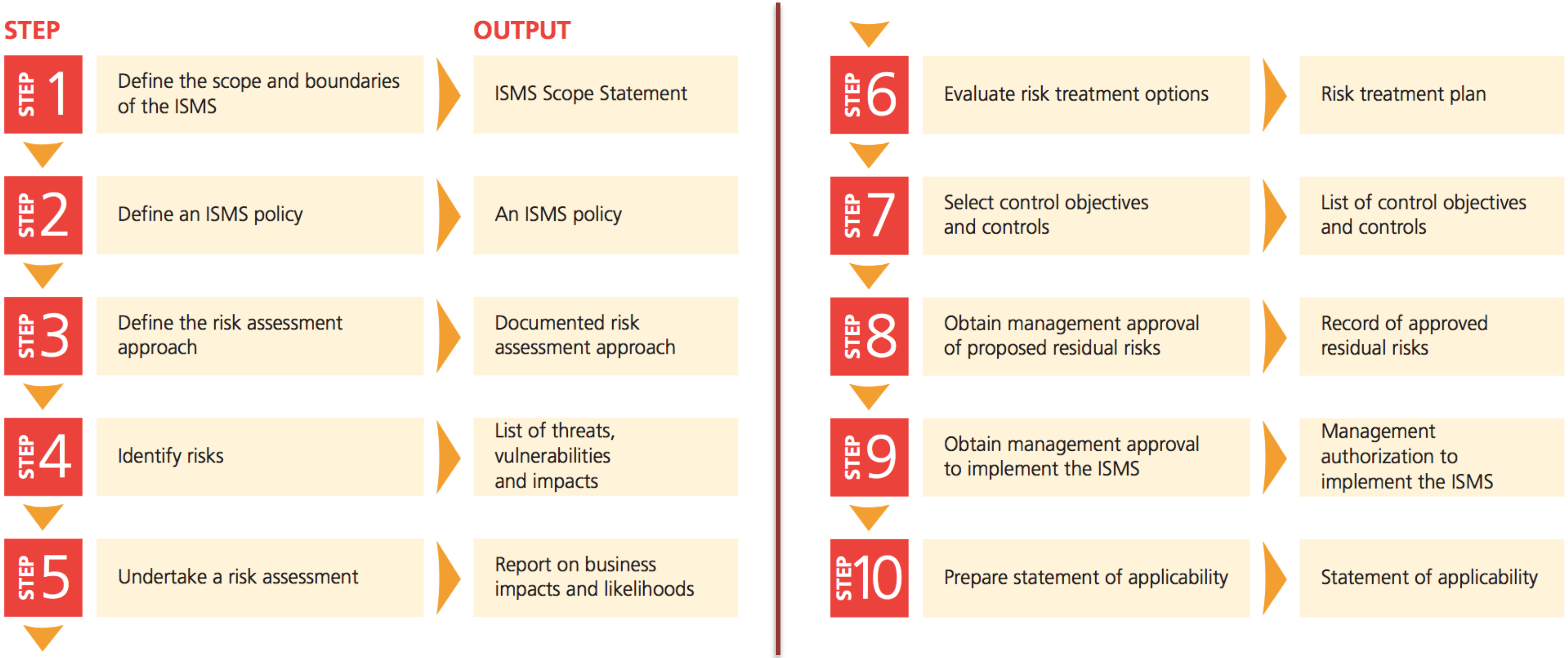
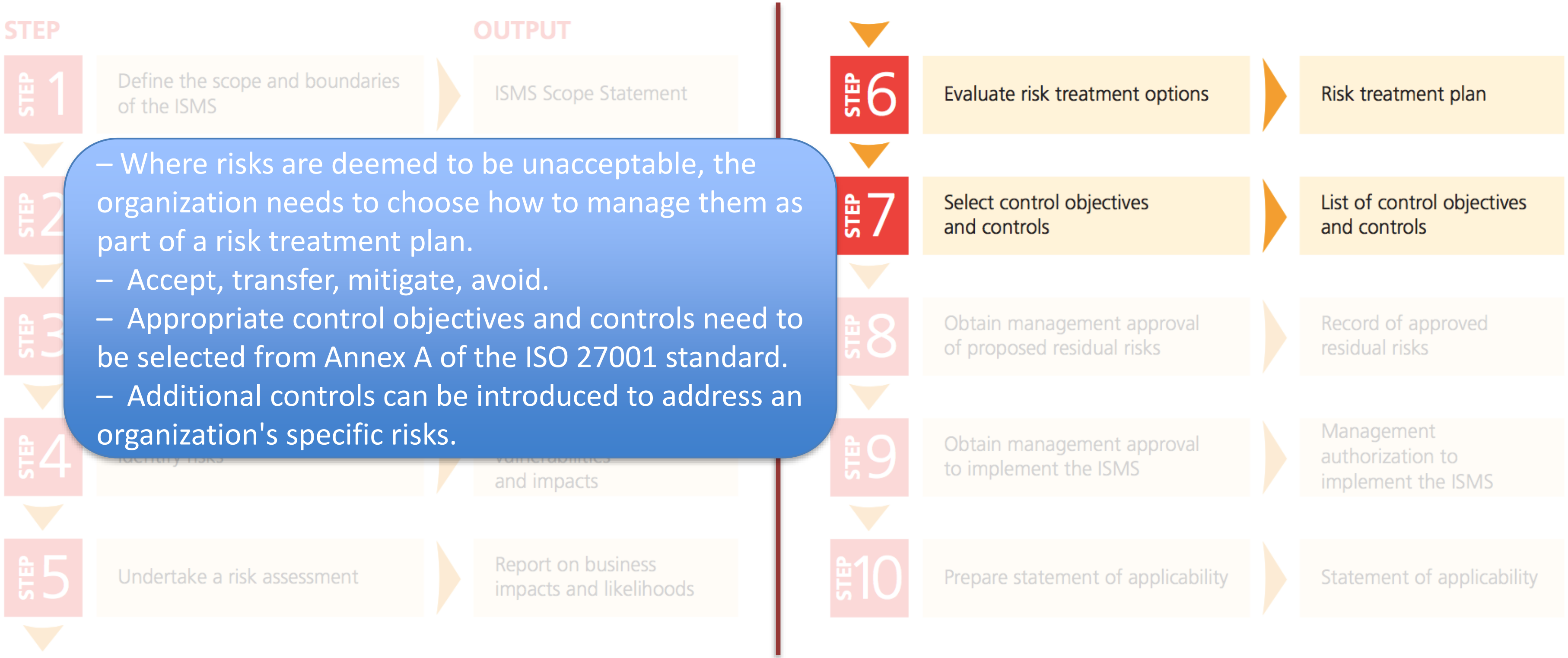
Information Security Management System (Part 2)

