Information Risk

Information Security Principles

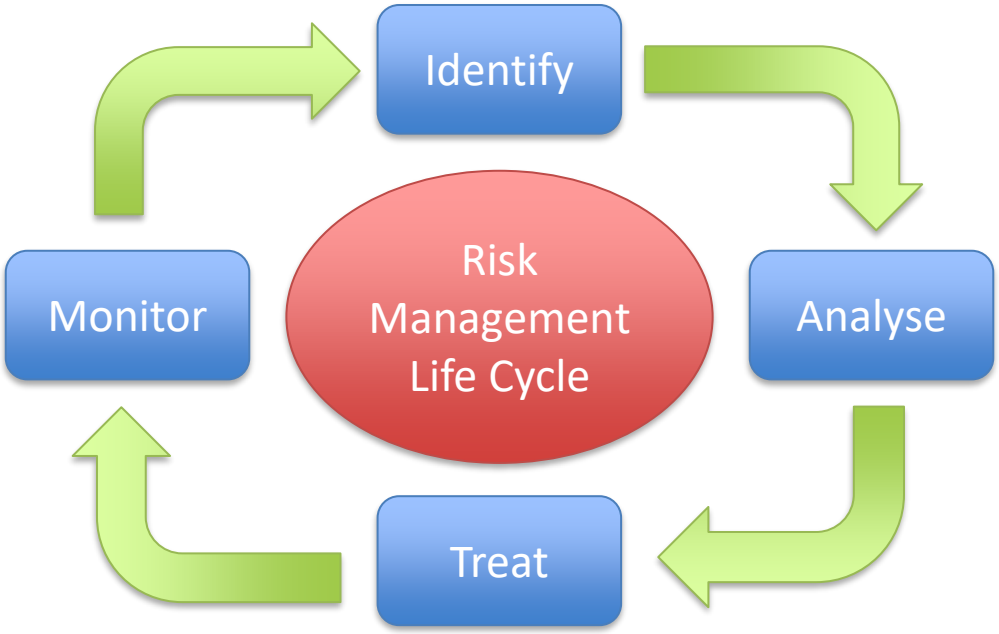
Confidentiality.
The property that information is not made available or disclosed to unauthorised individuals, entities or processes.

Integrity.
The property of safeguarding the accuracy and completeness of assets.

Availability.
The property of being accessible and usable upon demand by an authorised entity.

Asset.
Anything that has value to the organisation, its business operations and its continuity.

Managing Security = Managing Risk



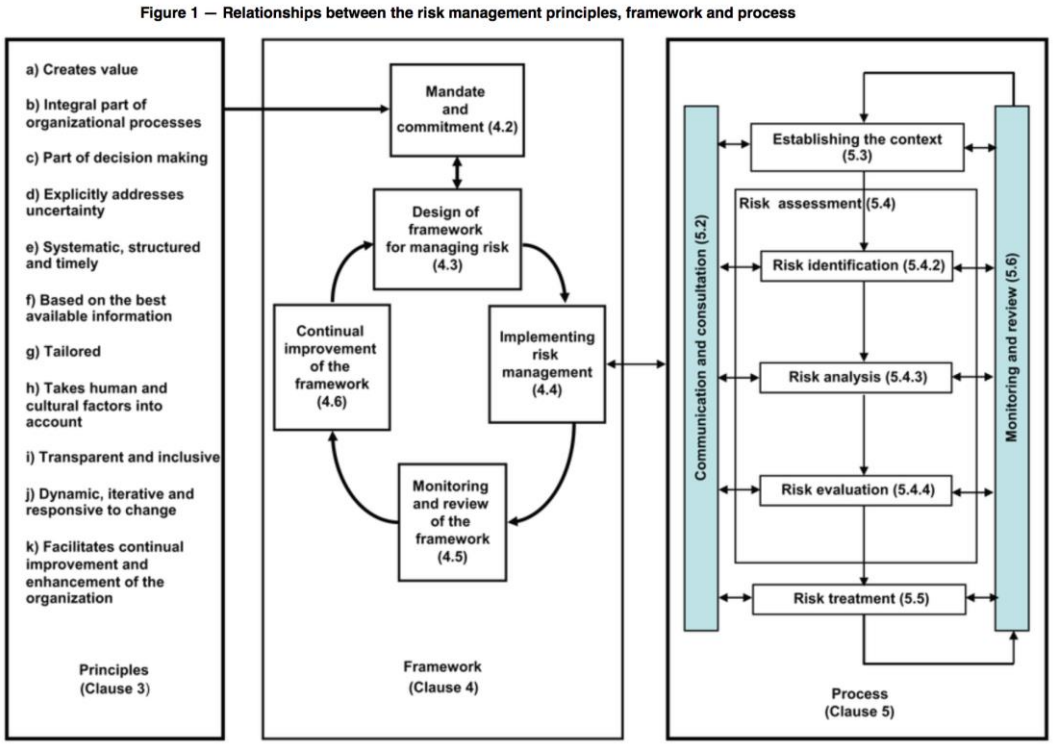
ISO31000: Risk Management Principles and Guidelines

