**Document Control**
Reference: BUL-ISMS-001
Issue No: 1.0
Issue Date: 18/01/2017

# ISMS Manual:

## Information Security Management System

# Brunel University London

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

Internal Use Only

**Mick Jenkins**

Head of Security and Emergency Planning

# Document Information.

## Confidentiality

This document is intended for internal use within Brunel University London. It may contain information of a sensitive nature, disclosure of which could lead to a loss of commercial advantage over our competitors. Therefore do not discuss any material contained herein with anyone other than Brunel University London employees without the express permission of management.

### Distribution

| Role | Name | Department / College | Location |
|---|---|---|---|
| | | | |

### Amendment Record

| Issue Status | Version | Date | Actioned By | Description |
|---|---|---|---|---|
| Draft | 0.1 | 12 September 2016 | Andrew Clarke | Development |
| Final | 1.0 | 18 January 2017 | Andrew Clarke | Approval from Exec |

### References

| Nr | Reference | Document Ref | Version |
|---|---|---|---|
| 1 | Information technology – Security techniques – Information Security management systems – Requirements | ISO/IEC 27001 | 2013 |
| 2 | Information technology – Security techniques – Code of practice for information security management | ISO/IEC 27002 | 2013 |
| 3 | Information technology – Security techniques – Information Security Risk Management | ISO/IEC 27005 | 2011 |
| 4 | Information Security Policy | ISP01 | 0.1 |
| 5 | UCISA Security Toolkit | | V3 |

### Approvals.

The contents of this document are confidential to Brunel University London (BUL). Proprietary information presented in this document may not be used without written consent from BUL and remains the exclusive property of BUL unless otherwise agreed to in writing.
This document requires the approval from BUL as defined in the ISMS Compliance document.

| | |
|---|---|
| Document Owner: Andrew Clarke | Document Approver: Paul Thomas |
| Cyber & Information Security Manager | Chief Operating Officer |

**Supporting Material**

| Nr | Reference |
|---|---|
| 1 | ISO/IEC 27001:2013 Information Security Standard |
| 2 | BUL Information Security Policy<br>BUL Physical Security and Environment Policy<br>BUL Physical Security and Environment Standard<br>BUL HR Information Security Policy<br>BUL HR Information Security Standard<br>BUL Acceptable Use Policy<br>BUL Information Handling and Protection Policy<br>BUL Information Handling and Protection Standard<br>BUL 3rd Party Management policy<br>BUL 3rd Party Management Standard<br>BUL Business Continuity Management Policy<br>BUL Business Continuity Management Standard<br>BUL IT Acquisition, Development and Maintenance Policy<br>BUL IT Acquisition, Development and Maintenance Standard<br>BUL IT Operations and Network Policy<br>BUL IT Operations and Network Standard |
| 3 | BUL Information Security Risk Assessment Methodology<br>BUL Information Security Training and Awareness Process<br>BUL Information Security Incident Management Process<br>BUL Information Security Internal Audit Process<br>BUL Information Security Management Review<br>BUL Information Security Forum<br>BUL Information Security Action Management<br>BUL Document and Record Control |

**Glossary** (Terms and abbreviations are defined below)

| Abbreviation | Description |
|---|---|
| BUL | Brunel University London |
| ISMS | Information Security Management System |
| SOA | ISO27001:2013 Statement of Applicability |

# Contents

# 1. Management Summary

It is the intention of the Brunel University London Senior Management to achieve and maintain compliance with ISO/IEC 27001:2013 Information Security Standard for the following reasons:

The University has an obligation to the staff, students and suppliers to protect the confidentiality, integrity and availability of information assets.

- Compliance will highlight to the educational community the strong commitment to information security & promote the University as a leader in this field.
- To ensure business continuity and minimise business damage by preventing and minimising the impact of security incidents.
- To facilitate business improvement through the adoption of secure business practice and business management.
- ISO/IEC 27001 will assist with the delivery of the requirements outlined within the Data Protection Act 1998 and the General Data Protection Regulation (GDPR).

This document defines the scope of the Information Security Management System (ISMS) for Brunel University London. It clearly identifies those parts of Brunel University London for which compliance is sought, and also which elements are specifically outside the scope. The Statement of Applicability scope definition is the basis upon which the plan and size of the extent of the assessment is based.

The Information Security Management Forum oversees reviews, develops and improves the overall ISMS within Brunel University London.

# 2. Introduction

## 2.1 Introduction

Brunel University London needs to protect the confidentiality, integrity and availability of important information assets and ensure that facilities provided by the University are available for educational operation. The University works in conjunction with many parties which can involve having access to large amounts of information; the loss, breach or unavailability of this information would have very serious repercussions to the University and loss of reputation and third party confidence.

