Integrated
Research Campus

UNIVERSITY OF LEEDS

Information Security
Risk Treatment Procedure

Version 1.0

Version Date 20/10/2016

Document Information

Reference	IRC ISRT PROC
Category	ISMS Documents
Title	Information Security Risk Treatment Procedure
Purpose	Procedure for risk treatment in the IRC
Version	1.0
Status	Approved, External
Owner	IRC Information Governance Management Group
Author	Samantha Crossfield
Compliance	ISO 27001 for scope defined in IRC Framework of the Information Security Management System
Review plan	Set in the IRC IS Documentation Procedure
Related Documents	University of Leeds Information Protection Policy IRC Framework of the Information Security Management System

Version History

Version	Date	Change description
0.1	27/06/2016	Initial version
1.0	20/10/2016	Submitted for sign off

Sign-Off

Name	Date	Role
Barry Haynes		Chair of IGMG and Head of Enterprise Architecture, University of Leeds

Master version:

Signature…….

Table of Contents

1. Purpose

The Integrated Research Campus (IRC) is a University of Leeds Central IT provision. It provides secure technical infrastructure and services for research data handling, analytics, application processing and development. This document is part of the IRC information security management system (ISMS).

The IRC Framework of the Information Security Management System sets the IRC IS objectives and which of these are met through the procedures defined in this document.

This document defines the standard operating procedure (SOP) for treating information governance and security risks to the IRC that have been logged during risk assessment. It sets out how to identify treatment options and implement the appropriate controls to modify risks and to sign-off residual risk in a justifiable way. This procedure sets a risk treatment process that aligns with international standards including ISO 27001 and ISO 31000.

2. Applicability

This SOP applies to the IRC Data Services Team and other employees or contractors who treat information security and governance risk within the scope of the IRC ISMS. It is also for use by the IRC Information Governance (IG) Management Group, IG Officer and Data Protection Officer who oversee and prioritise risk treatment plans and own residual risk.

3. Risk Treatment

Risk treatment involves reviewing, prioritising and implementing the risk-reducing controls recommended from the IRC Risk Assessment and IRC Project Risk Assessment. It is a cycle of assessment and implementation, triggered by system or project changes and by the IRC IG Management Group's annual ISMS review. The process is: the IRC Data Services Team fill out the IRC Risk Treatment Plan (Appendix 1), submit it to the IG Management Group for sign-off, and implement any approved controls.

While it is improbable that all risk is eliminated, the IG Management Group oversee that the most appropriate controls are employed to reduce risk to an acceptable level using the least-cost approach, with minimal adverse impact to the IRC. The IRC IS Risk Assessment Procedure defines 'acceptable' risk based on the IRC scope and

IS objectives set out in the **IRC Framework of the Information Security Management System**.

4. Risk Treatment Options

The following treatment options can be applied to mitigate risk:

1. **Risk Assumption:** Make an informed acceptance of the risk and continue system operations or apply controls to lower the risk to an acceptable level
2. **Risk Avoidance:** Eliminate the risk cause and/or consequence (e.g. forgo certain system functions or shut down the system when risks are identified)
3. **Risk Limitation:** Implement controls to minimize the adverse impact of a threat's exercising a vulnerability (e.g. use controls to support, prevent, detect)
4. **Risk Planning:** Manage risk by developing a risk mitigation plan that prioritises, implements, and maintains controls
5. **Research and Acknowledgment:** Lower the risk of loss by acknowledging the vulnerability or flaw and researching controls to correct the vulnerability
6. **Risk Transference:** Transfer the risk by using other options to compensate for the loss, such as purchasing insurance.

Points adapted from the US National Institute of Standards and Technology Special Publication 800-30

The situation will determine which risk treatment options are appropriate – none are mutually exclusive. The IRC Data Services Team selects the appropriate option for each risk and the prioritisation of treatments, based on the risks that have been assessed to pose greatest risk to IRC objectives. Any vendor security products and administrative measures to be utilised are also selected based on compatibility with IRC objectives. The treatment selection is recorded in the IRC Risk Treatment Plan (Appendix 1) and signed-off by the IG Management Group.

