Information Security Risk Management 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	09/12/2016
V 0.2	Mick Jenkins	Re-Org Draft	09/08/2017
V 1.0	Mick Jenkins	First release	
V 1.1	Mick Jenkins	Approved ISC	26/01/2018

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
	All Directors for Cascade		
	DCO's / DRO		
	COO		
	CIO		
	CFO		
	University secretary		

Contents

1 Introduction 4
1.1 Purpose 4
1.2 Policy scope 4
1.3 University Risk Management Framework 4
2 Information Risk Management Policy 6
3 Asset Risk Management 7
3.1 Information Asset Identification and Profiling 7
4 Risk Treatment 8
4.1 Determination of Controls 8
4.2 Comparison with Annex A of ISO/IEC 27001:2013 9

1 Introduction

Information is a vital university asset which requires an appropriate level of protection from unauthorised disclosure, access, modification or destruction. Information security risk management provides this level of risk analysis to apply sensible and proportionate protection by applying the correct level of resource and safeguards – thus reducing risks to information to a level that is acceptable to the organisation and provides information assurance to the Executive Board.

The successful implementation of an information risk management framework across Brunel university London (BUL) is essential to ensure that information, in whatever format, is provided the correct level of protection commensurate with its sensitivity and criticality to BUL business and operations.

ISO 27001 - Conformance

This section indicates the University Conformance to ISO27001:2013.

University ISMS Control Number	Clause 4 – Context of the Organisation - Risk Assessment and Management
ISO 27001:2013 Conformance Control	Information Classification Objective A.4.1 - Understanding the organisation and its context A.4.2 – Understanding the needs and expectations of interested parties A.4.3 – Determining the scope of the Information Security Management System

1.1 Purpose

The purpose of this Information Security Risk Management Policy is to provide assurance to the Executive Board that risks to information assets managed by, or on behalf of BUL, are being managed effectively and consistently across the organisation.

1.2 Policy scope

This policy applies to anyone who has access to BUL Information Systems whether they are employed or under a term of contact, including third parties. In effect, this policy applies to anyone working within BUL regardless of location. It also extends to University information held by third parties and partners.

This policy encompasses the people, processes and technology that process, transmit, or store BUL information, both physical and electronic.

1.3 University Risk Management Framework

The University has a comprehensive risk management framework that describes the University's approach to risk management based on our collective experiences of managing risks and set against good practice drawn from the Office of Government Commerce's (OGC) 'Management of Risk: Guidance for Practitioners', and BS ISO 31000 "Risk management - Principles and guidelines" standard.

The risk management framework comprises the Risk Management Policy and Risk Management Procedure, supported by the Risk Management Guidelines.

This Information Risk Management Policy is supplemental to the existing University Risk Management Framework policy and procedures, predicated on the requirement to operate a risk management system and methodology, specific to information security, and operating within the university ***Information Security Management System*** (ISMS).

Information security risk management has a number of differing industry wide models, specifically designed for the nuances of information security risk scoring and assessments. BUL will adopt the good practice methodologies of ISO 27005 – Information Security Risk Management – The precise methodology and scoring in set out in an accompanying BUL policy document – **BUL IRM02 Risk Management Methodology.**

2 Information Risk Management Policy

2.1 Information Security Risk Management.

The BUL cyber & INFOSEC team will apply an intelligence led, risk managed approach to organisational information security controls developed in alignment with the university risk appetite for securing information assets.

The risk management model that will be applied is based upon ISO 27005[1], aligned to ISO 27001 and 27002, and operates with other good practice drawn from COBIT[2] and UCISA[3]. Processes shall be implemented so that information risks are appropriately assessed, responded to, accepted, monitored and communicated to the Executive Board.

2.2 Information Security Risk Analysis

A documented risk analysis process is used as the basis for the identification, definition and prioritisation of risks. The risk analysis process shall include the following:

- Identification and prioritisation of the threats to Information assets.
- Identification and prioritisation of the vulnerabilities of Information assets.
- Identification of a threat that may exploit a vulnerability documented as a cyber vulnerability assessment (CVA).
- Qualitative identification of the impact to the confidentiality, integrity and availability of Information Resources if a threat exploits a specific vulnerability.
- Identification and definition of measures and/or controls used to protect the confidentiality, integrity and availability of Information assets

The risk analysis process is documented through a cyber & information risk register, informed by:

- Cyber vulnerability assessments (CVA).
- Security Assessment Reports (SAR) – An annual ISMS assessment.
- Penetration testing results.
- Threat assessments.
- Threat trends.
- Intelligence reports.