Brunel University London aims to be recognised as a University adhering to the highest level of Information Security best practice. Compliance to ISO 27001 helps to fulfil this objective.

## 2.2 General Requirements

The ISMS has been defined based on the following PDCA Model:
[

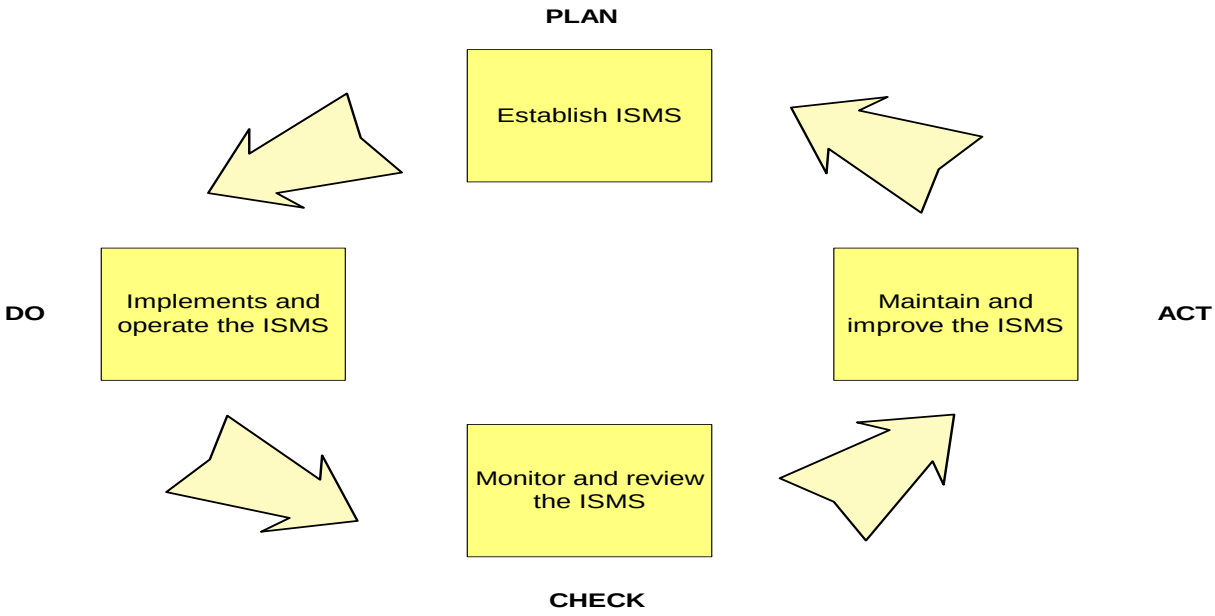


**Figure 1 PDCA Model**

As part of the Management Review process, the ISMS shall be reviewed and, when required, changes shall be made to the ISMS in order to ensure that it continues to meet requirements.

# 3. ISMS Objectives

The objective of the ISMS is to support the security policies of Brunel University London, and implement local Information Security processes that are aligned with industry best practice. Brunel University London's aim is to understand and manage the risks we face, and consequently protect our information and services we provide.

## 3.1 Security Policy and Objectives

The purpose of the Security Policy is to protect the Brunel University London and both our academics and students **Information Assets and Services** from all threats, whether internal or external, deliberate or accidental. Brunel University London will undertake regular risk assessments on our information, physical security and services provided by Third Parties.

It is the Policy of Brunel University London to ensure that:

- Information will be protected against unauthorised access;
- **Confidentiality** of Brunel University London and Customer information will be assured;
- **Integrity** of information will be maintained;
- **We will manage our systems** in accordance with best Practice;
- **Regulatory** and **legislative** requirements will be met;
- **Business Continuity plans** will be produced, maintained and tested to ensure **availability;**
- **Information security training** will be available to all staff;
- **All breaches of information security**, actual or suspected, will be reported to, and investigated by **the Cyber and Information Security Manager**.

The Information Security objectives will be monitored on a quarterly basis, but will be formally reviewed on a yearly basis as part of our Management review. Key ISMS performance targets will be identified and subsequently monitored, measured and reported to the Forum and Senior Management Team.

# 4. ISMS Scope Statement

The Information Security Management System covers Brunel University London and Supplier information assets and systems.

This includes information, data, software, equipment such as laptops / mobile devices, network components and communication networks owned or operated by or for Brunel University London as well as manual and paper based systems.

## 4.1 Locations

The locations in scope are the Brunel University London office at
Kingston Lane Uxbridge;

## 4.2 The Assets

Brunel University London's information assets may be owned, leased, hired, developed in-house or purchased and includes all computing facilities.

