Version 1.0

Last update: October 25, 2021

certm:nd

Syllabus

ISO 27001

Information Security Management System (ISMS) (ISO 27001:2013)

www.certmind.org

2021

Contenido

certm:nd

ISO 27001:2013 –Internal Auditor

Our goal at CertMind is to certify the skills of professionals working in the Technology context. To achieve this, we seek to ensure that professionals demonstrate their skills and knowledge through the application of an International Certification Exam.

Certification category

Main category: ISO Standards

Category: Information Security Management System (ISO 27001:2013)

Subcategory: : Internal Audit

Scope of certification

The purpose of the ISO 27001 - Internal Auditor Certification is to demonstrate that the professional has a practical understanding of the terminology, structure, and considerations for defining, implementing, monitoring and auditing an Information Security Management System (ISMS); following the guidelines of ISO 27001:2013 (information security) and ISO 19011:2018 (auditing).

Prerequisites

• Be of legal age, according to the minimum age determined by law (according to the National Identity Card that must be uploaded to the platform).

• Have basic knowledge of reading, writing and basic arithmetic: addition, subtraction, multiplication and division.

• Reading and acceptance of 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 attends a formal ISO 27001:2013 Internal Auditor training of at least 20 hours, segmented into 5 sessions of approximately 4 hours.

• It is recommended to have a minimum experience of one (1) year in the definition, implementation, monitoring, auditing and/or improvement of an Information Security Management System (ISMS).

Required competencies and job description

In order to ensure that the professional has the minimum competencies and knowledge that can be applied in a real environment, the following topics are addressed in the exam:

Module	Job Description	Required competencies
1. Introduction	Identify and master the basic concepts and context of the organization, its importance and general aspects for the development of an ISMS	1. History, contextualization and structure of ISO standards 2. Structure of the ISO 27000 family 3. Certification scheme and process 4. Basic concepts 5. Purpose and scope of application
2. Context of the organization	Plan and execute monitoring and review activities to identify the context of the organization.	1. Knowledge of the organization and its context. 2. Needs and expectations of interested parties. 3. Scope of the ISMS.
3. Leadership	Understand and determine if leadership exists within the organization to create an environment of commitment to the ISMS and define the information security policy.	1. Leadership and commitment to the definition of the ISMS. 2. Considerations for the definition of the information security policy. 3. Roles, responsibilities and authorities of the organization in the definition of the ISMS.
4. Planning	Define and evaluate the risks associated with the ISMS, and evaluate the information security objectives with their respective plans to achieve them.	1. Risk considerations 2. Risk and opportunity treatment planning 3. Defining information security objectives 4. Planning to achieve information security objectives
5 Support	Identify the necessary resources for the definition and implementation of an Information Security Management System.	1. Resources required 2. Competence 3. Awareness 4. Communication 5. Documented information 6. Recommendations for information control.

Module	Job Description	Required competencies
6. Operation	Perform the evaluation, planning, implementation and control of all processes involved in the achievement of the ISMS objectives.	1. Operational planning and control. 2. Information security risk assessment. 3. Information security risk treatment.
7. Performance evaluation	Identify and evaluate actions that contribute to the continuous improvement of the ISMS.	1. Monitoring, measurement, analysis and evaluation of the ISMS. 2. Internal audit 3. Review by top management
8. Improvement	Identify and evaluate actions that contribute to the continuous improvement of the ISMS.	1. Non-conformities and corrective actions. 2. Continuous improvement of the Information Security Management System.
Appendix A	Identify and understand the control objectives and controls listed in Annex A, and how they are to be used in context with 6.1 (Addressing Risks and Opportunities).	1. A.5 Information Security Policies 2. A.6 Information Security Organization 3. A.7 Human Resources Security 4. A.8 Asset Management 5. A.9 Access Control 6. A.10 Cryptography 7. A.11 Physical and Environmental Security A.12 Operations Security 8. A.12 Operations Security 9. A.13 Communications Security 10. A.14 Systems Acquisition, Development and Maintenance A.15 Supplier Relationships 11. A.15 Supplier Relations 12. A.16 Information Security Incident Management A.17 Information Security Issues 13. A.17 Information Security Aspects of Business Continuity Management A.18 Compliance 14. A.18 Compliance

Module	Job Description	Required competencies
9. Guidelines for the audit (Following the guidelines of the ISO 19011 standard, to carry out the audit of a management system).	• Define, implement, review and improve the audit program. • Prepare and disseminate the audit plan. • Coordinate and conduct the opening meeting. • Prepare reports of findings. • Conduct interviews with process owners and participants. • Classify audit findings. • Prepare the final audit report. • Coordinate and conduct the closing meeting. • Determine and evaluate the competencies required by an auditor.	**Management of an audit program** Clearly understand the considerations and guidelines of the standard for conducting the audit: 1. Principles of auditing 2. Definition of audit program objectives 3. Definition of the audit program 4. Implementation of the audit program 5. Follow-up of the audit program 6. Reviewing and improving the audit program **Realizar la auditoría** It includes the phases for the realization of an internal audit: 1. Initiation of the audit 2. Preparation of the audit activities 3. Conducting the audit activities 4. Preparation and distribution of the audit report 5. Completion of the audit 6. Conducting audit follow-up activities **Competence and evaluation of an auditor** Understand the importance of assessing and maintaining auditor competence: 1. Determine the auditor's competence. 2. Establishing the auditor's evaluation criteria 3. Selecting the auditor evaluation method 4. Conducting the auditor evaluation 5. Maintaining and improving auditor competence.

