Resources for Chapter 5 – Risk assessment

RESOURCES

- Template for information risk management principles
- Development and use of risk assessment templates – UCL, case study
- Project information risk assessment – Requirements and expectations – UCL
- Service information Risk assessment – Requirements and expectations – UCL
- Project information risk assessment – Capability - UCL
- Service information risk assessment – Capability - UCL
- Risk treatment plan – UCL
- Risk assessment methodology – Cardiff University
- Information asset register tool – University of Oxford

Template for information risk management principles

These top level guiding principles apply to all information handling activities, including project work and day to day operations. They are intended to be used to inform and guide organisations in their normal work, and to ensure that information is handled in a suitably secure fashion.

1	Business requirements drive security requirements	Security requirements should exist to support the requirements of a business activity and should be relevant and appropriate.
2	Protect the confidentiality, integrity and availability of information to the right levels	Information's requirements for confidentiality, integrity and availability should be identified and security measures should be matched to these requirements.
3	The campus network is not the security perimeter	Because the campus network connects thousands of machines under widely varying management regimes, it should be considered in the same risk category as the open Internet. Any machine which you would not connect to the Internet without some form of protection should have the same protection installed before enabling access from the general campus network.
4	Role-based access	Privileges should be assigned to roles, not individual people. People should then be assigned roles.
5	Least privilege	Each role should have the minimum set of privileges needed to carry out the tasks required of that role.
6	Separation of duties	Where the risk or impact of a failure to execute a process correctly is unacceptably high, the process should require appropriate oversight before it can be completed. For example, when placing a purchase order, it has to be approved by a second person before it can be placed, or when writing software, a code review is undertaken by a second person before release.
7	Segregation of environments handling information rated at different security levels	Systems which store, process or transmit information classified as secret should be physically segregated from other systems which operate with information at a different level (e.g. normal). Systems which store, process or transmit other levels of information should be logically separated. Logical segregation can be achieved by appropriate network architecture. Note that it is expected that development/test and pre-production/production systems will be handling information at different levels.
8	No sensitive data on test systems	Development systems should not hold any data rated other than *normal*. Test and pre-production systems which require data rated other than normal should be secured to the same standard (or better e.g. only accessible to a specific network or set of hosts) as the related production system.
9	Traceability of activity to individuals	This is restricted to operations involving information above *normal*. Actions carried out by an individual on information should be capable of being traced back to that individual.
10	Documented security standards	Information processing systems where data with a classification other than *normal* are processed should be designed, deployed and managed according to documented security standards (e.g. a secure software development lifecycle).
11	Competence and training	Individuals must be competent to carry out their responsibilities. Heads of Departments and Divisions must ensure that training to the appropriate level is provided.
12	Responsibility and accountability	Roles where there are activities which require access to information rated other than *normal* should have those activities clearly documented as part of the role description. In addition, the responsibility for protecting that data should also be clearly defined in the role description along with a path of accountability to the line management structure.
13	Continuous improvement	All roles should be responsible for identifying and highlighting opportunities for improvement to manage risk. Systems and processes should be improved as opportunities appear.
14	Defence in depth	No individual security measure should be relied upon in isolation to protect information.
15	Risk ownership	Information risks should be owned by a role at an appropriately senior level in the organisation i.e. one with sufficient authority to ensure the risk is effectively managed.

Development and use of risk assessment templates – UCL, case study

Development of the process and templates

The risk assessment templates were initially developed from the NIST SP 800-39 methodology (Managing Information Security Risk) and adapted to suit our environment. Since they were first developed, they have been put into practice and iteratively improved.

Using the process and templates

The process involves first completing the requirements and expectations document with the key people involved in the project/service; this looks at the type of information involved, and any internal and external requirements. The capability document is then completed; this looks at how the information is stored, processed and transmitted, and the risk scenarios involved. Once the risks have been identified and controls proposed, a risk register/treatment plan is created and managed by the project manager or service owner. If a server and/or web application is involved, then a penetration test is included in the process, and any vulnerabilities found are included in the risk register.

Integration with the Project Delivery Framework

We were fortunate to have support from our project management office, who agreed to include our process and templates into their project delivery framework. We are also included at project gates, and before projects were given any money. This enables us to identify whether a project has been through the risk assessment process, and, if they have, whether they have implemented our recommendations. If it is found that the project has not been through a risk assessment, they are asked to complete one before they may proceed to the next stage in the project delivery framework. This has been beneficial, as previously it was possible for projects to proceed without any input from the Information Security Group.

We are also included as approvers in the yearly bid process. This involves us reviewing all the bid documents and adding comments relating to the amount of input we will need to have and whether any penetration testing needs to be budgeted for.

