POLICY AND GUIDANCE
Do not Photocopy

Document Information Classification: Unrestricted

Title:	**Risk Management Process**
Effective Date:	**25 Sep 2019**
Reference Number:	**ISMS-02-05**
Version Number:	**3.5**
Owner:	**Risk Management Process Owner,**
Review Date:	**25 Sep 2021**

Table of Contents

1. Purpose

This document defines the risk management process for Information Security Management that is used to identify possible risks, problems or disasters before they happen. This process allows the organisation to assess the risks and to set up procedures to avoid the risks or minimize their impact. This also ensures the organisation complies with legal obligations and can establish and maintain a business continuity plan.

2. Scope

This document applies to all assets under the ownership or control of the TRE.

3. Responsibilities

Management Sponsor is responsible for:

- Assisting the Risk Owner in managing risks classified as “Very High”

The Information Security Steering Group (ISSG) is responsible for:

- Initiating a detailed risk assessment for all risks that exceed the risk assessment threshold
- Assisting the Risk Owner in managing risks classified as “High”
- Reviewing the output of risk assessment and risk treatment at ISMS Management Review meetings
- Reviewing the risk register at ISMS Board meetings

The ISMS Risk Management Process Owner is responsible for:

- Managing the Information Security Risk Register ISMS-02-06
- Routinely reviewing the Risk Register with the TRE Asset Owners and Risk Owners
- Making changes to the risk register if any information requires amendment

The Information Security Manager (ISM) is responsible for:

- Presenting risks classified as “Very High” or “High” at the ISMS Management Review meetings on behalf of the ISMS Risk Management Process Owner

TRE Asset Owners and are responsible for:

- Completing the high level and detailed risk assessments
- Identifying any changes to their risks and informing the ISMS Risk Management Process owner

The Risk Owner is responsible for:

- Managing their risks
- Identifying and completing the required treatment actions
- Reporting issues, requirements and potential knock-on effects for the proposed risk treatments
- Communicating risks and treatments to TRE staff, users and stakeholders as appropriate
- Identifying any changes to their risks and informing the ISMS Risk Management Process owner

4. Procedure

Organizations and people that use computers can describe their needs for information security and trust in systems in terms of three major requirements:

- Confidentiality: controlling who gets to read information;
- Integrity: assuring that information and programs are changed only in a specified and authorized manner; and
- Availability: assuring that authorized users have continued access to information and resources.

For the purpose of the risk assessment process it shall be considered that the primary asset is the data managed by the TRE and this is strictly confidential. If impacted it has the potential to cause serious damage or distress to individuals or serious damage to the University's interests e.g. highly sensitive private information about living individuals, business activity with the potential to seriously affect commercial interests and/or the University's corporate reputation, information that facilitates the protection of critical functions and key assets including passwords and administration account information. The individual assets that could affect this primary asset include, but are not limited to:

- Information e.g. passwords, source code, system documentation, intellectual property, data for regulatory requirements, network infrastructure design
- Technology e.g. servers, desktop computers, laptops, tablet, smart phones, server application software, end-user software, development tools, routers, network switches, PBXs, removable media, power supplies, uninterruptible power supplies
- Services e.g. batch scheduling, instant messaging, Active Directory service, Domain Name service (DNS), Dynamic Host controls Configuration Protocol service (DHCP), enterprise management tools, file sharing, storage, dial-up remote access, Telephony Virtual Private Networking (VPN) access, collaboration services
- People e.g. subject matter experts, administrators, developers, third party support, end-users

The effect these assets have on the TRE data is defined as their *impact* and assigned a numerical value [score] according to the severity of that impact.

