Examination Institute

Foundation in Information Security Management System (ISMS) according to ISO/IEC 27001

Specification Sheet

(Requirements, Details & Explanations)

ISO/IEC 27001 Foundation
TÜV SÜD Akademie

Examination Institute

Contents

1 Reading aid 4
2 ISO/IEC 27000 series – Introduction 4
3 Aim of the qualification 4
4 Benefit of the qualification 4
5 Target group of the qualification 5
6 ISO/IEC 27000 series qualification scheme structure 5
7 Specification of the exam 6
7.1 Exam name 6
7.2 Exam format 6
7.3 Exam prerequisites 6
7.4 Exam content 6
7.4.1 Weight of exam content 6
7.4.2 Detailed content 6
7.5 Exam terms 9
8 Description of the training 9
8.1 Training name 9
8.2 Training format 9
8.3 Training prerequisites 9
8.4 Training content 9
8.5 Requirements for training providers 10
8.6 Requirements for trainer 10
8.7 Training-related Requirements 10
8.8 Requirements of practical assignments 10
8.9 Training outline 11
9 Glossary 12
10 Further applicable information 13
10.1 Certification 13
10.2 Exam matrix / taxonomy & literature references 13
10.3 Appicable documents 14
10.4 Revision history 14
Annex 1 – Exam terms 15

The International Organization for Standardization (ISO) is a non-governmental organization which is a network of the national standards institutes of 163 countries.
ISO is the owner of the ISO/IEC 20000 and the ISO/IEC 27000 standard series.

Examination Institute

1 Reading aid

This document is designed to support training providers by the development of their trainings and training materials that meet with TÜV SÜD requirements.

The main objective of the specification sheet is to identify the exam subjects, the exam requirements and specifications, and the target audience.

2 ISO/IEC 27000 series – Introduction

Information and data are the most valuable capital of a company. The objective of a well-functioning information security management system (SMS) is to protect the confidentiality, integrity and availability of information.
The ISO/IEC 27000 series of standards addresses the requirements of information security.

The ISO/IEC 27001:2005 (revised version of BS 7799-2:2002) and ISO/IEC 27002:2005 (revised version of ISO/IEC 17799:2000, previously BS 7799-1:1999) standards lay the foundation for developing an effective information security management system. In this context, important assets must be controlled and protected and risks minimized. Given this, a well-functioning information security system also contributes to business success.

3 Aim of the qualification

The qualification of the Foundation in ISMS according to ISO/IEC 27001 is designed to provide knowledge of what an Information Security Management System is and the minimum requirements that companies should aspire to within the context of ISO/IEC 27001. It will test the capability of the candidate to “remember” and “understand” the concepts that are explained.

Successful candidates will receive a third-party, internationally recognized confirmation of knowledge (certificate) in management systems as per ISO/IEC 27001.

4 Benefit of the qualification

The qualification and certification program according to the ISO/IEC 27000-series familiarizes candidates with the contents of the ISO/IEC 27000 and the certification standard ISO/IEC 27001, its practice-oriented implementation in the form of a management system, including the relationship with other relevant standards within the ISO/IEC 27000-family and further standards as well, and the best practices, methods and frameworks associated therewith.

This well-structured training programme helps candidates to continuously improve their personal qualifications, thus supporting their continual professional development within their company or IT organization. The staff qualifications at the various levels, building on each other, are internationally recognized and comparable and cover the entire bandwidth – from management to processes and results for internal and external customers.

