1. **Scope** [ISO27002 Clause 18.2.1]

Retirement Capital’s entire ISMS is subject to independent review, as part of the Check - Act stages of the management system.

1. **Responsibilities**

The Director (CISO) is responsible for recruiting internal reviewers, for planning (including agreeing Manager when their employees/staff will need to be available to carry out reviews) and managing the internal review program, for ensuring that individual reviews occur as planned, and for collating and reporting on the results.

Manager whose employees/staff are also Internal Auditors are required to release their employees/staff to meet the requirements of the internal review program.

Internal Auditors are responsible for carrying out internal reviews in line with the requirements of this procedure.

1. **Procedure** 
   1. The Director (CISO) recruits internal review team members from amongst the existing employees/staff of Retirement Capital. The basis on which they are recruited is experience and suitability for the task.
   2. Internal Auditors are trained by the Director (CISO) to provide an understanding of how to conduct an audit, report findings and non-conformances and recommend corrective action before they carry out any reviews and undergo regular refresher training, annually.
   3. The Director (CISO) draws up an annual internal review plan, which is approved by the Chief Information Security Officer (CISO (DIRECTOR)) at least six weeks before the start of the new 12-month period.
   4. This plan (which is classified as confidential) ensures that all the high risk areas of the business are reviewed at least every six months and also ensures that the individuals carrying out the reviews are independent of the area being reviewed and adequately cleared to deal with the classification level of all information assets within the area of review.
   5. Internal Auditors are entitled to talk to any employees/staff involved in the processes that are under review but are not expected to carry out technical checking for which they have not been trained. They are expected to review any management actions that have been documented in line with [ISMS-C DOC 18.1.4a](ISMS-C_DOC_18.1.4a.docx).
   6. All identified non-conformances are reported to the Director (CISO) using [ISMS REC 10.1.1a](../Section%2010%20-%20improvement/MSS_REC_10.1.1A.docx)
   7. The Certification Body also carries out annual reviews of the ISMS.
   8. The non-conformance and any other reports produced by either the Internal Auditors or the CB are logged in Retirement Capital’s Non-Conformance Report Log ([ISMS REC 10.1.1b](../Section%2010%20-%20improvement/MSS_REC_10.1.1B.xlsx)). The Director (CISO) is responsible for ensuring that appropriate corrective (or preventive) action is identified, a time scale and responsibilities agreed, and for reporting on the successful conclusion of the corrective (or preventive) action.
   9. The updated Non-Conformance Report, together with the supporting documentation, is provided to the Management Review of information security which is carried out as required by [ISMS DOC 9.3](../Section%209%20-%20performance%20evaluation/MSS_DOC_9.3.docx).
   10. The Director (CISO) is responsible for escalating any non-conformances to the Chief Information Security Officer (CISO (DIRECTOR)) for immediate attention.

***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 Chief Information Security Officer (CISO (DIRECTOR)) 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 |
|  |  |  |  |
|  |  |  |  |