Information Risk Assessment Handbook

Title	Information Risk Assessment Handbook		
Document number	Add document number	**Document status**	Draft

Owner	CISO
Approver(s)	Information Security Team

Version	Version history	Version date
0.01-0.05	Initial drafts of handbook	26 Oct 2015

Preface and document control

This document is intended to provide information security policy, procedure, standards or guidance in respect of the University of Oxford and shall be reviewed at least annually to ensure validity.

1 Purpose 3
2 Scope 3
3 Responsibilities 3
4 Information risk assessments 3
4.1 Types of risk assessments 3
4.2 Information security risk register 4
4.3 Standard risk assessment 5
4.3.1 Risk scenario elements 5
4.3.2 Deriving the risk score 5
4.3.3 Risk scenario treatment options 6
4.3.4 Risk treatment plans and controls 6
4.3.5 Risk owners 6
4.3.6 Residual risks 6
4.4 Third Party Security Assessment (TPSA) 7
4.5 Cloud Security Checklist 7
4.6 Privacy impact assessment (PIA) 7
4.7 Business impact analysis (BIA) 7
5 Annexes 8
5.1 Asset scores 8
5.2 Likelihood scores 8
5.3 Impact scores 9
5.4 Risk scores, acceptance criteria and treatment options 9
5.5 Vulnerabilities and threats 10

1 Purpose

This handbook states the risk management approaches the Information Security Team (IST) will utilise to support the identification and management of information risks. The approaches within this handbook are aligned with industry good practice, including:

- ISO 27001: Information security management system – Requirements
- ISO 27002: Code of practice for information security controls
- ISO 27005: Information security risk management
- ISO 31000: Risk management — Principles and guidelines
- ISO 22301: Business continuity management systems – Requirements
- Cloud Security Alliance: Security, Trust & Assurance Registry (STAR)
- Information Commissioner's Office: Conducting privacy impact assessments code of practice

Additionally the risk management approaches within this handbook are aligned with the objectives stated in the University's Risk Management Policy.

2 Scope

The IST shall utilise the risk management approaches stated within this handbook to identify vulnerabilities, threats and mitigating controls associated with University business processes, people, technologies and services. This handbook and the supporting tools / resources can be adopted by any University department or college.

3 Responsibilities

The Chief Information Security Officer (CISO) is the owner of this handbook and shall ensure that it remains operationally fit for purpose and is appropriately communicated.

4 Information risk assessments

4.1 Types of risk assessments

The following risk management approaches will be capable of identifying the majority of known information security vulnerabilities and threats that could impact the University.

Standard risk assessment (CIA approach)	• **Used for generic asset based risk assessments, e.g. device or service** • Based on asset score, vulneranility level and threat likelihood • Risk mitigation based on industry good practice, e.g. ISO 27002
Third Party Security Assessment (TPSA)	• **Used to assess third parties who process University information** • Supports projects to identify risks relating to third parties • Supports procurement and legal due diligence
Cloud security checklist	• **Used to identify risks posed by cloud service providers (CSP)** • Identifies missing security controls in CSP's standard T&Cs or SLA • Can be used inconjunction with the TPSA
Privacy impact assessment (PIA)	• **Used to identify risks associated with processing personal information** • Can be applied to process, technologies or services
Business impact assessment (BIA)	• **Used to identify recovery time / recovery point objectives** • Can be applied to technologies, services, personnel and associated processes

4.2 Information security risk register

Risks identified from the varying risk management approaches shall be recorded in a suitable information security risk register. The IST shall maintain a central register on behalf of the University, to support the uniform recording of risks and management reporting.

As a minimum the following information shall be recorded for each risk:

- Unique risk number or identifier
- Date risk identified
- Asset(s) at risk
- Identified threat and vulnerability
- Risk scenario treatment option
- Risk owner or person accepting risk, e.g. Service Owner or Head of House/Department
- Identified risk treatment plan (RTP) or controls identified to mitigate risk
- Identified residual risk(s)
- Date risk last reviewed
- Risk closure date

4.3 Standard risk assessment

4.3.1 Risk scenario elements

The standard risk assessment utilises the formula built into Verinice and is aligned to ISO 27005:2011 Information security risk management and based on the Confidentiality, Integrity and Availability (CIA) of assets.

