Internal Audit Policy

Brunel University London

***An ISO/IEC 27001:2013:** Aligned Document - Implementing Cyber and Information Security Best Practice*

Internal Use Only

Mick Jenkins
Chief Information Security Officer

Document History

Version	Author	Comments	Date
V 0.1	Andrew Clarke	Initial Draft	22/02/2018
V 0.2	Andrew Clarke	Formatting changes	06/03/2018
V 1.0	Andrew Clarke	MJ: Add CIO approval, responsibilities	08/03/2018

Document Approval

This document requires the approval from BUL as defined in the ISMS Compliance document.

MG Jenkins	
Document Owner: Michael Jenkins	Document Approver: Pekka Kahkipuro
Chief Information Security Officer	Chief Information Officer

Document Distribution

Name	Title	Version	Date of Issue

Contents

1. About this document

1.1 Purpose of Document

This Policy establishes the area within Brunel University London covering Internal Audits of the Integrated Management System to determine its effectiveness.

Please refer to Brunel University London ISMS Document BUL-GLOS-000 - SyOPs Glossary of Terms for the glossary of terms, acronyms and their definitions for the suite of Brunel University London ISMS documentations.

1.2 Responsibilities

Table 1 – responsibilities

Title / Role	Description
Internal Auditors	Are responsible for conducting audits, opening & closing meetings, audit summary, report.
Chief Information Security Officer	Is responsible for planning Internal Audits and providing executive level visibility of risk management and risk exposure from audit programmes.
Cyber & Information Security Manager	Has overall management responsibility for the preparation, co-ordination and execution of the Internal Audit Plan, updating the corrective action register, tracking, report and closure
Senior Information Risk Owner	SIRO is responsible for the ownership of the organisation's information risk, acts as an advocate for information risk on the Executive Board, and provides advice to the board and Council on the Information risk governance and risk exposure.
Information Asset Owners	Information Asset Owners (IAOs) are Directors and Heads of Departments held accountable for the protection of particular Information Assets[1]. They are responsible for implementing ISMS policy within their business units and supporting ISMS audits. IAO's are also responsible for formulating corrective actions and to ensure timely closure of actions on detected non-conformances and their root cause(s).
Information Asset Custodians	Information Asset Custodians are IT services and / or locally appointed persons responsible for the technical environments and IT systems holding information assets.

1.3 ISO 27001 - Conformance

This section indicates the University Conformance to ISO27001:2013.

[1] The named asset owners are aligned to the ISMS information asset registers that have been completed within BUL.

University ISMS Control Number	SOA – Number A18 – Compliance
ISO 27001:2013 Conformance Control	Information Classification Objective A.18.1 Internal Audit policy

1.4 Scope

This policy is applicable to all University information systems and to all Information Asset Owners (IAO's) and users (whether employees, contractors or temporary staff and third party users) and all owners and custodians of University information assets or systems that are governed by ISMS Policies.

1.5 Objectives

The objectives of this policy are to:

- Determine the effectiveness of the University's management system by ensuring the conformance of processes to the relevant policies, standards, legislation or regulations in all the activities carried out by the University;
- Provide SIRO and executive board with assurance that activities are being carried out in accordance with policy and information security risk is being managed effectively;
- Systematically plan and effectively implement the internal audit programme covering the defined internal audit scope;
- Ensure that necessary actions are taken without undue delay to eliminate detected non-conformance and their root causes;
- Identify opportunities for improvement and input to management review;
- Maintain the Internal Audit records;

1.6 References

- REC 18MS-1A Internal Audit Schedule
- DOC 18MS-2 - Corrective And Preventive Action
- REC 18MS-2A Internal Audit Lead Sheet

2.0 Internal Audit Policy

2. Policy

2.1. Internal auditors & training

2.1.1. Internal Auditors shall be familiar with and competent in ISO 27001 audit techniques and shall have completed a training programme covering the conduct of Internal Audits.[2]

2.1.2. A Register of Internal Auditors shall be maintained and retained by the Cyber & Information Security Manager.

2.1.3. Internal Auditors shall not be asked to carry out audits in areas in which they normally work, or against processes for which they are responsible for.