A list of all assets covered by this scope can be found within:
Information Asset list
IT Asset list

In Summary the following key information assets are covered:

- Information about people including BUL staff and Students;
- Information about 3rd parties including potential and existing suppliers;
- BUL University Confidential Information included in the Security Aspects Letter;
- BUL Project Details including requirements, finance, project management and implementation and transformation plans;
- BUL University Confidential Information including contracts, future plans, etc.
- BUL University Confidential Information including finance, legal and regulatory details;
- BUL Infrastructure information including building and the BUL Secure Systems;
- BUL Policies, Processes and Procedures within the Business and Information Security Management System;
- BUL Management System Records such as Risk Assessment, Internal Audits, Performance Reviews.

## 4.3 Responsibilities

The Information Security Management System applies to all personnel working for or with Brunel University London, or who have been authorised to access Brunel University London or their customer's information systems. This includes all management, employees, contractors, temporary staff, consultants, agents and client personnel.

The **Cyber and Information Security Manager** as **Information Security Management Representative** is responsible for the overall direction and commitment to the Management System by ensuring an effective, two way communication between the Senior Management & Information Security Forum and for providing adequate resource.

All internal functions (e.g. IT, Facilities and HR) are responsible for ensuring that all the systems, infrastructure and services provided to the University comply with the relevant policies, processes procedures and standards documented within the Management System.

All Managers are directly responsible for implementing the relevant policies, processes procedures and standards within their business areas as relevant to their business, and for adherence by their staff.

## 4.4 Dependencies

The Information Security Management System covers Information Services which are contracted out or outsourced to other parties but which are operated for or on behalf of Brunel University London.

The following key Information Systems, Services, Controls and processes are provided and managed by 3rd Parties:

- ISPs
- Cloud Service Providers

Brunel University London will monitor and audit all 3rd Party's compliance to Brunel University London Policies as appropriate

## 4.5 Scope Overview

The Scope for the Initial compliance is Computer Centre, John Crank, Kingston Lane, Uxbridge UB8 3PH. This includes all staff and services utilised on the contract.

Staff and services not based at the mentioned locations will be outside the scope but will still be required to comply with the policies and procedures.

**Figure 2 High Level University Charts (required)**

**Figure 3 Network Topology Diagram (required)**

# 5. ISMS Documentation

All documents that form part of the Information Security Management System will be controlled and approved. As a minimum, the documents will be approved by the Security Forum and issued by the Cyber and Information Security Manager:

- Brunel University London - Information Security Policy;
- Brunel University London - ISMS Manual;
- All documents referenced in the Statement of Applicability;
- All documents referenced in the ISMS Manual;
- All documents referenced in the ISMS Document Register.

The Information Security Forum is responsible for approving this ISMS manual and all other supporting Policies and Procedures, and all subsequent issues. Changes to ISMS documentation, policies and procedures will be reviewed, authorised and published by the Information Security Forum.

The master released copy of all ISMS documents are held electronically by the Cyber and Information Security Manager, who will ensure that all appropriate documents are available and legible for the relevant users, and will ensure that changes and current revision status of all ISMS documents are maintained.

Once a revision has been adopted and released, the previous version is archived into a separate area (accessible by the Cyber and Information Security Manager) for reference purposes only. When informed of revisions (see above) Staff and Users will be informed that any previous versions are obsolete and that hard or electronic copies should be disposed in accordance with their classification.

## 5.1 ISMS Documentation

All records/documentation in relation to the ISMS will be securely maintained for three years and in accordance of the Data Protection Act 1998, and Freedom of Information Act 2000.

Records must be available to show evidence of conformity to requirements, performance of the ISMS and occurrence of incidents.

The following records must be maintained as part of the PDCA Cycle defined within the ISMS in accordance with ISO/IEC 27001:2013:

- Incident (& weakness) Reports, Findings and Recommendations
- Management Review Results and Recommendations
- Internal audit programme, preparation and reports of findings,
- Security Forum and /or Management approval of recommendations from Incident Reports, Management Reviews and Internal Audits
- Risk Assessment Programme and Risk Treatment Plans
- Results of corrective actions taken in response to Incidents, Management Review, Internal Audit and Performance Monitoring
- Results of preventive actions taken in response to Incidents, Management Review, Internal Audit and Performance Monitoring
- ISMS Monitoring and Metrics Programme, Performance Analysis and Recommendations
- Training records of education, training, skills, experience and qualifications.

Retained records will be labelled and identified accordingly.

Other records must be maintained to show that the applicable controls within Annex A of ISO/IEC 27001:2013 have been implemented. These records may be in hard copy or electronic form, they may be documents, reports, forms or database entries.

