Preparation Guide

Edition 202211

Content

1. Overview

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

Scope

EXIN Information Security Management Expert based on ISO/IEC 27001 certification confirms that the professional can establish and optimize an information security management system (ISMS) in the organization.

The topics of the certification are:

- information security management system (ISMS)
- information security policy
- risk management
- organizational change
- legislation and standards
- audit and certification

Summary

Globalization of the economy leads to an ever-growing exchange of information. This information not only crosses national borders but also the thin lines between private and business domains. Globalization leads to risks from for example:

- cybercrime
- non-observability of Artificial Intelligence (AI) output
- automation of security measures
- gathering data indiscriminately
- disinformation and half-truth

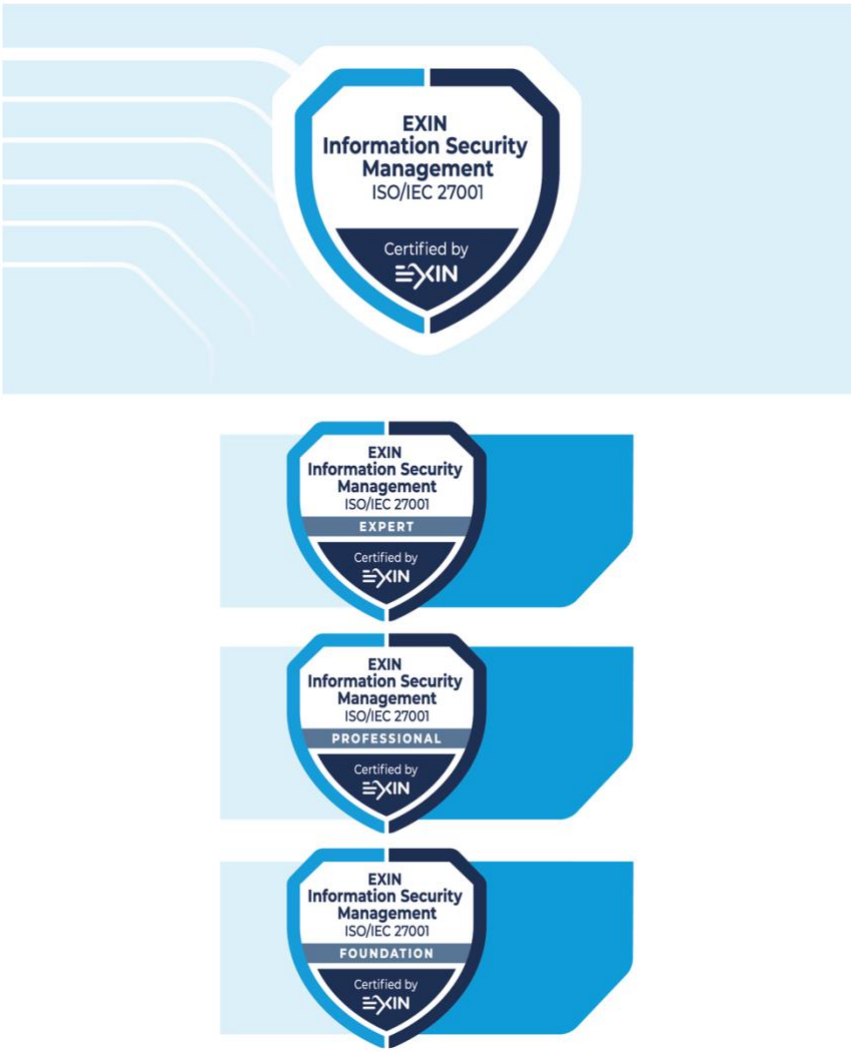
The scope of accountability grows together with the data that is managed.

Information is the most valuable asset of an organization. Protection of information, this includes both the capability of people and the capability in systems, is crucial for the continuity and proper functioning of the organization: reliable information generates trust. The international standard for information security management ISO/IEC 27001 structures the security of information.

In the EXIN Information Security Management based on ISO/IEC 27001 program, the following definition is used: Information security is the preservation of confidentiality, integrity and availability of information.

Context

The certification EXIN Information Security Management Expert based on ISO/IEC 27001 is part of the program EXIN Information Security Management based on ISO/IEC 27001.



Target group

The EXIN Information Security Management Expert based on ISO/IEC 27001 certification is tailored to the needs of the:

- chief information security officer (CISO)
- information security officer (ISO)
- information security manager
- security architect

Requirements for certification

- At least 2 years of practical experience in managing at least 2 areas of this certification (see exam requirements).
- Successful completion of the EXIN Information Security Management Expert based on ISO/IEC 27001 assessment.