2.2. Audit programme

2.2.1. Internal audits shall be carried out according to a defined programme. This programme shall be reviewed and approved during the management review. The Cyber & Information Security Manager shall produce the audit plan which shall cover the whole of the University and shall specify the parts that are covered by the various certificated management systems ISO 27001, ISO 14001, ISO 9001 and BS25999/ISO22301.

2.2.2. The programme shall ensure that areas of critical importance are audited more frequently and shall include areas with a previous high amount of audit findings.

2.2.3. The Internal audit programme shall be based upon identified key processes and will satisfy both internal University requirements and the requirements of relevant standards.

2.2.4. Each key process of the management system shall be audited at least once in two years.

2.2.5. The auditor shall ensure the whole of any standard's requirements are covered in the audit plan by identifying which areas of any appropriate standard have been reviewed during each process, and ensure these have been recorded.

2.2.6. The audit programme shall be made available here (REC 18MS-1A Internal Audit Schedule).

[2] And have attended an ISO 27001 lead implementer or lead auditor course. Business unit auditors will be trained by such qualified persons.

2.3. Audit Conduct

2.3.1. **"Opening meeting"** is the first activity in the audit cycle. The Chief Information Security Officer conducts the opening meeting attended by the IAO and or management of the college, directorate or department, and the auditors.

2.3.2. The Opening meeting covers:

- The scope of the audit cycle, projects and functions to be audited;
- The specific audit scope/criteria to be covered/audited;
- The audit process awareness including reporting and report closure requirements;
- Date & time of the review meeting;

2.4. Audit Preparation

2.4.1. **"Conducting the audit"**, the selected Lead Auditor shall:

- Open the audit process by meeting the auditee, and explain the purpose and duration of the audit;
- Explain the content of the audit and identify which areas/documents shall be audited;
- Explain all the auditing documentation to be used, including the resulting improvement opportunity process;
- Familiarise themselves with the findings of previous audits along with audits held at other business units and determine any specific area to be audited and checks to be made;
- Take into account any special business requirements and additional controls in place;
- As part of good practice, read appropriate defining documents beforehand;

2.5. Audit Conduct

2.5.1 Through questioning, listening and checking objective evidence, the auditor assesses whether the work is being conducted in line with the audit objectives.

- Where compliance is being audited and there is significant lack of compliance or compliance monitoring, the auditor can promote a more positive result by illustrating the business benefits of compliance;
- Auditors must balance objectiveness in assessing compliance with pragmatism derived from the University Department, College and commercial environment of the case in question. Risk assessment by the auditor in conjunction with the audited area should play an important part in agreeing the actions to be taken over findings;
- Notwithstanding the above need for balance and pragmatism, auditors and the audited function must ensure that the University's ISO27001:2013 aspiration is not prejudiced by a lack of appropriate action on any non-conformances or issues found in audit;

- Execute the audit by carrying out a review of the identified key process. Interviewees, documents seen, samples of records taken and any other audit findings, shall be recorded (BUL-REC 18 MS-2A Internal Audit Lead Sheet);
- Record any opportunities for improvement, and observations, on authorised documentation only;

2.6. Audit Reporting

2.6.1. The results of completed audits shall be summarised by the Lead Auditor on an Internal Audit Report Lead Sheet (REC 18MS-2A) along with any non-conformities noted;

2.6.2. Part 1 of the Audit Lead sheet shall be completed by the Lead Auditor, providing a management summary and including a suggested root cause;

2.6.3. Part 2 shall be completed by the Auditing team, identifying and detailing the non-conformities with impact and clause number along with the Operational person responsible for correcting the root cause;

