Information Security Management System (Part 1)

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.

International Organization for Standardization

Information Security Management System (ISMS)

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

Information Security Management System (ISMS) – Why?

- Trust
- Credibility
- Professional
- Secure

Information Security Management System (ISMS) – Why?

- **Can bring significant benefits including:**
  - 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 ISO 9001

Information Security Management System (ISMS) – Benefits?

- 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**

Information Security Management System (ISMS)

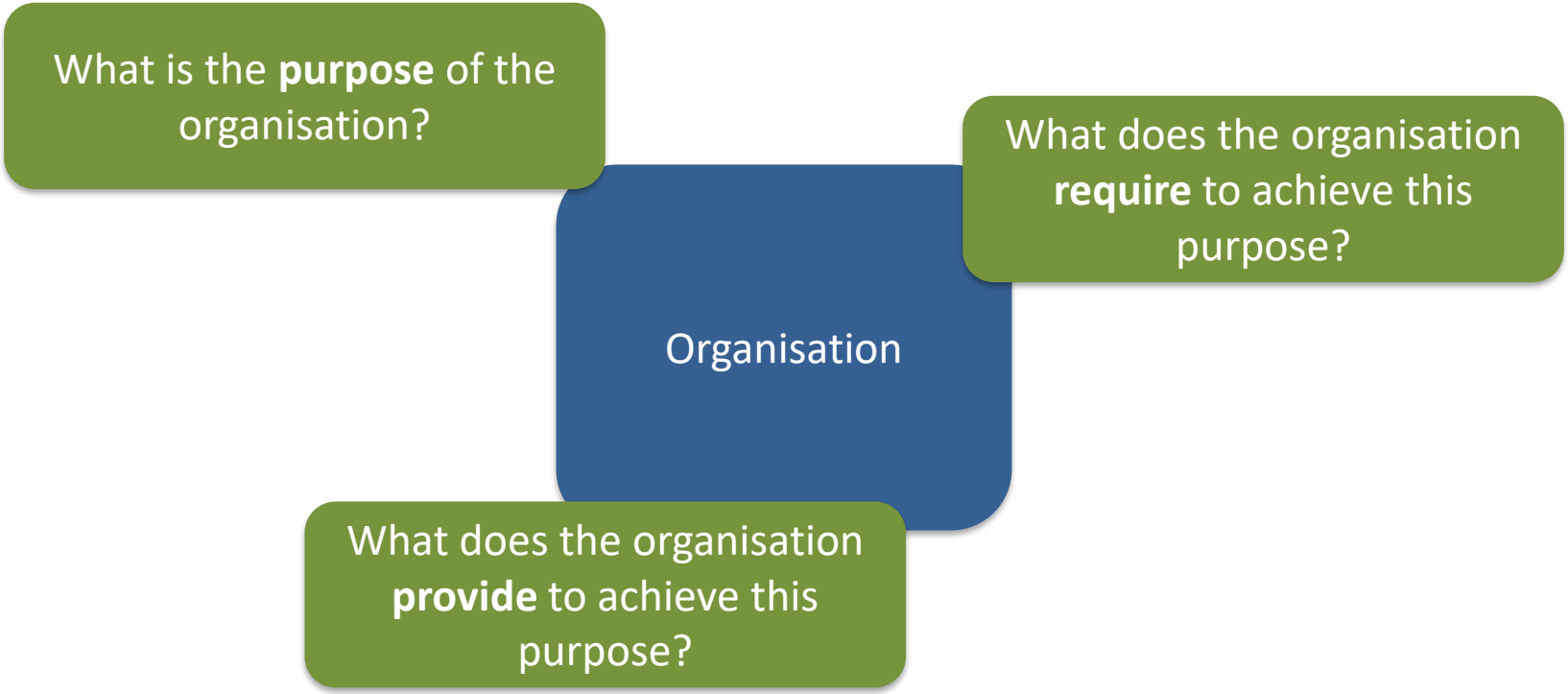
Part of the overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain, and improve information security.

(ISO 27001)

Recap: How to manage Security?

- Identify organisational objectives
- Identify key IT services
- Identify risks
  - Due to legal issues
  - Due to performance issues
- Plan for security (ISMS) – be proactive!
- Plan for disaster recovery – be ready to react!
- Continuous review and fine-tuning.