5. Risk Treatment Strategy

Figure 1 depicts the flow for identifying when a risk treatment strategy is required.

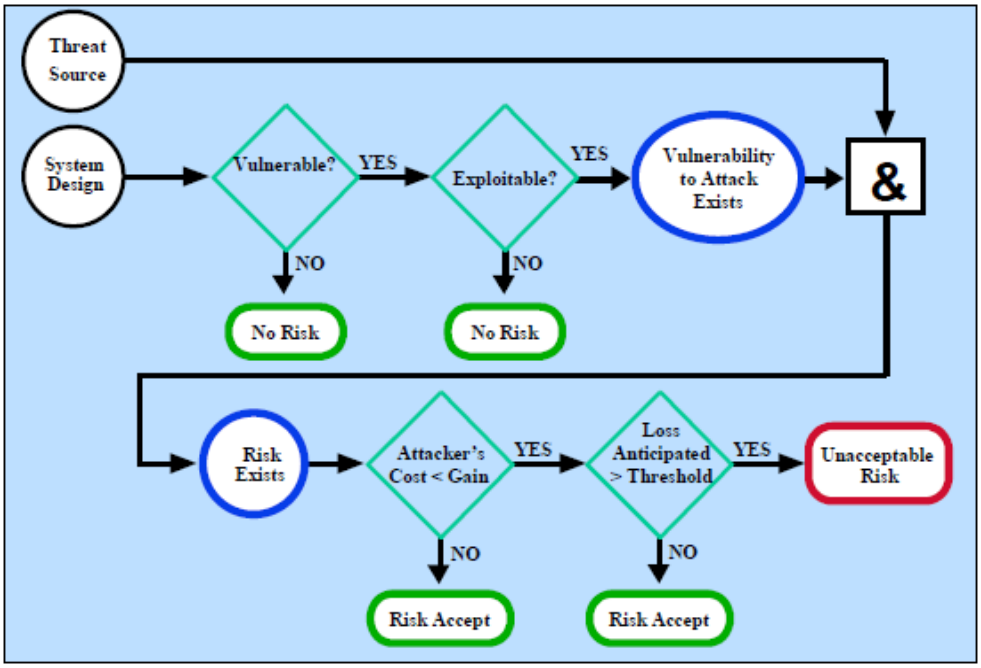

Figure 1 Flow chart for identifying a risk treatment requirement (*taken from the US National Institute of Standards and Technology Special Publication 800-30*)

The IG Management Group review the risk assessments using this flow. Where a 'yes' point is reached a risk treatment strategy is required:

1. When vulnerability (or flaw, weakness) exists → implement assurance techniques to reduce the likelihood of a vulnerability's being exercised
2. When a vulnerability can be exercised → apply layered protections, architectural designs, and administrative controls to minimize the risk of or prevent this occurrence
3. When the attacker's cost is less than the potential gain → apply protections to decrease motivation by increasing the attacker's cost (e.g. use system controls such as limiting what a user can do, to reduce an attacker's gain)
4. When loss is too great → apply design principles, architectural designs, and technical and nontechnical protections to limit the extent of the attack, thereby reducing the potential for loss

Points adapted from the US National Institute of Standards and Technology Special Publication 800-30

6. Approach for Control Implementation

When the need for a risk treatment strategy is identified (Section 5) then the below steps are taken to implement the most suitable control actions. This method is designed to mitigate risks based on their potential impact as calculated from an IRC risk assessment and to minimise the impact on capabilities and the cost of doing so.

The IRC Risk Treatment Plan (Appendix 1) takes the IRC Data Services Team through the steps for control implementation. The IG Management Group sign-off the plan.