2.6.4. After completing parts 1 and 2 of the notice, a copy shall be given to the Auditee, the original being filed by the auditor;

2.7. Audit Close

2.7.1. At **"Audit Close"** the Lead Auditor calls a closing meeting upon completion of the audit, to summarises the audit findings, inform the Auditee, of the audit findings, and to agree time-scales and content for any improvement opportunities (including corrective actions), implementation and responsibilities;

- Any non-conformances raised shall be subject to the corrective action policy;
- The concerned managers and/or business process owners shall ensure that the non-conformances are closed by means of implementing the identified corrective actions. A follow up audit may be necessary;
- The Cyber & Information Security Manager shall prepare a summary of non-conformances and submit the analysis report to the Chief Information Security Officer at Management Review;

Major NC

A nonconformity that is either:

- The absence (omission, not addressed) or total breakdown (commission, failure, not implemented) of a system to meet a specified requirement. A number of minor nonconformities against one requirement can represent a total breakdown of the system and thus be considered a major nonconformity.

- Any noncompliance that would result in the probable shipment of a nonconforming product. Conditions that may result in the failure of or materially reduce the usability of the products or services for their intended purpose.
- A noncompliance that, in the judgment and experience of the auditor, is likely to either to result in the failure of the management system or to materially reduce its ability to assure controlled processes and products.
- The IMS manager department consolidates all the audit findings and analyses them across the University.

Minor NC

It may be either:

- A nonconformity that, based on the judgment and experience of the auditor, is not likely to result in the failure of the management system or reduce its ability to assure controlled processes or products.
- A failure in some part of the function/project management system relative to a specified requirement.
- A single observed lapse in following one item of a function/project management system.

Observation

Any other relevant finding or opportunity for improvement that is not a major or minor non-conformance may be raised as an observation.

2.8. Follow Up Audits

2.8.1. Follow up audits shall be scheduled to be carried out within 30-60 working days of improvement action implementation date, to confirm the execution of any corrective actions;

2.8.2. If the follow-up audit still identifies further improvement opportunity, this shall be escalated to the Chief Information Security Officer and Information Asset Owner for review;

2.8.3. If the non-conformance is a critical issue the follow up shall be carried out within 24 hours and reported directly to either CSIRT or the Information Asset custodian (IT services).

2.8.4. All non-conformance, observations or areas for improvement shall be recorded;

2.9.Management Review

2.9.1. Findings in Internal Audit reports and associated corrective actions will be reviewed;

2.9.2. The internal audit plan will be reviewed by information security management (and information assurance board if formed by BUL) at least once a year. When undertaking the review of the audit plan, criticality of key processes and occurrence of non-conformities within each process shall be taken into account when assessing the priority and frequency of future audits;

Appendix A

Definition of Terms

Opportunity for Improvement

Information on matters that have come to light during the audit that management is well advised to consider. Although formal compliance to the management system standard is adequately met, based on auditor experience and knowledge, additional effectiveness or robustness might be possible with a modified approach to prevent a potential nonconformity in the future. An opportunity for improvement may be reviewed at a subsequent audit.

Minor Nonconformity

A single identified gap or a concern in meeting a requirement of the management system standard, which would not in itself raise significant doubt as to the capability of the management system to achieve its objectives. The identified gap is required to be resolved at a time mutually agreed between the auditor and responsible management representatives. **The remediation actions will be verified by the auditor at the agreed time or at the time of the next audit.** When multiple minor nonconformities are identified in the same logical area of the management system standard, the auditor may conclude that this constitutes a major nonconformity.

Major Nonconformity

An absence of, or the repeated failure to implement and maintain, one or more required mandatory management system standard element, ***or*** a situation which would, on the basis of objective evidence, raise significant doubt as to the capability of the management system to achieve its objectives. The auditor will require substantive proof **within an agreed period no longer than 90 days** that such major issues have been fully resolved before providing a positive conclusion of the audit.