

ISO/IEC 27001:2022 Implementer

Certification Syllabus

Last review: October 23, 2026

Contents

- Scheme Description 3
- Required Competencies and Job Description 4
- Competency Assessment 7
- Who Should Take This Exam? 8
- Certification Process 8
- Difficulty Levels: Bloom's Taxonomy 10
- Renewal, Surveillance and Withdrawal of Certification 12

certm:nd

ISO/IEC 27001:2022 Implementer

Our goal at CertMind is to certify the skills of professionals working in the field of Technology. To achieve this, we aim to ensure that professionals demonstrate their skills and knowledge by taking an International Certification Exam.

Certification Category



Main category: ISO/IEC Standards

Category: Information Security Management System

Subcategory: Implementation

Certification Scope

The purpose of the ISO/IEC 27001 Implementer Certification is to demonstrate that the professional understands the terminology, structure and considerations for the definition, implementation, operation, monitoring and improvement of an Information Security Management System (ISMS), in accordance with the ISO/IEC 27001:2022 standard.

Prerequisites



- Be of legal age, according to the minimum age determined by law (as shown on the national identity document that must be uploaded to the platform).
- Have basic reading and writing skills and basic arithmetic: addition, subtraction, multiplication and division.
- Read and accept the Code of Ethics available on the platform before taking the certification exam.

Code of Ethics

All certified professionals must know, accept and abide by the Code of Ethics, which is available for consultation on the platform.

Recommendations

- It is highly recommended that the professional attend formal ISO/IEC 27001:2022 Implementer training of at least 18 hours, divided into approximately 9 two-hour sessions.

Required Competencies and Job Description

To ensure that the professional has the minimum competencies and knowledge that can be applied in a real-world setting, the exam covers the following topics:

1. Introduction and Organizational Context

Skill assessed	Required competencies
Understand the purpose of the standard and determine the context, interested parties and scope of the ISMS.	1. Regulatory framework: purpose, structure and terms 2. External and internal issues 3. Interested parties and their requirements 4. Scope and information security management system

2. Leadership

Skill assessed	Required competencies
Establish the commitment of top management, the information security policy and the assignment of roles.	1. Leadership and commitment 2. Information security policy 3. Roles, responsibilities and authorities

3. Planning

Skill assessed	Required competencies
Assess and treat information security risks, prepare the Statement of Applicability and set security objectives.	1. Risks and opportunities 2. Information security risk assessment 3. Risk treatment and Statement of Applicability 4. Security objectives and planning of changes

4. Support and Operation

Skill assessed	Required competencies
Ensure the resources, competence, communication and documentation of the ISMS, and plan and control its operation.	1. Resources, competence and awareness 2. Communication 3. Documented information 4. Operational planning and control 5. Risk assessment and treatment in operation

5. Performance Evaluation and Improvement

Skill assessed	Required competencies
Evaluate the performance of the ISMS and manage its continual improvement.	1. Monitoring, measurement, analysis and evaluation 2. Internal audit 3. Management review 4. Continual improvement and corrective actions

6. Annex A: Organizational Controls

Skill assessed	Required competencies
Apply the 37 organizational controls of Annex A and justify their inclusion or exclusion in the Statement of Applicability.	1. Governance and organization 2. Assets, information and access 3. Third parties and incidents 4. Compliance and review

7. Annex A: People Controls

Skill assessed	Required competencies
Apply the 8 people controls of Annex A and their relationship to competence and awareness.	1. Onboarding and commitment 2. Awareness and reporting 3. Remote work and departure

8. Annex A: Physical Controls

Skill assessed	Required competencies
Apply the 14 physical controls of Annex A and justify their inclusion or exclusion in the Statement of Applicability.	1. Perimeter and access 2. Workplace protection 3. Equipment and media

9. Annex A: Technological Controls

Skill assessed	Required competencies
Apply the 34 technological controls of Annex A and complete the Statement of Applicability for all 93 controls with their justification.	1. Access and systems 2. Vulnerabilities and data 3. Traceability and networks 4. Development, encryption and changes

Competency Assessment

CertMind uses two types of assessment to ensure that the professional has the required competencies:

1. Single-answer multiple-choice questions: this type of assessment consists of theoretical single-answer multiple-choice questions that measure the degree to which the professional has understood the theoretical concepts of the certification.

2. Case study: its structure is similar to that of the questions described in the previous item; the difference is that, instead of asking about a particular concept, it presents the description of a situation from a real-world context, which the professional must analyze in order to first identify the problem and then evaluate which of the options presented reflects the best solution to that problem situation.