Evaluation of competencies

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

1. **Multiple choice questions with only one answer**: this evaluation modality consists of theoretical questions of multiple-choice single answer that seek to measure the degree to which the professional has understood the theoretical concepts of the certification.
2. **Case study:** It is structure is similar to that of the questions mentioned in the previous section, the difference being that, instead of asking about a particular concept, it presents a description of a situation that takes place in the real context and that must be analyzed by the professional in such a way that he/she can first identify the problem and then evaluate which of the options presented reflects the best solution to the problem situation.

Competition	Questions (1)	Case study (2)
Master the basic concepts and context of the ISO 27001:2013 standard.	X	
Understand the importance of understanding the context of the organization before launching an ISMS definition initiative.	X	X
To understand the importance of leadership and the involvement of the organization's top management to create an environment of commitment to the definition of the ISMS.	X	
Understand the considerations for carrying out risk management planning and ISMS objectives.	X	
Understand the considerations and aspects that are necessary for the definition, implementation, maintenance and improvement of the ISMS.	X	X

Competition	Questions (1)	Case study (2)
Understand the importance of implementing and monitoring defined plans to achieve information security objectives.	X	X
Understand how to assess information security performance and ISMS effectiveness through internal audit and senior management review.	X	
Understand the organization's responsibility for continuous improvement of information security, based on audit findings, monitoring and review by senior management.	X	
Identify and understand the control objectives and controls listed in Annex A, and how they are to be used in context with 6.1 (Addressing Risks and Opportunities).	X	
Clearly understand the considerations and guidelines of the standard for conducting the audit.	X	X
Understands the phases for the performance of an internal audit	X	X
Understand the importance of assessing and maintaining auditor competence.	X	X
Identify and understand the control objectives and controls listed in Annex A, and how they are to be used in context with 6.1 (Addressing Risks and Opportunities).	X	

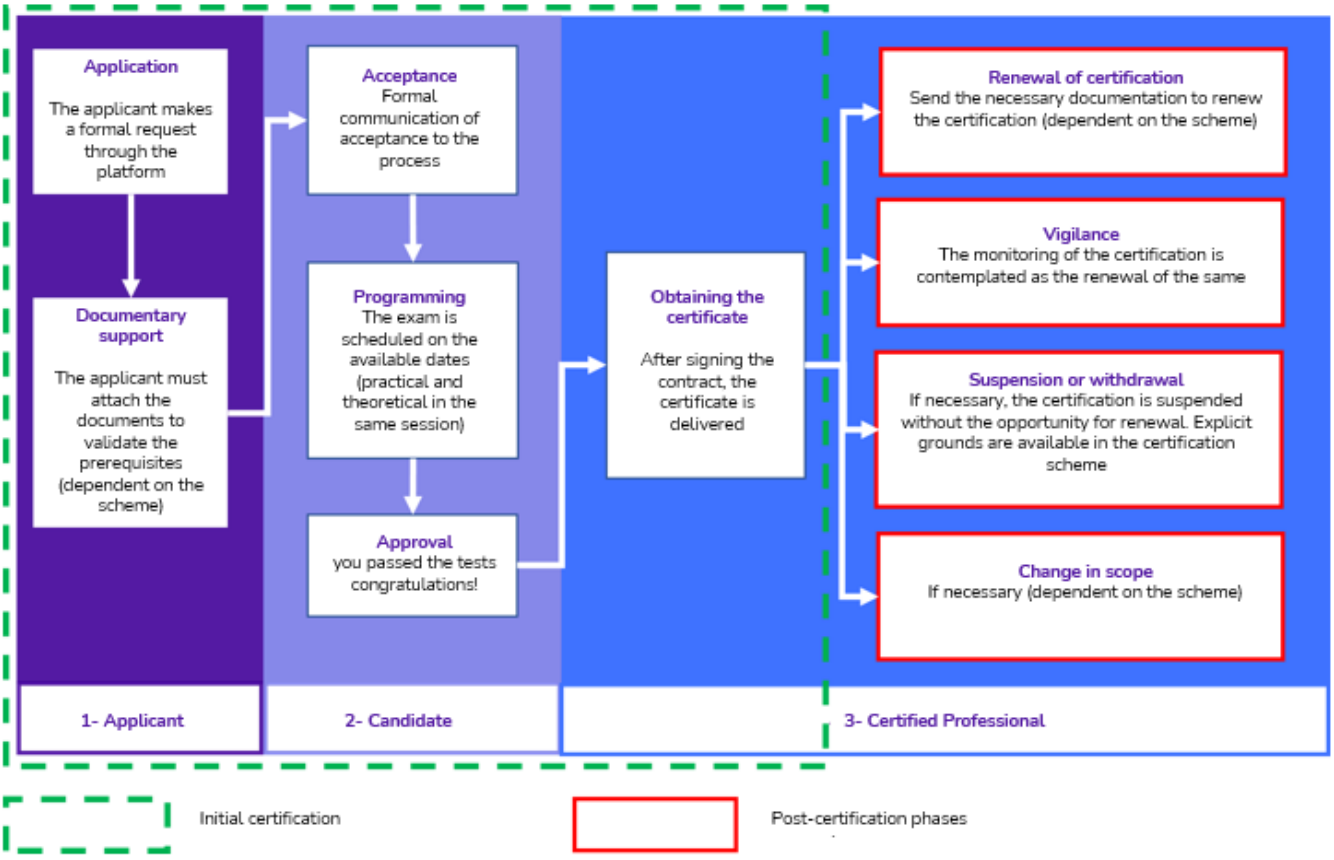
Who should take this exam?

