1. **Choice of risk assessment tool/methodology**

Retirement Capital has selected and uses a spreadsheet as its risk assessment tool. The tool was selected in line with this procedure.

1. **Requirements**

The requirements in respect of a risk assessment tool to deliver an ISO27001-compliant risk assessment, as detailed below, were drawn from ISO27001: 2013. The additional corporate requirement is that any tool selected must be the least expensive tool available that meets the selection criteria below.

The risk assessment tool must enable Retirement Capital to carry out a risk assessment that includes:

|  |  |
| --- | --- |
| Identification of assets - ISO27002 8.1.1 | Y |
| Identification and maintenance of information security risk acceptance criteria - ISO27001 6.1.2.a.1 | Y |
| Identification of potential consequences if risks were to materialize, taking account of the legal and business requirements and impacts resulting from a loss of confidentiality, integrity and availability - ISO27001 6.1.2.d.1 | Y |
| Identification of risks that might lead to loss of confidentiality, integrity or availability - ISO27001 6.1.2.c.1 | Y |
| Assessment of the realistic likelihood of the risk materializing - ISO27001 6.1.2.d.2 | Y |
| Calculation of risk - ISO27001 6.1.2.d.3 | Y |
| Evaluation of risk against a pre-defined risk scale - 6.1.2.e.1 | Y |
| Repeated information security risk assessments produce consistent, valid and comparable results - ISO27001 6.1.2.b | Y |
| Recording of risk treatment decisions taken, in light of pre-defined risk acceptance criteria - ISO27001 6.1.3.a and 6.1.3.b | Y |
| Risk treatment decisions should include selection of controls from ISO27001 Annex A or from other sources - ISO27001 6.1.3.a through c | Y |
| Storage of initial and subsequent risk assessment results enabling their future review - ISO27001 8.2 and 8.3 | Y |

1. **How the tool was selected**

Once it was clear that tool met Retirement Capital’s requirements and criteria, a copy of the software and an appropriate user license was purchased.

1. **How the tool actually works**

The tool is a spreadsheet-based programme.

1. **Training requirements**

Training requirements are limited.

The tool has detailed onscreen guidance. The Lead Risk Assessor is required to familiarise himself/herself with the principles of ISO27001 Risk Management; is then required to read the tool overview that is provided.

Users other than the Lead Risk Assessor will be guided, as appropriate, by the Lead Risk Assessor. Once the user is clear about how each step should be carried out, the risk assessment itself can begin.

The Information Security Manager 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 specified members of staff on the corporate intranet.

This procedure was approved by the Chief Information Security Officer (CISO) on 14th November 2020 and is issued on a version-controlled basis under his/her signature.

Signature: Date: 14/11/2020

**Change history**

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