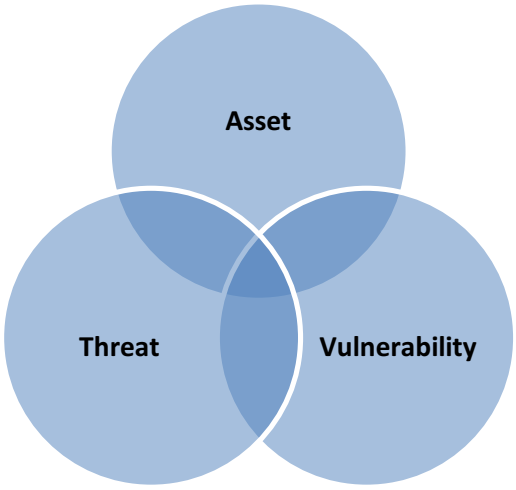
The definitions for CIA are:

- **Confidentiality** - property that information is not made available or disclosed to unauthorised individuals, entities, or processes
- **Integrity** - property of accuracy and completeness
- **Availability** -property of being accessible and usable upon demand by an authorised entity

(Definitions from ISO 27000 - Information security management systems - Overview and vocabulary)

The standard risk assessment approach is **risk scenario** based. Risk scenarios are built by considering three elements:

- Asset
- Vulnerability (ease of exploitation)
- Threat (likelihood of threat occurence)



E.g. unauthorised access (threat) by a hacker on a web server (asset) that is not adequately patched (vulnerability).

To support consistency of results and uniformity, the **risk scenario** shall utilise a common set of vulnerabilities and threats adapted from ISO 27005:2011 Information security risk management.

4.3.2 Deriving the risk CIA score

The risk analysis within Verinice requires the following scoring:

- Individual assets are scored for each CIA element, i.e. Low = 0, Medium = 1 and High = 2.
- Individual vulnerabilities are scored Very low = 0, Low = 1, Medium = 2 or High =3.
- Individual threats are scored Rare = 0, Annual = 1, Monthly = 2 or Weekly =3.

Once a vulnerability and threat has been associated with an asset, a risk analysis can be run within Verinice to derive the risk score for an asset. Each asset will have a derived risk score for CIA from adding the vulnerability and threat score to the original asset CIA score.

E.g. Asset CIA is Low, High, Medium (0, 2, 1) and vulnerability is Medium (2) and threat score is Weekly (3), then the derived risk CIA score for the asset is 5,7,6.

When summed the derived risk score will provide a numerical score between 0 and 24. Risk acceptance criteria and associated risk decision options have been set for these scores.

4.3.3 Risk scenario treatment options

The next step is to cross reference the risk score against the risk score matrix to identify one of the following risk scenario treatment options:

- **Accept** - a justifiable decision by the risk owner to accept and not implement a risk treatment plan to mitigate the risk.
- **Avoid** - typically involves either removing the asset, or changing or terminating the associated asset processes to avoid the risk.
- **Reduce** - implementation of a risk treatment plan to lower the residual risk to an acceptable level.
- **Transfer** – the risk is shared with another party that can most effectively manage the particular risk depending on risk evaluation.

The option to accept a risk shall be evaluated and periodically reviewed by the Information Security Team to ensure the original decision remains justifiable.

4.3.4 Risk treatment plans and controls

If the **risk scenario treatment option** is to avoid, reduce or transfer, then a **risk treatment plan (RTP)** shall be documented and communicated to the appropriate **risk owner** for approval and, where applicable, implementation.

The mitigating controls identified within the **RTP** shall be based on controls stated in ISO 27002 – Code of practice for information security, although where applicable, other security controls can be used.

