Dr. Phil Legg

Associate Professor in Cyber Security

Information Risk Management

2: Information Security Management System

Date

UWE Bristol | University of the West of England

InfoSec in the News

- A weekly round-up of news stories via Twitter
- Think about how the news and media relates to Information Risk Management

- We will do a round-up each week
- Please try to find stories to bring along and discuss!

Information Security Principles

CIA Triad

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.

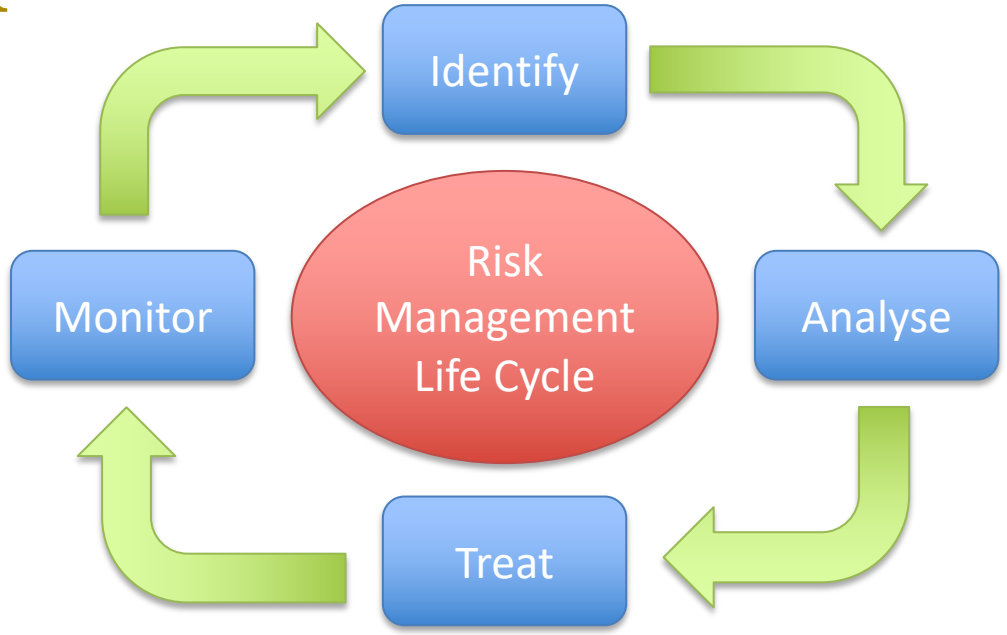
Availability.
The property of being accessible and usable upon demand by an authorised entity.

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

UWE Bristol University of the West of England

Definitions from ISO27000

Managing Security equals Managing Risk



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.

Definitions from ISO27000

Threats

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.

Deliberate Threats

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

Threats

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.

External Threats

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

Threats

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.

General vulnerabilities

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

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

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

- 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?

- 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)

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, Threat, Vulnerability

Consider a situation where you are living in a house near forest. If you keep the door wide open then a Tiger or any wild animal can enter and attack you, and may kill you.

*Here keeping the door open is the **Vulnerability**, Tiger/wild animal may attack you is the possible T**hreat** and the probability of Tiger/wild animal coming through that door and attacking you is the **Risk**.*

UWE Bristol University of the West of England

https://www.theresilience.ml/risk-threat-and-vulnerability/

Risk, Threat, Vulnerability

- ***V****ulnerability* refers to the weakness of a resource/asset that can be exploited by the attackers or threats.

- ***T****hreat* can be anything that exploit the vulnerability intentionally or unintentionally and can cause damage to resources/assets. There are natural threats like Earthquakes, intentional threats including malware and spyware, and unintentional threats like an employee entering the wrong information.

- ***R****isk* can be referred to as the potential loss or damage to resources/assets caused when a threat exploits a vulnerability.

Risk = Threat x vulnerability

UWE Bristol | University of the West of England

https://www.theresilience.ml/risk-threat-and-vulnerability/

Risk, Threat, Vulnerability, **Asset**

- In this example, the **Asset** is a person
- Less extreme examples will typically have data as the asset
- Risk Assessment requires knowing the value of the Asset that is compromised or attacked – e.g., is it confidential, can it be replaced?

ISO27001 / ISMS

ISO27001

- **ISO 27001** (formally known as ISO/IEC 27001:2005) is a specification for an Information Security Management System (ISMS).

- An ISMS is a framework of policies and procedures that includes all legal, physical and technical controls involved in an organisation's information risk management processes.

- The ISMS should fully detail all documentation, policies, practices, and all other aspects of information assurance, in order to support the business operation.

ISO27001 – Why?

- **Trust**
- **Credibility**
- **Professional**
- **Secure**

ISO27001 – Why?

- Providing a **risk-based** approach that is structured and proactive to help plan and implement an ISMS resulting in a level of organizational security that is appropriate and affordable
- Ensuring the right people, processes, procedures and technologies are in place to protect information assets
- Protecting information in terms of **confidentiality, integrity and availability**
- Aligns with other management standards such as ISO9001

ISO27001 – Why?