Examination Institute

Candidate benefits summarized:

- ✓ Aligned to international standards
- ✓ Recognized, third-party qualification of persons
- ✓ Qualification and training-course concept in line with company requirements
- ✓ Transfer of practice-oriented expertise in a well-structured training-course programme

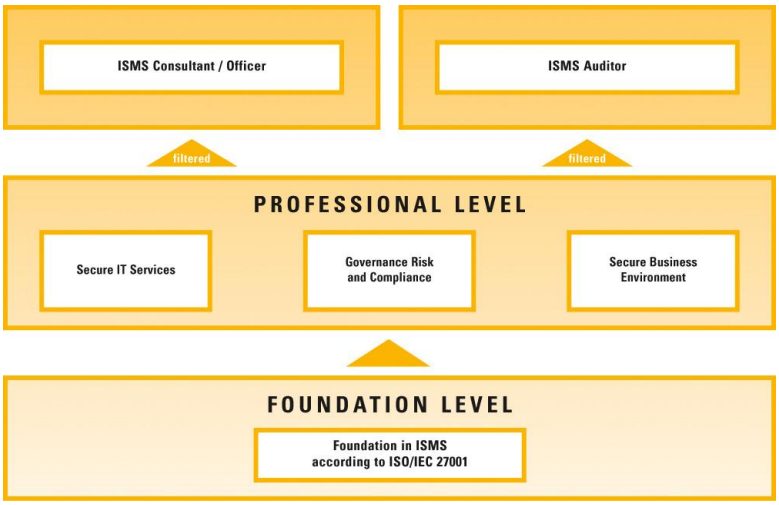
5 Target group of the qualification

The target audience includes both internal and external persons, who play a role in Information Security Management or have an interest in ISO/IEC 27000, even if such an organization is not (yet) certified. The certificate Foundation in ISMS is particularly aimed at this wider audience.

The certificate Foundation in ISMS according to ISO/IEC 27001 is a prerequisite for the other qualifications within the qualification scheme.

6 ISO/IEC 27000 series qualification scheme structure

The certificate Foundation in ISMS according to ISO/IEC 27001 is part of the “Qualification Scheme for Personnel according to the ISO/IEC 27000-series”, which covers a series of exams that are aligned with the various roles in Information Security Management.



Examination Institute

7 Specification of the exam

7.1 Exam name

The exam name is:

Foundation in ISMS Examination according to ISO/IEC 27001.

7.2 Exam format

Multiple-choice examination consisting of 40 questions. The examination is passed, if minimum 65% of the answers are answered correct (26 of 40).

Duration of the exam: 60 minutes.

7.3 Exam prerequisites

There are no prerequisites for this exam.

7.4 Exam content

7.4.1 Weight of exam content

Exam requirements	*Weight (%)*
1. The candidate understands the definitions and principles of Information Security Management	**10**
2. The candidate understands the position of ISO/IEC 27001 in the context of ISM	**15**
3. The candidate understands the concept and the content of ISM according to ISO/IEC 27001	**45**
4. The candidate has an overview of the Security Controls of ISO/IEC 27001 (insofar as control objectives exist)	**30**

7.4.2 Detailed content

1. The candidate understands the definitions and principles of Information Security Management

1.1 The candidate needs to demonstrate his knowledge and understanding of the principles
- 1.1.1 Understand of what a management system is and what components it should include.
- 1.1.2 Explain what is meant by assets in organizations.
- 1.1.3 Explain what information security includes in the broader sense
- 1.1.4 Understand possible kinds of IT applications and ICT

1.2 The candidate needs to demonstrate his knowledge and understanding of the term "Information Security"
- 1.2.1 Explain the most important Information Security aspects.
- 1.2.2 Define the influence of persons, processes and technology on information security.
- 1.2.3 Define the need of IT Security and possible information security targets for organizations.

1.3 The candidate needs to demonstrate his knowledge and understanding of the term "risk"
- 1.3.1 Understand the link between risks and threats and weaknesses of assets.
- 1.3.2 Define aspects that are crucial to quantify risks.
- 1.3.3 Understand options to manage risks.

1.4 The candidate needs to demonstrate his knowledge and understanding of the term "Continual Improvement"
- 1.4.1 Name the principles of the process model (previously PDCA-model).
- 1.4.2 Name possible inputs and outputs of the ISMS for continual improvement.
- 1.4.3 Explain the value and the need of continual improvement for a management system.

