# Information Security Management System Operational Group Terms of Reference

| 1. Document information | |
|---|---|
| **Document name** | SLMS-IG35 Information Security Management System Operational Group Terms of Reference |
| **Author** | Trevor Peacock |
| **Issue date** | 07/02/2020 |
| **Approved by** | Chair of SLMS IGSG |
| **Next review** | 06/02/2021 |

| 2. Document history | | |
|---|---|---|
| **Version** | **Date** | **Summary of change** |
| 0.1 | 12/05/2016 | First draft for discussion |
| 0.2 | 13/05/2016 | Incorporated comments from Anthony Peacock |
| 1.0 | 09/06/2016 | Approved by Chair of SLMS IGSG |
| 1.1 | 22/09/2016 | Added review of incidents to key responsibilities |
| 1.2 | 21/02/2018 | Amended Annex A names of role holders |
| 2.0 | 17/04/2018 | Approve by Operational Management Group |
| 2.1 | 06/02/2020 | Updated standing agenda items to include: root cause analysis, lessons learned from incidents, internal and external developments affecting the ISMS |
| 3.0 | 06/02/2020 | Approved by IG Steering Group |

## 1.0 Objective

The purpose of the ISMS Operational Group is to plan, operate, monitor and improve the Data Safe Haven ISMS. This group provides assurance and reports to the SLMS Information Governance Steering Group (IGSG), who have strategic oversight of the ISMS

## 2.0 Composition

### 2.1 Membership

Set out in Appendix A, membership will include management representation from WIS, IG & Research and ISG. Other members of those teams will attend as appropriate

### 2.2 The Chair

The Chair will be independent of the teams listed and will ensure the meetings run to time and adhere to the agenda. The Chair will present a summary of the group's activities at each IGSG, supported by other members of the group as required

## 3.0 Meetings

The focus of the meetings will be decisions that require input from all parts of the team. In order to be effective, initial discussions will take place and information be provided outside of the meeting.

### 3.1 Frequency

This group will meet at least once per term to fulfil its remit and to provide reports to the IGSG as a regular IGSG agenda item. Reports are taken to the IGSG by the chair.

### 3.2 Agenda and papers

The group will discuss each time that it meets:

- The previous meeting's minutes and actions
- Operational metrics for the Information Security Management System
- Incidents, major changes, audit findings and lessons learnt
- Internal and external developments affecting risks relating to the ISMS
- AOB

### 3.3 Periodic activities

The OMG will oversee the performance of routine ISMS activities, such as:

- Review of outstanding actions
- Root cause analysis and assignment of mitigating actions
- Review of risks
- Review of SoA
- Review of documentation
- Annual self assessment of performance against Terms of Reference

### 3.4 Actions/decisions

- Minutes of the meetings will be recorded and made available to IGSG and Operational Management Group
- All new actions will be recorded to the Action Tracker
- Decisions will be reported at, or if appropriate, escalated to IGSG

### 3.5 Quorum

The Chair and one member from each of WIS and IG & Research

## 4.0 Remit

### 4.1 Key responsibilities

Ensure that the ISMS is operated effectively:

4.1.1 Determine, review and monitor suitable operational metrics that support the ISMS objectives
4.1.2 Review audit outcomes and formulate appropriate responses
4.1.3 Review incidents and where appropriate, ensure that outcomes feed into the risk assessment
4.1.4 Ensure consequences of planned change are fully considered
4.1.5 Review risks and ensure risk assessment, Risk Treatment Plan and Statement of Applicability remain current
4.1.6 Ensure documentation is reviewed at appropriate intervals
4.1.7 Monitor and report on trends and changes affecting the ISMS
4.1.8 Escalate risks to the IGSG as appropriate

### 4.2 Accountability

The group is accountable to the Chair of the IGSG

### 4.3 Authority

The group has delegated authority from the IGSG to operate and amend the ISMS within this Terms of Reference
Where there is a change to the ISMS risk profile that requires escalation, this will be via the IGSG or in time-critical cases, the SIRO

## 5.0 Evaluation and review

To ensure that the group is fulfilling its duties, it will:

**5.1** Undertake an annual self-assessment of its performance against this Terms of Reference, which shall be reported to IGSG
**5.2** Provide any information the IGSG may request to facilitate its review of the group's performance and its members
**5.3** These Terms of Reference will be reviewed annually and any changes will be approved by the IGSG

**Appendix A – ISMS Operational Group Membership**

| Name | Job title | Role within group | Team within ISD |
|---|---|---|---|
| Tim Machin | Head of IT, Faculty of Population Health Sciences | Chair, Internal Audit | IT for SLMS |
| Anthony Peacock | Head of Windows Infrastructure Services | Service Owner, Data Safe Haven | Windows Infrastructure Services |
| Jazz Marsh | WIS Infrastructure Team Manager | Service Operation Manager, Data Safe Haven | Windows Infrastructure Services |
| Trevor Peacock | Head of Information Governance & Research, and Deputy Head of Information Security | Service Operation Manager, Data Safe Haven IG and ISMS | IT for SLMS |
| Jack Hindley | Information Governance Officer | Service Operation Manager, Data Safe Haven training | IT for SLMS |
| Robert Maughan | Head of Information Security | Information security / policy | Information Security Group |