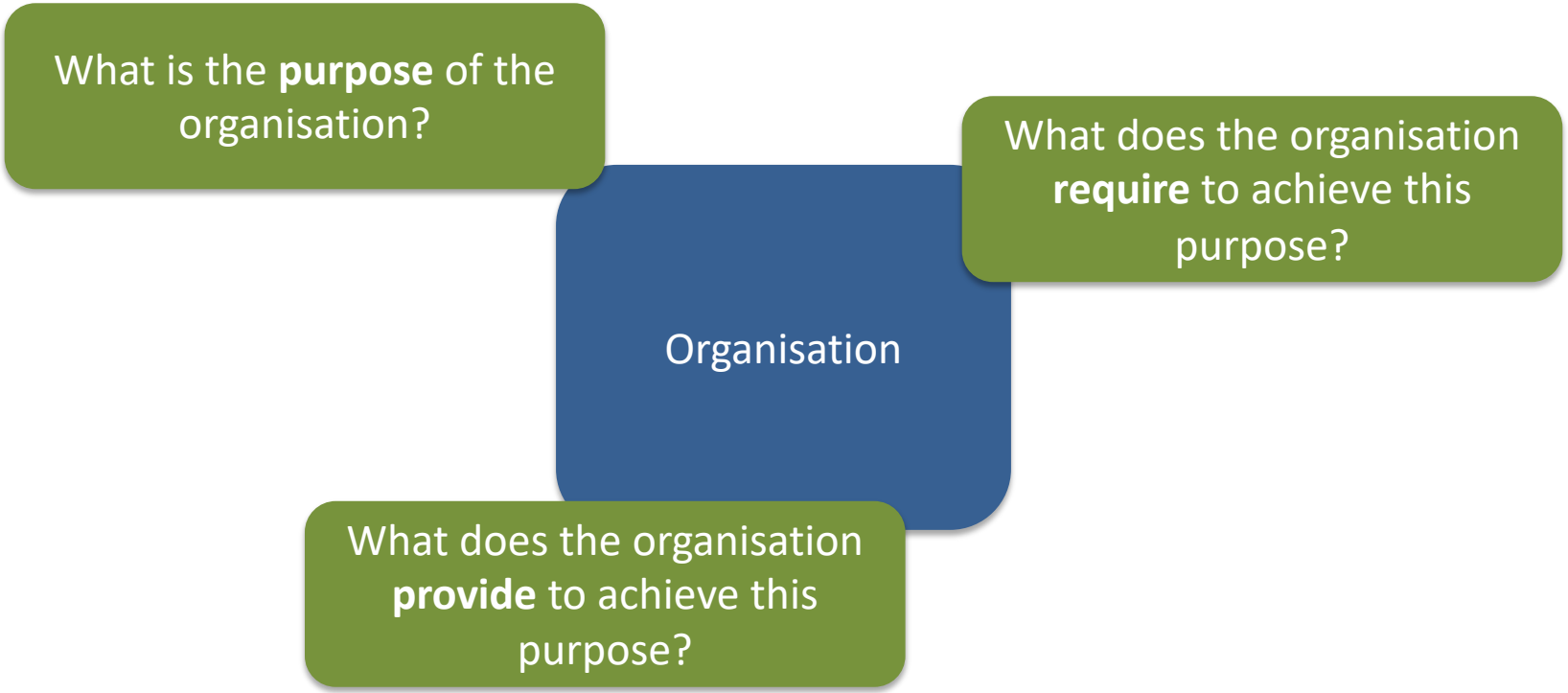
- Demonstrates **independent assurance** of an organization's internal controls therefore meeting corporate governance and business continuity requirements
- Provides third-party assurance that applicable **laws and regulations are observed**
- Provides a **competitive edge**, e.g., by meeting contractual requirements and demonstrating to customers that the security of their information is paramount
- Independently verifies that organizational **risks are properly identified, assessed and managed** while formalizing information security processes, procedures and documentation
- Proves senior management's **commitment to the security** of an organization's information.
- The regular assessment process helps an organization **continually monitor and improve**

ISO27001

Part of the overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain, and improve information security.

(ISO 27001)

Developing an ISMS



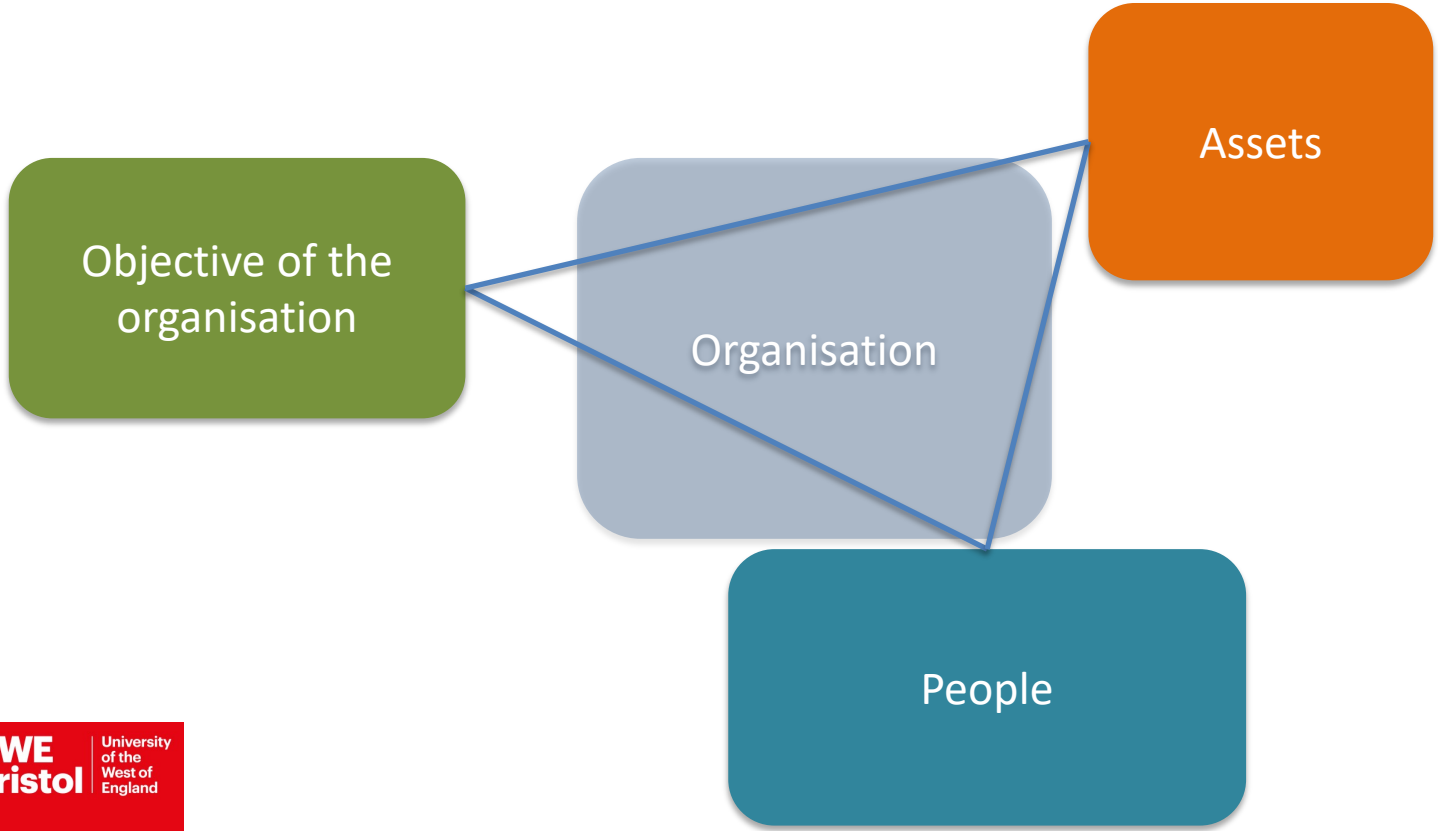
UWE Bristol | University of the West of England