2. The candidate understands the position of ISO/IEC 27001 in the context of ISM.

2.1 The candidate needs to demonstrate his knowledge and understanding of landscape of frameworks and standards.
- 2.1.1 Describe the link between ISO/IEC 27000 series and other management system standards (e.g. the ISO/IEC 9000 and ISO/IEC 20000 series) and their differences.
- 2.1.2 Define the purpose and the application/differences of COBIT™, Common Criteria (ISO 15408), *IT-Grundschutzkataloge* (respectively other national initiatives), COSO
- 2.1.3 Understand their relation to other standards of the organization or branch.

2.2 The candidate needs to demonstrate his knowledge and understanding of the terms used during certifications.
- 2.2.1 Understand the terms applicability, boundaries, and scoping
- 2.2.2 Define the benefits of the certification.
- 2.2.3 Understand the certification process with ISO/IEC 27001.
- 2.2.4 Identify the roles and responsibilities in the context of the certification program.

2.3 The candidate needs to demonstrate his knowledge and understanding of the objectives and the structure of the ISO/IEC 27000 series.
- 2.3.1 Name the basic progress (BS 7799 history) and the responsible groups (owner) of the ISO/IEC 27000 series.
- 2.3.2 Name the purpose and the benefits of ISO/IEC 27001.
- 2.3.3 Describe and explain the basic structure of ISO/IEC 27000 series.
- 2.3.4 Define the difference between ISO/IEC 27001 and ISO/IEC 27002.
- 2.3.5 Illustrate the concept of Security Controls.
- 2.3.6 Remember terms and definitions related to ISO/IEC 27000 series.

3 The candidate understands the concept and the content of ISM according to ISO/IEC 27001.

3.1 The candidate needs to demonstrate his knowledge and understanding of the prerequisites to establish, implement, and document the ISMS.
- 3.1.1 Understand the content of a ISMS policy and objectives of an ISMS.
- 3.1.2 Understand the security relevant requirements of business critical assets and the importance to be paid in handling them
- 3.1.3 Describe the process model approach to establishing the ISMS
- 3.1.4 Understand the documentation and record requirements of the ISMS and how they shall be protected.
- 3.1.5 Name critical success factors to establish, operate and improve the ISMS.

3.2 The candidate needs to demonstrate his knowledge and understanding of the requirements to establish, to implement, and to improve the risk management.
- 3.2.1 Name the influence of the business environment and business assets on risks that have to be considered.
- 3.2.2 Understand the steps of a methodical approach of a business-oriented risk assessment.
- 3.2.3 Explain the benefit of standardized criteria for risk evaluation and approval.
- 3.2.4 Understand the application and the benefit of Security Controls in the context of risk management.
- 3.2.5 Understand the activities of systematic management (including planning) and ongoing monitoring of risks.

3.3 The candidate needs to demonstrate his knowledge and understanding of the requirements for monitoring and improvement of the ISMS.
- 3.3.1 Explain the requirements for internal ISMS audits regarding planning and execution.
- 3.3.2 Name the requirements for the ISMS management reviews.
- 3.3.3 Describe the requirements for the evidence of effectiveness (indicators/characteristics) of the ISMS and of the Security Controls.
- 3.3.4 Name the requirements regarding improvement of the ISMS.
- 3.3.5 Understand information security incident management principles

3.4 The candidate needs to demonstrate his knowledge and understanding of the requirements for training, security awareness und security expertise.
- 3.4.1 Name the relevant roles of the ISMS and the required security expertise.
- 3.4.2 Explain the requirements of ISO/IEC 27001 regarding education and security awareness.