Competency	Questions (1)	Case study (2)
Understand the purpose of the ISO/IEC 27001:2022 standard and determine the context and scope of the ISMS.	X	
Establish the leadership, policy and roles of the ISMS.	X	
Assess and treat information security risks and prepare the Statement of Applicability.	X	X
Determine the resources, documentation and operational control of the ISMS.	X	X
Evaluate the performance of the ISMS and manage its continual improvement.	X	

Competency	Questions (1)	Case study (2)
Apply the organizational and people controls of Annex A.		X
Apply the physical and technological controls of Annex A and complete the Statement of Applicability.		X

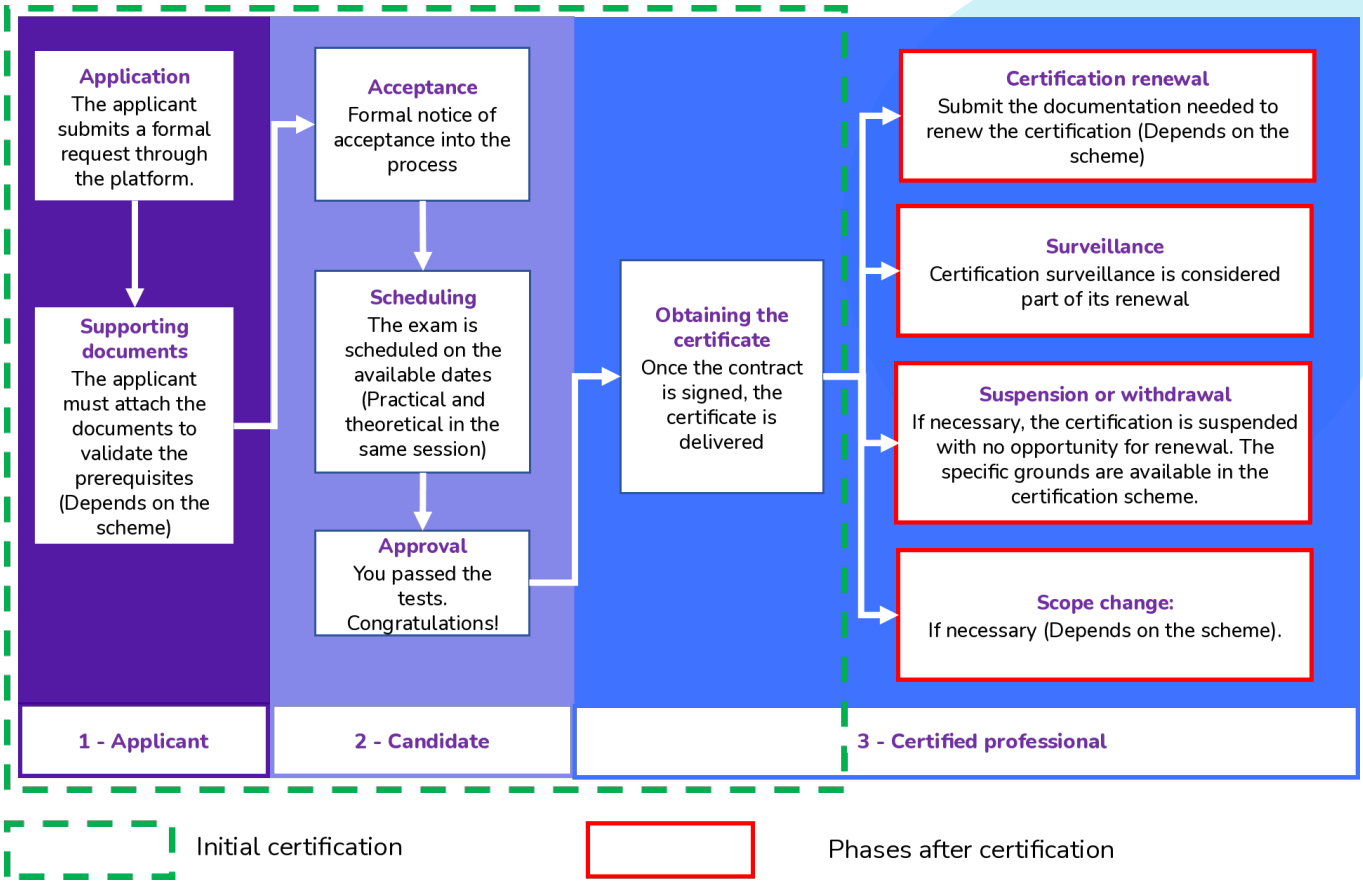
Who Should Take This Exam?

