Preparation Guide

Edition 201804

Content

1. Overview

EXIN Information Security Management Expert based on ISO/IEC 27001 (ISMES.EN[1])

Scope

The module Information Security Management Expert based on ISO/IEC 27001 (ISMES.EN) tests specialized knowledge, understanding and skills in structuring, maintaining and optimizing the security of information within an organization.

Summary

Information security is becoming increasingly important. Globalization of the economy leads to a growing exchange of information between organizations (their employees, customers and suppliers) and a growing use of networks, such as the internal company network, connection with the networks of other companies and the internet.

Other relevant trends include:
- (international) standards and certification in the field of information security
- continuing computerization of (IT) management
- development of automated security tools
- remote control
- outsourcing of management tasks
- compliancy

Furthermore, activities of many companies now rely on IT, and information has become a valuable asset. Protection of information is crucial for the continuity and proper functioning of the organization: information must be reliable.
The international standard for Information Security Management ISO/IEC 27001:2017 structures the organization of information security. For that reason, it is an important point of departure for this module.

In the Information Security modules the following definition is being used: Information Security deals with the definition, implementation, maintenance, compliance and evaluation of a coherent set of measures which safeguard the availability, integrity and confidentiality of the (manual and automated) information supply.

[1] The S in the module code stands for: based on the standard.

Context

The ISMES module is the continuation of EXIN Information Security Foundation based on ISO/IEC 27001 (ISFS.EN) and Information Security Management Professional based on ISO/IEC 27001 (ISMP.EN).

The ISFS module tests basic concepts of information security and their interrelationships. The ISFS target group consists of everyone in the organization.
The ISMP module tests organizational and management aspects of information security, and it is geared toward those who, due to their position, are involved in the implementation and evaluation of information security, like the Information Security Manager, ISM) and the Information Security Officer, (ISO) or the Line Manager and the Project Manager.

Target group

IT professionals responsible for the partial or overall set up and development of structural information security, like the Chief Information Security Officer, CISO, the Information Security Manager, ISM, or the Business Information Security Architect, BISA.
Since this certification is on an expert level, being in the possession of the EXIN Information Security Management Professional certification is highly recommended.

Requirements for certification

- The participant has to have at least 2 years of tangible practical experience at the management level in at least two of the main topic areas (examination requirements) of this module.
- Successful completion of:
  - an EXIN accredited training in Information Security Management Expert based on ISO/IEC 27001
    or
  - coaching track Information Security Management Expert based on ISO/IEC 27001 with an EXIN accredited training organization (ATO).
- Successful completion of the exam Information Security Management Expert.

Examination details

The EXIN Information Security Management Expert exam contains two parts:
1. The written part, a practical project
In the chapter on the structure of the exam, the procedure for the practical project is outlined.
2. The oral examination

In the chapter on the structure of the exam, the procedure of the oral exam is outlined.
The written part has to be successfully completed before the oral exam can be taken.
The language for all parts of the exam is English. The candidate can make use of translators and translations.

To prepare for your examination you can order the Guide for candidates at http://www.exin.com.

Number of questions:	Not applicable
Pass mark:	55%
Open book/notes:	Powerpoint presentation
Electronic equipment/aides permitted:	Yes, for Powerpoint presentation
Time allotted for examination:	90 minutes

The Rules and Regulations for EXIN's examinations apply to this exam.

Training

Contact hours

The training can consist of a course of several days, complemented with coaching or can consist of only coaching. The number of contact hours depends on how much coaching the participant needs in order to be ready for the exam.

Indication study effort

The estimated study load of the module EXIN Information Security Management Expert based on ISO/IEC 27001 is 200 hours, depending on existing knowledge and experience.

Procedure

A documented procedure for the ISMES training could be:

- Intake
- Filing
- Assessment of prerequisites (certificates, experience)
- Analysis of gaps between current level and required competencies and deliverables for ISMES
- Services offered to fill in the gaps (for example training, coaching, project paper evaluation, peer interaction) The services can be composed according to the individual's needs
- Design individual training plan
- Exam registration at EXIN
- Exam preparation (i.e. practice the oral exam, individually or in peer group)
- Evaluation

Training organization

You can find a list of our accredited training organizations at www.exin.com.

2. Exam requirements

The exam requirements are specified in the exam specifications. The following table lists the topics of the module (exam requirements) and the subtopics (exam specifications).