Findings so far

The general consensus has been very positive. However we have found the perception before a risk assessment has taken place to be quite negative, with people presuming that we would block their project or slow it down. By integrating ourselves into the project delivery process, we are hoping to stop the possibility of us slowing projects down; this would only happen if we were not consulted until the very last minute. We now try to make it clear at the beginning of the process that we are there to help project teams achieve what they need to achieve in a safe way; we are not there to stop them. We see this whole process as continually improving; the more risk assessments we do, the more we can add changes and improve the process.

Learning Points

- Do not reinvent the wheel - use approaches that have already been tested and adapt them to suit your organisation.
- Ensure you integrate with your organisation’s project delivery process; it’s the easiest way to make sure they involve you.
- Get buy-in; if those involved understand that you are ultimately trying to help them, you are less likely to find resistance.

Project information risk assessment – Requirements and expectations - UCL

Project Name:	
Project Manager:	
Service Owner:	
Author(s):	
Date completed:	
Date of next review:	
Scope:	

Information Classification

Classification(s) of information involved:

Classification	Description of classification	Is this information used, stored or affected by project?	Type(s) of Information
Secret	Loss, tampering or disclosure would seriously damage operations as a teaching, learning and research organisation. Example: identifiable patient information, personal financial details (bank account code, tax codes, payment card details), confidential investigations.	Y/N	Describe information which has been identified as being Secret.
Highly restricted	Loss, tampering or disclosure would result in significant legal liability, severe distress to individual(s), significant loss of asset value or severe damage to organisational reputation. Example: staff appraisal records, student profiles, unpublished commercially sensitive material	Y/N	Describe information which has been identified as being Highly Restricted.
Restricted	Loss, tampering or disclosure would cause significant upset to individuals, may result in financial penalty and harm organisational relationships. Example: main web page	Y/N	Describe information which has been identified as being Restricted.
Normal	Loss, tampering or disclosure would cause temporary inconvenience or minor reputational damage. Example: email requesting the location for a meeting on fridge cleaning.	Y/N	Describe information which has been identified as being Normal.

1 Information Security Attributes

Requirements of the information which the project is handling:

	Level of concern (low/medium/high)
Confidentiality	
Integrity	
Availability	

2 Internal requirements

What internal policies, procedures and other requirements apply to the security of the information being handled by the project?

3 External requirements

What external legislation, contracts and other requirements apply to the security of the information being handled by the project?

4 Penetration testing requirements

Web application	Y/N
Server	Y/N

Service information risk assessment – Requirements and expectations - UCL

Service Name:	
Service Owner:	
Service Operations Manager:	
Author(s):	
Date completed:	
Date of next review:	
Scope:	

1 Information Classification

Classification(s) of information involved: Classification	Description of classification	Is this information used, stored or affected by service?	Type(s) of Information
Secret	Loss, tampering or disclosure would seriously damage operations as a teaching, learning and research organisation. Example: identifiable patient information, personal financial details (bank account code, tax codes, payment card details), confidential investigations.	Y/N	Describe information which has been identified as being Secret.
Highly restricted	Loss, tampering or disclosure would result in significant legal liability, severe distress to individual(s), significant loss of asset value or severe damage to organisational reputation. Example: staff appraisal records, student profiles, unpublished commercially sensitive material	Y/N	Describe information which has been identified as being Highly Restricted.
Restricted	Loss, tampering or disclosure would cause significant upset to individuals, may result in financial penalty and harm organisational relationships. Example: main web page	Y/N	Describe information which has been identified as being Restricted.
Normal	Loss, tampering or disclosure would cause temporary inconvenience or minor reputational damage. Example: email requesting the location for a meeting on fridge cleaning.	Y/N	Describe information which has been identified as being Normal.

2 Information Security Attributes

Requirements of the information which the service is handling:

	Level of concern (low/medium/high)
Confidentiality	
Integrity	
Availability	

3 Internal requirements

What internal policies, procedures and other requirements apply to the security of the information being handled by the service?

4 External requirements

What external legislation, contracts and other requirements apply to the security of the information being handled by the service?

5 Penetration testing requirements

Web application	Y/N
Server	Y/N

Project information risk assessment – Capability - UCL

Project Name:	
Project Manager:	
Service Owner:	
Author(s):	
Date completed:	
Date of next review:	
Scope:	

1 Project Context

How is information stored as part of the project?

How is information processed[1] as part of the project?

How is information transmitted[2] as part of the project?