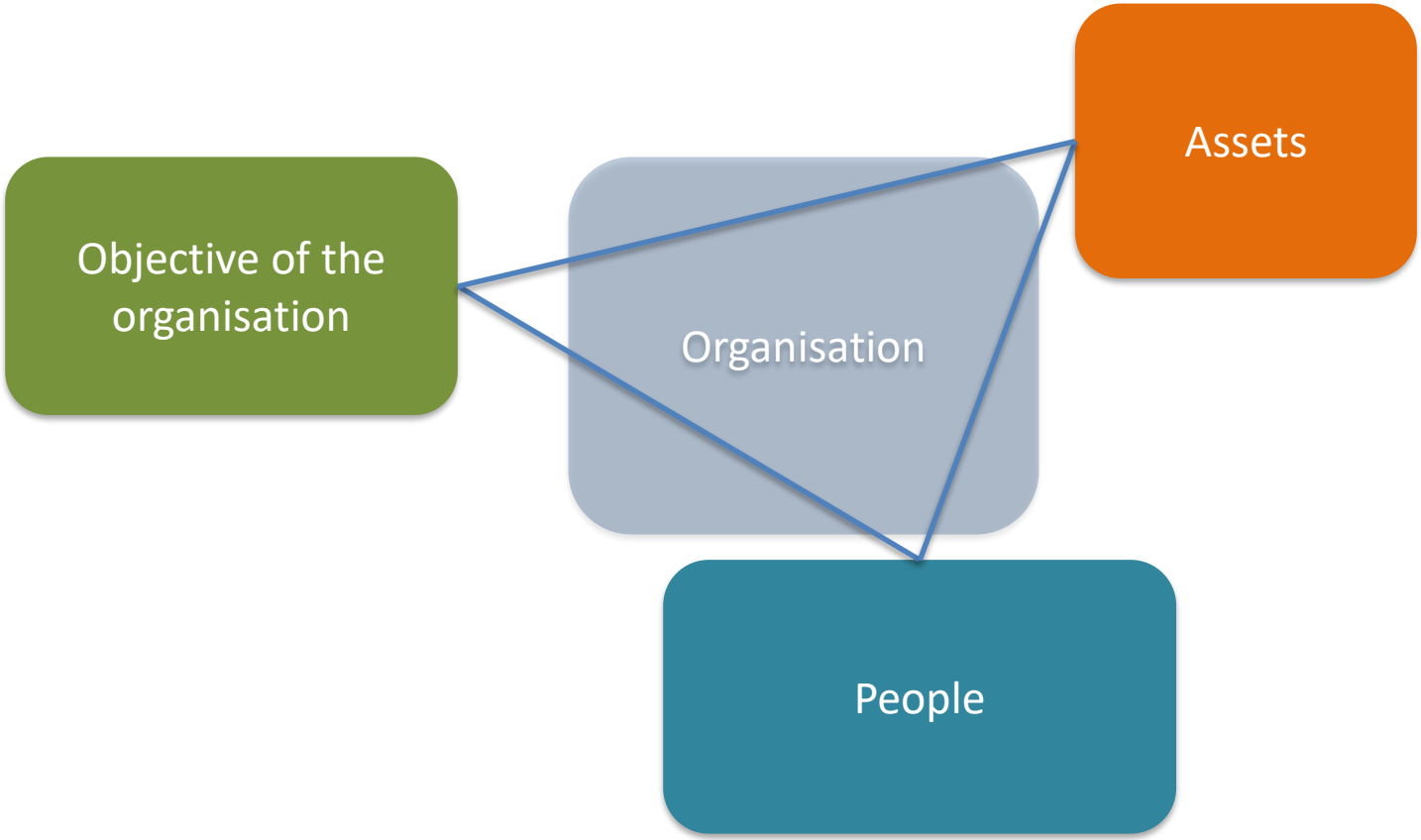
Developing an ISMS



Developing an ISMS

