1. **Scope**

This procedure applies to internal audits. 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 information security management system, 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 [ISMS-C DOC 12.7.1](../Control%20A12%20-%20operations%20security/ISMS-C_DOC_12.7.1.docx).

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

This procedure refers to Internal Auditors who are Retirement Capital Employees/Staff.

1. **Responsibilities**
   1. The Director (CISO) is responsible for the overview and implementation of this procedure.
   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.
   3. All Employees/Staff are responsible for assisting in the audit process, as and when required.
2. **Procedure** [ISO27001 Clause 9.2]
3. The Director (CISO) shall establish an Audit Schedule ([MSS REC 9.2.1](MSS_REC_9.2.1.xlsx)) of sufficient scope to ensure that each aspect of the Information Security Management System 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 Managing Director.
4. The Director (CISO) will propose the Audit Plan at least 3 months in advance of the start date, programming audits with due consideration to:

* Business Need
* 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.

1. Audit performance will be reviewed as part of the Management Review, (see [MSS DOC 9.3](MSS_DOC_9.3.docx)).
2. Audits will be assigned to an Internal Auditors who is competent to conduct that type of audit. Internal Auditors shall be deemed as ‘Competent’ at the discretion of the Director (CISO). Selection and conduct of audits will ensure objectivity and impartiality.
3. Internal Auditors may undergo a variety of development practices, to further develop their auditing skills, (e.g. accompanied audits and Internal Auditor Meetings).
4. For specific types of audit, Internal Auditors will require special skills, (i.e. technical audits for ISO27001 compliance, ISO22301 conformance, financial audits, etc.). Qualification requirements for the identified personnel are at the discretion of the Director (CISO). Solution may be through the appointment of a suitable third party.
5. The Director (CISO) maintains a record of training received by Internal Auditors, and their suitability to conduct certain types of audit.
6. The Director (CISO) 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.
7. During the planning and preparation for an audit, the Internal Auditors ensure that the following actions are taken:
   * + Preparation of an audit checklist based upon audit.

* Contact the auditee to agree a mutually convenient date(s) for the audit and to discuss the scope of the audit.

1. The Internal Auditors conduct the audit using a checklist(s) as a guide. He/she examines the objective evidence and records relevant details.
2. The Internal Auditors may expand a checklist if additional questions become necessary, to determine the compliance with specified requirements and/or the effectiveness of a management system element.
3. 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.
4. During an audit, the Internal Auditors evaluate the evidence found and analyse the apparent non-conformances to ensure their validity as audit findings.
5. 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.
6. Following completion of an audit, the Internal Auditors prepare a formal Audit Report comprising an Audit Lead Sheet ([MSS REC 9.2.2](MSS_REC_9.2.2.docx)), a number of Non-Conformance Reports ([MSS REC 10.1.1a](../Section%2010%20-%20improvement/MSS_REC_10.1.1A.docx)), 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.
7. 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.
8. 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 Director (CISO).
9. The Director (CISO) will file any working papers that do not form part of the official report separately.
10. On receipt of the completed Audit Report, the *Director (CISO)* logs the Audit Report, and progresses any Non-Conformance Reports through the Corrective, Preventive Action Procedure ([MSS DOC 10.1](../Section%2010%20-%20improvement/MSS_DOC_10.1.docx)), cross-referencing the Non-Conformance Report Log Number on the Audit Lead Sheet.
    * 1. The Director (CISO) and relevant staff should consider formally assessing the risks presented to the organization 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.
11. The Director (CISO) 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.
12. When all the non-conformities associated with an audit have been closed the Director (CISO) 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.
13. Where the Director (CISO) 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.
14. Should follow-up audits prove necessary, they shall be undertaken in accordance with the requirements of this procedure.
15. The results of audits shall be summarised by the Director (CISO) and reviewed at Management Review Meetings in accordance with MSS DOC 9.3.

***Document Owner and Approval***

The Director (CISO) is the owner of this document and is responsible for ensuring that this procedure is reviewed in line with the review requirements of the ISMS.

A current version of this document is available to all members of staff on the corporate intranet.

This procedure was approved by the Head of Risk on 14th November 2020 and is issued on a version-controlled basis under his/her signature.

Signature: Date: 14/11/2020

**Change History Record**

|  |  |  |  |
| --- | --- | --- | --- |
| Issue | Description of Change | Approval | Date of Issue |
| 1 | Initial issue | Gavin McCloskey | 14/11/2020 |
|  |  |  |  |
|  |  |  |  |