Internal audit

**1. Subject**

**1.1 Purpose**

**1.2 Scope**

**1.3 Glossary**

**2. Responsibility**

**3. Documents**

**3.1 Procedures**

**3.2 Instructions and records**

**4. Requirements of the ISO 22301: 2019 standard**

**5. Development**

**5.1 Context**

**5.2 Planning**

**5.3 Preparing**

**5.4 Initiating**

**5.5 Review of the situation**

**5.6 Completing**

**5.7 Follow-up**

**3.8 Retention**

History

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
| All | Creation | 01/01/2024 |
| **Page** | **Change** | **Date** |

**1. Subject**

**1.1 Purpose**

The purpose of this procedure is to define planning rules, preparation, conducting and monitoring internal audits.

**1.2 Scope**

This procedure is applicable to any type of internal audit (system, procedure, process, product) of the business continuity management system activities. The relevant internal and external issues for the BCMS and actions to address identified risks and found improvements opportunities are taken into account.

**1.3 Glossary**

Audit evidence – demonstrably true data related to audit criteria

Audit findings – every deviation from audit criteria

Audit plan – planned description of activities and means to conduct an audit

Audit programme – planning of audits for a fixed period (usually 1 year)

Audit – systematic and independent survey to determine whether activities and results comply with planned arrangements and are suitable to achieve objectives

Auditee – everyone who is audited

Auditor – everyone who is trained to conduct audits

Nonconformity – nonfulfillment of a specified requirement

BCMS – business continuity management system

**2. Responsibility**

The business continuity manager has the authority to write, update and implement this procedure. He has the authority to manage the audit program, conduct and supervise audits, train and assist auditors and is responsible for ensuring that corrective actions are implemented. He has the support of process owners that ensure optimum conditions for conducting audits related to their activities.

**3. Documents**

**3.1 Procedures**

Corrective actions

Continual improvement

Training

**3.2 Instructions and records**

List of internal auditors

Internal audit plan

Internal audit program

Internal audit questionnaire

Internal audit report

**4. Requirements of the ISO 22301: 2019 standard**

**9.2.1 General**

The organization shall conduct internal audits at planned intervals to provide information on whether the BCMS:

a) conforms to:

1) the organization’s own requirements for its BCMS;

2) the requirements of this document;

b) is effectively implemented and maintained.

**9.2.2 Audit program(s)**

The organization shall:

a) plan, establish, implement and maintain an audit program(s) including the frequency, methods, responsibilities, planning requirements and reporting, which shall take into consideration the importance of the processes concerned and the results of previous audits;

b) define the audit criteria and scope for each audit;

c) select auditors and conduct audits to ensure objectivity and the impartiality of the audit process;

d) ensure that the results of the audits are reported to relevant managers;

e) retain documented information as evidence of the implementation of the audit program(s) and the audit results;

f) ensure that any necessary corrective actions are taken without undue delay to eliminate detected nonconformities and their causes;

g) ensure that follow-up audit actions include the verification of the actions taken and the reporting of verification results.

**5. Development**

**5.1 Context**

The internal audit is conducted according to the following standards:

ISO 19011 (2018): Guidelines for auditing management systems

ISO 22301 (2019): Quality management systems. Requirements

The purpose of the audit is to verify the adequacy between the ISO 22301 standard, regulatory requirements to which our organization is subject and the audited sector. It is not to punish but simply to identify any gaps and propose actions to improve the performance of the audited sector. Throughout its work, the auditor should give a positive image of the audit and seek membership of the auditee to conclusions. It is essential that the audit findings are based on tangible evidence.

The audit reports, corrective action plans, timing and monitoring are internal documents and should not be released outside and must in all cases be commented positively in a process of continual improvement.

**5.2 Planning**

The business continuity manager establishes, implements and follows the annual audit planning. The results of previous audits and the importance of audited processes and services are taken into account during the preparation of the annual audit program. The objectives of the internal audit program are:

* compliance with the business continuity management system requirements
* improving the business continuity management system
* addressing the causes of identified nonconformities
* control of the claims of stakeholders
* the specific contribution of each process:
  + the purpose of the company
  + the establishment of the business continuity policy
  + optimization of necessary resources

Implementation of the internal audit program requires:

* communication to the parties concerned
* coordination in time
* evaluation of auditors
* compliance with the audit plans
* control of records
* verification, approval and distribution of audit reports
* follow-up of audits

Each auditor is trained and evaluated. Persons with the right to conduct the audits are recorded in the list of internal auditors. Auditor competence comes from professional knowledge, mastery of the ISO 19011 and ISO 22301 standards, personal qualities and audit experience.

An auditor cannot audit his own service.

Unplanned internal audit (following nonconformity or complaints by any stakeholder) may be triggered at the initiative of any department, after approval by the business continuity manager or top management.

**5.3 Preparing**

If necessary, the audit leader creates an audit team and defines the roles and missions. If deemed necessary, the leader can organize a preparatory meeting with the persons concerned. The audit questionnaire can be forwarded to the auditee few days before the audit. For business continuity management system audits, night teams must be compulsorily audited.

**5.4 Initiating**

Before beginning an audit, documented objectives, scope and criteria of the audit are defined. A documentation review is done early. This is to check whether the documentation meets the internal requirements of the company and those of ISO 22301.

An internal system, process or product audit plan, accepted by the audit client (often this is top management) and auditee, makes easy programming, implementation and coordination of the audit activities.

A valuable tool for the auditor is the interview guide, which will help record the obtained information. This document is the internal (system, process or product) audit questionnaire.

Before examining the situation, the audit leader provides auditees with the terms of conducting the audit (content, date, persons involved ...).

**5.5 Review of the situation**

It is to determine compliance or non-compliance of the elements examined in relation to prescribed requirements. Verify the effectiveness of a process, product or service is to ask questions to realize if nonconformities may appear. The review of the situation should be based on tangible evidence.

To find audit evidence the information sources can be:

* interviews with the auditees
* observation of activities
* documents (from business continuity policy to daily records)
* business continuity objectives, indicators
* customers and external providers’ feedback

After collection, verification and evaluation of the information they are part of the audit findings. A review with the auditee of such information is needed to obtain a mutual agreement on audit conclusions.

The following can be found in the conclusions:

* the level of compliance of the audited field
* opportunities and recommendations for improvement
* proposals for corrective action if nonconformities have been found
* compliments for good practice

**5.6 Completing**

The internal audit report is approved by a third person (this may be the audit client).

The internal audit report includes:

* the audit findings
* the audit conclusions
* recommendations
* proposals
* audit follow-up:
  + actions
  + responsible
  + deadline for implementing action
  + date of action review
  + checking during the following audit

Completing the audit is formalized either through a last audit meeting or by the distribution of the audit report. The results of internal audits (including their follow-up) are presented by the business continuity manager and examined during management review. This is an important input element to find opportunities to improve the business continuity management system (BCMS).

The coding for the audit reports is 1310AAxxyy, where AA is the year (24 for 2024), xx the audit number (there may be several audits per year) and yy the number of the index (revision). The distribution of the report includes the auditees, the head of the audited department and those involved in corrective actions.

**5.7 Follow-up**

The implementation schedule for corrective action is followed by the audit leader who may request progress reports. He validates every action in the audit report as they are realized. To revive unfinished corrective actions, the auditor may call a meeting with each action responsible or conduct a second audit. The audit is completed when all corrective actions are performed. More details in the Corrective actions procedure.

**3.8 Retention**

When corrective actions are completed the last index of the report is validated. Retention of audit reports is done on the server.