Developing an ISMS

Developing an ISMS

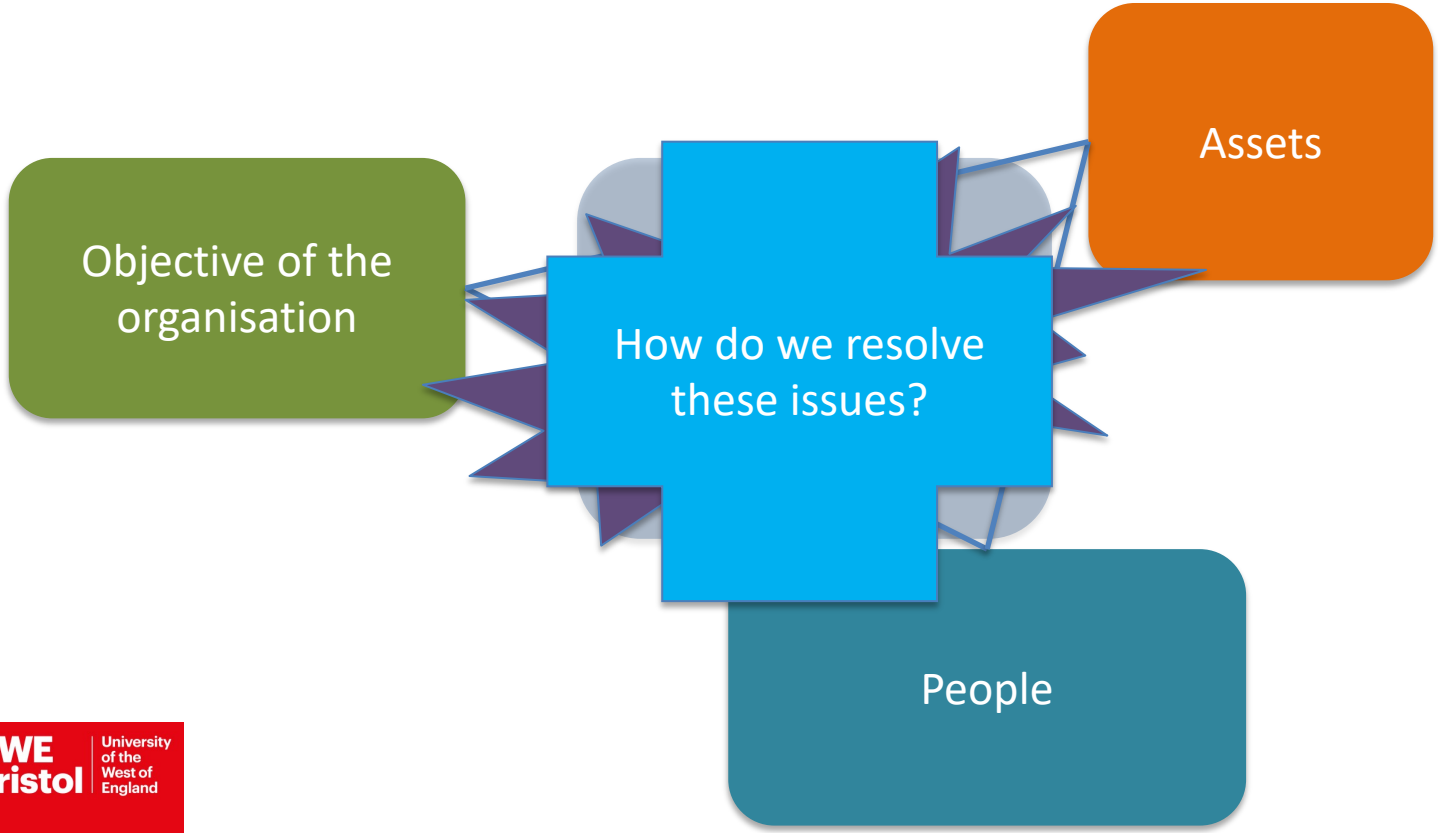
UWE Bristol | University of the West of England