ISO 31000:2009 provides principles and generic guidelines on risk management.

ISO 31000:2009 can be used by any public, private or community enterprise, association, group or individual. Therefore, ISO 31000:2009 is not specific to any industry or sector.

ISO 31000:2009 can be applied throughout the life of an organization, and to a wide range of activities, including strategies and decisions, operations, processes, functions, projects, products, services and assets.

ISO 31000:2009 can be applied to any type of risk, whatever its nature, whether having positive or negative consequences.



Information Security Principles

Threat.
A potential cause of an incident that may result in harm to a system or organisation.

Vulnerability.
A weakness of an asset or group of assets that can be exploited by one or more threats.

Risk.
The potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organisation.

Impact.
The result of an information security incident, caused by a threat, which affects assets.

Threat

Threat.
A potential cause of an incident that may result in harm to a system or organisation.

Threat

Threat.
A potential cause of an incident that may result in harm to a system or organisation.

Accidental Threats
Deliberate Threats
- **Internal Threats**
- **External Threats**

Hazards

Threat

Threat.
A potential cause of an incident that may result in harm to a system or organisation.

Accidental Threats

- Lost or stolen records.
- Distribution of data to wrong recipients.
- Forgetting to act in accordance to policy.

Threat

Threat.
A potential cause of an incident that may result in harm to a system or organisation.

Deliberate Threats

- Act with intent to cause harm to the organisation.
- May try to circumvent policy or security measures to conduct actions.

Threat

Threat.
A potential cause of an incident that may result in harm to a system or organisation.

Internal Threats

- Who has **access** and **knowledge** from within to pose as a threat?
- Employees, management, stakeholders, contractors.
- Could attack any of the CIA principles.

Threat

Threat.
A potential cause of an incident that may result in harm to a system or organisation.

External Threats

- Less **access** and **knowledge** than an insider
- Hackers, competitors, protest groups…
- Could attack Confidentiality, Integrity, and Availability.

Threat

Threat.
A potential cause of an incident that may result in harm to a system or organisation.

Hazards

- Outside of organisational control, and may be internal or external in origin.
- Examples may include fire, floods, and adverse weather conditions.

Vulnerability

Vulnerability.
A weakness of an asset or group of assets that can be exploited by one or more threats.

Vulnerability

Vulnerability.
A weakness of an asset or group of assets that can be exploited by one or more threats.

General vulnerabilities

- Software or hardware design
- Building and facilities
- People
- Processes and procedures

Vulnerability

Vulnerability.
A weakness of an asset or group of assets that can be exploited by one or more threats.

Information-specific vulnerabilities

- Unsecured computers and servers
- Personal devices, handheld devices, memory sticks.
- Networks, e-mail, wireless, operating systems
- Filing cabinets and printed documents

Impact

- Threats will exploit vulnerabilities in order to succeed in their objective
- What is the impact of this objective?
- What is the asset that is affected?

Impact.
The result of an information security incident, caused by a threat, which affects assets.