Establishing an ISMS



STEP		OUTPUT
STEP 1	Define the scope and boundaries of the ISMS	ISMS Scope Statement
STEP 2	Define an ISMS policy	An ISMS policy
STEP 3	Define the risk assessment approach	Documented risk assessment approach
STEP 4	Identify risks	List of threats, vulnerabilities and impacts
STEP 5	Undertake a risk assessment	Report on business impacts and likelihoods
STEP 6	Evaluate risk treatment options	Risk treatment plan
STEP 7	Select control objectives and controls	List of control objectives and controls
STEP 8	Obtain management approval of proposed residual risks	Record of approved residual risks
STEP 9	Obtain management approval to implement the ISMS	Management authorization to implement the ISMS
STEP 10	Prepare statement of applicability	Statement of applicability

Establishing an ISMS



– Where risks are deemed to be unacceptable, the organization needs to choose how to manage them as part of a risk treatment plan.

– Accept, transfer, mitigate, avoid.

– Appropriate control objectives and controls need to be selected from Annex A of the ISO 27001 standard.

– Additional controls can be introduced to address an organization's specific risks.

STEP
OUTPUT
STEP 1
Define the scope and boundaries of the ISMS
ISMS Scope Statement
STEP 2
STEP 3
STEP 4
and impacts
STEP 5
Undertake a risk assessment
Report on business impacts and likelihoods
STEP 6
Evaluate risk treatment options
Risk treatment plan
STEP 7
Select control objectives and controls
List of control objectives and controls
STEP 8
Obtain management approval of proposed residual risks
Record of approved residual risks
STEP 9
Obtain management approval to implement the ISMS
Management authorization to implement the ISMS
STEP 10
Prepare statement of applicability
Statement of applicability

Control Objectives and Controls

11 Control Objectives and Controls that are typically accounted for

(given in Annex A of ISO27001)

Control Objectives and Controls

1. Security Policy

- The documented policy helps communicate the organization’s information security goals.
- It should be clearly written and understandable to its readers.
- The policy helps management provide direction and support for information security throughout your organization.

Control Objectives and Controls

2. Organization of Information Security

- Outlines how management ensures implementation of information security within the organization.
- It provides a forum for reviewing and approving security policies and assigning security roles and responsibilities.

Control Objectives and Controls

3. Asset Management

- Managing both physical and intellectual assets are important to maintaining appropriate protection.
- It determines ownership, accountability and protection of information assets.

Control Objectives and Controls

4. Human Resources Security

- The assessing and assigning of employee security responsibilities and awareness enables more effective human resource management.
- Security responsibilities should be determined during the recruitment of all personnel and throughout their employment.