- Step 1 - Prioritize Actions

Prioritise actions based on the risk levels presented in the risk assessment. Priority in resource allocation is given to risk items with unacceptably high risk rankings (e.g., risk assigned a Very High or High risk level). These vulnerability/threat pairs will require immediate corrective action to protect the IRC's interest and mission.
Output from Step 1 - **Actions ranking from High to Low**

- Step 2 - Evaluate Recommended Control Options

The controls recommended from the risk assessment may not be the most appropriate and feasible for a specific organization and IT system. During this step, analyse the feasibility (e.g., compatibility, user acceptance) and effectiveness (e.g., degree of protection and level of risk mitigation) of the recommended control options. The objective is to select the most appropriate control for minimising risk.
Output from Step 2 - **List of feasible controls**

- Step 3 - Conduct Cost-Benefit Analysis

A cost-benefit analysis aids management in decision making and to identify cost-effective controls.
Output from Step 3 - **Cost-benefit analysis describing the cost and benefits of implementing or not implementing the controls**

- Step 4 - Select Control

Management determines the most cost-effective control/s for reducing risk in the IRC ISMS scope. The controls selected combine technical, operational, and management control elements[1] to ensure adequate security for the IT system and the IRC.
Output from Step 4 - **Selected control(s)**

- Step 5 - Assign Responsibility

Appropriate persons (in-house or external contracting staff) who have the expertise and skill-sets to implement each control are identified and assigned responsibility.
Output from Step 5 - **List of responsible persons**

- Step 6 - Develop a Safeguard Implementation Plan

During this step, the safeguard implementation plan is completed. The plan contains, at a minimum, the following information:

[1] The definitions for these control categories are used as defined NIST SP 800-18, *Guide for Developing Security Plans for Information Technology Systems*.

- Risks (vulnerability/threat pairs) and associated risk levels (output from risk assessment report)
- Recommended controls (output from risk assessment report)
- Prioritized actions (priority given to items with Very High and High risk levels)
- Selected planned controls (determined on the basis of feasibility, effectiveness, benefits to the organization, and cost)
- Required resources for implementing the selected planned controls
- Lists of responsible teams and staff
- Start date for implementation
- Target completion date for implementation
- Maintenance requirements

This plan prioritizes the implementation actions and projects the start and target completion dates. It will aid and expedite the risk mitigation process. The IRC IG Management Group sign-off this plan before the next step proceeds.
Output from Step 6 –Safeguard implementation plan

Step 7 - Implement Selected Control(s)
Implement controls that reduce the number of flaws, add targeted controls, or reduce the magnitude of threat impact. Depending on the situation, the implemented controls may lower the risk level but not eliminate the risk.
Output from Step 7 - **Residual risk log**

Input	Risk Mitigation Activities	Output

outlines the approach for control implementation.

Following control implementation, there is ongoing monitoring of IS controls. The IRC IS Audit and Management Procedure sets how this is audited.