Developing an ISMS



Developing an ISMS

Developing an ISMS



UWE Bristol University of the West of England

Mandatory requirements

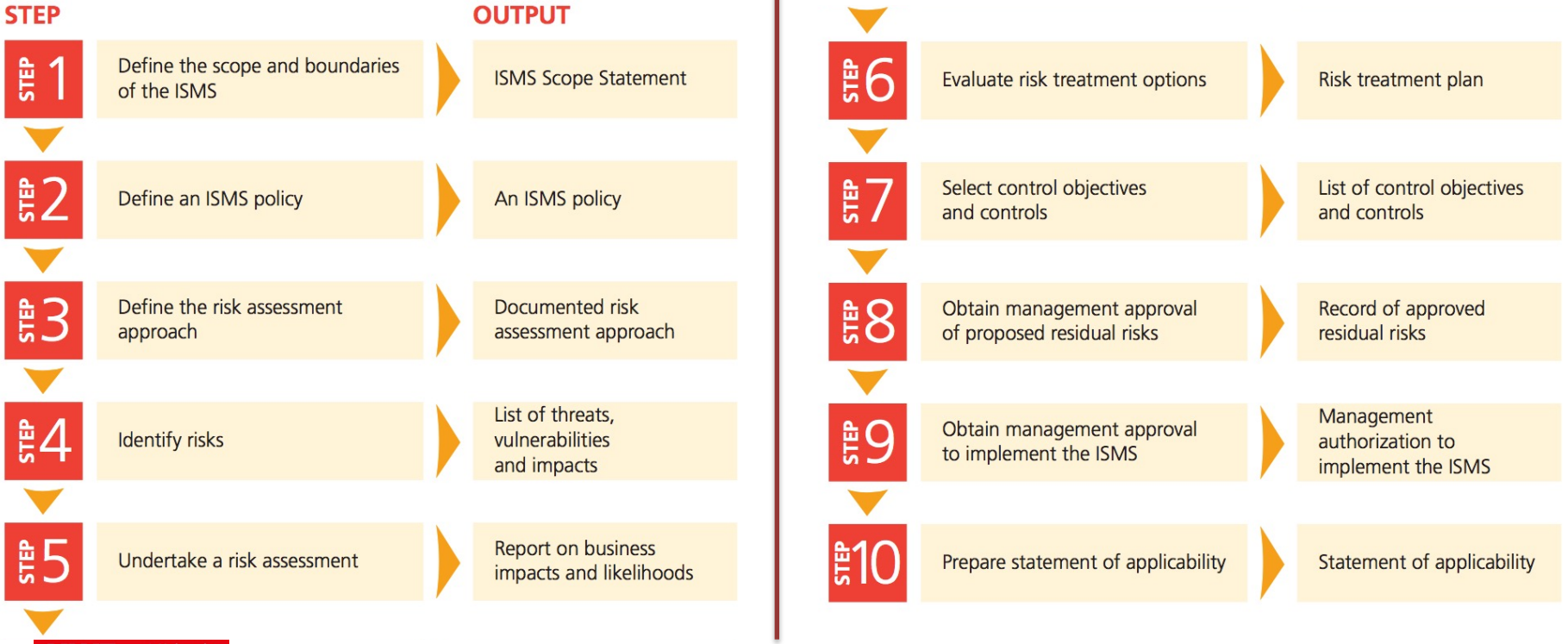
The following mandatory documentation (or rather "documented information" in the curiously stilted language of the standard) is explicitly required for certification:

- **ISMS scope (as per clause 4.3)**
- **Information security policy (clause 5.2)**
- **Information security risk assessment *process* (clause 6.1.2)**
- **Information security risk treatment *process* (clause 6.1.3)**
- **Information security objectives (clause 6.2)**
- **Evidence of the competence of the people working in information security (clause 7.2)**
- **Other ISMS-related documents deemed necessary by the organization (clause 7.5.1b)**
- **Operational planning and control documents (clause 8.1)**
- **The *results* of the risk assessments (clause 8.2)**
- **The *decisions* regarding risk treatment (clause 8.3)**
- **Evidence of the monitoring and measurement of information security (clause 9.1)**
- **The ISMS internal audit program and the results of audits conducted (clause 9.2)**
- **Evidence of top management reviews of the ISMS (clause 9.3)**
- **Evidence of nonconformities identified and corrective actions arising (clause 10.1)**
- Various others: Annex A, which is normative, mentions but does not fully specify further documentation including the rules for acceptable use of assets, access control policy, operating procedures, confidentiality or non-disclosure agreements, secure system engineering principles, information security policy for supplier relationships, information security incident response procedures, relevant laws, regulations and contractual obligations plus the associated compliance procedures and information security continuity procedures.

UWE Bristol University of the West of England

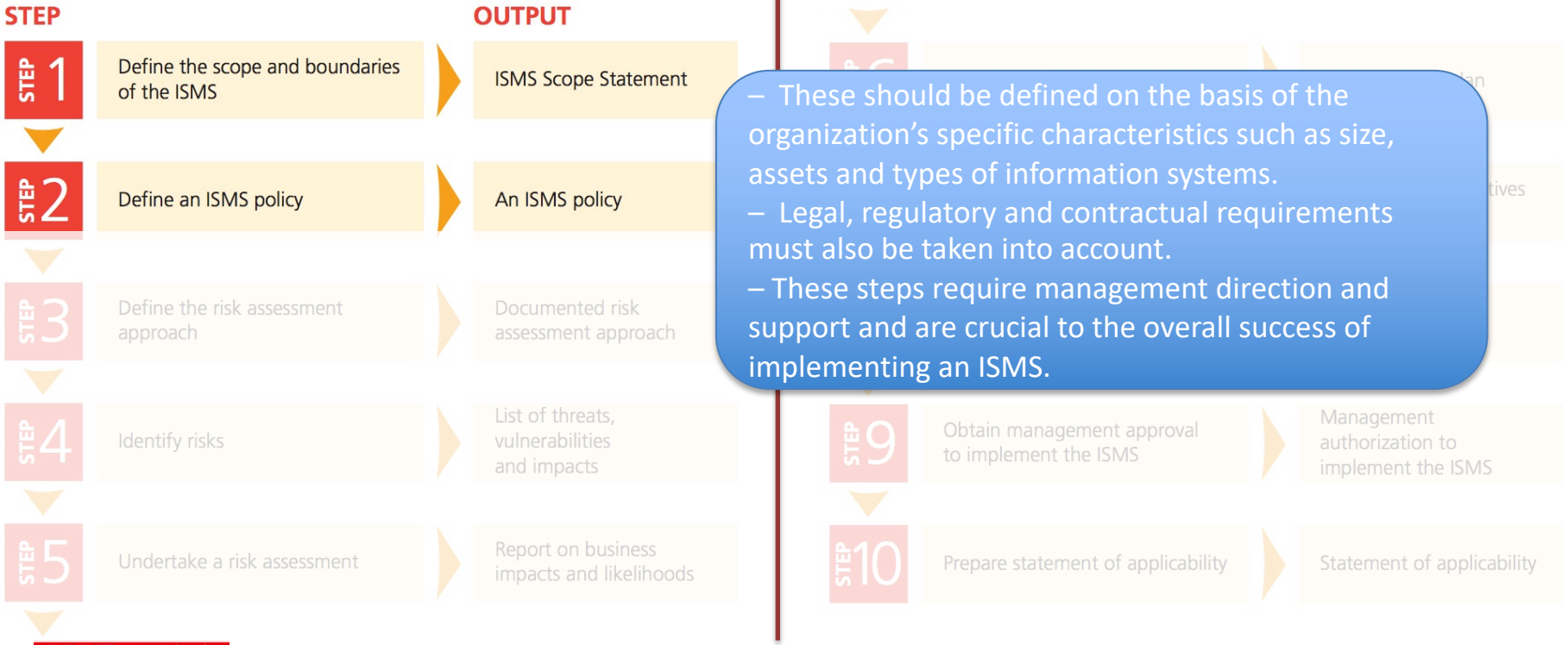
Certification auditors will almost certainly check that these fifteen types of documentation are (a) present, and (b) fit for purpose. The standard does not specify precisely what form the documentation should take, but section 7.5.2 talks about aspects such as the titles, authors, formats, media, review and approval, while 7.5.3 concerns document control, implying a fairly formal ISO 9000-style approach.