Examples of these records are listed below:-

- Evidence to show compliance to Access Policy such as:-
- Access Requests / Authorisation (Including changes / removal )
- 3rd party risk assessments / access approval
- Remote access authorisation
- Logs of Access to Sensitive areas (e.g. Data Centre room access )
- Visitors Book
- Removal of equipment Log
- Vulnerability Scan Log
- Backup Logs

Evidence to show monitoring / technical compliance:-

- Event Logs
- Fault Logs
- Help Desk Logs / Reports

Evidence to show management approval of processes:-

- New Information Processing
- Purchasing new Equipment / Systems
- System Change Management
- Acceptance Testing

# 6. University

## 6.1 Management Framework

Brunel University London has established an ISMS to ensure business continuity by protecting the Confidentiality, Integrity and Availability of information and to minimise business damage by preventing and minimising the impact of the security incidents.

It is University policy to ensure that all information security breaches will be investigated.

The Information Security Forum has been established to ensure that there is clear direction and visible management support for security initiatives and commitment to Information Security.

All managers and their employees are responsible for ensuring that the policies are implemented with their respective departments. The Information Security Forum has direct responsibility for maintaining the policies and providing guidance on its implementation.

The Cyber and Information Security Manager is responsible for implementing policy within Brunel University London, supported by the Information Security Forum. As part of the Information Security Forum the members will approve and accept any risk criteria as identified during any risk assessment.

The operation of the ISMS will be authorised by the Security Forum as appropriate and implemented by the Cyber and Information Security Manager, or delegated to members of Brunel University London.

## 6.2 Management Responsibility

A High Level Security Policy has been created and authorised by the Information Security Forum and the Brunel University London Senior Management. All other policies have been created and authorised by the Information Security Forum, A copy of these policies has been communicated to all users and is freely available from the Cyber and Information Security Manager.

The Information Security Policy establishes the objectives for information security.

Brunel University London Senior Management has appointed a Cyber and Information Security Manager and fully authorises and supports the implementation of this Information Security Management System:

- The Cyber and Information Security Manager for consideration by the Security Forum will recommend processes and other security initiatives that will improve the effectiveness of the ISMS.
- All enhancements to the ISMS will be documented with the Security Forum minutes and reviewed by the Brunel University London Senior Management Team.

The controls selected within the SOA from ISO/IEC 27001:2013 will be implemented in accordance with the risk treatment plan. The Cyber and Information Security Manager will conduct assessments to ensure that the controls are working successfully.

The Cyber and Information Security Manager will undertake a full risk assessment on all information assets at least yearly. All feedback from interested parties will be discussed at the Security Forum.

## 6.3 Identification of Legal, Regulatory & Contractual Requirements

The University's legal department will review all contracts, as well as any applicable legal and regulatory requirements to ensure the University is able to comply with any such requirements. Where necessary Brunel University London Senior Management or legal department will liaise with the Cyber and Information Security Manager to facilitate any information security requirements.

The high-level policy states that, legislative requirements will be adhered to. For the purpose of this scope legal requirements include, but are not limited to:

### 6.3.1 Data Protection Act, 1998

The Act obliges Brunel University to register use of "personal data" and "sensitive personal data". The Act imposes limitations on access to that data, including requirements for the destruction of data. The Seventh Principle addresses security directly. It requires data users to see that:

*"Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data."*

Brunel University London has an Information Access Officer to oversee the specific administrative implications of this particular Act.

### 6.3.2 Copyright, Design and Patents Act, 1988

Software must only be used in accordance with the terms of its licence. Generally, the making of copies without the owner's consent is forbidden and is a criminal offence.

The Act states that the copyright of bespoke software remains with the author, unless the Contract specifies otherwise.

### 6.3.3 Computer Misuse Act, 1990

The three main offences concern unauthorised access to IT systems, software or data. Severity of punishment depends whether the intent was to gain access only, to commit further offences after gaining access or to make a modification to "computer material" e.g. to introduce a virus, or alter data for gain.

### 6.3.4 Common Law

Normal civil responsibilities also apply. Information must only be used for the purpose for which it was intended. Reasonable steps need to be taken to safeguard it bearing in mind the damage which its loss, corruption, inaccurate or unauthorised dissemination might cause.

### 6.3.5 Other Legislation

Should other relevant laws be passed, they will apply whether or not specifically mentioned in this document.

## 6.4 Information Security Forum

An Information Security Forum has been established to ensure that there is clear direction and visible management support for security initiatives.

The forum is dedicated to the principles of Information Security best practice standards initiatives.

### 6.4.1 Information Security Forum Mission

The Information Security Forum is a focus for consideration of security and continuity issues which may affect Brunel University London ability to provide a confidential and robust service to customers. The forum is in place to provide a strategic lead to University wide security and continuity improvement and maintenance programmes. The long-term goal is to reduce the amount of time, money and effort involved in resolving security breaches, continuity issues and incidents by introducing management controls that prevent or avoid them.

### 6.4.2 Information Security Forum Scope

The Forum will consider, debate and set policy on security issues that affect the University. This includes security in terms of People, Physical, Procedural, Information and Technical (IT) protection arrangements.