This exam is ideal for responsible individuals or teams who seek to implement an Information Security Management System (ISMS) in accordance with the ISO/IEC 27001 standard, or who are involved in its definition, operation and improvement.

Roles such as: Information security officers, network administrators, support engineers, information systems risk analysts, consultants and ISMS implementers.

Certification Process

The following diagram presents the general life cycle for obtaining a certification:



The following describes each of the phases for obtaining the certification for the first time. The phases after obtaining the certificate (red-bordered boxes) will be explained later.

1. Certification request: the applicant submits their certification request on the QuizLab platform or through the partner company (where the applicant took their training). Once the request is approved, the applicant's profile is created in CertMind.

2. Supporting documents: the applicant must attach their identity document on the CertMind platform and also complete their résumé record.

3. Verification and acceptance: the platform verifies that the applicant meets the prerequisites; once verified, the request is accepted and the applicant becomes a candidate for the certification process.

4. Scheduling: the call for taking the exam is issued, directly on the platform or through the applicant's representative. The exam format is explained below:

- **Type:** Online exam of 40 multiple-choice, single-answer questions.
- **Duration:** 60 minutes.
- **Minimum passing score:** 28/40 or 70%.
- **Additional time:** If the professional does not take the exam in their native language, they will have 15 additional minutes and may also use a dictionary.
- **Supervision:** CertMind monitors the exams to ensure they are carried out correctly and transparently through the Invigilator Program (also known as "Proctor"). To learn more about this surveillance mechanism, visit the website www.certmind.org
- **Open book:** No.
- **Format:** Available online only on the CertMind platform.
- **Validity:** 5 years.
- **Other:** All applicants are required to read and accept the company's code of ethics and the terms and conditions.

Difficulty Levels: Bloom's Taxonomy

Bloom's Taxonomy is a well-known theory in the education sector because many teachers consider it suitable for assessing the cognitive level attained in a subject. The aim of this theory is that, after completing a learning process, the learner acquires new skills and knowledge. The following table describes the Bloom's taxonomy categories present in the certification exam, as well as the percentage of each type of question within the exam.

Module	Level 1	Level 2	Level 3
Description	Knowledge. This may involve recalling a wide range of items, from specific facts to complete theories. All that is required is to bring the appropriate information to mind.	Comprehension. This can be demonstrated by translating material from one form to another (words to numbers), interpreting material (explaining or summarizing), and estimating future trends (predicting consequences or effects).	Application. Refers to the ability to use learned material in new, concrete situations.
Percentage of questions in the exam	50%	30%	20%

Note: For more information about the supervision system, visit our website https://certmind.org

5. Obtaining the certificate: once the exam is passed and the terms and conditions contract is accepted, the certification is issued.

Renewal, Surveillance and Withdrawal of Certification

This phase takes place after the professional has obtained their certification. Renewal refers to the reissuance of the certification once its validity has expired. Surveillance refers to the monitoring that CertMind carries out of the professional's performance during the period between certification and recertification, to ensure compliance with the provisions of this certification scheme. The following describes the activities the certified professional must carry out in order to obtain recertification:

1. Recertification request: before the certification expires, the certified professional submits their recertification request on the QuizLab platform. If the certification expires, the professional must go through the certification process again.

2. Registration of PUCs: the certified professional is required to register 30 PUCs every 5 years to renew the certification.

For more information about the Professional Update Credits (PUC) system, visit our website https://certmind.org. The certified professional must attach the supporting documents that prove the PUCs on the CertMind platform.

3. Documentation validation: the platform verifies compliance with the PUCs of the certified professional; once verified, the recertification request is accepted.

4. Obtaining the recertification: once the documents are validated, the new certification is issued.

Criteria for Suspension or Withdrawal of the Certification

The certification will be withdrawn from the professional in the following cases:

1. Breach of the code of ethics or of the scheme requirements.

2. Unsatisfactory results of the surveillance process.

3. Continued inability to meet the competence requirements of the scheme.

Changes to the Certification Scheme

CertMind continually reviews its certification schemes to incorporate updates to the ISO/IEC 27001:2022 standard (new editions, amendments and corrigenda), relevant regulatory updates, and participant feedback (assessment results, performance metrics and complaints). Changes are notified at least 2 months in advance through the website and by email to certified professionals, and are documented with version, date and impact. When a change requires additional verification (e.g., new controls or requirements of the standard), public transition mechanisms are specified, such as targeted recertification or complementary modules, ensuring fair compliance and continued validity without unduly affecting those already certified.



certm:nd

www.certmind.org

b2b@certmind.org – partner@certmind.org

CertMind is a registered trademark of CertMind - Netherlands