Establishing an ISMS



UWE Bristol University of the West of England

Establishing an ISMS



– These should be defined on the basis of the organization's specific characteristics such as size, assets and types of information systems.
– Legal, regulatory and contractual requirements must also be taken into account.
– These steps require management direction and support and are crucial to the overall success of implementing an ISMS.

UWE Bristol | University of the West of England

Information Security Policy

- Examples Information Security policies:

- https://www1.uwe.ac.uk/its/informationsecuritytoolkit/policies/informationsecuritypolicy.aspx
- https://www2.mmu.ac.uk/isds/information-security/policies/risk-management/
- https://www.ed.ac.uk/files/atoms/files/uoe_informationsecuritypolicy_v1.0.pdf

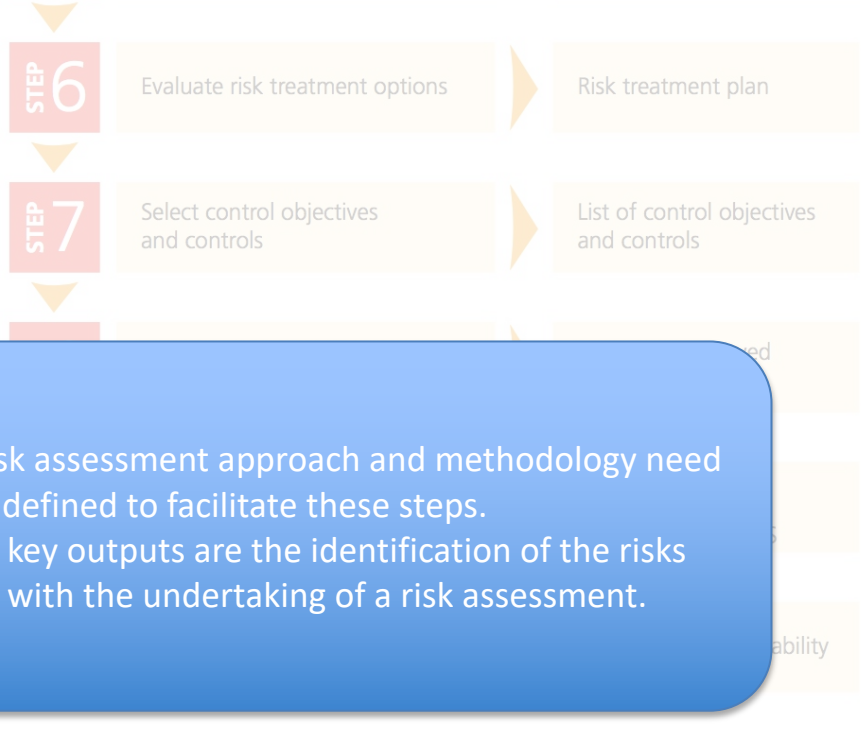
ISMS Policy

Examples of organisations that publicly share their ISMS policy – *aims to establish credibility and the organisation view of information security:*

- https://www.phoenixbs.com/isms-policy/
- https://www.ccas.org.uk/about-ccas/policies/isms-policy
- https://rehabagency.ai/ISMS/
- https://www.theemaillaundry.com/isms-policy/
- https://www.aztec.support/about/isms-policy/

Plenty more out there of course… this provides a small sample just to give an idea of how organisations may publicise such details…

Establishing an ISMS



– A risk assessment approach and methodology need to be defined to facilitate these steps.
– The key outputs are the identification of the risks along with the undertaking of a risk assessment.