4.3.5 Risk owners

For each **risk scenario** a **risk owner** shall be identified and recorded in the information security risk register. The **risk owner** shall be the person or entity with the accountability and authority to manage a risk. **Risk owners** are usually the asset or service owner, Heads of House or Heads of Department. Additionally there may be more than one **risk owner**.

4.3.6 Residual risks

Residual risk is the risk that remains after the risk treatment. Where applicable, **residual risks** shall be treated as a new **risk scenario** and be assessed accordingly.

4.4 Third Party Security Assessment (TPSA)

The **Third Party Security Assessment (TPSA)** is used to assess the security controls of third parties who will be processing University information as part of a contractual service or formal agreement. The **TPSA** is aligned to the control areas within ISO 27002 – Code of practice for information security. The **TPSA** control areas map to the headings used in the Security Schedule Template. Where applicable the Security Schedule Template shall be negotiated, agreed and included as an appendix within the overall contractual arrangement with relevant third parties.

4.5 Cloud Security Checklist

The **Cloud Security Checklist** is typically used to check whether a cloud service provider's standard terms and conditions or service level agreements contain adequate security controls to protect University information.

4.6 Privacy impact assessment (PIA)

A **privacy impact assessment (PIA)** is a process which helps the University to identify and reduce privacy risks that may exist within an information processing activity, e.g. business process, project, technology or service. A **PIA** enables the University to systematically analyse how a particular information processing activity will impact personal information and ensure that any processing is compliant with the Data Protection Act (DPA).

The University's Information Compliance Team provides services to enable compliance with risks relating to the DPA, personal information and privacy.

4.7 Business impact analysis (BIA)

The **business impact analysis (BIA)** is a process for assessing the impacts of disrupting activities on University business processes, people, technologies and services. The **BIA** shall include the following:

- identifying critical activities that support the day-to-day operations of the University;
- assessing the impacts over time of not performing these activities;
- setting prioritised timeframes for resuming these activities at a specified minimum acceptable level, taking into consideration the time within which the impacts of not resuming them would become unacceptable; and
- identifying dependencies and supporting resources for these activities, including suppliers, outsource partners and other relevant interested parties.

The output from a **BIA** supports the development of business continuity plans.

Individual departments and colleges are responsible for the development and maintenance of fit for purpose business continuity plans.

5 Annexes

5.1 Asset CIA scores and definitions

		Confidentiality	Integrity	Availability
0	**Low**	Information can be disclosed to any individual, entity, or process.	Information can be modified by all individuals, entities and processes.	No requirement to have continuous access to information.
1	**Medium**	Information is not public and available to a group of authorised individuals, entities and processes.	Information can be modified by a set of authorised individuals, entities and processes.	Short periods of information unavailability are tolerable but normally authorised individuals, entities and processes require access.
2	**High**	Information can only be disclosed to a privileged group of authorised individuals, entities and processes.	Information can only be modified by the owner or a privileged group of authorised individuals, entities and processes.	Information must be accessible to authorised individuals, entities and processes at all times.

5.2 Vulnerability level scores

Value	Explanation	Example
0	**Very low**	Vulnerability nearly impossible to exploit
1	**Low**	Vulnerability difficult to exploit and requires high level knowledge of asset
2	**Medium**	Vulnerability can be exploited with moderate knowledge of asset
3	**High**	Vulnerability can be easily exploited by any one

5.3 Threat likelihood scores

Value	Explanation	Example
0	**Rare**	Has not previously occurred in the last 2 years
1	**Annual**	Occurs once a year
2	**Monthly**	Occurs once a month
3	**Weekly**	Occurs once a week

