

**Internal Audit Procedure**

**Revision History**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Ver.** | **Date** | **Description of Change** | **Author/ Revised By** | **Reviewed By** | **Approved By** |
| 0.1 | 22nd Aug 2013 | Initial Draft | Rahul Raj | Dhananjay Kumar | Ajay Kumar Zalpuri |
| 1.0 | 30th Sep 2013 | Initial Release | Rahul Raj | Dhananjay Kumar | Ajay Kumar Zalpuri |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

**Table of Contents**

[1. Objectives 5](#_Toc380403677)

[2. Scope 5](#_Toc380403678)

[3. Entry Criteria 5](#_Toc380403679)

[4. Inputs 5](#_Toc380403680)

[5. Terms and Definitions 5](#_Toc380403681)

[6. Procedure 5](#_Toc380403682)

[6.1. General 5](#_Toc380403683)

[6.2. Planning an Audit Program 6](#_Toc380403684)

[6.2.1. Objectives of an audit program 6](#_Toc380403685)

[6.2.2. Extent of an audit program 6](#_Toc380403686)

[6.2.3. Audit program responsibilities 6](#_Toc380403687)

[6.2.4. Audit program resources 7](#_Toc380403688)

[6.2.5. Audit program procedures 7](#_Toc380403689)

[6.3. Audit Program Implementation 7](#_Toc380403690)

[6.3.1. Scheduling audits 7](#_Toc380403691)

[6.3.2. Competence and evaluation of auditors 7](#_Toc380403692)

[6.3.3. Selecting audit teams 7](#_Toc380403693)

[6.3.4. Directing audit activities 7](#_Toc380403694)

[6.4. Audit Program Records 8](#_Toc380403695)

[6.4.1. Maintaining records 8](#_Toc380403696)

[6.4.2. Retaining records 8](#_Toc380403697)

[6.5. Audit program Monitoring and Reviewing 8](#_Toc380403698)

[6.5.1. Monitoring and reviewing 8](#_Toc380403699)

[6.5.2. Corrective and preventive actions and opportunities for improvement 8](#_Toc380403700)

[7. Audit Activities 9](#_Toc380403701)

[7.1. Initiating the Audit 9](#_Toc380403702)

[7.1.1. Defining audit objectives, scope and criteria 9](#_Toc380403703)

[7.1.2. Determining the feasibility of the audit 9](#_Toc380403704)

[7.1.3. Composing the Audit Team 10](#_Toc380403705)

[7.2. Conducting Document Review 10](#_Toc380403706)

[7.3. Preparing for the On-site Audit Activities 10](#_Toc380403707)

[7.1.1. Preparing the audit plan 10](#_Toc380403708)

[7.1.2. Assigning work to the audit team 10](#_Toc380403709)

[7.1.3. Preparing work documents 11](#_Toc380403710)

[7.4. Conducting On-site Audit Activities 11](#_Toc380403711)

[7.4.1. Conducting opening meeting 11](#_Toc380403712)

[7.4.2. Collecting and verifying information 11](#_Toc380403713)

[7.4.3. Generating audit findings 11](#_Toc380403714)

[7.4.4. Preparing Audit conclusions 11](#_Toc380403715)

[7.4.5. Conducting the closing meeting 12](#_Toc380403716)

[7.5. Preparing, Approving and Distributing the Audit Report 12](#_Toc380403717)

[7.5.1. Preparing the audit report 12](#_Toc380403718)

[7.5.2. Approving and distributing the audit report 12](#_Toc380403719)

[7.6. Completing the Audit 13](#_Toc380403720)

[7.7. Conducting Audit Follow-up 13](#_Toc380403721)

[8. Output 13](#_Toc380403722)

[9. Exit Criteria 13](#_Toc380403723)

# Objectives

The purpose of this document is to explain the process for auditing QMS and ISMS implementation in the organization to assess its effectiveness and compliance with defined standards (as per ISO 9001, ISO 27001 and CMMi L3).

# Scope

This procedure stipules organizing QMS and ISMS Audits and follow up audit for verification of corrective actions.