[1] Includes creation and destruction

[2] Sent and received

2 Risks and mitigations

Risk scenario	Example(s)	Controls in place	Likelihood	Impact	Proposed additional controls
User deliberately or accidentally leaks information					
User accidentally or deliberately damages information					
Misuse of resources					
Premises break-in					
Acts of God, vandals, and terrorists					
Theft or loss of mobile devices					
Theft or loss of non-mobile device					
Theft or loss of paper-based information					
Software failure					
Hardware failure					
Power failure					
Internet/communications failure					
Hacking: brute-force, malicious code, spam, phishing, targeted					
Denial of Service					

3 Project Capability Rating

	Low, medium or high
Confidentiality	
Integrity	
Availability	

Service information risk assessment – Capability - UCL

Service Name:	
Service Owner:	
Service Operations Manager:	
Author(s):	
Date completed:	
Date of next review:	
Scope:	

1 Service Context

How is information stored as part of the service?

How is information processed[1] as part of the service?

How is information transmitted[2] as part of the service?

[1] Includes creation and destruction

[2] Sent and received

2 Risk and mitigations

Risk scenario	Example(s)	Controls in place	Likelihood	Impact	Proposed additional controls
User deliberately or accidentally leaks information					
User accidentally or deliberately damages information					
Misuse of resources					
Premises break-in					
Acts of God, vandals, and terrorists					
Theft or loss of mobile devices					
Theft or loss of non-mobile device					
Theft or loss of paper-based information					
Software failure					
Hardware failure					
Power failure					
Internet/communications failure					
Hacking: brute-force, malicious code, spam, phishing, targeted					
Denial of Service					

3 Service Capability Rating

	Low, medium or high
Confidentiality	
Integrity	
Availability	

Risk treatment plan – UCL

Risk Treatment Overview

This document describes how risk treatment is handled; in particular it details the approach to:

- Treating risk
- Formulating Risk Treatment Plans, ensuring that necessary controls have not been omitted and gaining approval for the risk treatment plan and residual risks

Treating risk

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 hoped 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. The organisation also needs to consider whether, by employing a particular control to reduce a particular risk for one variety of consequence it is increased for another. Consequently it is important that a wide range of risk treatment options are considered.

Risk Treatment Plans

Determination of controls

Each event is considered 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

At the conclusion of the process the organisation must be satisfied that the residual risk is acceptable which should be reflected in the Residual Risk Level. Controls can be designed or based on commercially available technology in order to modify risk to an acceptable level.

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 Annex A of the ISO/IEC 27001:2013 standard. Each control within the standard is considered and the following determined:

- Is it applicable to the organisation?
- If applicable does the organisational control exactly correspond to the version in the standard? If it is a variant the Annex A control is deemed as not being applicable and the reason for and explanation of the variant is recorded
- Why it is used? This is explained through a cross-reference to the associated event in the Risk Treatment Plan
- What is the implementation status (Implemented; In Progress or Not Started)

If as a result of this process an Annex A control is determined to be applicable, but isn’t already covered the Risk Treatment Plan is revised to include it.

Formulating risk treatment plans

The Risk Treatment Plan is sub-divided into sections relating to each risk event. Each section will document:

1. A description of the event;
2. The risks before treatment (with corresponding Risk Rating Graph);
3. The risk treatment detailing:
    a. Controls to prevent the event
    b. Controls to detect the event
    c. Controls which react to the consequences
4. The risks after treatment (with corresponding Risk Rating Graph) with an explanation of why the risk acceptance criteria are met;
5. Risk Owner and acceptance of residual risk

6. Reference to earlier versions of the plan

Calculations of residual risk are based on an appraisal of the likely outcome judged against the criteria documented in the Risk Assessment Process to ensure consistency.

Risk owner approval

The Information Security Group will meet with the risk owners to review the risk treatment plan. The risk owners ultimately approve the risk treatment plans. The results are recorded by both the Information Security Group and the risk owners.

Risk assessment methodology – Cardiff University

Section

1 Introduction

1.1 In order to ensure consistency, a standard methodology, which can be used across all information security risk assessments is required. The methodology selected for use at Cardiff University is described below.

2 Risk Assessment

2.1 What is an Information Security Risk Assessment?

A risk assessment is a process that sets out to establish:

- The existence of risks to the University's information assets (physical or electronic)
- The probability that these risks might occur
- The likely resultant impact of any such risk
- Any action which could be taken to mitigate the risk either in terms of prevention or reduction of impact should it occur

3 Risk Assessment Methodology - Annual Process

3.1 The following describe the steps involved in carrying out the risk assessment process and refer to the appropriate reference documents and templates and their location within the appendices.

