ISO 27001 DOMAINS AND CONTROLS OBJECTIVES

Course overview. ISO 27001 standard has, for the moment 11 Domains, 39 Control Objectives and 130+ Controls. In this course we talk about the Domains and Control Objectives.

1 Security policy
1.1 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
2.1 Internal organization
Objective: To manage information security within the organization.
2.2 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
3.1 Responsibility for assets
Objective: To achieve and maintain appropriate protection of organizational assets.
3.2 Information classification
Objective: To ensure that information receives an appropriate level of protection.

4 Human resources security
4.1 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.
4.2 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.
4.3 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

5.1 Secure areas

Objective: To prevent unauthorized physical access, damage and interference to the organization's premises and information.

5.2 Equipment security

Objective: To prevent loss, damage, theft or compromise of assets and interruption to the organization's activities.

6 Communications and operations management

6.1 Operational procedures and responsibilities

Objective: To ensure the correct and secure operation of information processing facilities.

6.2 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.

6.3 System planning and acceptance

Objective: To minimize the risk of systems failures.

6.4 Protection against malicious and mobile code

Objective: To protect the integrity of software and information.

6.5 Back-up

Objective: To maintain the integrity and availability of information and information processing facilities.

6.6 Network security management

Objective: To ensure the protection of information in networks and the protection of the supporting infrastructure.

6.7 Media handling

Objective: To prevent unauthorized disclosure, modification, removal or destruction of assets, and interruption to business activities.

6.8 Exchange of information

Objective: To maintain the security of information and software exchanged within an organization and with any external entity.

6.9 Electronic commerce services

Objective: To ensure the security of electronic commerce services, and their secure use.

6.10 Monitoring

Objective: To detect unauthorized information processing activities.

7 Access control

7.1 Business requirement for access control

Objective: To control access to information.

7.2 User access management

Objective: To ensure authorized user access and to prevent unauthorized access to information systems.

7.3 User responsibilities

Objective: To prevent unauthorized user access, and compromise or theft of information and information processing facilities.

7.4 Network access control

Objective: To prevent unauthorized access to networked services.

7.5 Operating system access control

Objective: To prevent unauthorized access to operating systems.

7.6 Application and information access control

Objective: To prevent unauthorized access to information held in application systems.

7.7 Mobile computing and teleworking

Objective: To ensure information security when using mobile computing and teleworking facilities.

8 Information systems acquisition, development and maintenance

8.1 Security requirements of information systems

Objective: To ensure that security is an integral part of information systems.

8.2 Correct processing in applications

Objective: To prevent errors, loss, unauthorized modification or misuse of information in applications.

8.3 Cryptographic controls

Objective: To protect the confidentiality, authenticity or integrity of information by cryptographic means.

8.4 Security of system files

Objective: To ensure the security of system files.

8.5 Security in development and support processes

Objective: To maintain the security of application system software and information.

8.6 Technical Vulnerability Management

Objective: To reduce risks resulting from exploitation of published technical vulnerabilities.

9 Information security incident management

9.1 Reporting information security events and weaknesses

Objective: To ensure information security events and weaknesses associated with information systems are communicated in a manner allowing timely corrective action to be taken.

9.2 Management of information security incidents and improvements

Objective: To ensure a consistent and effective approach is applied to the management of information security incidents.

10 Business continuity management

10.1 Information security aspects of business continuity management

Objective: To counteract interruptions to business activities and to protect critical business processes from the effects of major failures of information systems or disasters and to ensure their timely resumption.

11 Compliance

11.1 Compliance with legal requirements

Objective: To avoid breaches of any law, statutory, regulatory or contractual obligations, and of any security requirements.

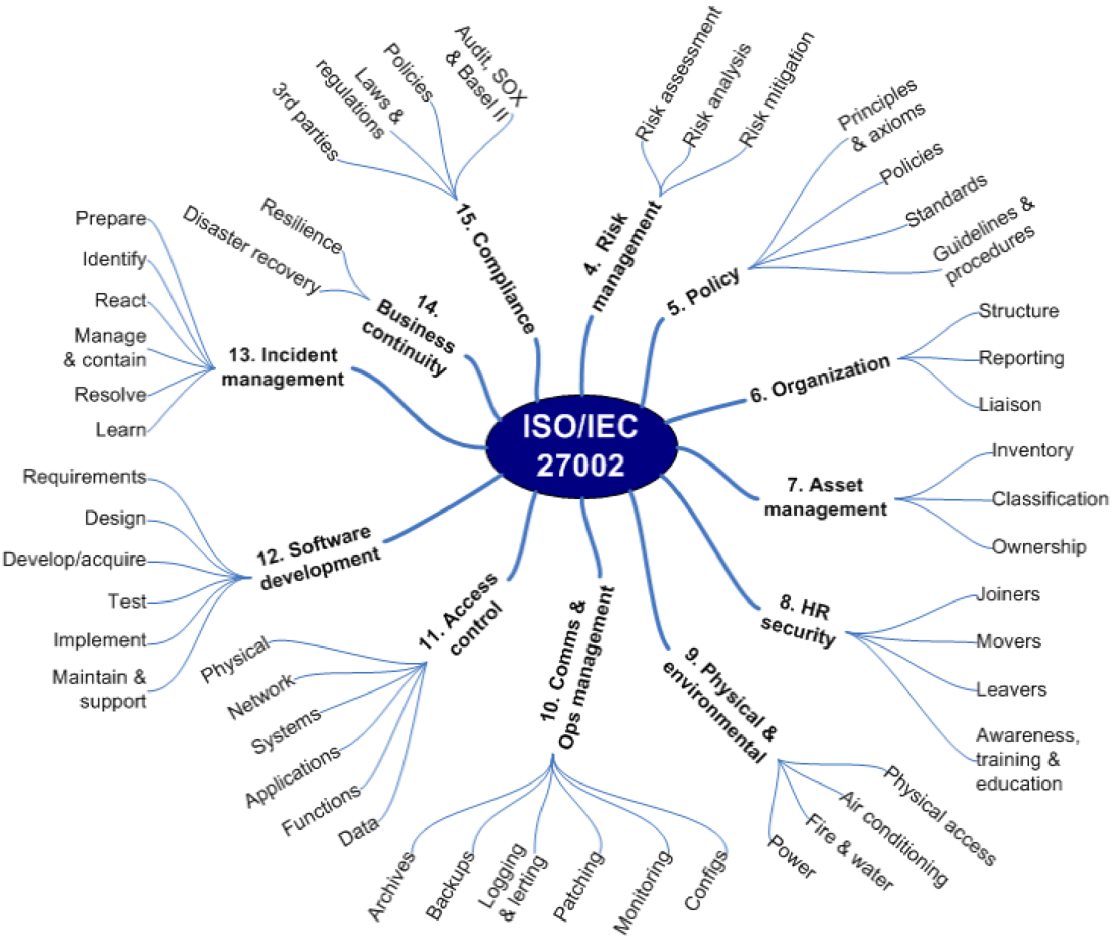
11.2 Compliance with security policies and standards, and technical compliance

Objective: To ensure compliance of systems with organizational security policies and standards.

11.3 Information systems audit considerations

Objective: To maximize the effectiveness of and to minimize interference to/from the information systems audit process.

12 Flowchart (graph) of connection between Domains and Control objectives



References

http://www.iso27001security.com/