These requirements will be used to assess the impact of risks to the organisation through the Risk Assessment process. This process has two levels:

- **High-level risk assessment:** the purpose of the high-level risk assessment is to identify all information assets in the organisation i.e. all assets that may affect the security of the data in the TRE. A value is assigned to each asset in terms of the worst-case impact the loss of confidentiality, integrity or availability of the asset may have on the organisation. This determines the value of the asset to the organisation and is used to assess if the asset should be taken through to the next stage of the process for a detailed risk assessment. High-level risk assessment can take the form of an audit or self-assessment by the operator or owner of the asset. Assets that are indicated as exceeding the risk assessment threshold will be required to undergo a detailed risk assessment.

- **Detailed risk assessment:** the purpose of the detailed risk assessment is to take into account the threats that may exploit vulnerabilities of the high-value assets and the likelihood of the breach or attack. This risk assessment should be conducted by an expert in the asset subject or asset owner.

4.1. High-level Risk Assessment

The steps for high-level risk assessment are as follows:

1. Identify the asset in the TRE and the individual required to perform the assessment. Note: assets such as people or groups of similar assets may have a group assessment.
2. Identify the value of the asset using the Confidentiality, Integrity and Availability (CIA) criteria (Table 1). Value = Confidentiality + Integrity + Availability.
3. Record the high-level risk assessment details in the Risk Register (ISMS-02-06)
4. Any asset with a single C, I or A value >=4 or a combined value of >=8 will require a detailed risk assessment.

4.2. Detailed Risk Assessment Procedure

The steps for a detailed risk assessment are as follows:

5. Identify the information asset in the TRE and confirm the value of the asset using the Confidentiality, Integrity and Availability (CIA) criteria (Table 1).
6. Identify any threats that may exploit vulnerabilities of the asset.
7. Define the associated risk and describe the impact on the CIA criteria
8. The values for each of the CIA criteria can be adjusted to account for specific incidents or risks.
9. The maximum of the CIA criteria shall be the Risk Impact.
10. Determine the Likelihood of the risk occurring (Table 2)
11. Calculate the Risk Score = Impact x Likelihood
12. Categorize the risk level e.g. “Very High”, “High” etc.(Table 3)
13. Assign a Risk Owner to manage the risk and complete the remaining activities
14. Identify the treatment approach to managing the risk including any mitigating actions and contingency plans as necessary
15. Update the risk details in the Risk Register (ISMS-02-06)
16. Communicate the risk to the relevant stakeholders and manage the risk throughout its lifecycle.

4.3. Risk Assessment Schedule

- The Risk Owners will review their existing risks on a bi-monthly basis and any changes will be updated into the Risk Register (ISMS-02-06).
- New risks can be identified by TRE Asset Owners or existing Risk Owners at any time.
- The ISSG will review any “Very High” or “High” risks during the ISMS Board Meetings that take place every 2 months. A review of any new risks will also take place during these meetings.

4.4. Risk Assessment Values

The following sections contain the information necessary to support the risk assessment process.

4.4.1. Assigning Risk Impact Values

Assets are valued on the maximum of the scores of the Confidentiality, Integrity and Availability (CIA) criteria. Each of the criteria is scored according to the table below dependent upon the ability of the asset to impact the TRE data (the Primary Asset).

Table 1: CIA score definition guidance

Value	Confidentiality	Integrity	Availability	Additional Value Measures (can be applied across all of the criteria)
1	• No impact on data confidentiality	• No impact on data accuracy or consistency • Any corruption or loss of data would not impact operations	• Temporary loss of availability would have a minor impact on normal operations • Asset can be quickly restored within 1 working day	• Small number of individual correspondence/ representations • No measurable impact on research activity within specific teams • No impact on research income • 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