# Entry Criteria

1. All the policies and procedures have been identified.
2. Audit team has been constituted by Security Council.

# Inputs

1. Audit Program
2. Audit Plan
3. Action items from last Security Council meeting.
4. Gaps and suggestions identified in the last audit (both internal and external).

# Terms and Definitions

|  |  |
| --- | --- |
| QMS | Quality management System |
| ISMS | Information Security Management System |

# Procedure

## **General**

The organization's top management shall assign an **audit manager** and grant him/her the authority for managing the audit program.

The Audit team shall give appropriate support to the audit manager for managing the audit program.

The audit manager shall

a) Establish, implement, monitor, review and improve the audit program. In addition, the audit program must be conducted on a regular basis (at least once a year) in coordination with the Audit team.

b) Identify the necessary resources and ensure they are provided.

Figure1 illustrates the process flow for the management of an audit program.



## **Planning an Audit Program**

### Objectives of an audit program

The audit manager shall establish the objectives of an audit program to direct the planning and conduct of audits.

### Extent of an audit program

To specify the extent of an audit program appropriately, the audit manager shall consider the following:

a) The scope, objective and duration of each audit to be conducted.

b) Conclusions of previous audits or results of previous audit program review.

c) Significant changes to an organization or its operations.

### Audit program responsibilities

The audit manager, as the top management of an audit program, shall be responsible for the following:

a) Establish the objectives and extent of the audit program.

b) Establish the responsibilities and procedures, and ensure resources are provided.

c) Ensure the implementation of the audit program.

d) Ensure that appropriate audit program records are maintained.

e) Monitor, review and improve the audit program.

### Audit program resources

When identifying resources necessary for the audit program, the audit manager should consider the following:

a) Audit techniques.

b) Processes to achieve and maintain the competence of auditors, and to improve auditor performance.

c) The availability of auditors and technical experts having competence appropriate to the particular audit program objectives.

d) The extent of an audit program.

e) Travelling time, accommodation and other auditing needs.

### Audit program procedures

To establish audit program procedures, the audit manager should consider the following:

a) Planning and scheduling audits.

b) Assuring the competence of auditors and audit team leaders.

c) Selecting appropriate audit teams and assigning their roles and responsibilities.

d) Conducting audits.

e) Conducting audit follow-up, if applicable.

f) Maintaining audit program records.

g) Monitoring the performance and effectiveness of the audit program.

h) Reporting to top management on the overall achievements of the audit program.

## **Audit Program Implementation**

### Scheduling audits

The audit manager shall conduct the following:

a) Communicating the audit program to relevant parties.

b) Coordinating and scheduling audits and other activities relevant to the audit program.

### Competence and evaluation of auditors

The audit manager shall evaluate the competence of auditors and their continual professional development.

### Selecting audit teams

The audit manager shall ensure the selection of audit teams.

### Directing audit activities

The audit manager shall conduct the following:

a) Providing necessary resources to the audit teams.

b) Ensuring audits are conducted according to the audit program.

c) Ensuring records of the audit activities are controlled.

d) Ensuring audit reports are checked & approved, and distributed to relevant parties.

e) Ensuring audit follow-up is conducted, if applicable.

## **Audit Program Records**

### Maintaining records

The audit manager shall maintain records to demonstrate the implementation of the audit program and shall include the following:

a) Records related to individual audit, such as

- Audit plans, and matters related to audit plan

- Audit reports and matters related to audit results

- The contents related to nonconformities

- The contents related to corrective and preventive actions

- Matters related to audit follow-up, if necessary.

b) Results of audit program review.

c) Records related to auditor covering subjects such as

- Auditor competence and performance evaluation.

- Audit team selection.

- Maintenance and improvement of competence.

### Retaining records

The audit manager shall retain records for 3 years in a searchable format and suitably safeguarded.

## **Audit program Monitoring and Reviewing**

The audit manager shall monitor the implementation of the audit program and, at appropriate intervals, review to assess whether its objectives have been met and to identify opportunities for improvement. The results shall be reported to top management.