The Forum scope is to include the following:-

- Review of major cyber security breaches and developing protective strategies to prevent their reoccurrence
- Provision of a strategic lead to Brunel University London security improvement programmes
- Reviewing existing and developing new security policies in line with ISO/IEC 27001 key controls
- Establishing small working groups to tackle special security projects
- Promotion of security awareness throughout the University
- Co-ordination of new security initiatives
- Review issues which may impact upon legal & regulatory security requirements
- Monitor and report on new or perceived security issues
- Improvement to the ISMS
- Review of corrective and preventive actions resulting from Audit
- Providing the information / reports to the Management Review

### 6.4.3 Membership of the Information Security Forum

Membership of the Forum comprises of the following representatives

- A Representative of the Senior Management Team
- Cyber and Information Security Manager
- Representatives from each business area

Representatives from the following supporting services

- System Manager (IT)
- Individual Facilities / Building Managers
- Procurement Managers
- HR Manager
- Legal Services

Invitations will be extended to other representatives as appropriate.

### 6.4.4 Assumptions

Representatives of the forum will be empowered to speak authoritatively on behalf of their management.

Where funds or resources become an issue, the forum, through the Cyber and Information Security Manager, will raise these matters through existing Brunel University London management structures for resolution.

#### 6.4.5 Reporting

Minutes of the Forum will be sent to all members of the Forum and presented at the Management Review.

#### 6.4.6 Frequency of Meeting

The Information Security Forum will meet at least twice per year to discuss information security issues and revisit policy documents, which require review. However, the forum may be called together at any time in the event of a significant security issue, which requires the forum's attention.

Additionally it is intended that a 'subset' of this forum can be drawn together to discuss or agree specific security issues. These will then be communicated to the rest of the forum via e-mail.

#### 6.4.7 Standing Agenda

The Information Security Forum will review the ISMS as a standing agenda.

As a minimum the following documentation will made available for review.

- External Audit Reports
- Risk Assessments
- Internal Audit Reports
- Non Conformance Reports
- Security Incidents
- ISMS Performance Reviews
- Control Performance Reviews
- Previous Information Security Forum Minutes

## 6.5 Resources

The Brunel University London Senior Management has authorised the Cyber and Information Security Manager and the Security Forum to manage resources and requirements to manage, implement, maintain and review this ISMS.

The Cyber and Information Security Manager and the Forum will manage resources to ensure that information security procedures support business requirements, and that adequate security is maintained with the correct application of implemented controls. The Cyber and Information Security Manager and the Information Security Forum will also ensure that personnel implementing ISMS controls and requirements have the necessary competencies and training.

Additional resources and requirements may be required to deal with specific issues, or to tackle new incidents / situations as they arise, or to review and improve the ISMS, which will be reviewed and managed by the Cyber and Information Security Manager and / or the Information Security Forum.

Where significant additional resources or funding is required, the Cyber and Information Security Manager will review and agree these requirements with the Senior Management Team.

## 6.6 Management of 3rd Party Products & Services

In the event that 3rd parties require access / exchanges to Brunel University London Information & Assets a further Information Security Risk Assessment will be carried out to determine what controls need to be put in place and built into any Contracts, Service Level Agreements or Exchange Agreements. All 3rd parties requiring access to IT Systems must undergo a **Vendor Assessment.**

A **Risk Assessment Programme** will ensure that all risk assessment takes place for all suppliers, additionally where considered appropriate Internal Audits of 3rd Parties will be included in the **Annual Internal audit programme.**

Brunel University London aims to build partnership relationships with its suppliers and business partners and will work with them to build confidence in the quality of the products or services they are providing, thus reducing the need for inspecting products / services received from suppliers.