UWE Bristol University of the West of England

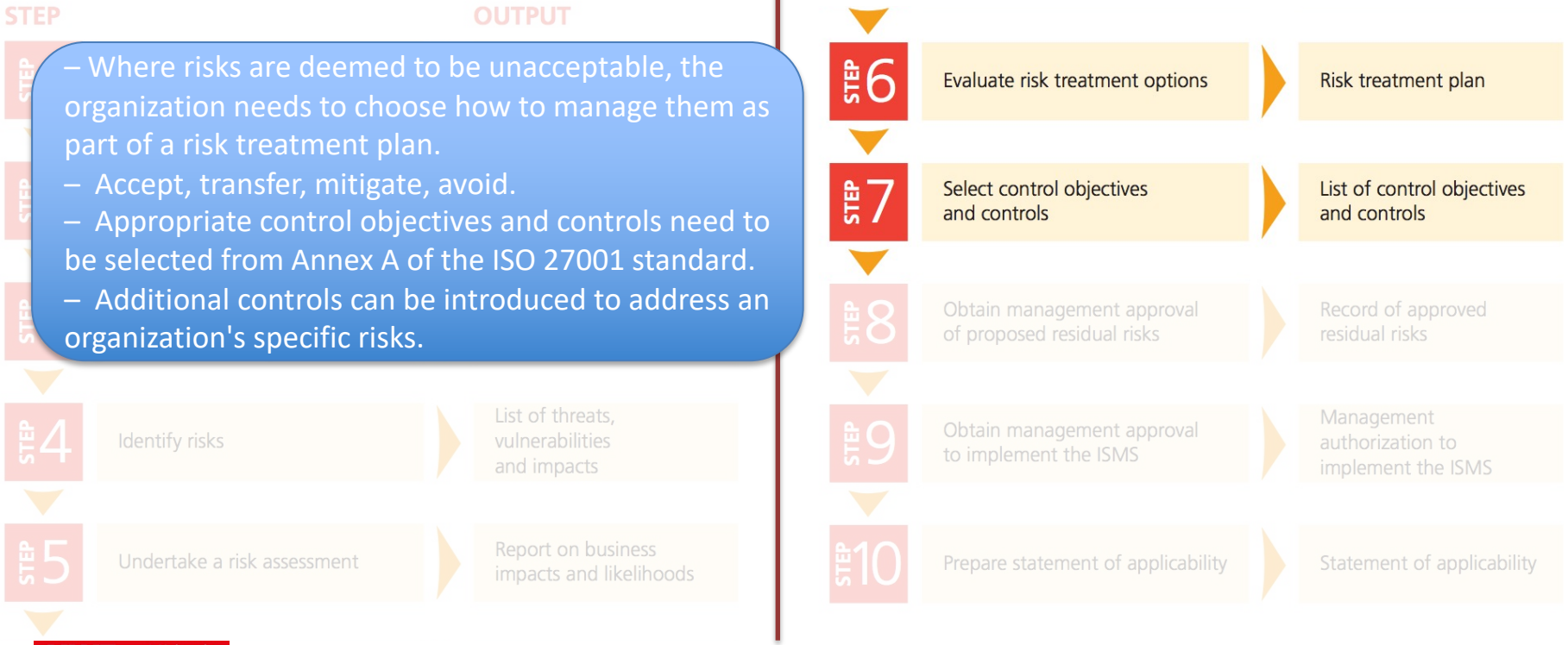
Risk Assessment

- ISMS Risk Assessment is based on a Risk Matrix
- Often uses 3 or 5 values (L,M,H, or L,L-M,M,M-H,H)
- Likelihood and impact (aka. severity)

Likelihood \ Impact	Negligible	Minor	Moderate	Significant	Severe
Very Likely	Low Med	Medium	Med Hi	High	High
Likely	Low	Low Med	Medium	Med Hi	High
Possible	Low	Low Med	Medium	Med Hi	Med Hi
Unlikely	Low	Low Med	Low Med	Medium	Med Hi
Very Unlikely	Low	Low	Low Med	Medium	Medium

Risk = Likelihood X Impact

Establishing an ISMS



UWE Bristol University of the West of England

Risk Treatment

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 *(most common)*
- **Risk transfer** – allow a third party to manage risk

UWE Bristol University of the West of England

https://www.theresilience.ml/risk-treatment-methods/

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.

UWE Bristol University of the West of England

https://www.theresilience.ml/risk-treatment-methods/

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.

UWE Bristol University of the West of England

https://www.theresilience.ml/risk-treatment-methods/

ISO27001 Controls

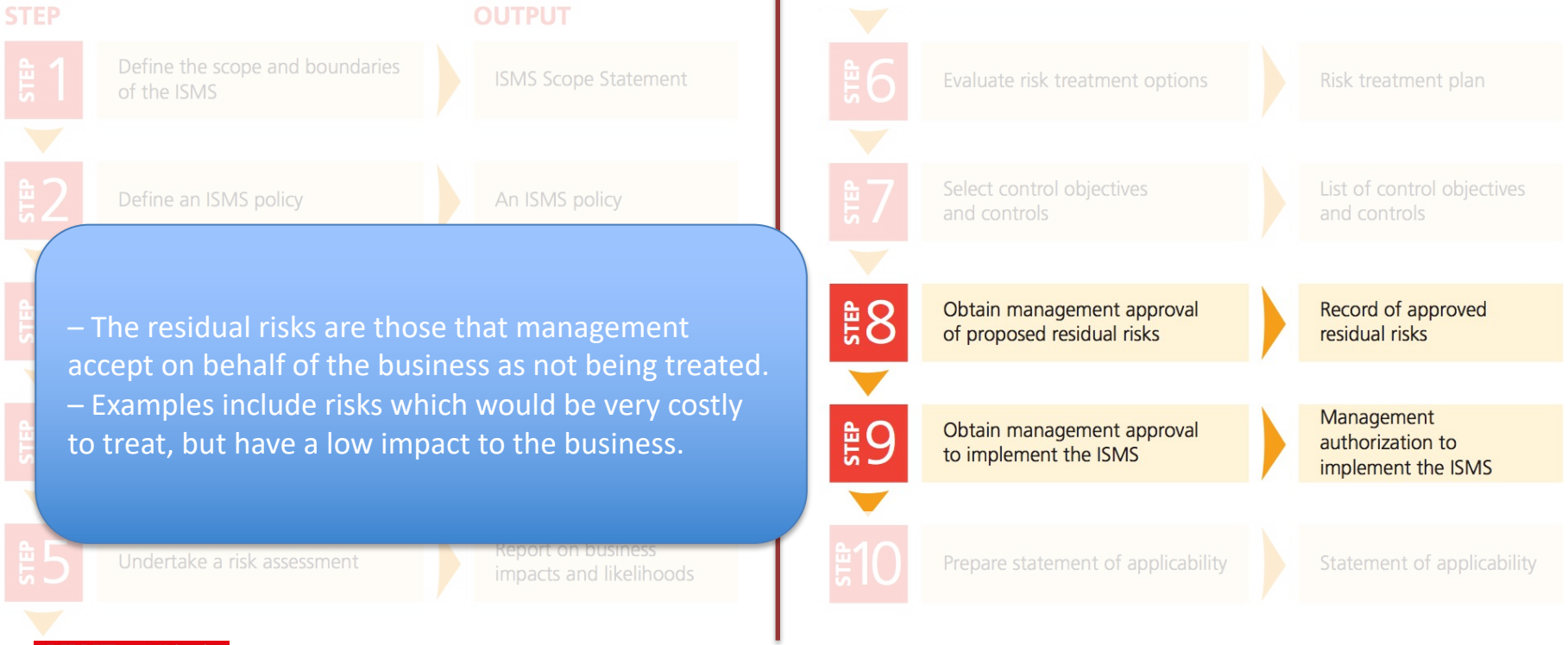
1. Security Policy
2. Organisation of Information Security
3. Asset Management
4. Human Resources Security
5. Physical and Environmental Security
6. Communications and Operations Management
7. Access Control
8. Information Systems Acquisition, Development and Maintanence
9. Incident Management
10. Business Continuity Management
11. Compliance