3.2 Each year a risk assessment of key information assets shall be carried out in accordance with section 4.4.2 of the University Information Security Policy.

3.3 The process will be initiated by the SIRO and coordinated by the Information Asset Owner for each Key Information Asset (see Appendix I).

3.4 The Information Asset Owner will direct Data Stewards to arrange for risk assessments of the systems or containers they manage e.g. SIMS to be carried out. N.B. These should not be carried out in isolation by the Data Steward but should involve suitable representation and input from users and administrators of the system.

3.5 Using the Information Classification Document (Appendix A) identify the classifications of information encompassed by the selected asset i.e. C1 Classified - Highly Confidential, C2 Classified - Confidential or NC Non-Classified.

3.6 Complete the Key Information Asset Profile (Appendix B).

3.7 Complete the Key Information Asset Risk Environment Map (Appendix C).

3.8 Consider the threats to the asset using the typical threats document (Appendix D) to assist in this process.

3.9 Brainstorm/Discuss the potential risks, ensuring you categorise their impact in terms of – confidentiality, integrity, availability and compliance.

3.10 Make a list of the risks to be quantified, take each in turn and using the key information asset template (Appendix E) describe a worst-case scenario in which the risk would become an issue i.e. how the risk would manifest. Whilst using a worst-case scenario, ensure you remain realistic and minimise the number of variables contributing to the risk, that is to say you should minimise the number of different factors which all have to occur in order to see the risk crystallise as an issue. A risk should be expressed in the terms of cause, event and effect:

Cause - As a result of ...

Event - There is a risk that ...

Effect - Which could ...

3.11 Use the Risk Measurement Criteria (Appendix F) to assess the impact of each risk against each impact area I.e. you must develop the scenario to describe the likely severity of impact against each impact area in that scenario. Having done this, total up the impact scores for each of the impact areas to give an overall risk impact score (pay careful attention to the Scoring table on the last page of the risk measurement criteria).

3.12 Having assessed the impact of each risk, determine the probability of occurrence. Using the Risk Measurement Criteria which provide definitions of likelihood (Appendix F).

3.13 Once an overall impact score and probability have been determined you can plot the risk on the Risk Acceptance Matrix (Appendix G).

3.14 Each section of the Matrix has a colour and the colour can be translated into the appropriate risk response action. I.e. a risk with a high likelihood and high impact score would plot onto a red section and would translate as a severe pool 1 risk which must be given immediate attention and priority over all lower rated risks.

3.15 Having plotted the risks into the matrix and consequently identified the risk response actions, appropriate risk control (mitigation) actions should be identified, discussed and documented in a risk register (see Appendix H). For each risk there must be one owner who is accountable for the management of that risk. Since one risk may have a number of distinct control actions, the risk owner shall identify who is responsible for ensuring that each control is implemented and managed.

3.16 The process will generate a completed: Key Information Asset Profile, Key Information Asset Risk Environment Map, Risk Identification and Assessment Worksheet, a populated Risk Acceptance Matrix and Risk Register.

3.17 The Risk register shall be reviewed by the Data Steward and Asset Owner in order to determine the overall level of information risk exposure as well as to agree and sign off asset specific security requirements and priorities for implementation. However all risks which plot as Severe or Substantial should be referred via the Information Asset Owner to the SIRO for referral to the Information Security Risk Group (ISRG) to determine whether the risks should be added to the University Risk Register

3.18 N.B. where a risk assessment was carried out the previous year, reference should be made to the relevant paperwork as a primer for the current years risk assessment. However it is not simply enough to review the risks from the previous year as it is possible that new risks may have arisen in the intervening 12 months due to changes in legislation, reporting requirements, technological developments etc.