# 7. ISMS Overview

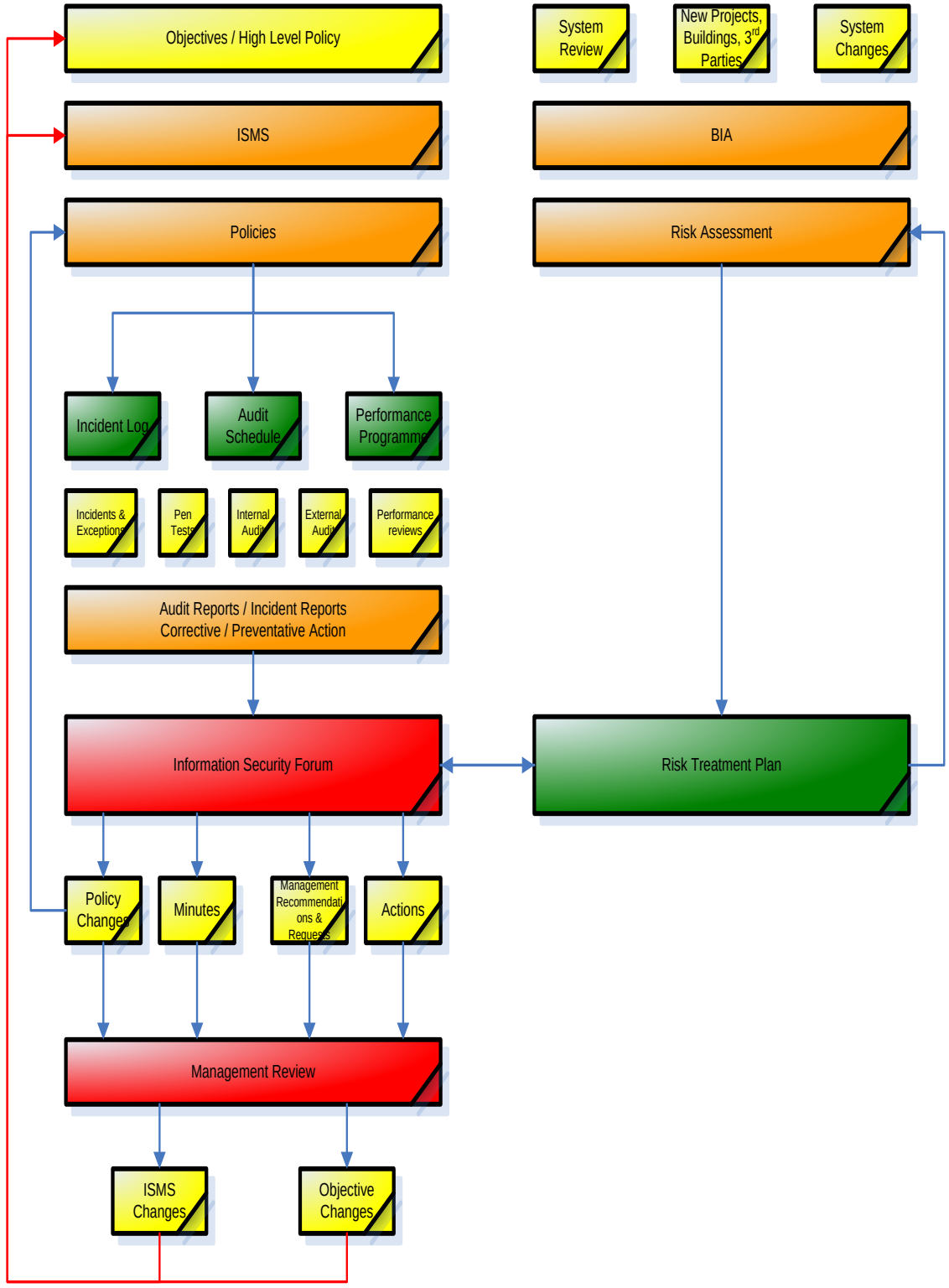


**Figure 3 ISMS Overview**

# 8. Risk Assessment

## 8.1 RA Methodology

Brunel University London adopts a basic approach for assessing the security risks based on the following activities:

- Information gathering
- Interviews and discussions with staff
- Review of current security arrangements
- Consolidated Analysis (based on information gathered, manager assessments, requirements, current security arrangements)
- Assets and their business value
- The threats and vulnerabilities related to these assets

## 8.2 Ongoing Risk Management

Ongoing management of risks will be controlled by information received from incident reports, audit results, technical advisories and confirmed or potential technical or process vulnerabilities.

The Cyber and Information Security Manager is responsible for ensuring that changes to the University, its technology, business objectives, processes, legal requirements and identified threats are incorporated into the ISMS.

Where appropriate the Cyber and Information Security Manager will initiate the risk assessment process to ensure that the security controls are relevant.

The Cyber and Information Security Manager can, if required, implement additional controls without undertaking a risk assessment, if the threat or vulnerability could have a significant impact on the University, its partners or staff.

The Cyber and Information Security Manager will maintain a Risk Assessment Programme to ensure that all major 3rd parties, major information systems undertake a risk assessment within a 3 year cycle.

All changes to the ISMS will be reviewed by the Information Security Forum and documented within the Forum Minutes.

## 8.3 Risk Treatment

4 methods of risk treatment have been established:

- Risk Reduction;
- Risk Retention;
- Risk Avoidance
- and Risk Transfer.

Future reviews and risk assessments may result in borderline cases or cases where there may be factors that do not affect the impact level. The management will also apply their judgement to set priorities for implementation commensurate with the impact level or changes to the University i.e. are the asset about to be replaced?

The Risk treatment Plan contains details of unacceptable risks and the activities planned to address them.