This exam is ideal for individuals or teams interested in internal information security auditing according to ISO 27001, or related to an Information Security Management System (ISMS).

Roles such as: Information security officers, network administrators, support engineers, auditors, information systems risk analysts.

Certification process

The following chart shows the general life cycle for obtaining a certification:



Certification process

Each of the phases for obtaining certification for the first time is described below; the phases after obtaining the certificate (red-bordered boxes) will be explained later.

1. **Request for certification:** the applicant submits his or her certification application, on the QuizLab platform or through the partner company (where the applicant has taken his or her training). Once the application is approved, the applicant's profile is created in CertMind.

2. Documentary support: the applicant must attach in the CertMind platform his or her identity document and additionally complete the registration of his or her resume (CV).

3. Verification and acceptance: the platform verifies the applicant's compliance with the prerequisites, once verified, the application is accepted and the applicant becomes a candidate for the certification process.

4. Programming: the call for the presentation of the exam is made, directly on the platform or through its representative. The format of the exam is explained below:

- **Type:** 40-question, multiple-choice, single-answer online exam.
- **Duration:** 60 minutes.
- **Minimum passing grade:** 28/40 or 70%.
- **Additional time:** If the professional does not take the exam in his/her native language, he/she will have an additional 15 minutes and is also allowed to use a dictionary.
- **Supervision:** CertMind monitors the tests to ensure that they are performed correctly and transparently through the Invigilator Program (also known as "Proctor"). To learn more about this surveillance mechanism, please visit the following website www.certmind.org
- **Open book:** No.
- **Modality:** Available online only on the CertMind platform.
- **Validity :** 5 Years.
- **Others:** All applicants are required to read and accept the company's code of ethics and terms and conditions.

Levels of Difficulty: Bloom's Taxonomy

Bloom's Taxonomy is a theory known in the educational sector because many teachers consider it suitable for evaluating the cognitive level acquired in a subject. The objective of this theory is that after a learning process, the learner acquires new skills and knowledge. The following table presents a description of the categories of Bloom's taxonomy present in the certification exam, as well as a description of in the certification exam, as well as the percentage of each type of question in the exam.

Module	Level 1	Level 2	Level 3
Description	**Knowledge. It can comprise remembering a wide range of elements, from specific data to complete theory. But all that is needed is to bring to mind the appropriate information.**	**Compression. This can be demonstrated by passing, or translating, material from one form to another (words to numbers), interpreting the material (explaining or summarizing), and estimating future trends (predicting consequences or effects).**	**Application. Refers to the ability or capacity to use the material learned in concrete, new situations.**
Percentage of questions present in the exam	50%	30%	20%

Note: For more information on the monitoring system visit our web site https://certmind.org.

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

Renewal, surveillance and withdrawal of certification

This phase occurs after the professional has obtained his or her certification. Renewal refers to the reissuance of the certification once its validity has come to an end. Surveillance refers to CertMind's supervision of the professional's performance during the period between certification and recertification to ensure compliance with the stipulations of this certification scheme. The activities that the certified professional must perform in order to obtain recertification are described below:

1. Application for recertification: before the certification becomes invalid, the certified professional submits his or her recertification application on the QuizLab platform. In case the certification loses its validity, the professional must go through the certification process again.

2. Registration of PUC's: the certified professional is required to register 30 PUC's every 5 years for certification renewal.

For more information about the Professional Update Credits (PUC) system visit our website https://certmind.org. The certified professional must attach the supports that accredit the PUC's in the CertMind platform.

3. Validation of documentation: the platform verifies compliance with the PUC's of the certified professional, once verified, the recertification application is accepted.

4. Obtaining recertification: Once the documents have been validated, the new certification is delivered.

Criteria for suspension or withdrawal of certification

Certification will be withdrawn from the professional in the following cases:

1. Failure to comply with the code of ethics.
2. Failure to comply with the requirements of the scheme.
3. Unsatisfactory results of the surveillance process.
4. Inability to continuously meet the competency requirements of the scheme.

Changes to the certification scheme

The ISO 27001 - Internal Auditor certification scheme does not contemplate changes in the scope as currently no extensions or reductions in the scope or level of the certification are applied.

certm:nd

www.certmind.org

b2b@certmind.org – partner@certmind.org