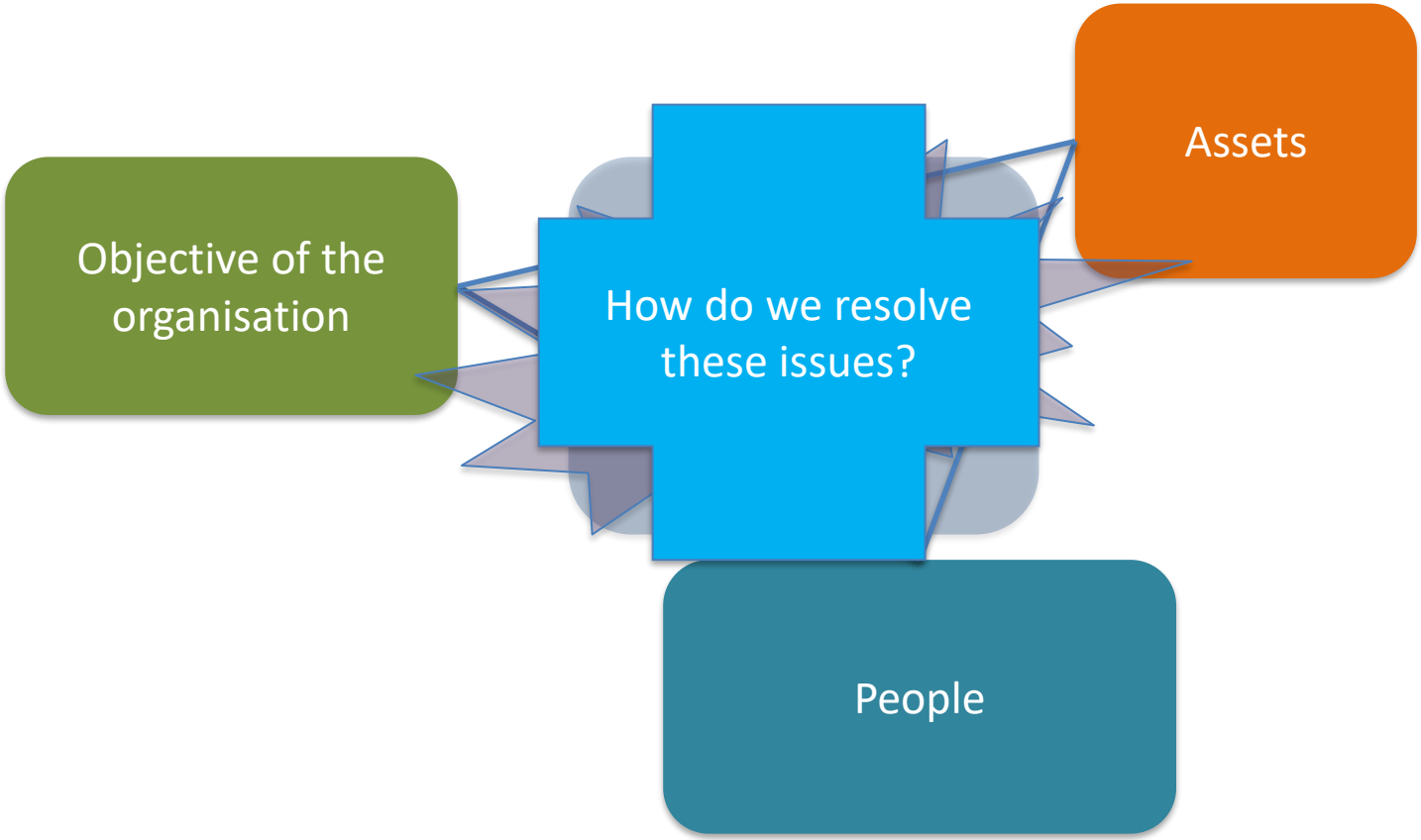
Developing an ISMS

Developing an ISMS



Developing an ISMS