Appendix A

INFORMATION CLASSIFICATION V2.0

Category Title	Classified C1 HIGHLY CONFIDENTIAL	Classified C2 CONFIDENTIAL	NC Non -Classified
Description	Has the potential to cause serious damage or distress to individuals or serious damage to the University's interests if disclosed inappropriately *Refer to Impact levels of 'high' or 'major' on the Risk Measurement Criteria* Data contains highly sensitive private information about living individuals and it is possible to identify those individuals *e.g. Medical records, serious disciplinary matters* Non-public data relates to business activity and has potential to seriously affect commercial interests and/or the University's corporate reputation *e.g. REF strategy* Non-public information that facilitates the protection of individuals' personal safety or the protection of critical functions and key assets *e.g. access codes for higher risk areas, University network passwords.*	Has the potential to cause a negative impact on individuals' or the University's interests (but not falling into C1) *Refer to Impact levels 'Minor' or 'Moderate' on the Risk Measurement Criteria* Data contains private information about living individuals and it is possible to identify those individuals *e.g. individual's salaries, student assessment marks* Non-public data relates to business activity and has potential to affect financial interests and/or elements of the University's reputation *e.g. tender bids prior to award of contract, exam questions prior to use* Non-public information that facilitates the protection of the University's assets in general *e.g. access codes for lower risk areas*	Information not falling into either of the Classified categories e.g. Current courses, Key Information Sets, Annual Report and Financial Statements, Freedom of Information disclosure
Type of protection required	Key security requirements: Confidentiality and integrity This information requires significant security measures, strictly controlled and limited access and protection from corruption Back up requirements will need to be considered in relation to the importance of the information: is it the master copy of a vital record, how difficult would it be to recreate and how much resource would it require to recreate it?	Key security requirements: Confidentiality and integrity This information requires security measures, controlled and limited access and protection from corruption Back up requirements will need to be considered in relation to the importance of the information: is it the master copy of a vital record, how difficult would it be to recreate and how much resource would it require to recreate it?	Key security requirement: Availability This information should be accessible to the University whilst it is required for business purposes Back up requirements will need to be considered in relation to the importance of the information: is it the master copy of a vital record, how difficult would it be to recreate and how much resource would it require to recreate it?

General advice:

Always aim to keep Classified Information (C1 and C2) within the University's secure environment.

Where this is not possible consider whether the information can be redacted or anonymised to remove confidential or highly confidential information, thereby converting it to Non-Classified Information (NC).

Report any potential loss or unauthorised disclosure of Classified Information to the IT Service Desk on 74xxx

Seek advice on secure disposal of equipment containing Classified Information via the IT Service Desk on 74xxx

Use the Confidential Waste Service for disposal of paper and small electronic media xxx@cardiff.ac.uk

Appendix B

KEY INFORMATION ASSET PROFILE

Name of Key Information Asset and sub category	Rationale for selection *Why is this information asset important to the organisation?*	Description *What is the agreed-upon description of this information asset?*
Information Asset Owner *The role/post title of the person*		
Information Classification	□ Classified - Highly Confidential □ Classified - Confidential □ Classified - Protect □ Non-Classified	
Security requirements		
□ Confidentiality	Only authorised staff can view this information asset, as follows:	
□ Integrity	Only authorised staff can modify this information asset, as follows:	
□ Availability	This asset must be available for these staff to do their jobs as follows:	
□ Compliance	This asset has special regulatory compliance protection requirements as follows:	
Most important security requirement *select as relevant*		
Confidentiality / Integrity / Availability / Compliance		

Appendix C

KEY INFORMATION ASSET RISK ENVIRONMENT MAP

NAME OF KEY INFORMATION ASSET & SUB CATEGORY: ....

Containers	*Tick all that apply*	Specific locations	Owner(s) /staff depts
Internal (University owned)			
Filestore: shared drives			INSRV
Centrally maintained databases			INSRV
Department maintained databases			
Filestore: personal network drive			INSRV
IT Network			INSRV
Lotus Notes email accounts			INSRV
CU web pages			
PC hard drive			
Laptop hard drive			
University mobile device (e.g. Blackberry)			
Removable media (e.g. CD, USB stick)			
Paper filing systems			
Internal postal system			
Staff			
Computer Screens			
External			
Staff home PC			
Staff owned laptop			
Staff owned mobile device			
Staff owned removable media			
Company under University contract			
Service provider not under University contract (including private email)			
Postal/courier service Staff owned vehicle			
Students			
Computer Screen			

Appendix D

List of Typical Threats

- Fire
- Water damage – flood or leak
- Destruction of equipment or media
- Dust, corrosion, freezing
- Failure of air-conditioning or water supply system
- Loss of power supply services
- Failure of telecommunication equipment
- Remote spying
- Theft of media, documents or equipment
- Retrieval of recycled or discarded media
- Disclosure
- Tampering with hardware or software
- Equipment failure
- Saturation of the information system
- Breach of information system maintainability
- Unauthorised use of equipment
- Use of counterfeit or copied software
- Corruption of data
- Illegal processing of data
- Error in use
- Abuse of rights
- Forging of rights
- Denial of actions
- Breach of personnel availability

Appendix E

Information Security Framework

Key Information Asset – Information Asset: Risks

Guidance on using this template:

- Enter your 5 risks in order of priority with 1 being the most significant risk.
- Name the risk
- Provide a description of the risk (how it would occur and why)
- Indicate whether it would affect confidentiality, integrity, availability or compliance if it did occur
- Estimate how likely it is to occur and any controls you know about that are designed to limit or prevent it, views on their effectiveness
- What impact the risk would have on the University if the worst case scenario of this risk did occur. Referring to the Risk Measurement Criteria as a guide, then score each risk against the listed impact areas in the table.

