EXIN Information Security Foundation (ISO/IEC 27001)

Introduction

EXIN Information Security Foundation is a relevant certification for all professionals who work with confidential information. It tests the understanding of concepts and value of information security as well as the threats and risks.

Scope

EXIN Information Security Foundation based on ISO/IEC 27001 is a certification that validates a professional's knowledge about:

- Information and security: the concept, the value, the importance, and the reliability of the information.
- Threats and risks: the concepts of threat and risk and the relationship with the reliability of the information.
- Approach and organization: the security policy and security organization including the components of the security organization and management of (security) incidents.
- Measures: the importance of security measures including physical, technical, and organizational measures.
- Legislation and regulations: the importance and impact of legislation and regulations.

Course Outline

MODULE 1: Information and Security

1.1 The Concept of Information
- 1.1.1 Explain the difference between data and information.
- 1.1.2 Explain what information management is.

1.2 Value of Information
- 1.2.1 Describe the value of data and information for organizations.
- 1.2.2 Describe how the value of data and information can influence organizations.
- 1.2.3 Explain how applied information security concepts protect the value of data and information.

1.3 Reliability Aspects
- 1.3.1 Name the reliability aspects of information.
- 1.3.2 Describe the reliability aspects of information.

MODULE 2: Threats and Risks

2.1 Threats and Risks
- 2.1.1 Explain the concepts of threat, risk, and risk analysis.
- 2.1.2 Explain the relationship between a threat and a risk.
- 2.1.3 Explain various types of threats.
- 2.1.4 Describe various types of damage.
- 2.1.5 Describe various risk strategies.

MODULE 3: Approach and Organization

3.1 Security Policy and Security Organization
- 3.1.1 Outline the objectives and the content of a security policy.
- 3.1.2 Outline the objectives and the content of a security organization.

3.2 Components
- 3.2.1 Explain the importance of a code of conduct.
- 3.2.2 Explain the importance of ownership.
- 3.2.3 Name the most important roles in the security organization.

3.3 Incident Management
- 3.3.1 Summarize how security incidents are reported and what information is required.
- 3.3.2 Give examples of security incidents.
- 3.3.3 Explain the consequences of not reporting security incidents.
- 3.3.4 Explain what an escalation entails (functionally and hierarchically).
- 3.3.5 Describe the effects of escalation within the organization.
- 3.3.6 Explain the incident cycle.

MODULE 4: Measures

4.1 Importance of Measures
- 4.1.1 Describe various ways in which security measures may be structured or arranged.
- 4.1.2 Give examples for each type of security measure.
- 4.1.3 Explain the relationship between risks and security measures.
- 4.1.4 Explain the objective of the classification of information.
- 4.1.5 Describe the effect of classification.

4.2 Physical Measures
- 4.2.1 Give examples of physical security measures.
- 4.2.2 Describe the risks involved with insufficient physical security measures.

4.3 Technical Measures
- 4.3.1 Give examples of technical security measures.
- 4.3.2 Describe the risks involved with insufficient technical security measures.
- 4.3.3 Understand the concepts of cryptography, digital signature, and certificate.
- 4.3.4 Name various types of malware, phishing, and spam.
- 4.3.5 Describe the measures that can be used against malware, phishing, and spam.

4.4 Organizational Measures
- 4.4.1 Give examples of organizational security measures.
- 4.4.2 Describe the dangers & risks involved with insufficient organizational security measures.
- 4.4.3 Describe access security measures such as the segregation of duties & use of passwords.
- 4.4.4 Describe the principles of access management.
- 4.4.5 Describe the concepts of identification, authentication, and authorization.
- 4.4.6 Explain the importance to an organization of a good set-up business
- 4.4.7 Make clear the importance of conducting exercises.

MODULE 5: Legislation and Regulations

5.1 Legislation and Regulations
- 5.1.1 Explain why legislation and regulations are important for the reliability of the information.
- 5.1.2 Give examples of legislation related to information security.
- 5.1.3 Give examples of regulations related to information security.
- 5.1.4 Indicate possible measures that may be taken to fulfill the requirements of legislation & regulations.

Prerequisites

Successful completion of the EXIN Information Security Foundation based on the ISO/IEC27001 exam.

Target Audience

The EXIN Information Security Foundation based on ISO/IEC 27001 certification is intended for everyone in the organization who is processing information. The module is also suitable for entrepreneurs of small independent businesses for whom some basic knowledge of information security is necessary. This module is a good start for new information security professionals.

Duration

14 Hours Training Course