Developing an ISMS



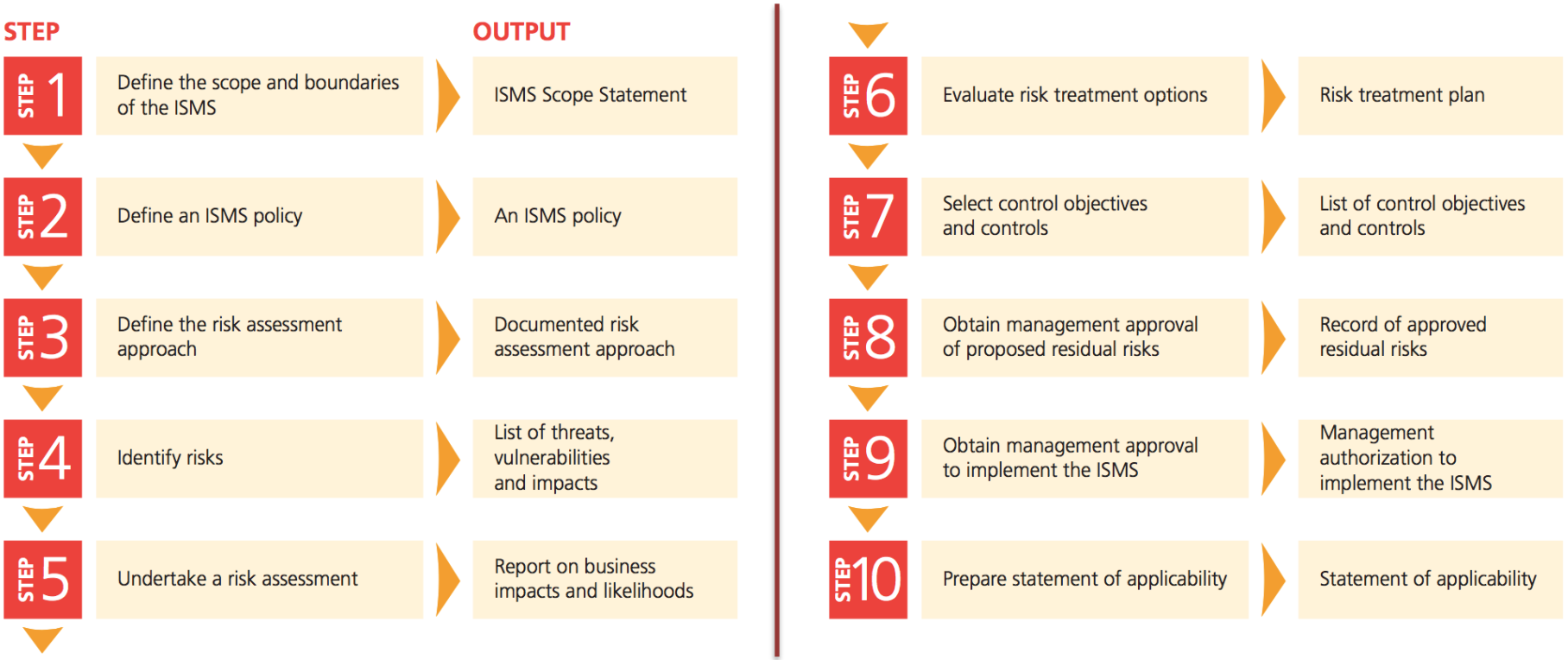
Mandatory requirements for certification