An example risk is shown below (The risk description is fictional)

1. 1.
2. Risk Name - Unauthorised staff access to information on XYZ system
3. Risk Description: Staff are able to access and amend records on the system they are not permitted to and can access information beyond that required for them to carry out their role. That access has the potential to cause significant issues with data integrity as users will be able to delete or change records which indicate invoices received. This would also have the effect of undermining the purpose of the system and the confidence that staff have in it and the organisation. It would also impact on supplier confidence in the organisation if invoices were late being paid. This risk could materialise through staff having over privileged access rights to information beyond that required to undertake their role due to permissions not being set correctly or not being amended according to role changes.
4. Confidentiality ☐ Integrity ⍰ Availability ☐ Compliance ⍰
5. Likelihood (and existing controls): Likelihood is high as there are a great deal of staff role changes and people joining the organisation. Current controls rest with those who administer account access and insufficient resource to administer accounts has been identified meaning there is a significant lag in access changes to XYZ system being requested and their implementation.
6. Impact: See Table

	Impact Value					
Impact Area	**No (0)**	**Negligible (1)**	**Minor (2)**	**Moderate (4)**	**High (6)**	**Major (8)**	**Relative Risk Score**
Corporate Reputation			X				2
Research Profile & Income	X						0
Student Experience	X						0
Financial Sustainability			X				2
Health & Safety	X						0
Staff Experience				X			4
Legal Obligations					X		6
							14

Risks

Which sources of information, if compromised, would have an adverse impact on the organisation (as defined by the risk measurement criteria) if one or more of the following occurred?

– The asset or assets were disclosed to unauthorised people.

– The asset or assets were modified without authorisation.

– The asset or assets were lost or destroyed.

– Access to the asset or assets was interrupted.

- Information Asset R1.
- Risk Name:

- Risk Description:
- Confidentiality □ Integrity □ Availability □ Compliance □
- Likelihood (and existing controls):
- Impact: See Table

	Impact Value						
Impact Area	**No (0)**	**Negligible (1)**	**Minor (2)**	**Moderate (4)**	**High (6)**	**Major (8)**	**Relative Risk Score**
Corporate Reputation							
Research Profile & Income							
Student Experience							
Financial Sustainability							
Health & Safety							
Staff Experience							
Legal Obligations							

Appendix F

RISK MEASUREMENT CRITERIA (INFORMATION SECURITY FRAMEWORK) V2.0

Definitions: short term: 1 week to 5 months medium term: 6 months to one year long term: in excess of a year

Risk Area	Impact				
	Negligible	Minor	Moderate	High	Major
Corporate Reputation	Small number of individual correspondence/ representations Limited social media pick up, low reach	Reputation is minimally affected with little or no targeted effort or expense required to recover; Low key local or regional interest media coverage Mild stakeholder correspondence/ representations Negative, short term social media pick up, limited platforms (fewer than 500 followers)	Reputation is damaged in the short to medium term with targeted effort and expense required to recover. Public stakeholder comment and correspondence expressing concern Adverse regional or national interest media coverage Negative social media pick up, more than 500 followers Achievement of KPIs threatened	Significant public and private comment from stakeholders expressing serious concerns Adverse high profile, national media coverage from reputable/ influential media, with some international interest Sustained social media criticism, shared across multiple platforms with wide reach	Reputation damaged for the long term or irrevocably destroyed – requiring re-branding
Research Profile & Research Income	Small impact on research activity within specific teams short term/ localised effect; negligible impact on research income	Minor impact on research income or productivity for wider group REF outcome remains unaffected	Noticeable impact on REF profile Medium term effect on productivity within discipline Up to 1% overall reduction in research income due to loss of confidence/lack of compliance Achievement of KPIs threatened	Significant impact on REF profile Medium to long term effect on productivity in more than one discipline 1 to 4% overall reduction in research income due to loss of confidence/lack of compliance	Major impact on REF profile Long term/pan university effect More than 5% reduction in research income due to loss of confidence/lack of compliance

RISK MEASUREMENT CRITERIA (INFORMATION SECURITY FRAMEWORK)

Definitions: short term: 1 week to 5 months medium term: 6 months to one year long term: in excess of a year