A strategic risk register is provided to executive board that provides an overall summary of strategic risk, derived from the operation risk register and CVA's. These are regularly updated when environmental, operational or technical changes arise that impact the confidentiality, integrity or availability of Information assets such as incidents, lessons identified, and technical changes, or new threats.

2.3 Information Risk Assessment

A systematic and structured information risk assessment methodology has been established so that the BUL can appropriately assess and respond to risks to its information assets. This methodology is shown in the accompanying paper 'Information Security Risk Management Methodology' BUL-POL-IRM02.

2.4 Threat and vulnerability

Information assets shall be evaluated for threats and vulnerabilities on a regular basis or when a significant change or incident occurs. Threat and vulnerability shall be actively monitored via threat and intelligence reports received by the cyber & INFOSEC team from a variety of sources.

2.5 Control Evaluation

Information security controls and countermeasures, which have been implemented in response to risks, shall be evaluated regularly for effectiveness and suitability. Controls will be emplaced via the risk management principles of intelligence led, risk based, with controls aligned to the ISMS statement of applicability (SoA).

2.6 Information Asset Responsibilities

All information assets shall be recorded and Information Asset Owners identified in accordance with the defined principles of the ISMS and 'Role and Responsibilities' Policy Paper. Information asset owners are responsible for the classification and risk management of the assets.

3 Asset Risk Management

The asset risk management process determines the specific threats and risks which affect the confidentiality, integrity and availability of all university information assets.

3.1 Information Asset Identification and Profiling

[1] Information Security Risk Management
[2] Control Objectives for Information and Technology
[3] Universities and Colleges Information Systems Association

An information asset is essentially a distinct set of information which has some value to the organisation.

When evaluating risk against an information asset, BUL information asset owners shall assess and document the assets to cover its profile entirety including:

- Exactly what the asset is
- Its requirements for confidentiality, integrity and availability
- The lifecycle of the asset
- The business processes which affect it
- The value of the asset to the organisation
- The expected value of the asset to an attacker
- Its classification (see Information Security Classification Policy)
- its expected lifespan.

4 Risk Treatment

Risk is treated by applying controls that modify the risk in such a way that it meets the specified Risk Acceptance Criteria. This is achieved through controls which either:

- Reduce the likelihood of the risk occurring by attempting to prevent the occurrence of the event, or detect it in sufficient time for the organisation to deal with it or
- Reduce the severity of the risk by reacting to the consequence.

Through the use of controls it is planned that the likelihood or impact of the event can either be eliminated or reduced greatly. The control may be performed by this organisation or another external organisation.

4.1 Determination of Risk Treatment

BUL shall adopt an information risk treatment methodology that provides an auditable trail of decision making regarding each assessed risk. Aligned to the university risk treatment policy, information security risk treatment will be documented as one of four option in the risk register:

- Avoidance – ceasing the activity due to it being unacceptable risk
- Reduction – placement of controls and contingency plans
- Transfer – where applicable to third parties or using insurance
- Tolerate – accepting the risk within risk appetite parameters

Cyber & Information security risk decision making shall be undertaken via the relevant committees assigned to review and monitor risk, with the Senior Information Risk Owner (SIRO) providing oversight to executive board.

Where reduction measures are emplaced, each risk event is analysed and documented to determine:

- Controls which are required to prevent the event

- Controls which are required to detect the event
- Controls which are required to react to the associated consequences of the event

4.2 Monitoring and Reviewing Risks

All risks cyber & information security risks will be monitored and reviewed in accordance with the arrangements specified in the University Risk Management Procedure. As a minimum, operational and strategic cyber & INFOSEC risks will be reviewed every six months.

Information Asset Owners, shall review the relevant risks to their own assets, on a 6 monthly basis and provide reports and assessments to the SIRO, or asa required.

4.3 Comparison with Annex A of ISO/IEC 27001:2013

In order to ensure that necessary controls have not been omitted from the Risk Treatment Plan they are compared with the controls in the statement of applicability (SoA) for ISO 27001:2013 standard. Each control within the standard is considered and the following determined:

- Is it applicable to the university SoA.
- If it is a variant of an SoA control, or deemed as not being applicable, the reason for this shall be recorded.
- What is the implementation status (Implemented; In Progress or Not Started)
- If as a result of this process an SoA control is determined to be applicable, but isn't already covered - the Risk Treatment Plan is revised to include it.

4.4 Risk owner approval

The Information Security team shall engage and support the asset and risk owners to review risk assessments and risk treatment plans. The risk owners ultimately approve the risk treatment plans.

-End-