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

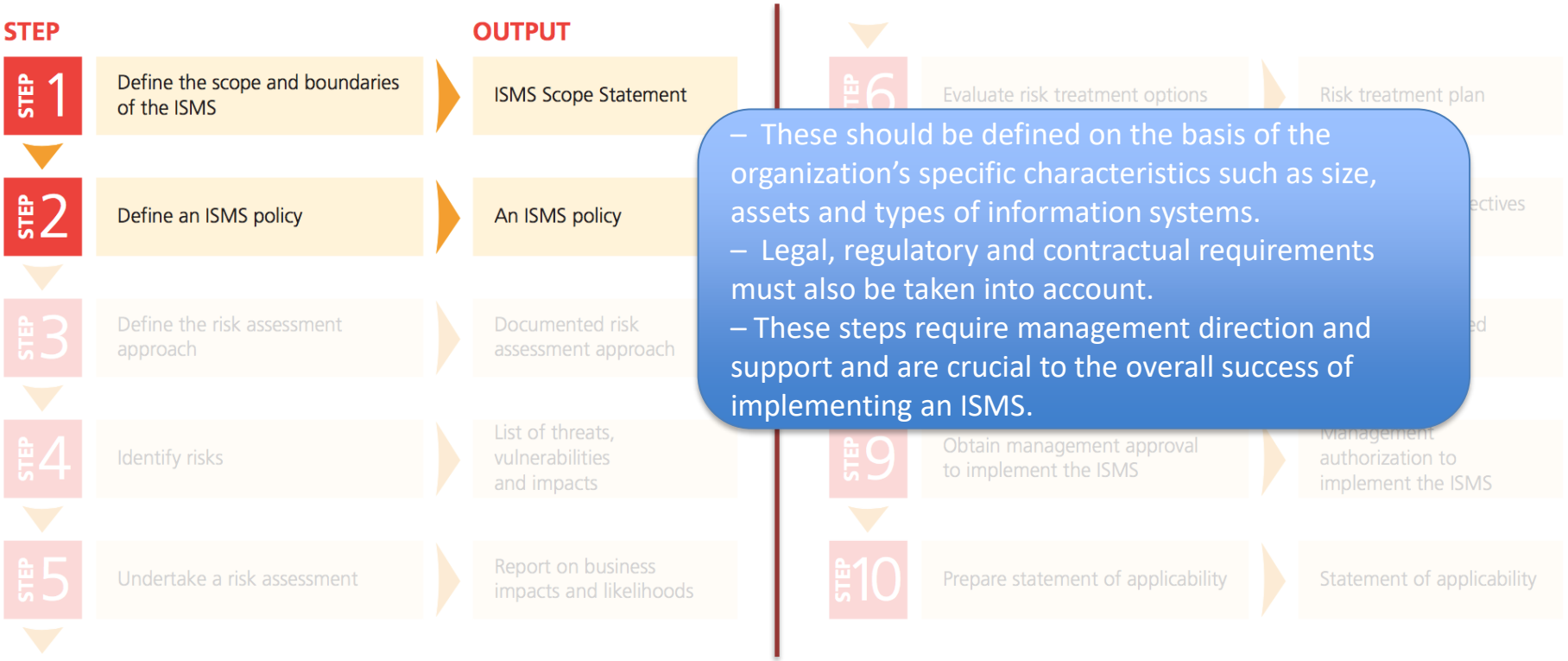
- **ISMS scope (as per clause 4.3)**
- **Information security policy (clause 5.2)**
- **Information security risk assessment *process* (clause 6.1.2)**
- **Information security risk treatment *process* (clause 6.1.3)**
- **Information security objectives (clause 6.2)**
- **Evidence of the competence 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.