### Monitoring and reviewing

a) Appropriate performance indicators shall be used to monitor characteristics such as

- The ability of the audit teams to implement the audit plan.

- Conformity with audit programs and schedules.

- Feedback from the audited division and auditor.

b) In the audit program review, the audit manager should consider the following:

- Results and trends from monitoring.

- Conformity with procedures.

- Evolving needs and expectations of interested parties.

- Audit program records.

- Alternative or new auditing practices.

- Consistency in performance between audit teams in similar situations.

### Corrective and preventive actions and opportunities for improvement

Based on the results of audit program reviews, the audit manager shall gather elements that can lead to corrective and preventive actions and the improvement of the audit program.

# Audit Activities

Figure 2 illustrates the overview flow for audit activities.



## Initiating the Audit

### Defining audit objectives, scope and criteria

Within the overall objectives of an audit program, the objectives, scope, and criteria of an each audit shall be clarified and documented. The audit objectives shall be defined by the audit manager. The audit scope and criteria shall be defined between the audit manager and audit team leader in accordance with audit program procedures. Any changes to the audit objectives, scope or criteria shall be agreed to by the same parties.

### Determining the feasibility of the audit

The feasibility of the audit shall be determined in consideration of the availability of the following factors:

- Sufficient and appropriate information for planning the audit.

- Adequate cooperation from the auditee.

- Adequate time and resources.

Where the audit is not feasible, an alternative (review or walkthrough) shall be proposed by audit manager, in consultation with the auditee.

### Composing the Audit Team

When the audit has been declared feasible, the audit manager shall select an audit team, taking into account the competence necessary to achieve the audit objectives. With regard to composing the audit team, the audit manager shall receive support from the Audit team , where necessary.

## Conducting Document Review

Prior to on-site audit activities, the audit team shall review the auditee's documentation system to determine its conformity with audit criteria within the scope of those already documented. The documents may include relevant management system documents, records, and previous audit reports.

If the audit team has already had a good knowledge of the auditee's management system document, preliminary document review is omissible. In some situations, this document review may be deferred until on-site activities commence.

## Preparing for the On-site Audit Activities

### Preparing the audit plan

The audit manager shall prepare an audit plan to provide the basis for the agreement between the audit team and the auditee regarding the conduct of the audit.

The audit plan shall cover the following:

a) The audit objectives.

b) The audit criteria and any reference document.

c) The audit scope, including identification of organizational and divisional units and processes to be audited.

d) The dates and places where the on-site audit activities are to be conducted.

e) The roles and responsibilities of audit team members and accompanying persons.

f) The allocation of appropriate resources to critical areas of the audit.

The audit plan shall also cover the following, as appropriate:

g) Identification of the auditee's representative for the audit.

h) Matters related to confidentiality.

i) Any audit follow-up actions.

The audit plan shall be reviewed and accepted, and presented to the auditee before the on-site audit activities begin.

### Assigning work to the audit team

The audit manager, in consultation with the audit team members, shall assign to each team member responsibility for auditing specific processes, divisions, sites, areas or activities. Such assignment shall take into account the need for the independence and competence of auditors and the effective use of resources, as well as different roles and responsibilities of auditors, auditors-in-training and technical experts. The auditor must not audit his/her own work.

### Preparing work documents

The audit team members shall review the information relevant to their audit assignments and prepare work documents as necessary for reference and for recording audit proceedings.

Such work documents may include

- Checklist and audit sampling plans, and

- Forms for recording information, such as supporting evidence, audit findings and records of meetings.

Work documents, including records resulting from their use, shall be retained as per frequency defined.

## Conducting On-site Audit Activities

### Conducting opening meeting

An opening meeting shall be held with the auditee's top management or where appropriate, those responsible for the divisions or processes to be audited. The purpose of an opening meeting is as follows:

a) To confirm the audit plan.

b) To provide a short summary of how the audit activities will be undertaken.

c) To confirm communication channels.

d) To provide an opportunity for the auditee to ask questions.

