

# Internal Audit Procedure

Reference: ISMS DOC 9.2

DocumentKits Issue No: 1.0

Organisation Issue No:

DocumentKits Issue Date: 28/11/2019

Organisation Issue Date:

## 1. Scope

This procedure applies to internal audits.

"If your organisation needs to separate internal management system audits from other internal audit activity, you should clarify the exact scope of this procedure here."

It establishes the requirements for planning, preparation, performance, reporting, follow-up and close-down of them.

The objective of this procedure is to establish an independent system for verification of the implementation of the ISMS, and its improvement by means of a controlled method for planning, scheduling, coordinating and performing internal audits and related activities.

For IT Technical Compliance Audits, see the [Systems Auditing Procedure](#).

Internal audits of financial aspects may result in third-party Internal Auditors being appointed. The process for these audits is defined by Organisation Name contract with the appointed supplier and the Annex to this section.

This procedure refers to Internal Auditors who are Organisation Name Employees/Staff.

## 2. Responsibilities

2.1 The Lead Auditor is responsible for the overview and implementation of this procedure.

2.2 Appointed Internal Auditors are responsible for the preparation, execution and reporting of audits assigned to them for completion in accordance with their necessary competence and the requirements of this procedure. This may require third parties to be appointed to conduct Internal Audits to compensate where necessary expertise is not

available.

2.3 All Employees/Staff are responsible for assisting in the audit process, as and when required.

### **3. Procedure** [ISO27001 Clause 9.2]

3.1 The Lead Auditor shall establish an Internal Audit Schedule of sufficient scope to ensure that each aspect of the ISMS is audited at least annually. It will identify the scope and frequency of audits, along with identifying the type of auditor (Internal or Supplier) to conduct the audit. The Audit Plan will be reviewed and agreed by the Chief Executive Officer (CEO).

3.2 The Lead Auditor will propose the Audit Plan at least 3 months in advance of the start date, programming audits with due consideration to:

- Its ISMS and business requirements
- Severity of findings at most recent Internal Audit
- Programming of other audits in the same area
- Latest/proposed major revisions to processes, etc.
- Any other valid reason that may justly impact on the timing of an audit.

3.3 Audit performance will be reviewed as part of the Management Review Procedure.

3.4 Audits will be assigned to Internal Auditors who are competent to conduct that type of audit. Internal Auditors shall be deemed as 'Competent' at the discretion of the Lead Auditor. Selection and conduct of audits will ensure objectivity and impartiality.

3.5 Internal Auditors may undergo a variety of development practices to further develop their auditing skills (e.g. accompanied audits and Internal Auditor Meetings).

3.6 Internal Auditors will require special skills for this audit. Qualification requirements for the identified personnel are at the discretion of the Lead Auditor. Solution may be through the appointment of a suitable third party.

3.7 The Lead Auditor / HR Department maintains a record of training received by Internal Auditors, and their suitability to conduct certain types of audit.

3.8 The Lead Auditor informs the Internal Auditors of the impending audit at least one month in advance of the required completion date. The Internal Auditors will be told the

relevant audit number.

3.9 During the planning and preparation for an audit, the Internal Auditors ensure that the following actions are taken:

- Preparation of an audit checklist -

"Set out how checklists are produced and maintained. These might be fixed template checklists, for instance, or customised to the audit. Link to a procedure if necessary."

- Contact the auditee to agree a mutually convenient date(s) for the audit and to discuss the scope of the audit.3.10 The Internal Auditors conduct the audit using a checklist(s) as a guide. He/she examines the objective evidence and records relevant details.

3.11 The Internal Auditors may expand a checklist if additional questions become necessary, to determine the compliance with specified requirements and/or the effectiveness of an ISMS element.

3.12 Confidentiality during audit: when an internal audit or third-party surveillance necessitates checking client files or databases, precautions must be taken to ensure that client confidentiality is preserved. Wherever possible, access is limited to satisfying the Internal Auditors that a file or database exists, is properly identified and is secure. If it is essential to check content, then access is limited to non-sensitive data.

3.13 During an audit, the Internal Auditors evaluate the evidence found and analyse the apparent non-conformances to ensure their validity as audit findings.

3.14 Where non-conformances are found and the corrective action agreed, the Internal Auditors will note the actions against the non-conformance. Where actions were completed at time of audit, the Internal Auditors may sign off the non-conformance.

3.15 Following completion of an audit, the Internal Auditors prepare a formal Audit Report comprising an [Internal Audit Report Lead Sheet](#), a number of [Non-Conformance Reports](#), one relating to each non-conformance identified (including those closed at the time of the audit), and additional sheets covering observations. The findings of the audit are summarised on the Audit Lead Sheet, including the number and nature of non-conformances.

3.16 Where the Internal Auditors use support documentation, this may be inserted into the Audit Report as Observations, at the discretion of the Internal Auditors and in addition to the normal Audit Lead Sheet.

3.17 The Internal Auditors obtain the signature of the main auditee on the Audit Lead Sheet, acknowledging the findings, and on each Non-Conformance Report to agree the non-conformance. A copy of the Audit Lead Sheet is given to the auditee for information and the complete report, together with all working papers, are sent to the Lead Auditor.

3.18 The Lead Auditor will file any working papers that do not form part of the official report separately.

3.19 On receipt of the completed Audit Report, the Lead Auditor logs the Audit Report, and progresses any Non-Conformance Reports through the Non-Conformity and Corrective Action Procedure, cross-referencing the Non-Conformance Report Log Number on the Audit Lead Sheet.

3.19.1 The Lead Auditor and relevant staff should consider formally assessing the risks presented to Organisation Name of the nonconformity (e.g. if it concerns a major flaw in plans for a high-impact critical activity) until it has been closed and adding them to the risk register if appropriate. Short term "workaround" corrective action might be considered pending full root cause analysis and formal closure of the long term corrective action.

3.20 The Lead Auditor reviews the Observations, with a view to raising a Non-Conformance Report relating to each issue. This then serves to address the findings without a formal non-conformance being raised at audit, and without the Audit Report remaining open for an unnecessarily extended period of time.

3.21 When all the non-conformities associated with an audit have been closed, the Lead Auditor signs the Internal Audit Report Lead Sheet as completed. A complete copy of the Audit Report is sent to the auditee for confirmation of the closing of the report.

3.22 Where the Lead Auditor has reason to believe that the cause of the non-conformance may have resulted in similar non-conformances elsewhere, he/she may require follow-up audits to be carried out on that item, either in the originating area or other affected areas. These are planned in accordance with the process described above.

3.23 Should follow-up audits prove necessary, they shall be undertaken in accordance with the requirements of this procedure.

3.24 The results of audits shall be summarised by the Lead Auditor and reviewed at

Management Review Meetings in accordance with the [Management Review Procedure](#).

### ***Document Owner and Approval***

The Lead Auditor is the owner of this document and is responsible for keeping it up to date.

The current version of this document is available to

"Specify which members of staff this document is intended for"

and is published

"Describe the location(s) – electronic and physical – where this document is available"

Its approval status can be viewed in [Master List of Document Approval](#).