# Scope

## The Information Security Policy, QEMS and ISMS arrangements are subject to development, review, evaluation and continuous improvement.

# Responsibilities

## The Director (CISO), who is the defined owner of the Information Security Policy, is responsible for its development, review and evaluation.

## Board of Directors is responsible for carrying out reviews in line with this procedure and for driving continuous improvement in the ISMS & QEMS.

## The Director (CISO) is responsible for convening meetings of the Board of Directors, either after there have been (or it is planned that there will be) significant changes in the organisational environment, business circumstances, legal conditions or technical environment and which is likely to have an impact on business continuity, or at least annually.

# Management review inputs

## Management reviews must consider:

### Status of actions from previous management reviews

### Changes in internal and external issues relevant to the ISMS & QEMS

### Information on ISMS & QEMS performance including trends in

#### Non-conformities and corrective actions

#### Monitoring and measurement evaluation results

#### Internal and external audit reports

#### Results and/or trends from the measurement of progress towards the fulfillment of information security objectives.

## ISMS performance must be considered, including

### Follow-up actions from previous management reviews

### Need for changes to the ISMS including its policy and objectives

### Opportunities for improvement

### Results of ISMS & QEMS audits and reviews

### Results of ISMS & QEMS audits and reviews of key suppliers and partners

### Techniques, products or services which could be used to improve ISMS & QEMS effectiveness

### Status of corrective actions

### Results of exercises and tests

### Risks or issues not adequately addressed in previous risk assessments

### Changes (internal or external) that could affect the ISMS & QEMS

### Adequacy of Information Security Policy

### Recommendations for improvement (internally or externally generated)

### Lessons learned

### Actions arising from disruptive incidents (post-incident reports)

### Emerging good practice and guidance

# Management review outputs

## Improving Retirement Capital’s assessment of the risks, including updating the risk assessment and business continuity and incident management plans.

## Examination of the information security objectives and modifying or improving them to ensure their fulfilment and that they can be usefully validated.

## Any variations to the scope of the ISMS & QEMS that may be required.

## Modifying or improving the policies and procedures and their effectiveness, including improvements to how effectiveness of tests is measured, and ensuring that any changes to business or business processes, or changes to statutory, regulatory or contractual requirements are accommodated.

## Update of risk assessments, ISMS & QEMS plans and related procedures.

## Modification of procedures and controls to respond to internal or external events that may impact on the ISMS & QEMS including changes to:

### Business and operational requirements

### Risk reduction and security requirements

### Operational conditions and processes

### Legal and regulatory requirements

### Contractual obligations

### Levels of risk; criteria for accepting risks

### Resource needs

### Funding and budget requirements

## Reviewing and improving how the effectiveness of controls and ISMS & QEMS measures is measured

## Improving the allocation of resources and responsibilities, including ensuring that the ISMS & QEMS has adequate resources, funding and budget

## Formulating and agreeing any changes to the Information Security Policy which would be necessary to give effect to any improvements identified

## Through all these activities, to continuously improve the ISMS & QEMS.

## The Director (CISO) is responsible for ensuring that the meeting is recorded, with the record signed by its chair, and required actions identified for follow up.

## The Director (CISO) is responsible for ensuring that

### results of management reviews are communicated as appropriate to relevant interested parties;

### appropriate actions are taken as a result of management review.

## Board of Directors must approve any changes to the policy at its next scheduled meeting and prior to its implementation.

## ***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.

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

This document is approved by the Board of Directors on the issue date shown 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 |
|  |  |  |  |
|  |  |  |  |