4 **The candidate has an overview of the Security Controls of ISO/IEC 27001 (insofar as control objectives exist).**

4.1 The candidate needs to demonstrate his knowledge and understanding of the required controls for the ISMS organization.
- 4.1.1 Illustrate the targets and requirements for the ISMS organization and the ISMS related (internal and external) communication.
- 4.1.2 Describe the targets and requirements for the management of external parties.
- 4.1.3 Describe the targets and requirements for the asset management (responsibility and classification).
- 4.1.4 Describe the targets and requirements for human resources (HR processes).
- 4.1.5 Describe the targets and requirements for user access management and user responsibilities.
- 4.1.6 Describe the targets and requirements for compliance (aspects regarding technology, law, regulations, policies, standards).

4.2 The candidate needs to demonstrate his knowledge and understanding of the required controls for the secure administration of the ISMS (basic conditions and operations).
- 4.2.1 Describe the targets and requirements for operational procedures and responsibilities.
- 4.2.2 Define the targets and requirements for protection of system and network security (Change, Capacity, Back-up).
- 4.2.3 Describe the targets and requirements for data storage, media handling, and exchange of information.
- 4.2.4 Define the targets and requirements for monitoring of systems and networks.
- 4.2.5 Describe the targets and requirements for access control of systems and networks.
- 4.2.6 Describe the targets and requirements for cryptographic controls.

4.3 The candidate needs to demonstrate his knowledge and understanding of the controls for the development of secure systems.
- 4.3.1 Describe the targets and requirements for acquisition, development and maintenance of systems and networks.
- 4.3.2 Describe the security requirements for development, test and operational systems.
- 4.3.3 Describe the role of security controls at development or enhancements of systems and networks (part of system requirements).
- 4.3.4 Describe the requirements for installation of software and systems and for the protection of program source code.

4.4 The candidate needs to demonstrate his knowledge and understanding of the required controls for physical and environmental security.
- 4.4.1 Describe the targets and requirements for the physical security (perimeter, access, delivery and loading areas).
- 4.4.2 Describe the targets and requirements for equipment.
- 4.4.3 Describe the requirements for protecting environmental threats.

4.5 The candidate needs to demonstrate his knowledge and understanding for the controls for security issues and for contingency plans (BCM).
- 4.5.1 Define the targets and requirements for the security incident management process.
- 4.5.2 Describe the targets and requirements for the business continuity management process.
- 4.5.3 Describe the targets and requirements to avoid technical vulnerability.

7.5 Exam terms

The terms the candidates should be familiar with are listed in Annex 1 and are intended as a guide for the trainers.

8 Description of the training

8.1 Training name

Foundation in ISMS Training according to ISO/IEC 27001

8.2 Training format

The training has to be provided by one lecturer. Assignments and mock exams should be performed but are not mandatory.
Number of participants for a Foundation in ISMS Training according to ISO/IEC 27001: minimum 6 participants, maximum 25 participants.

8.3 Training prerequisites

None

8.4 Training content

The training covers the following subject areas:
- Principles of information security management
- The significance of information security management as per ISO/IEC 27001
- Basic aspects of an information security management system (ISMS)
- Security controls of ISO/IEC 27001

8.5 Requirements for training providers

The training may only be held by a certified training institute. The requirements to be met by the training institute, the trainer and the training materials are outlined in the relevant specification sheets for certification.

8.6 Requirements for trainer

The training courses must be held by trainers certified by TÜV SÜD. This obligation is mandatory and offers the possibility of presenting the trainers' special qualifications as an additional benefit to clients (cf. 8.5). The requirements for trainers are listed in the specification sheet for trainer certification.

Trainers must attend a train-the-trainer workshop or the Governance Risk and Compliance professional module and pass either the Foundation exam or the Governance Risk and Compliance exam. Trainers will be charged for attendance to the TTT workshop or the professional module, but can take the subsequent exam free of charge.

8.7 Training-related Requirements

For this Foundation in ISMS training, the training institutes may either use the training material of TÜV SÜD as basic material against payment of a licence fee which depends on the number of trainers providing this training per training institute, or submit their own training material for certification. The requirements of this "Foundation in Information Security Management System (ISMS) according to ISO/IEC 27001“ specification sheet and of the specification sheet for the certification of training materials must be fulfilled.