Show which controls map to which risks in statement of applicability, and why controls may be omitted

UWE Bristol University of the West of England

https://www.uninett.no/sites/default/files/webfm/Information%20Security%20Management%20Systems%20-%20Oivind%20Hoiem%2C%20Sofia%2017.06.2014.pdf

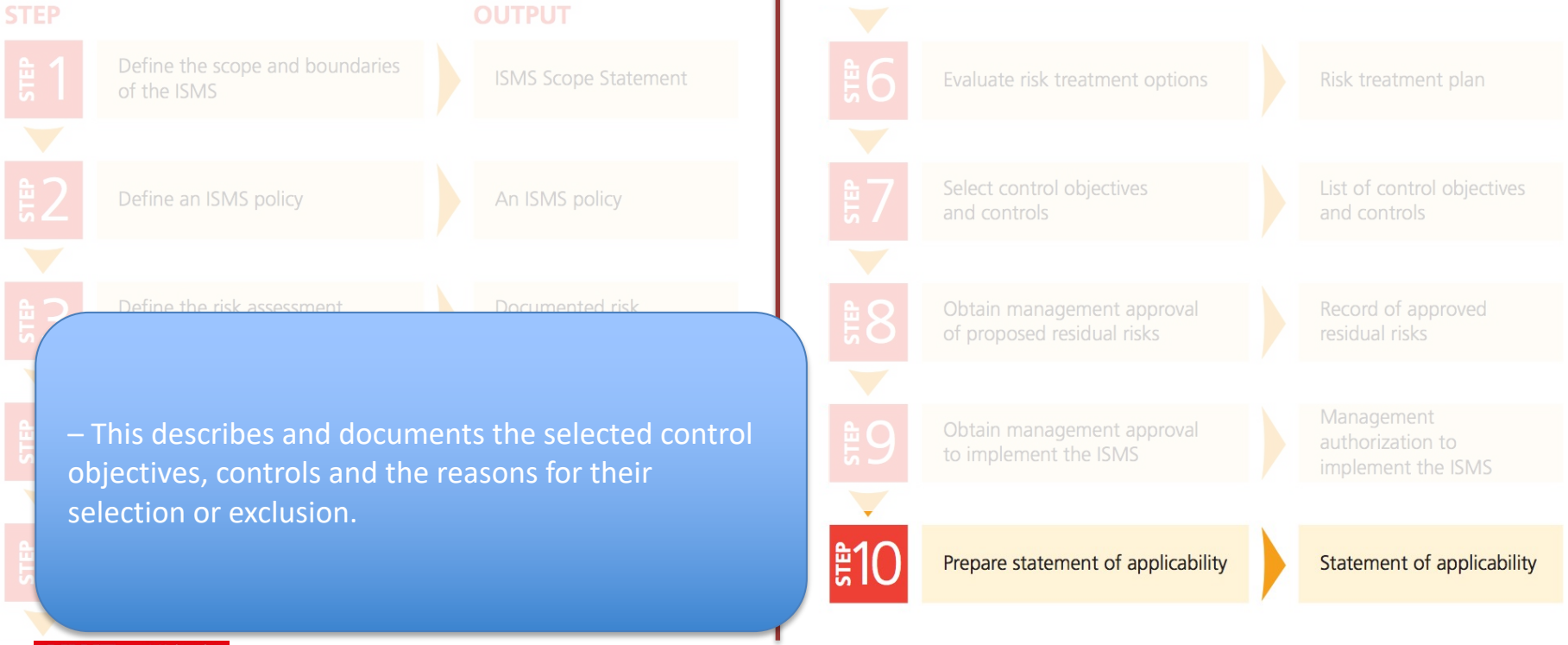
Establishing an ISMS



– The residual risks are those that management accept on behalf of the business as not being treated.
– Examples include risks which would be very costly to treat, but have a low impact to the business.