Risk Area	Impact				
	Negligible	**Minor**	**Moderate**	**High**	**Major**
Student Experience	Student satisfaction affected (localised short term effect) little or no targeted effort or expense required to recover Individual student appeals or complaints No impact on student recruitment	Noticeable impact on NSS scores in localised area and some effort and expense required to recover Small increase in student appeals or complaints in specific area Small impact on student recruitment (number of applicants) Small impact on progression rates	Student satisfaction/NSS scores adversely affected across multiple areas and some effort and expense required to recover Increase in appeals across multiple disciplines or group complaints Significant impact on student recruitment (numbers of applicants) Drop in entry standards (but above quality thresholds) Achievement of KPIs threatened	Student satisfaction/NSS scores significantly adversely affected across multiple areas and significant effort and expense required to recover Significant increase in appeals across multiple disciplines or group complaints Significant decrease in progression rates Significant impact on student recruitment requiring drop in intake quality thresholds	Widespread and extreme student dissatisfaction with protests Quality of academic provision seriously jeopardised and long term viability undermined
Financial Sustainability	Operating costs increase, revenue loss (excluding that deriving from damage to research reputation) or one time financial loss of less than £500K	Operating costs increase, revenue loss (excluding that deriving from damage to research reputation) or one time financial loss of between £500K-£1M	Operating costs increase, revenue loss (excluding that deriving from damage to research reputation) or one time financial loss of between £1M-£2.5M	Operating costs increase, revenue loss (excluding that deriving from damage to research reputation) or one time financial loss of between £2.5M-5M	Operating costs increase, revenue loss (excluding that deriving from damage to research reputation) or one time financial loss of greater than £5M

RISK MEASUREMENT CRITERIA (INFORMATION SECURITY FRAMEWORK)

Definitions: short term: 1 week to 5 months medium term: 6 months to one year long term: in excess of a year

Risk Area	**Impact**				
	Negligible	**Minor**	**Moderate**	**High**	**Major**
Health & Safety	Minor distress caused to individual environmental damage – small scale, locally contained, short term and reversible (no threat to health) Short term loss of/ access to facilities or specialist equipment	Reportable (RIDDOR) Dangerous Occurrences or Minor Injuries Short term minor stress caused to individual or minor distress caused to group environmental damage – short term, not reversible or with minor local impact on health Medium term loss of/ access to specific facilities or loss of specialist equipment	Reportable (RIDDOR) Major Injuries and incidents affecting individuals Moderate distress or stress caused to individuals or a group Individual cases of life-threatening disease Medium term or locally contained environmental damage with minor to moderate local impact on health Medium term loss of key facilities or individual buildings	Major life changing injuries (e.g. tetraplegia) to individual Major Injury, distress or stress caused to group Spread of life threatening disease Long term environmental damage Hazardous material escape causing external environmental damage and short term effect on public health Long term/ permanent loss of key facilities or individual buildings	Fatalities Hazardous material escape causing irreparable external environmental damage and serious threat to public health Long term/ permanent loss of use of entire sites
Staff Experience	Individual staff dissatisfied or morale of small a group minimally affected Small number of individual grievances Short term/ localised effect	Staff morale of a group affected with some targeted effort required to recover	Staff morale of a large group damaged with targeted effort and expense required to recover Significant increase in grievances Adverse effect on staff retention and recruitment in affected area	Significant and widespread damage to staff morale and significant effort and expense required to recover Action short of a strike and threat of wider industrial action	Widespread and extreme staff dissatisfaction, protests and industrial action Significant adverse effect on staff retention and recruitment Long term/pan University effect

RISK MEASUREMENT CRITERIA (INFORMATION SECURITY FRAMEWORK)

Definitions: short term: 1 week to 5 months medium term: 6 months to one year long term: in excess of a year

Risk Area	Impact				
	Negligible	Minor	Moderate	High	Major
Legal obligations	Technical breaches which may result in complaints to the University but complainant does not resort to legal action or regulatory referral Breach results in minimal or no damage or loss	Fines or claims brought of less than £50K Case referred by complainant to regulatory authorities who may request information or records as a result Regulatory action unlikely or of only localised effect. Advisory/ improvement notices	Fines or claims brought of between £50K-£250K Case referred by complainant to regulatory authorities and potential for regulatory action with more than localised effect Enforcement action notices.	Fines or claims brought of more than £250K University required to report serious matter to regulators Formal external regulatory investigation into organisational practices with potential for suspension of significant elements of University operations	Formal external regulatory investigation involving high profile criminal allegations against management and threat of imprisonment Withdrawal of status or imposition of sanctions resulting in forced termination of mission critical activities