Impact

- Assets – intellectual property, HR records, financial records, hardware, equipment, infrastructure…
- What is the likelihood of this happening?
- Impact may be assessed:
  - Quantitatively – statistical (£100k)
  - Qualitatively – subjective (e.g., high, low)

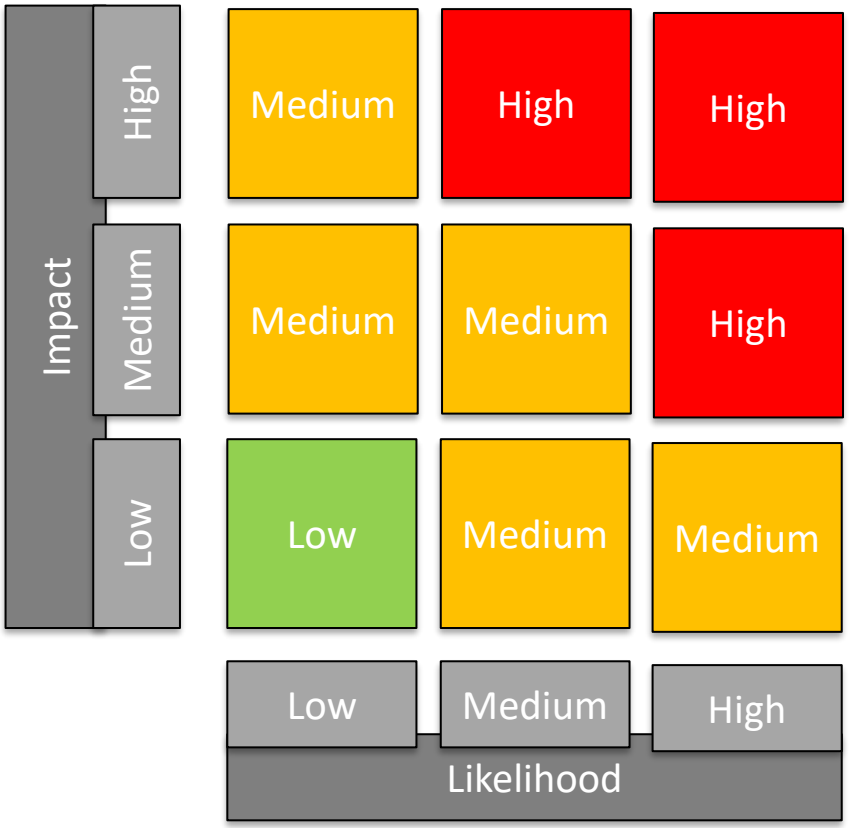
Impact.
The result of an information security incident, caused by a threat, which affects assets.

Risk

Risk.
The potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organisation.

- Combination of the impact and the likelihood that the threat can be carried out.
- What is the potential risk for further security breaches?

Risk Assessment



Risk.
The potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organisation.

Matrix can be rescaled as deemed appropriate

Risk Treatment

Risk.
The potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organisation.

Four actions that may be possible:
Risk avoidance – eliminate the possibility of risk
Risk acceptance – accept that the risk is possible
Risk mitigation – reduce the likelihood of the risk
Risk transfer – allow a third party to manage risk

Residual Risk

'the risk remaining after risk treatment' (ISO Guide 73:2009).

Once all other risk treatment options have been explored, it is often the case that some (usually small) risk remains. It is normal to accept or tolerate this, since further treatment might either have no effect, or might be prohibitively expensive. Because residual risks are often very small, they are occasionally (incorrectly) overlooked.

Risk Appetite

'the amount and type of risk that an organisation is willing to pursue or retain' (ISO Guide 73:2009)

Organisations will have differing levels of risk appetite for different types of information; and different types of organisation will have vastly differing levels of risk appetite, depending on their sector.

Questions

Which of the following is not a threat?

- Failure of the local mains power supply
- An easily guessed password
- A transmission circuit cable break
- Flooding of a data centre

Questions

If the accuracy of information is a major concern, which of the following would be used to ensure this is covered effectively?

- Confidentiality
- Availability
- Integrity
- None of these

Recap

- Understanding how threats, vulnerabilities, risk, and impact relate to the organisation.
- How may the organisation assess the risk?
- How may the organisation treat the risk?

Seminar 2: Information Security Policy

- Look at the policies : http://www.bristol.ac.uk/infosec/policies/docs/
- ***In groups, study 4-5 of the policies. Think about:*** *What are the key points from the policy? Why is the policy important? How can the policy be addressed? How will you ensure that policy is enforced?*

- How to write an Information Security Policy

Other examples:
NHS
https://www.england.nhs.uk/wp-content/uploads/2013/06/info-sec-1.pdf
POLICE
http://www.westyorkshire.police.uk/sites/default/files/files/publication-scheme/wyp_information_security_policy.pdf
FIRE AND RESCUE
http://www.avonfire.gov.uk/guide-to-published-information/our-policies-and-procedures