The Cyber and Information Security Manager is responsible in establishing and maintaining a Risk Treatment Plan in order to achieve the identified control objectives. The risk treatment plan will identify priorities based upon the perceived risk, and will consider funding, responsibilities, actions and estimated date of completion.

## 8.4 ISO/IEC 27001 Control Selection

Risk Management is concerned with taking mitigating and remediation action to reduce the likelihood of a risk occurring or reducing the impact of the risk should it occur. The controls selected to address the risks identified in the Risk Treatment Plan will relate to ISO/IEC 27001 control objectives.

Information security controls will be a combination of policies, procedures, University structures and physical or technical measures.

The Statement of Applicability provides the detail of how an individual control is implemented.

Each control that is selected from ISO/IEC 27001 to reduce the risk measure i.e. the actions taken to eliminate or reduce a vulnerability will be recorded on to a treatment plan which will show the control selected, the implementation priority, expected implementation date and who is responsible for the work. The University will whenever possible and depending on the risk measure aim to prioritise the reduction of vulnerabilities in accordance with the perceived or actual likelihood

## 8.5 Risk treatment Plan

The Cyber and Information Security Manager is responsible for establishing and maintaining a **risk treatment plan** in order to achieve the identified control objectives. The risk treatment plan will identify priorities based upon the perceived risk, and will consider funding, responsibilities, actions and estimated date of completion.

# 9. Statement of Applicability

The **Statement of Applicability** will list all controls that have been selected and will identify whether the control is fully or partially implemented in relation to the requirements of the control objectives.

Reasons for selecting controls are documented as part of the gap analysis / risk assessment process. The justification for controls that have not been selected will be documented with the Statement of Applicability. Where it is not possible to implement a control or the risk cannot be mitigated the justification will be authorised by the Information Security Forum and approved by the Senior Management Team.

# 10. Information Security Reports / Performance Metrics

Brunel University London will determine the effectiveness of the ISMS and implemented controls by measuring adherence to the following:

As a minimum, Brunel University London will determine the effectiveness of the implemented ISMS by measuring the following:

- The level of Conformance to policy / processes (monitoring the number of non-conformities identified in Internal Audit & Incident Management)
- The agreement and completion of corrective and preventive actions (resulting from RTP, Internal Audit, Incidents, Management Review etc.) within agreed timescales
- The identification and reduction in risk
- Achievement against:
    - Risk Assessment Programme;
    - Audit & Technical Programme Compliance;
    - Awareness Programme;
    - Business Continuity Programme;
    - Performance Measurement Programme.

Brunel University London will also determine the effectiveness of a few selected controls.

The metrics that will be measured will be determined on annual basis as part of the **Performance Measurement Programme.**

Where possible the selection and prioritization of metrics will be based upon the results of risk assessments. Brunel University London may revise the type of the processes that are monitored to reflect the following:-

- Changes or updates to Business processes, and objectives;
- Information discovered during the investigation of security incidents or security events;
- Internal and External Audit reports;
- Suggestions from Staff;
- Information Security Forum recommendations;
- Management Review recommendations;
- Legal / Regulatory Requirements;
- Customer Requirements.

The Information Security Forum is responsible for reviewing the effectiveness of implemented controls, is responsible for approving any amendments to this policy, and approving the type of processes and controls that are measured.

# 11. Information Security Education and Awareness

The University has established a training and awareness programme for all Brunel University London staff and students. All users are provided with access to relevant security guidance documents that explain their responsibilities in accordance with the University's Information Security Policy.

Training will be given as part of the induction process to new starters. The objectives of the training and awareness programme are to:

- make people aware of the value and importance of data resources and assets;
- reduce the risk of human error causing the failure of any installed security measures;
- make people aware of their responsibilities;
- security advisory process.

Elements may include:

- basic security awareness education as part of induction training organised by personnel;
- awareness sessions on appropriate management courses organised by personnel;
- awareness sessions during staff meetings by line managers;
- awareness sessions during management meetings by line managers;
- distribution of posters, pamphlets, development and maintenance of intranet pages and other memory aids.

Additional training, recommended by the Information Security Forum, will be given to existing users as deemed necessary.

Brunel University London HR Department will keep a record of all training provided. As part of their training, all users are made aware of the importance of information security, the impact a security breach will have upon the University, its customers and partners and the business benefits of a ISO/IEC 27001:2013 certified information security management system.

# 12. Information Security Incident / Event Management

An cyber security incident / event are an identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of safeguards.

Information Security breaches are investigated by the Cyber and Information Security Manager and CSIRT in accordance with the **Incident Management Process**, supported by relevant department managers as appropriate.

The Cyber and Information Security Manager collates information about security incidents, analyses trends and recommends the implementation of further controls if required.

# 13. Management Review

The Cyber Security Forum will review the ISMS as a standing agenda. As a minimum the following documentation will made available for review.