5.4 Risk scores for CIA

Vulnerability level	Threat Likelihood	Confidentiality			Integrity			Availability		
		L	M	H	L	M	H	L	M	H
Very low	Rare	0	1	2	0	1	2	0	1	2
	Annual	1	2	3	1	2	3	1	2	3
	Monthly	2	3	4	2	3	4	2	3	4
	Weekly	3	4	5	3	4	5	3	4	5
Low	Rare	1	2	3	1	2	3	1	2	3
	Annual	2	3	4	2	3	4	2	3	4
	Monthly	3	4	5	3	4	5	3	4	5
	Weekly	4	5	6	4	5	6	4	5	6
Medium	Rare	2	3	4	2	3	4	2	3	4
	Annual	3	4	5	3	4	5	3	4	5
	Monthly	4	5	6	4	5	6	4	5	6
	Weekly	5	6	7	5	6	7	5	6	7
High	Rare	3	4	5	3	4	5	3	4	5
	Annual	4	5	6	4	5	6	4	5	6
	Monthly	5	6	7	5	6	7	5	6	7
	Weekly	6	7	8	6	7	8	6	7	8

5.5 Acceptance criteria for summed CIA scores

Range	Acceptance Criteria
Risk Score between 0 and 8	Within this range accepting the risk scenario without implementing controls may be considered. Before accepting a risk scenario, careful consideration shall be given to individual asset CIA , scores. A decision to accept a risk scenario within this range shall be justifiable and recorded in the information security risk register.
Risk Score between 9 and 16	Within this range it is **strongly advised** the risk scenario is reduced by implementing applicable controls. If a decision is made to accept a risk scenario within this range then the reason shall be justifiable, recorded in the information security risk register and have a designated risk owner.
Risk Score between 17 and 24	Within this range a risk scenario **cannot be accepted**.

5.6 Risk decision option definitions

Accept	A justifiable decision by the asset/risk owner to accept and not implement a risk treatment plan to mitigate the risk.
Avoid	Typically involves either removing the asset, or changing or terminating the associated asset processes to avoid the risk.
Reduce	Implementation of a risk treatment plan to lower the likelihood and/or impacts if a risk scenario occurred.
Transfer	The risk is shared with another party that can most effectively manage the particular risk depending on risk evaluation.

5.7 Vulnerabilities and threats

From ISO 27005: Information security risk management

Type	Examples of vulnerabilities	Examples of threats
Hardware	Insufficient maintenance/faulty installation of storage media	Breach of information system maintainability
Hardware	Lack of periodic replacement schemes	Destruction of equipment or media
Hardware	Susceptibility to humidity, dust, soiling	Dust, corrosion, freezing
Hardware	Sensitivity to electromagnetic radiation	Electromagnetic radiation
Hardware	Lack of efficient configuration change control	Error in use
Hardware	Susceptibility to voltage variations	Loss of power supply
Hardware	Susceptibility to temperature variations	Meteorological phenomenon
Hardware	Unprotected storage	Theft of media or documents
Hardware	Lack of care at disposal	Theft of media or documents
Hardware	Uncontrolled copying	Theft of media or documents
Software	No or insufficient software testing	Abuse of rights
Software	Well-known flaws in the software	Abuse of rights
Software	No 'logout' when leaving the workstation	Abuse of rights
Software	Disposal or reuse of storage media without proper erasure	Abuse of rights
Software	Lack of audit trail	Abuse of rights
Software	Wrong allocation of access rights	Abuse of rights
Software	Widely-distributed software	Corruption of data
Software	Applying application programs to the wrong data in terms of time	Corruption of data
Software	Complicated user interface	Error in use
Software	Lack of documentation	Error in use
Software	Incorrect parameter set up	Error in use
Software	Incorrect dates	Error in use
Network	Lack of identification and authentication mechanisms like user authentication	Forging of rights
Network	Unprotected password tables	Forging of rights
Network	Poor password management	Forging of rights
Network	Unnecessary services enabled	Illegal processing of data
Network	Immature or new software	Software malfunction
Network	Unclear or incomplete specifications for developers	Software malfunction
Network	Lack of effective change control	Software malfunction
Network	Uncontrolled downloading and use of software	Tampering with software
Network	Lack of back-up copies	Tampering with software
Network	Lack of physical protection of the building, doors and windows	Theft of media or documents
Network	Failure to produce management reports	Unauthorised use of equipment
Network	Lack of proof of sending or receiving a message	Denial of actions
Network	Unprotected communication lines	Eavesdropping
Network	Unprotected sensitive traffic	Eavesdropping
Network	Poor joint cabling	Failure of telecommunication equipment
Network	Single point of failure	Failure of telecommunication equipment
Network	Lack of identification and authentication of sender and receiver	Forging of rights
Network	Insecure network architecture	Remote spying
Network	Transfer of passwords in clear	Remote spying
Network	Inadequate network management (resilience of routing)	Saturation of the information system
Network	Unprotected public network connections	Unauthorised use of equipment
Personnel	Absence of personnel	Breach of personnel availability
Personnel	Inadequate recruitment procedures	Destruction of equipment or media