The candidate is highly recommended to have attended an EXIN Information Security Management Expert training or coaching track with an EXIN Accredited Training Organization (ATO).

Examination details

Examination type:	Project presentation and interview
Number of questions:	Not applicable
Pass mark:	55%
Open book:	No
Notes:	Yes
Electronic equipment/aides permitted:	Yes
Exam duration:	60 minutes

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

Bloom level

The EXIN Information Security Management Expert based on ISO/IEC 27001 certification tests candidates at Bloom level 5 and 6 according to Bloom's revised taxonomy:

- Bloom level 5. Evaluate - make judgements based on criteria and standards through checking and critiquing. This includes justifying a decision or course of action.
- Bloom level 6. Create - put elements together to form a coherent or functional whole; reorganize elements into a new pattern or structure through generating, planning, or producing. This includes generating new ideas, products, or ways of viewing things.

Training

Contact hours

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 to be ready for the assessment.

Indication study effort

168 hours (6 ECTS), depending on existing knowledge.

Requirements for accreditation

The ATO is accredited for EXIN Information Security Management Professional based on ISO/IEC 27001 (ISMP). The ATO confirms that they follow this procedure:

- Intake of the candidate
- Filing
- Assessment of prerequisites (certificates, experience)
- Analysis of gaps between current level and required competences and deliverables for EXIN Information Security Management Expert based on ISO/IEC 27001
- Services offered to fill the gaps
    - For example, training, coaching, intake by EXIN, peer interaction.
    - The services can be composed according to the individual's needs.
- Offer training or a coaching track
- Assessment preparation
    - For example, practice the project presentation and interview, 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 requirements	Exam specifications	Weight
1. Information security management system (ISMS)		**10%**
	1.1 Scope	
	1.2 Roles	
	1.3 Review	
2. Information security policy		**10%**
	2.1 Policy design	
	2.2 Policy implementation	
3. Risk management		**20%**
	3.1 Risk assessment	
	3.2 Risk treatment	
4. Organizational change		**40%**
	4.1 Plan	
	4.2 Awareness	
	4.3 Intervention	
5. Legislation and standards		**10%**
	5.1 Legislation	
	5.2 Standards	
6. Audit and certification		**10%**
	6.1 Audit program	
	Total	**100%**

Exam specifications

1 Information security management system (ISMS)

1.1 Scope

The candidate can…

1.1.1 define the scope of the ISMS.

1.2 Roles and responsibilities

The candidate can…

1.2.1 determine the roles, responsibilities, and authorities in the ISMS.

1.2.2 identify the information sharing community of the organization.

1.3 Review

The candidate can…

1.3.1 review the ISMS for suitability and effectiveness.

1.3.2 define opportunities for improvement.

1.3.3 facilitate a management review.

2 Information security policy

2.1 Policy design

The candidate can…

2.1.1 define the elements of the information security policy.

2.1.2 draft an information security policy.

2.1.3 ensure top management commitment to the information security policy.

2.2 Policy implementation

The candidate can…

2.2.1 promote the information security policy.

2.2.2 guide implementation of the information security policy.

3 Risk management

3.1 Risk assessment

The candidate can…

3.1.1 define an information security risk assessment process.

3.1.2 apply an information security risk assessment process.

3.2 Risk treatment

The candidate can…

3.2.1 define an information security risk treatment process.

3.2.2 apply an information security risk treatment process.

4 Organizational change

4.1 Plan

The candidate can…

4.1.1 evaluate the maturity of the ISMS.

4.1.2 identify the impact of organizational culture on the ISMS.

4.1.3 define a strategy for change.

4.2 Awareness

The candidate can…

4.2.1 design an information security awareness program.

4.2.2 guide the implementation of an information security awareness program.

4.2.3 review the results of an information security awareness program.

4.3 Intervention

The candidate can…

4.3.1 determine which interventions are needed to improve the ISMS.

4.3.2 evaluate the outcome of an intervention.

5 Legislation and standards

5.1 Legislation

The candidate can…

5.1.1 indicate which legislation is relevant for the ISMS.

5.1.2 guide the process of complying to legislation.

5.2 Standards

The candidate can…

5.2.1 indicate the consequences of applying a particular standard.

5.2.2 guide the process of applying a particular standard.

5.2.3 evaluate the implemented framework.

6 Audit and certification

6.1 Audit program

The candidate can…

6.1.1 design an internal audit program.

6.1.2 guide execution of the internal audit program.

6.1.3 prepare the organization for certification audit.

6.1.4 suggest improvements, based on the results of audits.

3. List of basic concepts

The basic concepts as required by EXIN Information Security Foundation based on ISO/IEC 27001 (ISFS) and EXIN Information Security Management Professional based on ISO/IEC 27001 (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 exam requirements and exam specifications.