Scoring and Weighting

Risk Area	Impact					
	No impact	Negligible	Minor	Moderate	High	Major
Corporate Reputation	0	1	2	4	6	8
Research Profile & Research Income	0	1	2	4	6	8
Student Experience	0	1	2	4	6	8
Financial Sustainability	0	1	2	4	6	8
Health & Safety	0	1	2	4	6	8
Staff Experience	0	1	2	4	6	8
Legal obligations	0	1	2	4	6	8

Likelihood Definitions

Classification	Low	Medium	High
Likelihood	Unlikely	Possible	Likely
Description	0% - 20% chance of occurrence in the next 5 years. Slight chance of occurrence. Has not occurred before, but may occur in exceptional circumstances Not dependent on external factors	21 – 50% chance of occurrence in the next 5 years. Moderate possibility of occurrence History of similar occurrences, situations or near misses. Could be difficult to control due to external factors.	At least a 50% chance of occurrence in the next 5 years. Strong possibility of occurrence History of previous occurrence. Very difficult to control due to significant external factors.

Appendix G

RISK ACCEPTANCE V1.0

RELATIVE RISK MATRIX

High	> 50%	🟨	🟨	🟧	🟧	🟥
Medium	21 - 50%	🟩	🟩	🟨	🟧	🟥
Low	< 20%	🟩	🟩	🟨	🟨	🟧
Likelihood Impact score (cumulative)		1-7	8-19	20-31	32-44	45-56

RISK ACCEPTANCE CRITERIA

	Description	Setting Risk Management Priorities	Project based risk assessment
Pool 1 Risks	Severe	Immediate priority to be addressed or suspend/close activity	Planned project should not proceed without mitigation.
Pool 2 Risks	Substantial	Next priority to be addressed after pool1 risks are mitigated	Requires very careful on-going management with frequent, regular evaluation of the risk factors.
Pool 3 Risks	Moderate	Next priority to be addressed after pool 1 and 2 risks are mitigated	May be acceptable for major projects but not normally acceptable in the context of individual staff activities or student projects.
Pool 4 Risks	Tolerable	No active mitigation currently required	Lowest and preferred level of risk. Re-assessment or risk factors conducted at regular intervals.

Appendix H

Risk Register

Risk ID	Date Identified	Risk Description	Likelihood	Impact	Risk Rating	Control Measure (mitigation)	Control Owner	Target Risk Rating	Target Date	Risk Owner
1.0	01/01/2013	Risk expressed in the terms: As a result of... There is a risk that.... Which may...	Low Medium High	1 - 56	Severe Substantial Moderate Tolerable		Is responsible (name and role) for actioning the mitigation action	Medium x 31 = Substantial	01/01/2014	Is accountable (name and role) for ensuring the risk is effectively managed.

Appendix I

KEY INFORMATION ASSETS

Research information:

- Data collected for/used in analysis
- Research management info
- Research outputs
- Intellectual property

Financial information:

- External expenditure
- Income received
- Internal allocation
- Financial forecasting
- Assets & liabilities

Estates information:

- Inventory of buildings & rooms
- Consumption
- Usage (including hazardous materials)
- Maintenance
- Access control systems

Student & Applicant information:

- Academic record
- Administrative Info
- Pastoral support

Student Recruitment information:

- Marketing strategy & materials
- Open day and outreach event information
- International Foundation programme student information

Education information:

- Taught course delivery
- Assessment delivery
- Educational resources
- Timetabling

Staff information:

- Management of employment
- Training & development
- Welfare & health

Other business critical information:

- External engagement/ Fundraising/Alumni
- Policy & committee records
- Library catalogue and borrowing records
- Student Residences management Information

Information asset register tool – University of Oxford

A pragmatic approach, deploying a quick and easy-to-use tool, has been used to identify information assets that are extremely important for the business of the University (crown jewel assets) and are at the same time potentially vulnerable. The tool is designed to be used by departments, faculties, colleges and institutes. 'Assets' in this context include lists or documents or tables or spreadsheets holding information which has value (either electronically or in filing cabinets).

This Information Asset Register tool enables: identification and recording of crown jewel assets; assigning those accountable for the assets; and performing a risk assessment against the identified assets. It enables a university to focus its mitigation efforts on the most important areas.

The tool has been used by Oxford and also by universities across the world. A significant level of consistency is beginning to emerge in terms of identification of specific types of crown jewel assets that are considered to be vulnerable and require mitigation.

Further details of the Information Asset Register tool are given at: http://www.it.ox.ac.uk/policies-and-guidelines/is-toolkit/information-asset-management#d.en.158803; the tool can be downloaded from the same web page. It is intended to develop the tool, please send proposals for improvement to the email address given.