Value	Confidentiality	Integrity	Availability	Additional Value Measures (can be applied across all of the criteria)
2	• Minor impact on data confidentiality (e.g. small subset of non-traceable data released) • Disclosure of the information would cause only minor embarrassment or minor operational inconvenience	• Minor impact on data accuracy or consistency but does not affect collaborators • Any corruption or loss of data is retrievable with minimal effort	• Temporary loss of availability would have a minor impact on normal operations • Asset can be restored within 3 working days	• Reputation is minimally affected with little or no targeted effort or expense required to recover; • Small impact on research activity within specific teams • Mild stakeholder correspondence/ representations • Minor impact on research income or productivity for wider group • Regulatory action unlikely or of only localised effect. • Advisory/improvement notices
3	• Moderate impact on data confidentiality • Disclosure of the information would cause some reputational damage and has a short-term impact on operations	• Data corruption or loss has a noticeable impact on collaborators • Corruption requires resources and time to resolve	• Loss of availability of this asset would impact normal operations and prevent collaborators from accessing our services or data • Asset and availability can be restored within 5 working days	• Reputation is damaged in the short to medium term with targeted effort and expense required to recover. • Public stakeholder comment and correspondence expressing concern • Low key local or regional interest media coverage • Medium term effect on productivity within discipline • Case referred by complainant to regulatory authorities who may request information or records as a result • Enforcement action notices.

Value	Confidentiality	Integrity	Availability	Additional Value Measures (can be applied across all of the criteria)
4	• Significant proportion of the data is accessible or released • Disclosure of the information has a significant impact on operations or tactical objectives	• Corruption or loss of data/asset would restrict operations and cause loss of collaborator confidence • Corruption requires significant resources and time to resolve	• Loss of availability of this asset would affect several processes and would prevent collaborators from accessing our services or data • Availability cannot be restored within 10 working days and requires specific skills/personnel or significant resources	• Significant public and private comment from stakeholders expressing serious concerns • Adverse regional or national interest media coverage • Medium to long term effect on productivity in more than one discipline • Incident requires escalation to UoM Data Protection Officer or IG SIRI • University required to report serious matter to regulators • Case referred by complainant to regulatory authorities and potential for regulatory action with more than localised effect
5	• All of the data is accessible or released • Disclosure of the information has a serious impact on long term strategic objectives or puts the survival of the organization at risk.	• Corruption or loss of data halts all operations and would cause major loss of collaborator confidence. • Corruption requires extensive resources and time to resolve	• Loss of this asset would prevent the TRE from operating and providing any of its services to its collaborators • Availability cannot be restored within 20 working days and requires specific skills/personnel or significant resources	• Reputation damaged for the long term or irrevocably destroyed • Adverse high profile, national media coverage from reputable/ influential media, with some international interest • Incident requires escalation to UoM Data Protection Officer or IG SIRI • Formal external regulatory investigation into organisational practices with potential for suspension of significant elements of University operations • Withdrawal of status or imposition of sanctions resulting in forced termination of mission critical activities

4.4.2. Assigning Likelihood Values

The examples given cover either the frequency of attack or whether the attacker would require specified levels of knowledge, experience or determination.

Table 2: Likelihood:

Value	Explanation	Examples
1	Never	Not happened in more than 3 years or The asset is heavily protected from threats, advanced expertise would be needed, and/or exploitation would require excessive effort. Exploitation of weaknesses is almost never seen in this or similar organisations.
2	Rare	Expected to occur once a year or Significant expertise and determination would be required to exploit weaknesses. Exploitation is possible but not likely.
3	Periodic	Expected to occur once a quarter or Moderate knowledge of processes and technology would be sufficient to exploit the asset. Effort required to exploit weaknesses is moderate.
4	Regular	Expected to occur once a fortnight or Some knowledge of processes and technology would be sufficient to exploit the asset. Effort required to exploit weaknesses is minor.
5	Frequent	Expected to occur once a week or No specific knowledge or experience is required to exploit processes and technology. No effort required to exploit weaknesses.