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

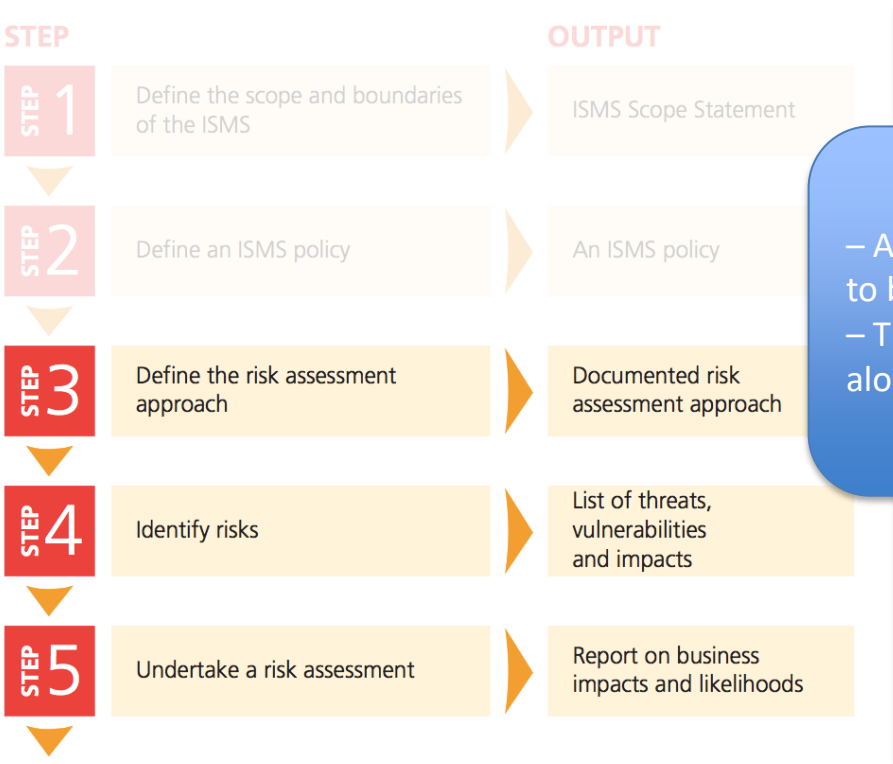


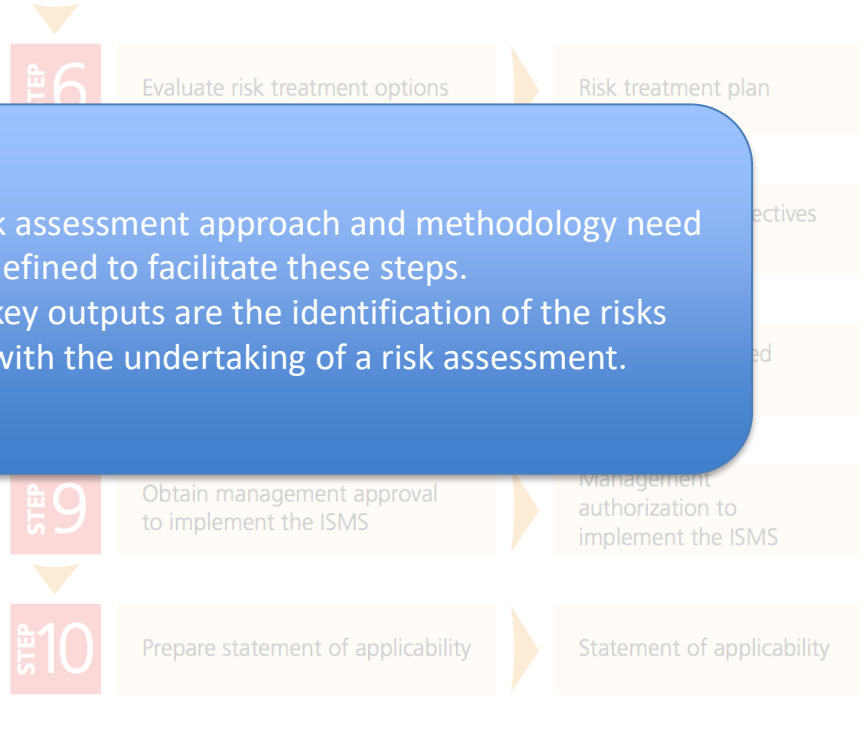
Establishing an ISMS



– 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.