A. ISO/IEC 27001:2022
Information security, cybersecurity and privacy protection — Information security management systems — Requirements
Switzerland, ISO/IEC, 2022
www.iso.org

B. ISO/IEC 27002:2022
Information security, cybersecurity and privacy protection — Information security controls
Switzerland, ISO/IEC, 2022
www.iso.org

C. ISO/IEC 27000:2020
Information technology – Security techniques – Information security management systems – Overview and vocabulary
Switzerland, ISO/IEC, 2020
www.iso.org

D. ISO/IEC 27005:2018
Information technology – Security Techniques – Information security risk management
Switzerland, ISO/IEC, 2018
www.iso.org

E. ISO/IEC 27701:2019
Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines
Switzerland, ISO/IEC, 2019
www.iso.org

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

G. NIST Cybersecurity Framework
Framework for Improving Critical Infrastructure Cybersecurity
NIST, 2018
https://www.nist.gov/cyberframework

H. Hodges, J.
Managing and Leading People through Organizational Change: The Theory and Practice of Sustaining Change through People
Kogan Page, 2021 (2nd edition)
ISBN: 978 1 78966 797 4

5. Assessment process

General

The assessment EXIN Information Security Management Expert based on ISO/IEC 27001 consists of a project presentation and an interview.

This chapter describes the procedure of the assessment.

Confidentiality

The assessors have a Non-Disclosure Agreement with EXIN. The information in the project presentation and the interview is confidential.

Procedure

- Submit project presentation and curriculum vitae in pdf format to EXIN.
- Check of completeness and viability (2 weeks / EXIN)
- Payment (1 week / candidate)
- Preparation assessment (4 weeks / EXIN)
- Invitation for the session; physical or remote (EXIN)
- Session and recommended result (Assessors)
- Final result and score, certificate and badge (4 weeks / EXIN)

Project

Project presentation file

The presentation shows a project in a maximum of 20 slides.

The project is not older than two years and suits the objectives of the organization the candidate is working for. The candidate is the author of the presentation and had a high level of involvement in the project.

The presentation contains an introductory slide, a core and a final slide.

The introductory slide is a management summary describing:
- the core issue or question to be resolved or improved with the project
- the role of the candidate in the project
- the position of the project in the context of the organization

The core slides cover one of the following topics:
- information security management system (ISMS)
- information security policy
- risk management
- organizational change
- legislation and standards
- audit and certification

The final slide covers:

- reflections on the various stages in the project: the candidate's performance; what the candidate encountered, what alternatives presented themselves, what choices were made, what could be improved next time, etc.
- conclusions and recommendations, asking approval for one recommendation

Evaluation

The project is evaluated by two assessors. The evaluation tools that are used for this are in chapter 6 of this preparation guide. These forms can also be used as a structure for the presentation.

Depending on the chosen subject, one of the tables in chapter 6 is used for evaluating the project.

Session

The session is recorded. Recordings are deleted 6 months after the session.

I The presentation by the candidate

The session starts with a presentation by the candidate. The candidate presents the project they worked on. The presentation simulates a situation in which the candidate gives a presentation to the management team with the purpose of gaining approval of a certain proposal. The presentation is about the project, it is not about the career of the candidate, and not a description of the company the candidate works for. The assessors can ask questions for clarification. The presentation is (a maximum of) 20 minutes.

II Interview based on the presentation

The second part of the session consists of a conversation with the assessors about the presentation. The assessors question the candidate as if they were members of the management team. This conversation is (a maximum of) 20 minutes.

III Interview about the other exam requirements

In the third and last part of the session, the assessors ask questions about the exam requirements that were not the focus of the project. The assessors no longer play the part of the management team. What will be assessed is whether or not the candidate is capable to use the content of this certification outside their own professional context and whether they have knowledge of recent developments. This part of the session lasts 20 minutes.

IV Conclusion

Immediately following the assessment, the assessors come to a pass/fail conclusion, resulting in a recommendation to EXIN. This takes 20 minutes. After that, the assessors will notify the candidate of their recommendation and will explain it. This takes 10 minutes.