Exam requirement	Exam specification	Weight
1. Organization of information security (establishing ISMS)		**20%**
	1.1 Risk management	
	1.2 Roles	
	1.3 Reporting	
2. Information security policy		**10%**
	2.1 Establish policy	
	2.2 Promote policy	
3. Risk analysis		**10%**
	3.1 Conduct analysis	
	3.2 Analyze	
4. Organizational change and –development pertaining to Information Security		**40%**
	4.1 Plan	
	4.2 Awareness	
	4.3 Interventions	
5. Standards and norms		**10%**
	5.1 Choose standards	
6. Audit and certification		**10%**
	6.1 Execute audit	
	6.2 Evaluate ISMS	
	Total	100%

Comment

The number of questions per exam, is dependent upon what the candidate has presented/answered during the oral exam. During the exam, the examiners will determine which specifications warrant further questioning, and doing so, they weigh the significance of each area carefully.

Exam specifications

1 Organization of Information Security

1.1 The candidate can substantiate the risk management process in relationship with the ISMS.
Within a particular organization, in a specific situation, the candidate can…
- 1.1.1 pinpoint the importance and the consequences of various ISMS activities for the organization.
- 1.1.2 define the scope of the ISMS in terms of the characteristics of the business activities, the organization, the location, assets and technology.
- 1.1.3 describe the importance of the ISMS in a convincing way.

1.2 The candidate can define the roles of information security.
Within a particular organization, in a specific situation, the candidate can…
- 1.2.1 determine and explain the different tasks, responsibilities and authorities.
- 1.2.2 determine and implement the different procedures, guidelines and rules.

1.3 The candidate can set up and use a reporting system for the management.
Within a particular organization, in a specific situation, the candidate can…
- 1.3.1 review the ISMS for suitability and effectiveness.
- 1.3.2 define opportunities for improvement.

2 Information Security Policy

2.1 The candidate can participate in the process of establishing the information security policy.
Within a particular organization, in a specific situation, the candidate can…
- 2.1.1 indicate what steps need to be taken to establish an information security policy.

2.2 The candidate can formulate, present and promote an information security policy.
Within a particular organization, in a specific situation, the candidate can…
- 2.2.1 formulate an information security policy, while taking into account the goals of the organization, the legal framework and the organizational and technical options.
- 2.2.2 present and promote the established information security policy.
- 2.2.3 ensure acceptance of the consequences at the management level.

3 Risk Analysis

3.1 Based on an understanding of various risk analysis methods, the candidate can conduct a risk analysis or guide the execution of a risk analysis.
Within a particular organization, in a specific situation, the candidate can…
- 3.1.1 apply the risk analysis method of choice.
- 3.1.2 clarify various steps of the risk analysis.

3.2 The candidate can analyze the results of the risk analysis.
Within a particular organization, in a specific situation, the candidate can…
- 3.2.1 evaluate the various intermediate results of the risk analysis.
- 3.2.2 evaluate the relationship between intermediate results from the risk analysis for consistency.
- 3.2.3 evaluate the end result of the risk analysis based on usefulness and comprehensiveness.

4 Organizational change and -development, pertaining to Information Security

4.1 In a certain situation, the candidate is able to come up with or adapt a plan for change.

Within a particular organization, in a specific situation, the candidate can…

- 4.1.1 evaluate the developmental level (level of growth) of the ISMS.
- 4.1.2 name the characteristics of the organizational culture as well as the opportunities and limitations for the development of the ISMS.
- 4.1.3 define a strategy for change and formulate the intended results.

4.2 The candidate can come up with an awareness program, communicate it, present it and implement it.

In a particular situation within the organization, the candidate can…

- 4.2.1 determine for specific target groups, which change in knowledge, attitude and behavior, can contribute to the improvement of the ISMS.
- 4.2.2 name the success factors and compare the effectiveness of resources.
- 4.2.3 develop an approach to a communication plan.
- 4.2.4 present, defend and -if necessary- adjust proposals for change or the policy of the ISMS at management level, verbally as well as in writing.

4.3 The candidate can, if the situation so requires, implement the changes or guide this process

In a particular situation within an organization, the candidate can…

- 4.3.1 clarify, implement and guarantee interventions in the organization.
- 4.3.2 deal effectively with opinions and feelings of members of the organization, and have different options for interventions.
- 4.3.3 evaluate the interventions that were implemented and reflect on one's own role.

5 Standards and Norms

5.1 In a particular situation, the candidate can choose and use relevant standards.

Within a particular organization, in a specific situation, the candidate can…

- 5.1.1 indicate what the consequences are when choosing a particular standard.
- 5.1.2 guide the process of using a particular standard.
- 5.1.3 evaluate and maintain the implemented framework of norms or a baseline construction.

6 Audit and Certification

6.1 The candidate can organize the execution of audits.

Within a particular organization, in a specific situation, the candidate can…

- 6.1.1 draft an audit program.
- 6.1.2 guide the execution of an audit.
- 6.1.3 suggest improvements, based on the results of the audit.

