1. **Scope**

This applies to the risk management framework in Retirement Capital and will be conducted in line with [MSS DOC 4.1](../Section%204%20-%20context%20of%20organisation/MSS_DOC_4.1.docx) and [DOC 4.2](../Section%204%20-%20context%20of%20organisation/MSS_DOC_4.2.docx).

1. **Responsibilities**
   1. The Information Security Manager is responsible for identifying management system risks, and for the development, testing and maintenance of plans to manage those risks.
   2. The Operations Director is responsible for managing business continuity on a day-to-day basis and is also responsible for carrying out the risk assessments relevant to business continuity.
   3. The Information Security Manager is responsible for ensuring that all information security issues have been included and appropriately treated under this risk management framework.
   4. The Information Security Manager is responsible for ensuring that all quality management issues have been included and appropriately treated under this risk management framework.
   5. The Department Managers are responsible for key processes and are also responsible for implementing controls relating to those processes as determined in the risk assessment.
2. **Risk management**
   1. Risk management is conducted within the internal and external context of Retirement Capital, as identified in MSS DOC 4.1.
   2. Risk management takes Retirement Capital’s legal and regulatory requirements into account, as identified in MSS DOC 4.2.
   3. The Information Security Manager defines risk criteria accordingly:
      1. A Risk is anything that will affect the operation, financial status or integrity of the company, its employees, contractor and customers and takes into account the following:
   * the nature and types of causes and consequences that can occur and how they will be measured;
   * the likelihood of the risk occurring;  
     the consequences of the risk occurring;

The risk is determined as one of the following categories:

* + Not business affecting (LEVEL 1).
  + Will detriment the internal operation of Retirement Capital but will not affect customers or other external agencies. (LEVEL 2)
  + Will detriment customers or external organisations. (LEVEL 3)
  + Has serious financial implications or may constitute a legal or information security breach. (LEVEL 4)
    1. Information Security Manager determines risk acceptance criteria as appropriate to the management systems.
  1. The risk assessor for the management system identifies risks to its management systems.
  2. The risk assessor for the management system analyses the risks to determine their relation to the risk criteria, including their likelihood and impact.
  3. The risk assessor for the management system evaluates the risks by comparing the level of risk identified in 3.5 above to the risk criteria established in 3.3.
  4. The risk assessor for the management system determines risk treatments:
     1. Treatments are selected by agreement with the appropriate process, risk or asset owner.
     2. Risk treatment options are as follows:
        1. Eliminate the risk by removing the activity affected by the risk
        2. Accepting the risk to pursue an opportunity
        3. Removing the source of the risk
        4. Changing the likelihood of the risk coming to pass
        5. Changing the consequences of the risk coming to pass
        6. Sharing the risk with another party or parties (such as via suppliers, insurance or other third parties)
        7. Accepting the risk by informed decision
  5. The risk assessor creates a risk treatment plan providing the following information:
     1. The reasons for selected treatments, including expected benefits
     2. Those responsible for approving the risk treatment plan
     3. Those responsible for implementing the risk treatment plan
     4. Proposed actions
     5. Resource requirements and contingencies
     6. Treatment performance measures and limitations
     7. Requirements for reporting and monitoring
     8. Timing and schedule for the risk treatment
  6. The risk treatment plan is agreed with the appropriate stakeholders.
  7. The risk treatment plan is implemented in accordance with Retirement Capital’s processes and the risk treatment plan itself.

**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.

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

This document is approved by the Chief Information Security Officer on the issue date shown and is issued on a version-controlled basis under his/her signature.

Signature: Date: 18/11/2019

**Change History Record**

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