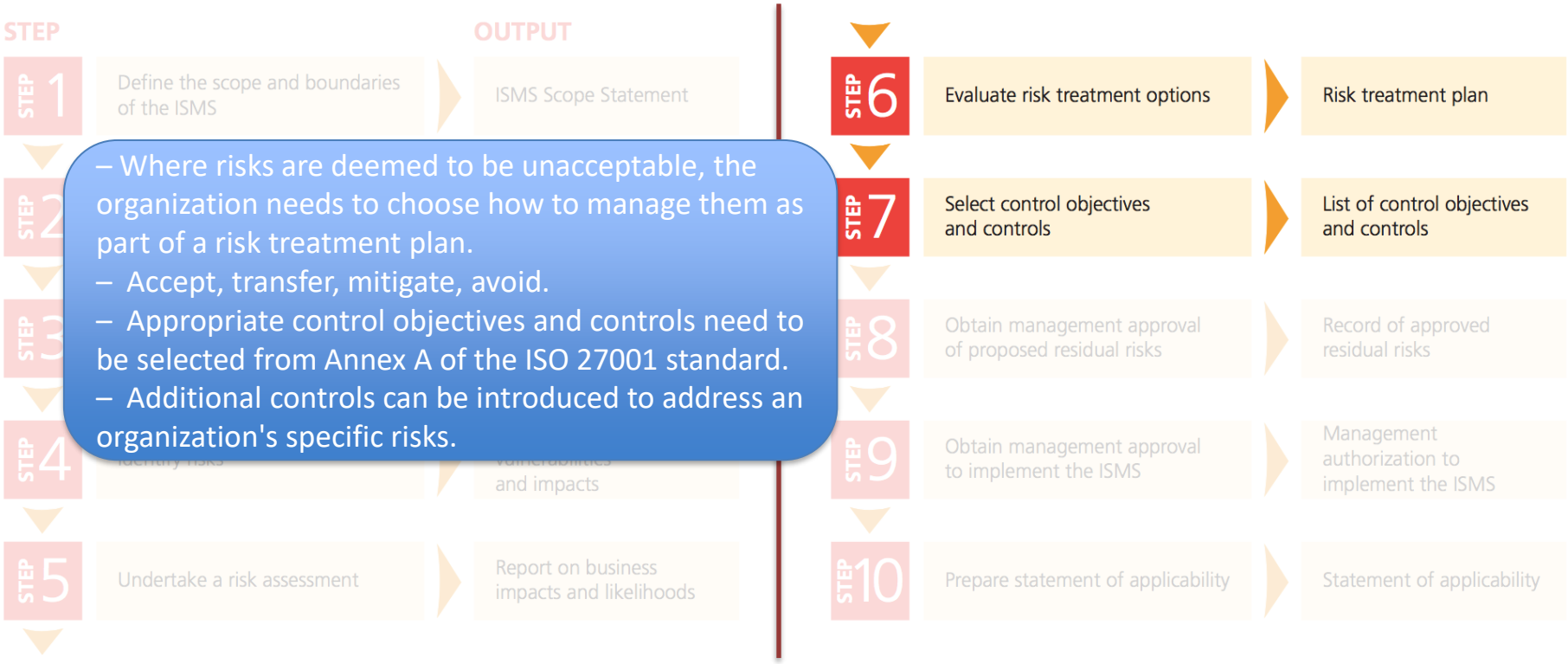
Establishing an ISMS



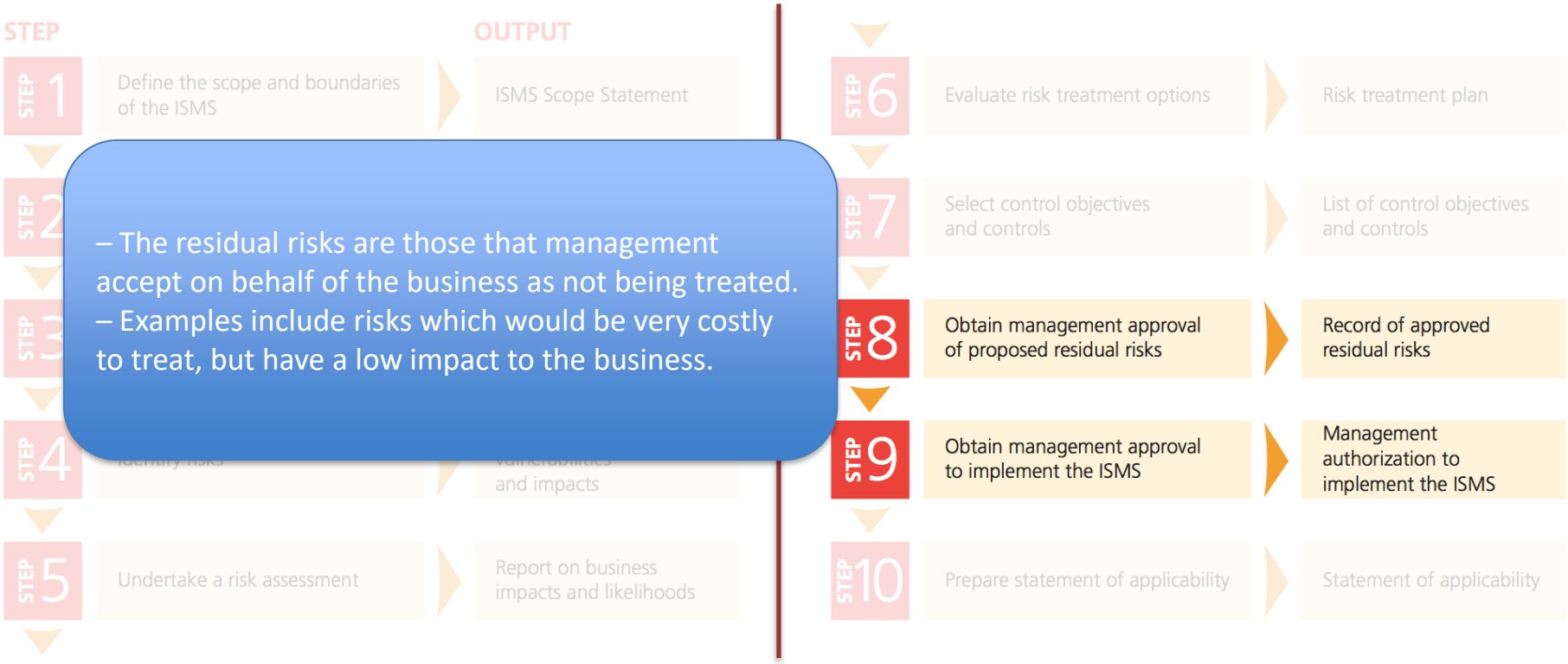


– A risk assessment approach and methodology need to be defined to facilitate these steps.
– The key outputs are the identification of the risks along with the undertaking of a risk assessment.