4.4.3. Risk Score Calculation

Risk Impact = Maximum of Confidentiality, Integrity or Availability
Risk Score = Risk Impact x Likelihood

Example:	Confidentiality	= 3
	Integrity	= 2
	Availability	= 5
	Likelihood	= 4

Risk Score = 5 x 4 = 20

Table 3: Risk Level

Score range	Risk level	Treatment Action
1-5	Low	Accept Risk
6-12	Medium	Possible action determined by ISM
13-18	High	Action determined by the ISSG
19-25	Very High	Priority action determined by Management sponsor

4.5. Risk Treatment

Risk treatment is part of the risk management process and is required to modify risks to the organisation using one of the following approaches:

- **M ITIGATE** the risk. Change the likelihood of the risk occurring or the consequences of the risk
- **A VOID** the risk. Choose to not start or continue a project, procedure or process that brings unacceptable risk to the organisation.
- **S UBSTITUTE** the risk. Remove the risk source and find a less risky alternative
- **T RANSFER** the risk. Share the risk with a 3rd party via contracts, agreements or insurance
- **A CCEPT** the risk by informed choice. Choose to accept possible unacceptable levels of risk in order to pursue an opportunity. Note: Mitigation is optional but contingency is mandatory.

Accepting a risk may leave the organisation exposed to unidentified risks, and risk treatment may create or modify existing risks therefore continuous monitoring and risk assessment is necessary.

Risk treatment may not initially modify the risk to an acceptable level, therefore repeated rounds of assessment, monitoring and treatment may be required to adequately manage the residual risk.

4.5.1. Risk Treatment Constraints

In addition to the impact of the risk on the organisation, and the perception of 3rd parties, the risk owner needs to consider various constraints that affect the range of treatment options. The constraints include, but are not limited to:

Constraints from pre-existing processes: Projects are not necessarily developed simultaneously. Some depend on pre-existing processes.

Technical constraints: relating to infrastructure, hardware and software, and rooms or sites housing the processes:

- Files (requirements concerning organisation, media management, management of access rules, etc.)
- General architecture (requirements concerning topology (centralised, distributed, client-server), physical architecture, etc.)
- Application software (requirements concerning specific software design, standards, etc.)
- Package software (level of evaluation, quality, compliance with standards, security, etc.)
- Hardware (build approach, quality, compliance with standards, etc.)
- Communication networks (coverage, standards, capacity, reliability, etc.)
- Building infrastructure (civil engineering, construction, power supply, etc.)

In some cases, it may be appropriate to apply procedural controls rather than physical controls.

Financial constraints: Available budget may restrict the implementation of security controls.

Environmental constraints: These arise from the geographical or economic environment in which the processes are implemented

Time constraints: The time required for implementing security controls should be considered in relation to the time to upgrade the information system; if the implementation time is very long, the risks for which the control was designed may have changed.

Resource constraints: The availability of personnel, skills and resources may affect the treatment options.

Constraints related to methods: Methods appropriate to the organisation's know-how will be used for project planning, specifications, development and so on.

Organisational constraints: Various constraints may follow from organisational requirements:

- Operation (lead-times, supply of services, surveillance, monitoring, emergency plans, degraded operation, etc.)
- Maintenance (incident troubleshooting, preventive actions, rapid correction, etc.)
- Human resources management (operator and user training, qualification for posts such as system administrator or data administrator, etc.)
- Administrative management (responsibilities, etc.)
- Development management (development tools, acceptance plans, organisation to be set up, etc.)
- Management of external relations (organisation of third-party relations, contracts, etc.)

Ease of use of the applied controls: the effect of controls on normal operations and personnel should be considered as there is little point applying controls that result in the creation of ‘work-arounds’.

Ethical and social constraints: Relating to social norms, the research being conducted and the organisations involved.