8.8 Requirements of practical assignments

Within this training no practical assignments are mandatory, but to receive better training results the training institute should perform some practical assignments during the training.

8.9 Training outline

The training outline indicates the possible structure of the course. This is an indication only that by no means dictates how training should be conducted. However it provides a logical order for the exam topics and gives a time indication that corresponds with the exam requirements percentage, the overall course lecturing/assignment duration is 15 hours (20 teaching units) plus a 1 hour examination:

No.	Training description and -duration including exam (15+1 hour)	Mininum hours

FND01	**Introduction**
	• Training Logistics
	  ○ Assignments -- optional
	  ○ Exam format
	  ○ Training structure
	• ISO/IEC 27000-series Qualification scheme
		ca. 0,5 hours

FND02	The aim of this unit is to impart the definitions and principles of Information Security Management Specific: • Impart the knowledge and unterstanding of the principles of Management System and asset • Define the term "Information Security" • Define the term "risk" • Define the term "Continual Improvement"	ca. 1,5 hours
FND03	The aim of this unit is to impart the position of ISO/IEC 27001 in the context of ISMS. • Describe the landscape of frameworks and standards. • Define the terms used during certifications. • Impart the objectives and the structure of the ISO/IEC 27000 series.	ca. 2 hours
FND04	The aim of this unit is to impart the concept and the content of ISM according to ISO/IEC 27001. • Explain the prerequisites to establish, implement, and document the ISMS. • Impart the requirements to establish, to implement, and to improve the risk management. • Describe the requirements for monitoring and improvement of the ISMS. • Define the requirements for training, security awareness und security expertise.	ca. 6,5 hours
FND05	The aim of this unit is to impart an overview of the Security Controls of ISO/IEC 27001 (insofar as control objectives exist). • Define the required controls for the ISMS organization. • Define the required controls for the secure administration of the ISMS (basic conditions and operations). • Define the controls for the development of secure systems. • Define the required controls for physical and environmental security. • Define the controls for security issues and for contingency plans (BCM).	ca. 4,5 hours

9 Glossary

Exam matrix / taxonomy

The exam matrix specifies the number and weight of the questions assigned to each topic, based on the exam requirements and specifications.

Exam requirement

The exam requirements are the main topics of a module. The candidate must have a thorough command of these topics.

Exam specification

The exam specifications elaborate on the exam requirements. The exam specifications have two levels. The Mastery level defines what candidates must know, understand and what they must be able to apply, analyze, or solve. The Testing level defines what will be tested and how this will be tested.

Literature

The specification sheet provides a list of required and suggested materials for the exam.

Target group

The target group is the audience for whom the module is intended.

Testing level

The testing level gives an indication of what may be asked in the exam.

Weight

The weight of an exam requirement or exam specification indicates the relative importance of the requirement or specification and is expressed as a percentage. The weight of an exam requirement or exam specification determines the number of questions for each topic in the exam.

10 Further applicable information

10.1 Certification

TÜV SÜD Akademie greatly values the examinees to be trained by Accredited Training Organizations before taking the exam at an Accredited Examination Organization. For more information about the Accreditation process, which is intended to improve and safeguard the quality of the courses and independent certification, please refer to information available at:
TÜV SÜD Akademie:
TÜV SÜD Examination Institute:

www.tuev-sued.com/examination-institute, or

mailto:akd.it@tuev-sued.de, or

TÜV SÜD Akademie GmbH
Certification Body for Persons/
Examination Institute
Westendstrasse 160
80339 Munich / Germany
Phone: +49 89 5791-1909
Fax: +49 89 5791-2247

10.2 Exam matrix / taxonomy & literature references

The exam matrix / taxonomy specifies the number and weight of the questions in the exam, based on the exam requirements and specifications.