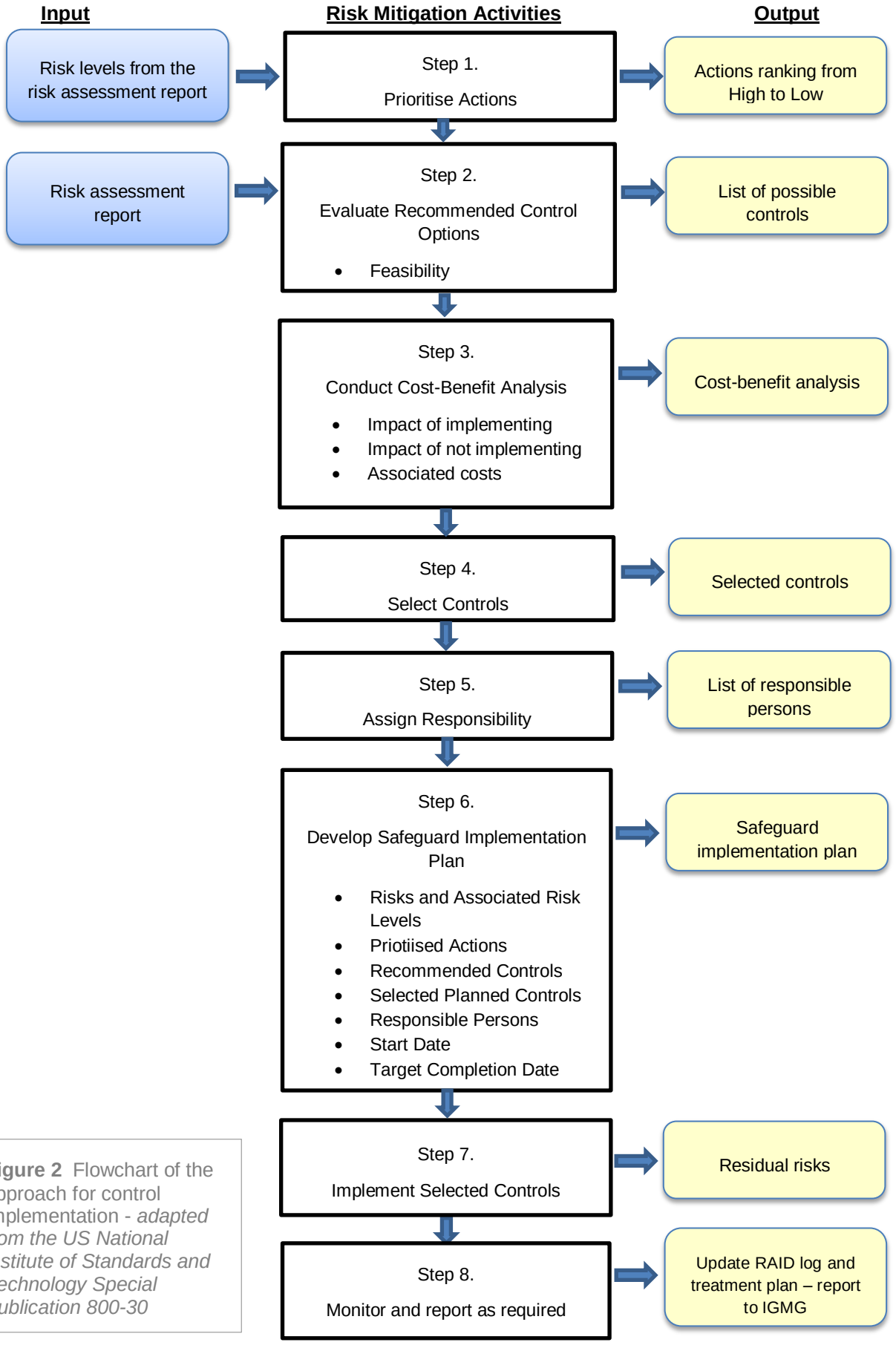

Figure 2 Flowchart of the approach for control implementation - *adapted from the US National Institute of Standards and Technology Special Publication 800-30*

7. Cost – Benefit Analysis

A cost-benefit analysis is conducted by the IRC Data Services Team during step 3 of the control implementation procedure (Section 6). It ensures that controls are appropriate – their cost of implementation can demonstrably be justified by the anticipated reduction in risk level. The cost of the control should be less than the cost of the risk (in terms of impact on organisational capability and credibility).

The cost-benefit analysis determines the impact of implementing *and* not implementing the new or enhanced control. This involves estimating the costs of implementation in terms of purchases, licences, further policy implementation, maintenance, training, staff costs and any reduction in operational effectiveness that results from enhanced security. The criticality of any systems and data involved is considered in order to determine any costs and the effect of non-implementation on the risk criteria defined in the IRC IS Risk Assessment Procedure**.**

The analysis outputs an assessment of which controls should be implemented, based on the IS objectives (**IRC Framework of the Information Security Management System**). The IRC IG Management Group review and sign this off. It is recognised that cost – benefit may not always be quantifiable, but one of the below outcomes should be justifiably assigned to each control:

1. If control reduces risk more than is needed, then see whether a less expensive alternative exists
2. If control costs more than the risk reduction provided, find another control
3. If control does not reduce risk sufficiently, then look for more controls or a different control
4. If control provides enough risk reduction and is cost-effective, then use it

Points from the US National Institute of Standards and Technology Special Publication 800-30

8. Residual Risk

Having implemented the selected controls, the IRC Data Services Team completes the residual risk log in the IRC Risk Treatment Plan (Appendix 1). This records the extent of risk reduction that has occurred in terms of reduction to threat likelihood and impact to the IRC's mission, and logs the residual risk. The IG Management Group signs the residual risk log to accredit the controls, accept the residual risk and authorise continued operations. The risk management cycle of assessment and treatment is re-iterated if residual risk is above the acceptable threshold for the risk criteria highlighted in the **IRC IS Risk Assessment Procedure**.