Establishing an ISMS

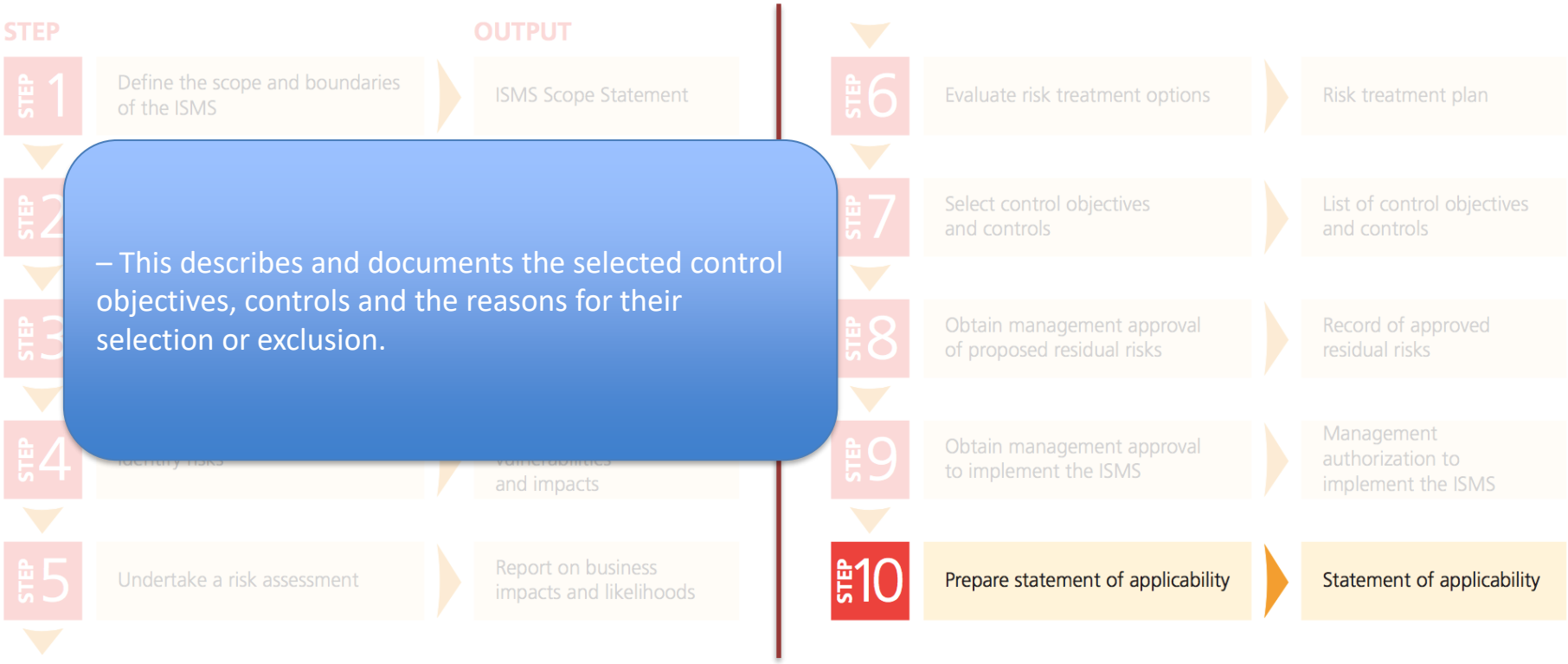


Establishing an ISMS



– 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.

Establishing an ISMS



Seminar 3: British Standards Online

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

Search for the **ISO27000** and **ISO27001** documents.
(you may also want to find other related documents in the **ISO27000** series).

Individually, start to consider:
What are the benefits of an ISMS? (Section 3.7 27000)
What are the critical success factors for the ISMS to succeed? (Section 3.6 27000)

What organisation will you focus your assignment on?
How does the implementation of an ISMS fit with your chosen organisation?