Personnel	Insufficient security training	Error in use
Personnel	Incorrect use of software and hardware Error in use	Error in use
Personnel	Lack of security awareness Error in use	Error in use
Personnel	Lack of monitoring mechanisms	Illegal processing of data
Personnel	Unsupervised work by outside or cleaning	Theft of media or documents
Personnel	Lack of policies for the correct use of telecommunications media and messaging	Unauthorised use of equipment
Site	Inadequate or careless use of physical access control to buildings and rooms	Destruction of equipment or media
Site	Location in an area susceptible to flood	Flood
Site	Unstable power grid	Loss of power supply
Site	Lack of physical protection of the building, doors and windows	Theft of equipment
Organisation	Lack of formal procedure for user registration and de-registration	Abuse of rights
Organisation	Lack of formal process for access right review (supervision)	Abuse of rights
Organisation	Lack or insufficient provisions (concerning security) in contracts with customers and/or third parties	Abuse of rights
Organisation	Lack of procedure of monitoring of information processing facilities	Abuse of rights
Organisation	Lack of regular audits (supervision)	Abuse of rights
Organisation	Lack of procedures of risk identification and assessment	Abuse of rights
Organisation	Lack of fault reports recorded in administrator and operator logs	Abuse of rights
Organisation	Inadequate service maintenance response	Breach of information system maintainability
Organisation	Lack or insufficient Service Level Agreement	Breach of information system maintainability
Organisation	Lack of change control procedure	Breach of information system maintainability
Organisation	Lack of formal procedure for ISMS documentation control	Corruption of data
Organisation	Lack of formal procedure for ISMS record supervision	Corruption of data
Organisation	Lack of formal process for authorisation of public available information	Data from untrustworthy sources
Organisation	Lack of proper allocation of information security responsibilities	Denial of actions
Organisation	Lack of continuity plans	Equipment failure
Organisation	Lack of e-mail usage policy	Error in use
Organisation	Lack of procedures for introducing software into operational systems	Error in use
Organisation	Lack of records in administrator and operator logs	Error in use
Organisation	Lack of procedures for classified information handling	Error in use
Organisation	Lack of information security responsibilities in job descriptions	Error in use
Organisation	Lack or insufficient provisions (concerning information security) in contracts with employees	Illegal processing of data
Organisation	Lack of defined disciplinary process in case of information security incident	Theft of equipment
Organisation	Lack of formal policy on mobile computer usage	Theft of equipment
Organisation	Lack of control of off-premise assets	Theft of equipment
Organisation	Lack or insufficient 'clear desk and clear screen' policy	Theft of media or documents
Organisation	Lack of information processing facilities authorisation	Theft of media or documents
Organisation	Lack of established monitoring mechanisms for security breaches	Theft of media or documents
Organisation	Lack of regular management reviews	Unauthorised use of equipment
Organisation	Lack of procedures for reporting security weaknesses	Unauthorised use of equipment
Organisation	Lack of procedures of provisions compliance with intellectual rights	Use of counterfeit or copied software