Summary of time frames:

- 20 minutes (maximum) for the presentation
- 20 minutes (maximum) for discussing the presentation
- 20 minutes for the assessment interview about the other exam requirements
- 20 minutes evaluation meeting among the assessors
- 10 minutes for discussing the outcome with the candidate

6. Project and evaluation tools

Information security management system (ISMS)

Candidate :
Project :

Subject	Evaluation elements	Comments
1. Description ISMS	• scope • purpose • description	
2. Organization	• objectives of the organization • roles, responsibilities, authorities in ISMS • information sharing community	

3. Set-up ISMS	• elements
	  ○ policy
	  ○ plan
	  ○ organization
	  ○ training & awareness
	  ○ sub-processes (for example: risk assessment, incident handling)
	  ○ measurement
	  ○ evaluation
	  ○ reporting	

4. ISMS process	• plan, do, check, act (PDCA) • registrations • improvements • management review	
5. Communication	• correct language • clear structure	

Information security policy

Candidate :
Project :

Subject	Evaluation elements	Comments
1. Foreword, introduction, background, principles	• motivation, importance, priority • purpose • introduction, operational area • gearing to target group level • top management commitment	
2. Policy statements	• completeness • realistic • strategic level	
3. Subjects	• organization • responsibilities • authorities • incident handling • asset management • information sharing community • information security continuity • awareness, education & training • reporting, maintenance policy • deviations from the policy • information life cycle	
4. Implementation	• planning • implementation	
5. Communication	• correct language • clear structure	

Risk management

Candidate :
Project :

Subject	Evaluation elements	Comments
1. Introduction, background, principles	• purpose • scope • relationship with information security policy • risk strategy • management summary	
2. Process description	• description of the process	

3. Execution	• which threats were identified
	  ○ technical threats (i.e. cybersecurity)
	  ○ legal threats (i.e. privacy & data protection)
	  ○ other threats
	• how were they classified
	• which controls were determined
	• implementation plan (planning, prioritization, responsibilities)
	• monitoring
	• evaluation	

4. Communication	• correct language • clear structure	

Organizational change

Candidate :
Project :

Subject	Evaluation elements	Comments
1. Introduction, background, principles	• purpose • scope • relationship with information security policy • description of the major change/project • relationship with risk assessment • management summary	
2. Preparation and organization	• justification • steering group • key roles (management, expertise, reputation) • vision of the project • which part(s) of the organization • contribution of each team/department	
3. Execution	• communicating the vision • dealing with resistance • coordinating education and training of staff in the implemented controls (knowledge, tools, expertise) • planning the short-term benefits • consolidating the benefits • institutionalizing the new approach • evaluation	
4. Communication	• correct language • clear structure	

Legislation and standards

Candidate :
Project :

Subject	Evaluation elements	Comments
1. Introduction, background, principles	• purpose • scope • relationship with information security policy • top management commitment • information sharing community	
2. Research	• relevant legislation • privacy & data protection • possible standards • gap analysis legal compliance • justification selected standard(s) • gap analysis standard vs organization	
3. Plan	• implementation plan • project group	
4. Execution	• execution of the plan • communication	
5. Evaluation and continuation	• closing the gap • maintenance and improvement plan • management review	
6. Communication	• correct language • clear structure	

Audit and certification

Candidate :
Project :

Subject	Evaluation elements	Comments
1. Foreword, introduction, background, principles	• introduction • scope • purpose • focus • top management support	
2. Basis of the plan	• selected references, standards • internal audit program • training internal auditors • reporting	
3. Execution	• execution details • confidentiality • responsibilities • report details • feed into management review • feed into improvement • evaluation	
4. Communication	• correct language • clear structure	

7. Evaluation

I – Presentation of the project

The candidate...	Comments
explains the subject sufficiently and within the set time frame.	
handles the details of the subject correctly.	
handles the subject at the appropriate level and for the appropriate target group.	
discusses the subject in a convincing manner and can justify their own viewpoints.	
sets out their own viewpoints in a comprehensible manner.	

II - Interview based on the project

The candidate...	Comments
gives correct answers and can justify them.	
justifies viewpoints in a professional manner.	
deals professionally with questions or comments from the assessors.	
shows capacity to reflect upon their own actions in a work context.	
shows capacity to reflect upon their own actions during a presentation and assessment conversation.	

III - Interview other exam requirements

Exam requirements	Exam specifications	Comments
1. Information security management system (ISMS)	1.1 Scope 1.2 Roles 1.3 Review	
2. Information security policy	2.1 Policy design 2.2 Policy implementation	
3. Risk management	3.1 Risk assessment 3.2 Risk treatment	
4. Organizational change	4.1 Plan 4.2 Awareness 4.3 Intervention	
5. Legislation and standards	5.1 Legislation 5.2 Standards	
6. Audit and certification	6.1 Audit program	

IV - Final evaluation EXIN Information Security Management Expert based on ISO/IEC 27001

Part	Weighting	Result	Comments
I. Project and presentation	**30%**		
II. Interview based on the project	**40%**		
III. Assessment other exam requirements	**30%**		
	100%		

Contact EXIN

www.exin.com