Exam matrix / taxonomy				
Exam Requirements	**Exam Specification**		**Weight (%)**	**Number of questions**
	Mastery level	**Testing level**		
1	1.1	1.1.1-1.1.4	**10**	**4**
	1.2	1.2.1-1.2.3		
	1.3	1.3.1-1.3.3		
	1.4	1.4.1-1.4.3		
2	2.1	2.1.1-2.1.3	**15**	**6**
	2.2	2.2.1-2.2.4		
	2.3	2.3.1-2.3.6		
3	3.1	3.1.1-3.1.5	**45**	**18**
	3.2	3.2.1-3.2.5		
	3.3	3.3.1-3.3.5		
	3.4	3.4.1-3.4.2		
4	4.1	4.1.1-4.1.6	**30**	**12**
	4.2	4.2.1-4.2.6		
	4.3	4.3.1-4.3.4		
	4.4	4.4.1-4.4.3		
	4.5	4.5.1-4.5.3		

The literature references shown in the table on the next page refer to those below which are recommended reading for the training provider:

A Humphreys, Edward / Plate, Angelika:
Guidelines on Requirements and Preparations for ISMS Certification based on ISO/IEC 27001
London, BSI, 2005

B ISO/IEC
ISO/IEC 27001-2005(D+E)
Schweiz, ISO, 2005

C ISO/IEC
ISO/IEC 27000-2009(E)
Schweiz, ISO, 2009

D ISO/IEC
ISO/IEC 27002-2005(D+E)
Schweiz, ISO, 2005

10.3 Appicable documents

- Specification sheet for Training Institute Certification
- Specification sheet for Trainer Certification
- Specification sheet for Training Material Certification

10.4 Revision history

Date	Version	Change
22.10.2010	1.1	8.6 Availability of English training material is planned for January 2011
09.11.2011	1.2	Literature references amended
10.02.2012	1.3	Literature references abbreviated
06.11.2012	1.4	General corrections / layout

Annex 1 – Exam terms

This chapter contains the terms and basic knowledge candidates should be familiar with. Terms are listed in order of exam requirements.

1 The candidate understands the definitions and principles of Information Security Management

1.1 The candidate needs to demonstrate his knowledge and understanding of the principles

- Management system
- Process model
- Quality
- Characteristics
- Efficiency, effectiveness
- Measurability
- Information
- Security
- Asset
- Evaluation of assets (importance, classification)
- ICT

1.2 The candidate needs to demonstrate his knowledge and understanding of the term "Information Security"

- Information classification
- Business critical information
- Confidentiality
- Integrity
- Availability

1.3 The candidate needs to demonstrate his knowledge and understanding of the term "risk"

- Definition of risk (based on likelihood, impact)
- Threats
- Vulnerabilities
- Risk analysis
- Risk assessment
- Risk evaluation
- Risk treatment
- Levels of risk
- Residual risk
- Risk management

1.4 The candidate needs to demonstrate his knowledge and understanding of the term "Continual Improvement"

- Process scope and objective
- Process owner
- Improvement
- Metrics for improvement
- Evaluation of improvement
- Continual
- PDCA cycle (plan-do-check-act approach)

2 The candidate understands the position of ISO/IEC 27001 in the context of ISM.

2.1 The candidate needs to demonstrate his knowledge and understanding of landscape of frameworks and standards.

- ISO/IEC 27000 series
- ISO/IEC 20000 series
- ISO/IEC 9000 series
- Relation of the series with each other
- Common Criteria (ISO 15408)
- COBIT™
- COSO
- Relation of these models with ISO 27001

2.2 The candidate needs to demonstrate his knowledge and understanding of the terms used during certifications.

- Auditor
- Internal (1st party) audit / external (2nd party and 3rd party) audit
- Review / management review
- Conformity
- Major non-conformity
- Minor non-conformity
- Recommendation
- Scope
- Certification program
- Certification bodies
- ISMS owner
- Accreditation bodies: IAF, EA

2.3 The candidate needs to demonstrate his knowledge and understanding of the objectives and the structure of the ISO/IEC 27000 series.

