1. **Scope**

This method of risk assessment is applied throughout Retirement Capital in respect of all risks.

1. **Responsibilities**

The Information Security Manager is responsible for carrying out risk assessments wherever they are required by the ISMS.

1. **Procedure**

**Identify the risks**

1. The risks to Retirement Capital’s information are identified through a desktop audit by the Information Security Manager with the departmental managers under the headings of risks to availability, confidentiality and integrity, and are documented in the risk log.
2. The effect that losses of availability, confidentiality and integrity might have on Retirement Capital are identified and documented by the Information Security Manager as part of 3.1 above
3. For each risk, identify the risk owner.
4. **Assess the risks**
5. The impact – the business harm - that might result from the loss of availability, confidentiality or integrity, for each of these risks, is assessed by the Information Security Manager as part of 3.1 above.
6. The realistic likelihood that each of these risks might occur is assessed by the Information Security Manager as part of 3.1 above.
7. The risk levels are assessed by the Information Security Manager as part of 3.1 above.
8. A decision is made, for each of the risks, as to whether it is acceptable or if it must be controlled in line with criteria established in [RM-ISMS DOC 6.1.2a](RM-ISMS_DOC_6.1.2a.docx) by the Risk Owner.
9. **Identify and evaluate options for the treatment of risks**
10. For each of the risks, identify the Information Security Manager and departmental Manager assess the possible options for treating it in line with the decision made in 4.4 above.
11. For each of the risks, document which treatment action (accept, reject, transfer or control) is going to be taken by the Information Security Manager and departmental Manager and document in the Risk Treatment Plan, [RM-ISMS REC 6.1.3 Part 1](RM-ISMS-REC-6-1-3%20Pt%201.pdf) , [Part 2](RM-ISMS-REC-6-1-3%20Pt%202.pdf), [Part 3](RM-ISMS-REC-6-1-3%20Pt%203.pdf), [Part 4](RM-ISMS-REC-6-1-3%20Pt%204.pdf), [Part 5](RM-ISMS-REC-6-1-3%20Pt%205.pdf), [Part 6](RM-ISMS-REC-6-1-3%20Pt%206.pdf). The Information Security Manager and departmental Manager determine and log the reasons for each choice.
12. **Select control objectives and controls for treatment of the risks**
13. Appropriate control objectives are selected or designed the Information Security Manager and departmental Manager according to the specific needs of the risk and the organization and controls to achieve those objectives are selected from a variety of sources.
14. Controls selected in 6.1 above are compared against those from Annex A of ISO27001:2017 to ensure that none have been missed.
15. The final selection of controls and control objectives and the reasons for the selections (whether inclusion or exclusion) are documented.
16. These control objectives and controls are then summarised in the Statement of Applicability.

***Document Owner and Approval***

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 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 |
|  |  |  |  |
|  |  |  |  |