Commented [270017]: Insert the name of your organization.

2. Reference documents

- ISO/IEC 27001 standard, clause 9.2, A.5.30, A.5.35, and A.8.34
- ISO 22301 standard, clause 9.2
- Information Security Policy
- Business Continuity Management Policy
- Procedure for Corrective Action

Commented [270018]: Delete this item if the procedure refers only to business continuity management.

Commented [270019]: Delete this item if the procedure refers only to information security.

Commented [2700110]: Delete this item if the procedure refers only to business continuity management.

Commented [27A11]: You can find a template for this document in the ISO 27001 & ISO 22301 Premium Documentation Toolkit folder "10_ISO_22301_Core_Business_Continuity_Documents".

Commented [27A12]: You can find a template for this document in the ISO 27001 & ISO 22301 Premium Documentation Toolkit folder "14_Corrective_Actions".

3. Internal audit

3.1. Purpose of internal audit

The purpose of internal audit is to determine whether procedures, controls, processes, arrangements

most critical partners and suppliers.

Commented [2700113]:

Commented [2700114]:

Commented [2700115]: Delete this paragraph if the internal auditor will not perform this job.

3.2. Internal audit planning

well as results of previous audits; they are usually conducted before management review.

Commented [2700116]: E.g.: Business Continuity Manager, Security Manager, Information Security Manager, Compliance Officer, etc.

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

- audit criteria (standards, legislation and regulations, internal documentation, corporate [illegible]
- [illegible]
- [illegible] leader)

Appointed internal auditors must record the conducted audits in the Annual Internal Audit Program.

3.3. 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:

- [illegible]
- [illegible]
- [illegible]

[illegible]

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

[illegible]

[illegible] is the one identified as Audit Team Leader.

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

- [illegible]
- [illegible]
- [illegible]
- [illegible]

The following must be documented as internal audit results:

- [illegible]
- [illegible]

Commented [27A17]: These are all mandatory; do not delete any of the items, and make sure you include this information in the Annual Internal Audit Program.

Commented [2700118]: E.g.: Business Continuity Manager, Security Manager, Information Security Manager, Compliance Officer, Compliance Officer, Business Unit Responsible, etc.

Commented [27A19]: [illegible]

Commented [2700120]: To be deleted if the procedure refers only to business continuity management.

Commented [2700121]: To be deleted if you are not implementing business continuity.

Commented [2700122]: E.g.: Security Manager, Information Security Manager, Compliance Officer, Business Unit Responsible, etc.

Commented [2700123]: Or ISO 22301.

Commented [2700124]: For tips on how to perform effective audits, read this article:

7 ways to improve the internal audits of your ISO 27001 ISMS https://advisera.com/27001academy/blog/2017/08/28/7-ways-to-improve-the-internal-audits-of-your-iso-27001-isms/

Commented [2700125]: E.g.: Business Continuity Manager, Security Manager, Information Security Manager, Compliance Officer, Business Unit responsible, etc.

Commented [27A26]: [illegible]

4. 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

Commented [2700127]: Adapt the period in this column to your specific needs.

Commented [2700128]: Usually the person who approved the annual program.

Commented [2700129]: Usually in PDF format.

Commented [2700130]: Usually in PDF format.

[redacted]

5. 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.

Commented [2700131]: E.g.: Business Continuity Manager, Security Manager, Information Security Manager, Compliance Officer, etc.

Commented [2700132]: 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:

- [redacted]

6. Appendices

- Appendix 1 – Annual Internal Audit Program

- [redacted]
- [redacted]

[job title]
[name]

_____
[signature]

Commented [2700133]: Only necessary if the Procedure for Document and Record Control prescribes that paper documents must be signed.