- BS7799 series
- Relation of BS779 series to ISO 27000 series
- Relation of ISO/IEC 27000 series with each other (purpose, content, references)
- Committees responsible for ISO/IEC 27000 series (JTC1, etc.)
- Structure of ISO 27001 (management system requirements, security controls)
- Code of practice

3 The candidate needs to demonstrate his knowledge and understanding of the objectives and the structure of the ISO/IEC 27000 series.

3.1 The candidate needs to demonstrate his knowledge and understanding of the prerequisites to establish, implement, and document the ISMS.

- Business requirements
- Security requirements
- Scope, boundaries
- Security policy
- Security objectives
- Critical success factors (for ISMS see ISO 27002, chapter 0.7)
- Security controls
- Control objectives

- Relation of risks and security controls
- ISMS documentation
- Statement of applicability
- Role model (including ownership)
- Security relevant documents/records

3.2 The candidate needs to demonstrate his knowledge and understanding of the requirements to establish, to implement, and to improve the risk management.

- Business asset
- Asset classification
- Risk assessment methodology
- Asset based risk management
- Risk acceptance criteria
- Risk mitigation by security controls
- Risk assessment review
- Risk assessment report

3.3 The candidate needs to demonstrate his knowledge and understanding of the requirements for monitoring and improvement of the ISMS.

- Characteristics/indicators (ISMS effectiveness)
- Measurement of control effectiveness
- Security incidents
- Security incident management
- Non-conformity
- Corrective action (security incident)
- Preventive action (security)
- Prioritization of actions
- Etc.

3.4 The candidate needs to demonstrate his knowledge and understanding of the requirements for training, security awareness und security expertise.

- Security relevant roles (responsibility and competences)
  - Employee
  - Application developer
  - System administrator
  - IT security manager / security manager
  - IT manager
  - Business management
  - ISMS internal auditor
- Awareness
- Training program

4 The candidate has an overview of the Security Controls of ISO/IEC 27001 (insofar as control objectives exist).

4.1 The candidate needs to demonstrate his knowledge and understanding of the required controls for the ISMS organization.

- Authorization process
- Service agreement (security relevance)
- Contractual obligation regarding information security
- Confidentiality agreements

- Ownership of assets
- Inventory of assets
- Screening
- Access rights
- Access control
- Password management
- Privilege management
- Compliance
- Intellectual property rights
- Legal requirements (laws, order, statutory, regulatory or contractual obligations, etc.)

4.2 The candidate needs to demonstrate his knowledge and understanding of the required controls for the secure administration of the ISMS (basic conditions and operations).

- Change management
- Capacity management
- Segregation of duties / two-person integrity
- Documented operating procedures
- acceptance criteria (for information systems)
- Malicious code
- Mobile code
- Information back-up
- Network service
- Removable medium
- Communication types
- Electronic messaging
- Electronic commerce
- Business information system
- IT terms
    - Logging
    - Routing
    - Ports
    - Session
    - On-line transaction
    - Remote diagnostic
- Identification vs. authentication
- Cryptography
- Electronic keys (PKI)
- Key management

4.3 The candidate needs to demonstrate his knowledge and understanding of the controls for the development of secure systems.

- Maintenance
- Message integrity
- Installation
- Operational software

4.4 The candidate needs to demonstrate his knowledge and understanding of the required controls for physical and environmental security.

- Physical security perimeter
- Physical entry controls
- External and environmental threats
- Supporting utilities
- Off-site equipment

4.5 The candidate needs to demonstrate his knowledge and understanding for the controls for security issues and for contingency plans (BCM).

- Technical vulnerability
- Security incident, security event
- Security weakness
- Business continuity management (BCM)
- BCM plan
- Framework for BCM planning
- Critical business process
- Major failure
- Collection of evidence

Justification of choices

To avoid repetition, terms have usually been listed under the first examination specification where they are used. Note that questions based on one of the examination requirements may also use terms listed under the heading for other requirements.