

# EXIN Information Security Management Professional (ISO/IEC 27001)

## Introduction

Information is crucial for the continuity and proper functioning of both individual organizations and the economies they fuel; this information must be protected against access by unauthorized people, protected against accidental or malicious modification or destruction, and must be available when it is needed. The module Information Security Management Professional based on ISO/IEC 27001 tests understanding of the organizational, physical, and technical aspects of information security.

## Scope

The module Information Security Management Professional based on ISO/IEC 27001 (ISMP.EN) tests understanding of the organizational and managerial aspects of information security.

The subjects of this module are:

- Information security perspectives: business, customer, service provider/supplier
- Risk Management: analysis, controls, remaining risks
- Information security controls: organizational, technical, physical.

## Course Outline

### MODULE 1: Information Security Perspective

- 1.1 The candidate understands the business interest of information security.
  - 1.1.1 Distinguish types of information based on their business value.
  - 1.1.2 Explain the characteristics of a management system for information security.
- 1.2 The candidate understands the customer perspective on governance.
  - 1.2.1 Explain the importance of information governance when outsourcing.
  - 1.2.2 Recommend a supplier based on security controls.
- 1.3 The candidate understands the supplier's responsibilities in security assurance.
  - 1.3.1 Distinguish security aspects in service management processes.
  - 1.3.2 Support compliance activities.

### MODULE 2: Risk Management

- 2.1 The candidate understands the principles of risk management.
  - 2.1.1 Explain the principles of analyzing risks.
  - 2.1.2 Identify risks for classified assets.
  - 2.1.3 Calculate risks for classified assets.
- 2.2 The candidate knows how to control risks.
  - 2.2.1 Categorize controls based on Confidentiality, Integrity, and Availability (CIA).
  - 2.2.2 Choose controls based on incident cycle stages.
  - 2.2.3 Choose relevant guidelines for applying controls.

- 2.3 The candidate knows how to deal with the remaining risks.
  - 2.3.1 Distinguish risk strategies.
  - 2.3.2 Produce business cases for controls.
  - 2.3.3 Produce reports on risk analyses.

### **MODULE 3: Information Security Controls**

- 3.1 The candidate has knowledge of organizational controls.
  - 3.1.1 Write policies and procedures for information security.
  - 3.1.2 Implement information security incident handling.
  - 3.1.3 Perform an awareness campaign in the organization.
  - 3.1.4 Implement roles and responsibilities for information security.
- 3.2 The candidate has knowledge of technical controls.
  - 3.2.1 Explain the purpose of security architectures.
  - 3.2.2 Explain the purpose of security services.
  - 3.2.3 Explain the importance of security elements in the IT infrastructure.
- 3.3 The candidate has knowledge of physical, employment-related, and continuity controls.
  - 3.3.1 Recommend controls for physical access.
  - 3.3.2 Recommend security controls for the employment life cycle.
  - 3.3.3 Support the development and testing of a business continuity plan.

### **Prerequisites**

- Successful completion of the EXIN Information Security Management Professional based on ISO/IEC 27001 exam.
- Accredited EXIN Information Security Management Professional based on ISO/IEC 27001 training, including completion of the Practical Assignments.
- Basic knowledge of Information Security is recommended, for instance through the EXIN Information Security Foundation based on ISO/IEC 27001 certification.

### **Target Audience**

Security professionals. This module is intended for everyone who is involved in the implementation, evaluation, and reporting of an information security program, such as an Information Security Manager (ISM), Information Security Officer (ISO), or a Line Manager, Process Manager, or Project Manager with security responsibilities.

### **Duration**

20 Hours Training Course