6.2 The candidate can participate in a management review of the ISMS.

Within a particular organization, in a specific situation, the candidate can…

- 6.2.1 facilitate the introduction of a management review.
- 6.2.2 suggest improvements, based on the review results.
- 6.2.3 document the results of the management review.

Comment

Examination requirement 4 is the core of the structure of information security within an organization, requirement 1 specifies what needs to be put in place, and the remaining requirements detail the set-up. The specifications do not contain any concrete techniques, because these techniques are part and parcel of the curriculum of the candidate. Between candidates there can be differences regarding content due to the contents of the presentation or alternatively, due to the selected curriculum.

Examination design

The exam for the module Security Management Expert based on ISO/IEC 27001 (ISMES.EN) is divided into two parts:

1. the candidate's practical project
2. the oral exam

The candidate's project

The written part contains a practical project of approximately 6000 words about one of the following ISMES subjects:

- Security Awareness plan
- Risk analysis
- Change plan
- ISMS plan
- Audit plan
- Quick scan
- Information Security policy

About eight weeks prior to the proposed date for the oral exam, three copies of this project have to be sent to EXIN. The candidate is expected to include and send a management summary of the project. The criteria for the summary can be found in the Guide. The candidate also has to include a short resume to the project, outlining that he or she has had at least 2 years of management work experience at the management level in the areas of at least 2 examination requirements. The trainer will add an account of the relation between the selected topic and the examination requirement.

The content of the practical project has to be related to the professional context of the candidate. The heart of the project could consist of one (of the aforementioned) documents, provided that the candidate is the author or co-author who has had a clear say in the contents of the document. In that case it should -at least- be supplemented by an introductory and final chapter, making clear what the level of involvement of the candidate has been.

Some of the elements of an introductory chapter are:

- the reason for introducing this particular document to the organization, and the relating question and purpose;
- the role the candidate played in the creation of the document;
- the role/status of the document within the organization.

Some of the elements of the final chapter are:

- Well-thought out reflections on the different components of the process. This demonstrates how the candidate was involved; what the candidate encountered, what alternatives presented themselves, what could be improved upon next time, etcetera.
- A link to the introductory chapter, e.g. to the question and purpose.

Ideally, the entire practical project should be written for ISMES; for example, as the logical continuation of an ongoing project, or because of the needs of the organization the candidate works for. The aforementioned guidelines for an introductory and final chapter also apply.

There are criteria for every one of the aforementioned types of projects. These are listed in detail in a candidate's Guide.

It is highly recommended that the candidate sends a plan for the project paper to EXIN in an early stage in order to have the minimum requirements checked.

When a candidate is not able to write a practical paper based on his or her work environment, the candidate can write a paper based on the case study. This decision is taken by the trainer together with the candidate. The case study is available in the ISMES Guide. Should the candidate choose to use the case study, he or she needs to make clear what kind of personal experience was used, what relevant similarities/differences there are with his/her own work professional context, what he/she has learned from the case study that is relevant to his/her own professional environment etcetera.

The project is evaluated by two EXIN examiners. Criteria have been developed for the aforementioned ISMES sections, and a project needs to meet those criteria. Apart from the contents, the layout and motivation of the project will also be evaluated (including correct use of language and style). After the evaluation, EXIN will send project feedback to the trainer.

Oral exam

The candidate only has access to the oral exam when his or her practical project has received a satisfactory rating (55% or more). The oral exam for Information Security Management Expert based on ISO/IEC 27001 (ISMES) consists of four parts:

I - A presentation by the candidate
The exam starts with a presentation by the candidate. He or she will do a presentation about the project they worked on. The presentation will simulate a situation in which the candidate gives a presentation to the management team with the purpose of persuading management, and to gain acceptance for certain proposals. The presentation will be evaluated on the basis of whether or not it was sufficiently geared toward the management team. The presentation lasts for a maximum of 15 minutes. An overview of the evaluation criteria can be found in the ISMES Guide (oral section).

II - An examination interview based on the presentation
The second part of the exam consists of a conversation with the examiners about the presentation. The examiners will question the candidate in a critical way, as if they were members of the management team. The examiners could ask questions about the contents of the presentation. This conversation takes up (a maximum of) 15 minutes. An overview of the evaluation criteria can be found in the Guide.

III - An examination interview about the other examination requirements
In the third and last part of the exam, the examiners will ask questions about the examination requirements that were not the focus of the presentation, or in the conversation about the presentation. The examiners no longer play the part of the management team. What will be assessed is whether or not the candidate is capable to use the contents of ISMES outside their own professional context, if they can relate the project and the presentation, to their own professional context and recent developments in this specialty. Apart from that, the candidate's ability to reflect on their own conduct in relation to the contents of the module, can be assessed. This means that the candidate also has to be able to step outside the way their company operates, and they should have an understanding of the topics listed in the examination requirements. This final examination interview lasts 25 minutes.