UWE Bristol University of the West of England

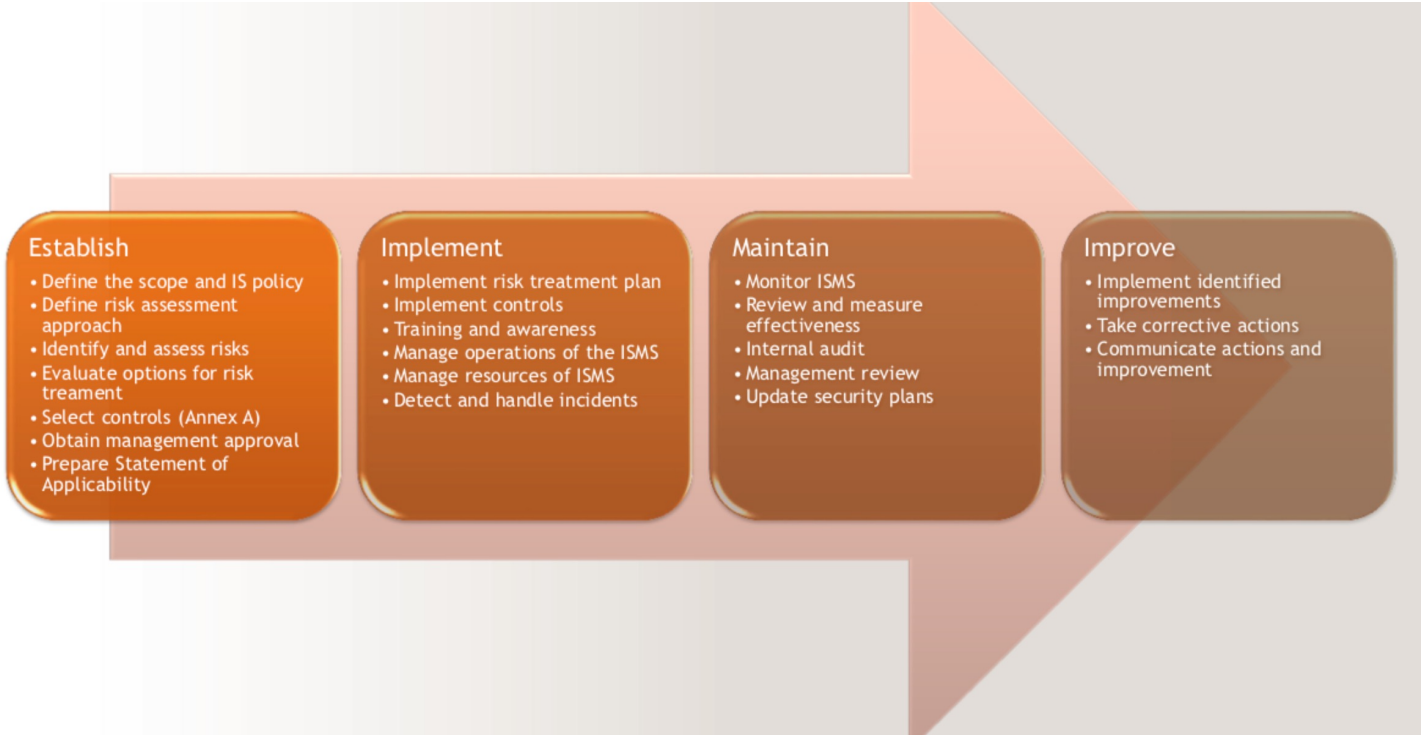
Establishing an ISMS



– This describes and documents the selected control objectives, controls and the reasons for their selection or exclusion.

UWE Bristol | University of the West of England

ISMS Process



https://www.uninett.no/sites/default/files/webfm/Information%20Security%20Management%20Systems%20-%20Oivind%20Hoiem%2C%20Sofia%2017.06.2014.pdf

Question

Which of the following is not a threat?

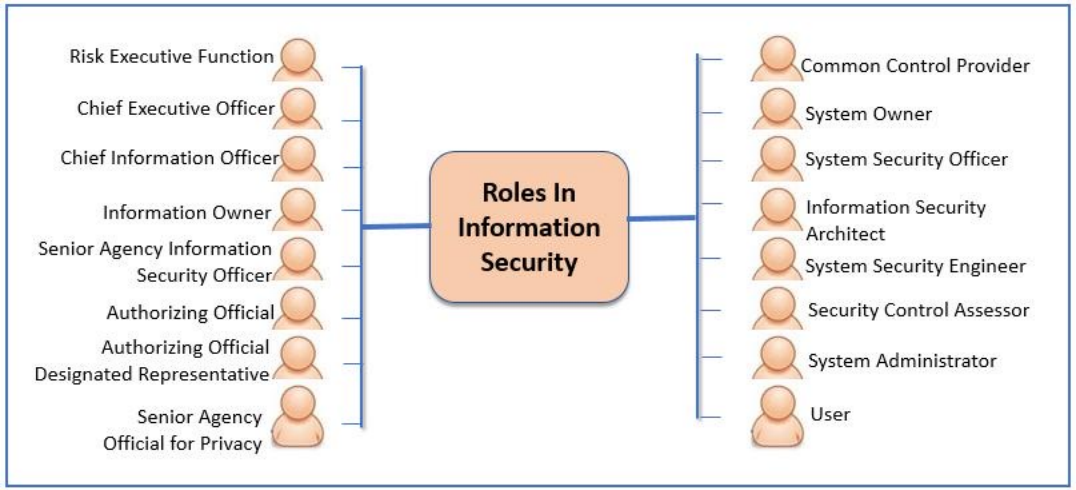
- Failure of the local mains power supply
- An easily guessed password
- A transmission circuit cable break
- Flooding of a data centre

Question

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

Roles and Responsibilities



https://www.bitsight.com/blog/cio-vs-ciso

See the Supplementary slides on Roles

Resources

- http://www.infosectoday.com/Articles/ISMS/Information_Security_Management_Systems.htm
- http://www.pjr.com/downloads/webinar_slides/2.15.17_Scope%20of%20Your%20ISMS.pdf
- https://www.itgovernance.co.uk/iso27001
- https://www.iso.org/isoiec-27001-information-security.html
- http://cs.ru.nl/~kursawe/SiO2011/Slides/02_IS_IMPL_20v0.51.pdf
- http://gender.govmu.org/English/Documents/activities/gender%20infsys/AnnexIX1302.pdf
- https://advisera.com/27001academy/blog/2016/05/30/what-should-you-write-in-your-information-security-policy-according-to-iso-27001/
- https://advisera.com/27001academy/blog/2016/05/23/information-security-management-system-isms-according-iso-27001/

British Standards Online

- Look at the British Standards Online webpage (UWE Library has subscription access):
  - https://bsol.bsigroup.com

- Search for the **ISO27000** documents (e.g., there will be others in the 27k series that are of interest, e.g. 27032, 31111, 9001)

- Start to consider:
  - What are the benefits of an ISMS (Section 3.7 27000)?
  - What are the critical success factors for an ISMS to succeed (Section 3.6 27000)?
  - How would an ISMS be adopted for a given organization?