- Performance Measurements;
- External Audit Reports;
- Risk Assessments;
- Internal Audit Reports;
- Non Conformance Reports;
- Security Incidents;
- Previous Security Forum Minutes.

Senior Management will undertake a review of the ISMS at least annually. To undertake the review, Senior Management will be provided with a report by the security forum, the report will included the following information.

- Audit results (internal, Compliance Surveillance and other 3rd parties);
- Risk assessment valuations;
- Information Security Forum minutes;
- Suggestions from staff;
- Feedback from interested parties;
- Preventative and correctives actions;
- Additional vulnerabilities;
- Status of actions from previous reviews;
- Techniques, products or procedures (which could be used in the University to improve the ISMS performance and effectiveness).

The Results of the Management Review will be documented by the Cyber and Information Security Manager and released to the Security Forum.

The Management review report will include the following:

- Any recommendations covering the effectiveness of the ISMS;
- Recommended modifications to procedures, business processes as result of internal / external events;
- Updates to the risk assessment and risk treatment plan;
- It will take into consideration any changes in business, security, regulatory or legal requirement;
- It will high light any changes in risk and identify any areas of high risk that require risk acceptance;
- Any additional resource needs (Systems, Tools or People ).

# 14. Corrective / Preventative Actions

Corrective actions are raised when non-conformities to the ISMS and associated policies are identified. Corrective actions are raised in order to eliminate the root cause and so prevent re-occurrence of non-conformities.

Preventive actions are raised when potential non-conformities to the ISMS and associated policies are identified. A Preventive action is designed to prevent the reoccurrence of a non-conformity.

Non-conformity is defined as:

- the absence of, or the failure to implement and maintain one or more ISMS requirements,
- a situation which would, on the basis of available objective evidence, raise significant doubt as to the capability of the ISMS to fulfil the Information Security Policy and security objectives of the University.

Actual or potential non-conformities may be identified from the following:

- Internal / external audits;
- Reviews;
- Monitoring;
- Security incidents and events;
- Observations made by members of staff during day to day activities.

All actual or potential non-conformities will be communicated to the Cyber and Information Security Manager. The Cyber and Information Security Manager will communicate and work with the relevant area / personnel to resolve / prevent the non-conformities.

The Cyber and Information Security Manager will maintain a list of corrective / preventive actions, which will contain as a minimum:

- Date raised, and target date for resolution;
- Responsibilities allocated;
- Recommended corrective / preventive actions;
- Actions taken and statuses of actions.

Results and statuses of corrective / preventive actions will be presented / reviewed at the Information Security Forum meetings.

Results of corrective / preventive actions may generate additions to the Risk Treatment Plan, and may generate changes to the audit schedule to review actions taken to treat corrective / preventive actions.

# 15. Compliance Reviews

To ensure compliance with the requirements of ISO27001, the Cyber and Information Security Manager is responsible for creating an audit schedule. It is anticipated that each control will be audited throughput the duration of the compliance.

Auditing of applicable legal and regulatory requirements is the responsibility of the relevant employee as dictated by the roles and responsibilities, though these audits may be carried out in conjunction with the Cyber and Information Security Manager.

Internal audits within Brunel University London will be carried by the Cyber and Information Security Manager. The performance of Internal Audits is approved by the Senior Management Team and the Security Forum. Audits of the ISMS are carried out by a third party in line with good audit practice, not to audit your own work.

The Audit schedule will include plans to audit:

- Compliance to Policy, Processes and Procedures;
- Technical Compliance;
- Managed Service providers;
- Key 3rd parties / suppliers;
- New / Key Information Systems;
- any additional requirements to confirm successful implementation of the Risk Treatment Plan and any other initiative affecting information security.

The Cyber and Information Security Manager ensuring that each section of the ISMS is verified at least annually maintains an ISMS Audit Programme. Audits may be organized more frequently depending on the importance of the activities being audited.

The following sources of information are reviewed to determine the audit programme:

- Previous audit reports (Internal or Outsourced);
- Feedback from University users and staff;
- Senior management directives which might affect any services / policies;
- Changes in operational systems;
- Changes to relevant standards (i.e. ISO/IEC 27001:2013);
- Information Security Training records and results.

The programme covers audits that are carried out:

- internally within Brunel University London;
- external audits;
- by other 3rd parties on ad hoc basis;
- Penetration/Technical testing.

The programme is reviewed on a monthly basis to check progress and consider any changes (e.g. to policy, system or service provision) that might need to be reflected.

The Cyber and Information Security Manager ensures the Audit results are discussed at the next Information Security Forum.

Once corrective and preventative actions are implemented they are reviewed by the Cyber and Information Security Manager to verify that the initiatives are working correctly. The results of these checks are presented to the Security Forum.