### Collecting and verifying information

During the audit, information relevant to the audit objectives, scope and criteria shall be collected by appropriate sampling and shall be verified. Only information that is verifiable may be audit evidence. Audit evidence shall be recorded.

### Generating audit findings

Audit evidence shall be evaluated against the audit criteria to generate the audit findings. Audit findings can indicate either conformity or nonconformity with the audit criteria.

When specified by the audit objectives, audit findings can identify an opportunity for improvement and evaluated point (strong point).

Conformity with the audit criteria shall be summarized to indicate locations, divisions or processes that were audited. If included in the audit plan, individual audit findings of conformity and their supporting evidence shall also be recorded.

Nonconformities and their supporting audit evidence shall be recorded. Nonconformities shall be graded appropriately. Nonconformities shall be reviewed with the auditee.

### Preparing Audit conclusions

The audit team shall have a team meeting prior to the closing meeting to conduct the following:

a) To review the audit findings, and any other appropriate information collected during the audit, against the audit objectives.

b) To agree on the audit conclusions, taking into account uncertainty inherent in the audit process.

c) To prepare recommendations, if specified by the audit objectives.

d) To discuss audit follow-up, if included in the audit plan.

### Conducting the closing meeting

A closing meeting, chaired by the audit manager, shall be held to present the audit findings and the audit conclusions, and to agree, if appropriate, on the time frame for the auditee to present a corrective and preventive action plan. In principle, participants in the closing meeting shall include the auditee and the person in charge of process (or his/her substitute).

## Preparing, Approving and Distributing the Audit Report

### Preparing the audit report

The audit team members shall be responsible for the preparation and contents of the audit report for their respective area of audit.

The audit report shall provide a complete, accurate, concise and clear record of the audit, and shall include or refer to the following:

a) The audit objectives.

b) The audit scope, particularly identification of the organizational and divisional units or processes audited and the time period covered.

c) Identification of audit manager.

d) Identification of audit team leader and members.

e) The dates and places where the on-site audit activities were conducted.

f) The audit criteria.

g) The audit findings.

h) The audit conclusions.

The audit report may also include or refer to the following, as appropriate.

1. The audit plan.
2. j) List of the auditee representatives.
3. k) Summary of the audit process, including the uncertainty and/or any obstacles encountered that could decrease the reliability of the audit conclusions.
4. l) Confirmation that the audit objectives have been accomplished within the audit scope in accordance with the audit plan.
5. m) Any areas not covered, although within the audit scope.
6. n) Any unresolved diverging opinions between the audit team and the auditee.
7. o) Recommendations for improvement, if specified in the audit objectives.
8. p) Agreed follow-up action plans.
9. q) Description related to the confidential nature of the contents.
10. r) The distribution list for the audit report.

### Approving and distributing the audit report

The audit report shall be issued within the agreed time period.

The audit report shall be dated, reviewed and approved.

The approved audit report shall be distributed to recipients designated by the audit manager. The audit report is the property of the organization that planned the audit programme. The audit team members and all report recipients must respect and maintain the confidentiality of the report.

## Completing the Audit

The audit is completed when all activities described in the audit plan have been carried out and the approved audit report has been distributed.

Documents pertaining to the audit shall be retained or destroyed by agreement between the participating parties and in accordance with audit program procedures and applicable statutory, regulatory and contractual requirements.

Unless required by law, the audit team and audit manager shall not disclose the contents of documents, any other information obtained during the audit, or the audit report, to any other party, where necessary, without the explicit approval of the auditee. If disclosure of the contents of an audit document is required, the auditee shall be informed as soon as possible.

## Conducting Audit Follow-up

The conclusions of the audit may indicate the need for corrective, preventive or improvement actions, as the need arises. The auditee shall keep the audit manager informed of the status of these actions.

The audit manager is required to confirm the completion and effectiveness of corrective actions. This verification may be part of a subsequent audit.

# Output

1. Audit Report
2. Updated NCs

# Exit Criteria

Audit has been conducted as planned.