9. Risk Ownership and Review

The IRC IS Audit and Management Procedure sets the Chair of the IRC IG Management Group as the **Senior Information Risk Owner**. The **Data Protection Officer** and **Information Governance Officer** are responsible for ensuring that the IRC Data Services Team conduct risk assessments and implement risk treatment plans as set out in the **IRC IS Audit and Management Procedure**, **IRC IS Risk Assessment Procedure**, and **IRC IS Risk Treatment Procedure**. In summary, this is following:

1. A security breach or near-miss
2. A change or proposed change to IRC ISMS or projects
3. To inform the annual risk review by the IG Management Group

Documentation produced during the process are maintained as per the IRC IS Documentation Procedure.

Appendix 1: IS Risk Treatment Plan

IRC Information Security Risk Treatment Plan

Risk Treatment Plan Details

Title	IRC_RiskTreatmentPlan_[ccyymmdd of approval]
Assessor	IRC Data Services Team
Approval	IRC Information Governance Group Chair
Date of approval	
Related documents	IRC Framework of the Information Security Management System, IRC IS Risk Assessment Procedure, IRC IS Risk Treatment Procedure

1. Prioritise Options

Take treatment recommendations from the prioritised risk registry and risk evaluation in the risk assessment. The IRC risk acceptance level (IRC IS Risk Assessment Procedure) is low so fill in the table for risks with a current risk rating above one:

Option: *Outline the option*
Priority: *Current risk rating, 1 (low to 5 (high)*
Sort the table based on priority and assign an ID, 1 to n

Risk ID	Option ID	Priority	Option

2. Option Evaluation

Costs: *outline the resources required, including staff time, training, maintenance, infrastructure, licence or hardware purchases, reduction in operational effectiveness,*
Compatibility: *outline the compatibility with IRC aims and user acceptance*
Effectiveness: *outline the afforded degree of protection and risk mitigation*

Option ID	Costs	Compatibility	Effectiveness

3. Cost-Benefit Analysis

Use the above information to fill in the following table:
Feasibility: *anticipated cost, compatibility and likelihood of success, 1 (low) to 5 (high)*
Residual risk rating: *anticipated rating after the treatment is conducted, 1 (low) to 5 (high)*

Option ID	Priority *1-5*	Feasibility *1-5*	Residual risk rating *O*	Risk change *C - O*

4. Select and Assign Controls

Select the most effective control/s to reduce IS risk. A control must be selected when one or more of the following apply:

- Priority > 3
- Risk change > 3
- Feasibility > 3

For remaining options, either:

- Select the control *(record this in Section 5)*
- Accept the risk

Order the selected controls first by Priority, then by Risk change and Feasibility, and set the safeguard implementation plan:

- Sort the above table by a) Priority; b) Risk change; c) Feasibility
  Select Table Tools > Layout > Data > Sort
- Assign the Option IDs to an Action order, 1 to n *1 = first to be actioned*
- For each control, determine:
  - Implementation start and completion date
  - New maintenance or monitoring requirements to ensure effectiveness
  - Where responsibility lies (person, team or organisation)

Action	Option ID	Start date	End date	Maintenance / monitoring	Responsible persons
1					
2					
3					
4					
5					
6					
7					
8					
9					
10					
11					
12					
13					
14					
15					

5. Risk Acceptance

Record the following in the residual risk log:

- Any accepted risks (Section 4)
- Any residual risks (calculated in Section 3) that will remain following the implementation of controls (Section 4)

Residual Risk	Option ID	Risk Rating *1-5*	Justification

6. Statement of Applicability

The IRC Information Governance (IG) Management Group sign-off the safeguard implementation plan and own any residual risk, based on the justifications in this treatment plan.

IG Management Group Chair:

Name……

Signature……...

Date……