Control Objectives and Controls

5. Physical and Environmental Security

- Securing physical areas and work environments within your organization contributes significantly toward information security management.
- Anyone who deals with your physical premises, whether they are employees, suppliers or customers, play a key role in determining organizational security protection.

Control Objectives and Controls

6. Communications and Operations Management

- Covers the secure delivery and management of the daily operations of information processing facilities and networks.

Control Objectives and Controls

7. Access Control

- Managing access levels of all employees helps to control information security in your organization.
- Controlling levels of systems and network access can become a critical success factor when protecting data or information network systems.

Control Objectives and Controls

8. Information Systems Acquisition, Development and Maintenance

- Involves the secure development, maintenance and acceptance of business applications, products and services into the operational environment.

Control Objectives and Controls

9. Incident Management

- Facilitates the identification and management of information security events and weaknesses and allows for their appropriate and timely resolution and communication.

Control Objectives and Controls

10. Business Continuity Management

- Using controls against natural disasters, operational disruptions and potential security failures helps the continuity of business functions.

Control Objectives and Controls

11. Compliance

- To assist organizations with the identification and compliance with contractual obligations, legal and regulatory requirements.

ISMS Certification

- The ISO runs a number of certification schemes against its standards, including ISO 27001.
- This enables an organisation to have its information assurance governance and management processes certified against ISO 27001.
- To gain accreditation, the organisation’s ISMS (information security management system) has to undergo an external audit carried out by an accredited third-party organisation.
- The auditors use standard processes to check the organisation’s ISMS policies, standards and procedures against the ISO 27001 requirement and then look for evidence that they are being used within the organisation.

ISMS Certification

- The findings from the audit are reported back to the organisation and certification is granted if successful.
- After the initial certification, periodic follow-ups (reassessments) take place to ensure that the standards are still being met.
- There is also an ISO standard (ISO 27006) that is used to guide the accredited certification bodies on the formal processes for certifying or registering other organisations' information assurance management systems.

Resources

- BCS offer a Certificate in Information Security Management Principles:
  - http://certifications.bcs.org/category/15735
  - http://certifications.bcs.org/upload/pdf/infosec-ismp-syllabus.pdf

Recap

- Understanding what threat, vulnerability, and threat can be for an organisation.
- Assessing the risk likelihood and impact

Security Management in Practice

- **ISO 27001** has for the moment 11 Domains, 39 Control Objectives and 130+ Controls. Following is a list of the Domains and Control Objectives.
- 1. Security policy
  Information security policy
  Objective: To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.
- 2. Organization of information security
  Internal organization
  Objective: To manage information security within the organization.
  External parties
  Objective: To maintain the security of the organization’s information and information processing facilities that are accessed, processed, communicated to, or managed by external parties.
- 3. Asset management
  Responsibility for assets
  Objective: To achieve and maintain appropriate protection of organizational assets.
  Information classification
  Objective: To ensure that information receives an appropriate level of protection.
- 4. Human resources security
  Prior to employment
  Objective: To ensure that employees, contractors and third party users understand their responsibilities, and are suitable for the roles they are considered for, and to reduce the risk of theft, fraud or misuse of facilities.
  During employment
  Objective: To ensure that all employees, contractors and third party users are aware of information security threats and concerns, their responsibilities and liabilities, and are equipped to support organizational security policy in the course of their normal work, and to reduce the risk of human error.
  Termination or change of employment
  Objective: To ensure that employees, contractors and third party users exit an organization or change employment in an orderly manner.
- 5. Physical and environmental security
  Secure areas
  Objective: To prevent unauthorized physical access, damage and interference to the organization’s premises and information.
  Equipment security
  Objective: To prevent loss, damage, theft or compromise of assets and interruption to the organization’s activities.
- 6. Communications and operations management
  Operational procedures and responsibilities
  Objective: To ensure the correct and secure operation of information processing facilities.
  Third party service delivery management
  Objective: To implement and maintain the appropriate level of information security and service delivery in line with third party service delivery agreements.
  System planning and acceptance
  Objective: To minimize the risk of systems failures.
  Protection against malicious and mobile code
  Objective: To protect the integrity of software and information.
  Back-up
  Objective: To maintain the integrity and availability of information and information processing facilities.
  Network security management
  Objective: To ensure the protection of information in networks and the protection of the supporting infrastructure.
  Media handling
  Objective: To prevent unauthorized disclosure, modification, removal or destruction of assets, and interruption to business activities.
  Exchange of information
  Objective: To maintain the security of information and software exchanged within an organization and with any external entity.
  Electronic commerce services
  Objective: To ensure the security of electronic commerce services, and their secure use.
  Monitoring