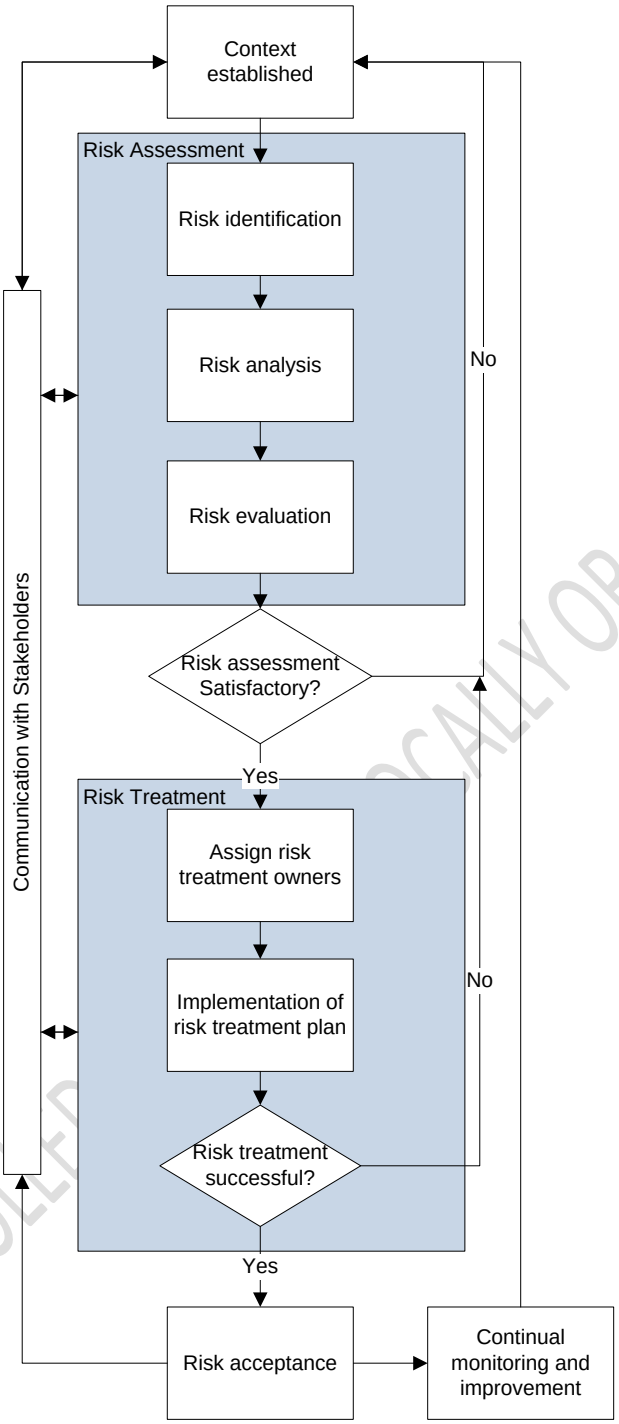
Legal constraints: Government guidance and codes, health and safety, legislative and regulatory compliance may affect the range of treatment options available.

4.6. Risk Treatment Process

Risk treatment follows on from successful and sufficient risk assessment and starts with a ranked set of risks in the Risk Register (ISMS-02-06).
The summary of risk treatment steps are as follows:

1. The appropriate manager will review the list of prioritised risks
2. Risk treatment activities will then be managed until all actions are responded to and closed
3. The appropriate manager (risk owner) will review the treatment and record if the treatment has been successful.
4. Treatment will be communicated by the appropriate manager to the relevant stakeholders
5. Any amendment to the Risk Register (ISMS-02-06) must only be done in response to a formal change request submitted within the Q-Pulse system. This prevents unauthorised modifications, and provides a clear summary of updates that can be references during periodic risk register reviews
6. The Risk Register (ISMS-02-06) will be updated and any residual risk will be recorded.
7. Risk treatments and their outcomes will be reviewed at the ISMS Review meetings (ISMS-04-01).

Risk treatment follows on from the risk assessment stage of the risk management process and is one stage in the continuous Plan-Do-Check-Act cycle. The diagram below details the high-level steps in the risk management process:



5. Cross-referenced ISMS Documents

Number	Type	Title
ISMS-02-06	ISMS\Policy & Guidance\ISMS Management - policy & guidance	Information Security Risk Register
ISMS-04-01	ISMS\Policy & Guidance\ISMS Improvement - policy & guidance	ISMS Management Review

SOP-03-08	ISMS\SOP\TRE Operations - SOP	TRE Change Control

6. Appendices

None