# Control of ISMS Management Reviews

## 1 Introduction

### 1.1 Scope

This procedure sets out <Short Name>'s arrangements for conducting periodic formal management reviews of our information security management system.

### 1.2 Revision History

| Revision | Date | Record of Changes | Approved By |
|---|---|---|---|
| 0.0 | [Date of Issue] | Initial Issue | |
| | | | |
| | | | |
| | | | |

### 1.3 Control of hardcopy versions

The digital version of this document is the most recent version. It is the responsibility of the individual to ensure that any printed version is the most recent version. The printed version of this manual is uncontrolled, and cannot be relied upon, except when formally issued by the <Document Controller> and provided with a document reference number and revision in the fields below:

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Document Ref. | | Rev. | | Uncontrolled Copy | X | Controlled Copy | |

### 1.4 References

| Standard | Title | Description |
|---|---|---|
| ISO 27000:2014 | Information security management systems | Overview and vocabulary |
| ISO 27001:2013 | Information security management systems | Requirements |
| ISO 27002:2013 | Information technology - security techniques | Code of practice for information security controls |

### 1.5 Terms and Definitions

"we" and "our" refer to <Short Name>.

### 1.6 Responsibilities

The <ISMS Manager> is responsible for all aspects of the implementation and management of this procedure, unless noted otherwise.

Managers and supervisors are responsible for the implementation of this procedure within the scope of their responsibilities and that reports are prepared as required by the <ISMS Manager> for circulation in good time before each meeting.

# 2 Conducting Management Reviews

## 2.1 Purpose

The <Senior Management Team> formally reviews the suitability, adequacy and effectiveness of the Information Security Management System through periodic 'Information Security Management Review Meetings'.

## 2.2 Frequency and attendance

Information security management review meetings are scheduled, organised and held, as a minimum, every <MRM Months> Months.

Those attending should include:

- <ISMS Manager>
- <HR Manager>
- MRM Attendees

*List the top management and other attendees*

If any of these attendees are unavoidably absent, they should send an alternate if at all possible.

Others attend as required by the <ISMS Manager> for a specific purpose or to meet the requirements of the agenda set out below.

Where an attendee or member of staff wishes to add an item to the agenda they should make that request to the <ISMS Manager> in good time.

## 2.3 Agenda

The agenda includes the assessment of opportunities for improvement, and the need for changes to, the information security management system, including the information security policy and objectives.

The agenda for the information security management review meeting, as a minimum, includes the following items:

**Actions from the previous meeting**

The <ISMS Manager> reports on the status of action itISMS from previous meeting. Items that are not completed are carried forward to the next meeting.

**Information security context**

The <Senior Management Team> / <ISMS Manager> highlights any changes to the external and internal information security context, including changes to the needs and expectations of interested parties, that are relevant to the information security management system.

The meeting reviews progress / changes to the Information Security Context Log.

**Information security management system**

The <ISMS Manager> reports on system performance data including monitoring, measurement, analysis, evaluation,

**performance**

nonconformities and supplier conformance/performance (where relevant).

**Identification, evaluation and treatment of risks**

The <ISMS Manager> reports on risk identification, risk criteria, risk evaluation, statement of applicability and the status of the risk treatment plan.

**Internal and external audits**

The <ISMS Manager> reports on the results of internal and external system audits. This includes: summaries of results for the current period and a comparison to the previous period, the frequency of negative findings against particular elements of the information security management system, and discussion of particularly important findings.

**Corrective and preventative actions**

The <ISMS Manager> reports on any high risk corrective/preventive actions implemented through the period and the status of pending actions.

**Information Security Incidents**

The <ISMS Manager> reports on any information security incidents.

**Emergency preparedness and response**

The <ISMS Manager> reports on tests and any changes, or proposed changes, to emergency / business continuity preparedness and response.

**Compliance obligations**

The <ISMS Manager> presents their information security compliance review and reports on any changes or proposed changes to compliance obligations.

**Awareness and Communication**

The <ISMS Manager> reports on communication / awareness activities, both internal and external and on any complaints or other correspondence received regarding our information security matters.

**Changes that affect the ISMS**

The <ISMS Manager> highlights any process, capacity, or other operational or organisational changes that affect the information security management system and proposes any consequential actions to update or modify the system.

**Training, development and resources**

The <HR Manager> reports on the status of training programs, the effectiveness of training provided, and meeting manpower, skill and other resource issues.

**Continual improvement**

The <ISMS Manager> presents data demonstrating progress toward achieving continual improvement goals, reviews current and completed improvement projects and proposes new improvement projects.

**Risks and opportunities**

The <ISMS Manager> ensures that the following information security related risk and opportunity updates are made and considered:

- all new, amended or proposed regulations
- changing expectations and requirements of relevant

interested parties

- new or modified activities, products or services
- advances in technology and science
- changing customer expectations

**Corporate policies, objectives, targets and KPI's**

The <ISMS Manager> reviews progress on any issues related to corporate information security policies, objectives, targets, metrics and key performance indicators.

Where information security objectives have not been achieved on time or inadequate progress has been made, the review investigates the causes and consider whether to:

- take additional actions, such as increasing resources or reallocating responsibilities
- drop or reduce the scope of the objective
- extend the due date for achieving the objective

New information security objectives may be established where it is desired or necessary to improve performance.

The management review also considers, from time to time and as appropriate, such issues as:

- the cost / benefit of information security performance
- appropriate measures of information security performance
- integration / overlaps of the information security management system with other operations and activities

### 2.4 Actions arising

The information security management review meeting may generate corrective and / or preventive action reports, or agree to take other actions so as to improve the information security management system, services, processes or resourcing.

### 2.5 Minutes

Outputs from the management review are recorded in the form of minutes where actions arising are clearly set out and include the appropriate personal responsibilities, timeframe and resources.

The <ISMS Manager> is responsible for ensuring that the minutes are prepared and issued in good time.

## 3 Records

Records retained in support of this procedure are listed in the Controlled ISMS Records Register and controlled according to the Control of Management System Records Procedure.