An overview of the examination criteria can be found in the Guide.

IV - Final result
Immediately following the exam, the examiners will reach mutual agreement and will come to a final conclusion, resulting in a final mark. This takes 25 minutes. After that, the examiners notify the candidate verbally of the final mark, and they will clarify their final decision. This takes 10 minutes. The entire exam will take a maximum total of 90 minutes.

The examination session

- During the presentation, the candidate is required to use power point slides from a cd or from their own laptop.
- Immediately before the presentation, the examiners are provided with two sets of one-sided prints of the slides.
- The presentation starts with:
    - One slide with the title of the presentation.
    - One slide with the name of the candidate, his/her job title, the company and the type of company.
- The presentation is about the practical project, so it is not about the career history of the examinee, and it is **not** a description of the company the candidate works for or a description of the candidate's own company.
- During the presentation, the examiners can only ask clarification questions.
- The entire oral exam is documented using recording equipment.
- It is not permitted to influence the examiners by disclosing business- or private matters.

The following persons are present at the oral exam:
- the candidate
- two examiners

The candidate's trainer/supervisor can attend the oral exam as observer, when the candidate has given his or her approval. The exam session can be done via a web conference with video and audio facilities. In that case an EXIN accredited supervisor should be present on the candidate's side.

Time frame

The entire examination session lasts a maximum of 90 minutes, including communication of the result. The examination is structured as follows:
- 15 minutes (maximum) for the presentation
- 15 minutes for discussing the presentation
- 25 minutes for the examination interview about the other exam requirements
- 25 minutes evaluation meeting among the examiners
- 10 minutes for discussing the outcome with the candidate

Conclusion

The examiners evaluate the three parts of the exam based on three evaluation tools. Once the exam is over, the examiners discuss and determine the final mark and justify the result.

3. List of Basic Concepts

The basic concepts as required by ISFS and ISMP are expected to be common knowledge.

4. Literature

Exam literature

The literature as required by ISFS and ISMP is expected to be common knowledge. The following list contains reading suggestions pertaining to the examination requirements and examination specifications.

A. ISO/IEC 27001:2017 (EN)
Information technology – Security techniques – Information security management systems – Requirements
Switzerland, ISO/IEC, 2017
www.iso.org

B. ISO/IEC 27002:2017 (EN)
Information technology – Security techniques – Code of practice for information security controls
Switzerland, ISO/IEC, 2017
www.iso.org

C. ISO/IEC 27000:2018 (EN)
Information technology – Security techniques – Information security management systems – Overview and vocabulary
Switzerland, ISO/IEC, 2018
www.iso.org

D. ISO/IEC 27005:2011 (EN)
Information technology – Security Techniques – Information security risk management
Switzerland, ISO/IEC 2011
www.iso.org

E. ISO/IEC 27799:2016 (EN)
Health informatics – Information security management in health using ISO/IEC 27002
Switzerland, ISO/IEC, 2016
www.iso.org

F. FIPS 2000
Minimum Security Requirements for Federal Information and Information Systems
http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf

G. ISO/IEC 21827:2008
Information technology – Security techniques – Systems Security Engineering – Capability Maturity Model® (SSE-CMM®)
Switzerland, ISO/IEC, 2008
www.iso.org

H. ISO/IEC 27035:2016
Information technology – Security techniques – Information security incident management
Switzerland, ISO/IEC, 2016
www.iso.org

I. Carnal, C.A.
Managing Change in Organizations
Financial Times/Prentice, fourth ed., 2007
ISBN-10: 0273704141
ISBN-13: 9780273704140

J. J. Slocum and D. Hellriegel
Principles of Organizational Behavior
England, South-West Thomson Learning, 2010
ISBN: 9780538743341

K. Robbins, S.P.
Organizational Behavior
Prentice Hall, 13th edition, 2008
ISBN-10: 013207964X
ISBN-13: 9780132079648

L. Cazemier, Jacques A., Paul Overbeek and Louk Peters
Security Management Best Practice
Van Haren, January 2010
ISBN: 978-90-8753-548 3

Comment

At expert level, candidates are responsible for their own information needs. In order to guide this process, suggestions of pertaining literature, articles have been included. This is not a comprehensive list, and there is no guarantee that the curriculum is covered in its entirety. On the other hand, the available literature is quite comprehensive, making the choices quite arbitrary and it does not do justice to the freedom of choice a candidate has at this level.

Contact EXIN

www.exin.com

YOUR ICT COMPETENCE PARTNER