

EXIN Information Security Management Expert (ISO/IEC 27001)

Introduction

EXIN Information Security Management Expert tests the candidate's knowledge, understanding, and skills around the Information Security Management System (ISMS). This includes structuring, maintaining, and optimizing the security of information within an organization. The certification is based on the international standard ISO/IEC 27001. The exam consists of a project paper, a presentation, and an interview.

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.

Course Outline

MODULE 1: Organization of Information Security

- 1.1 The candidate can substantiate the risk management process in relationship with the ISMS.
 - 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.
 - 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.
 - 1.3.1 Review the ISMS for suitability and effectiveness.
 - 1.3.2 Define opportunities for improvement.

MODULE 2: Information Security Policy

- 2.1 The candidate can participate in the process of establishing the information security policy.
 - 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.
 - 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.

MODULE 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.
 - 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.
 - 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.

MODULE 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.
 - 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 & implement it.
 - 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 the 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
 - 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.

MODULE 5: Standards and Norms

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

MODULE 6: Audit and Certification

- 6.1 The candidate can organize the execution of audits.
 - 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.
 - 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.

Prerequisites

- 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 the exam Information Security Management Expert.
- 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).

Target Audience

IT professionals are 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.

Duration

20 Hours Training Course