



# ISO 27001 FOUNDATION

## I27001F



I127001F Version 112022

**CertiProf**<sup>®</sup>

## ISO 27001 Foundation

### Syllabus V112022

Introduction	3
Objectives	3
Exam format and duration	3
Eligibility for certification	3
Content	4



## Introduction

The ISO 27001:2022 Foundation—I27001F certification aims to describe the requirements for establishing, implementing, maintaining, and continually improving an information security, cybersecurity, and privacy protection system in an organization's context. ISO 27001 is an international standard published by the International Organization for Standardization (ISO).

Information security and privacy protection are nowadays invaluable assets, as their loss for various reasons can have a great impact on organizations and negatively affect their reputation. ISO 27001:2022 can be implemented in any type of organization, whether for-profit or not-for-profit, private or state-owned, small or large.

The training will consist of presentations on topics using slides and examples from the facilitator's experience. The trainees are expected to learn the fundamental practices for implementing and managing an ISMS during the training. It is highly recommended that they work with the official translation of each country's standard.

## Objectives

- Understand and analyze the fundamentals of ISO 27001:2022.
- Become familiar with the principles, concepts, and requirements of ISO/IEC 27001:2022.
- Understand how to develop an ISMS.
- Review and understand Annex A of ISO 27001.

## Exam format and duration

This syllabus has an exam in which the candidate must achieve a score to obtain certification in ISO/IEC 27001:2022.

- Type: Multiple choice
- Questions: 40
- Passing score: 32/40 or 80%
- Duration: 60 minutes
- Open book: No
- Delivery: This exam is available online
- Supervised: At the discretion of the Partner

## Eligibility for certification

Anyone interested in expanding their knowledge of the ISO/IEC 27001 standard.

## Agenda

### 1. Introduction and background

Introduction

History of the Standard

ISO/IEC 27001:2022 - Structure ISO 27000 - Family of Standards

### 2. Key Concepts

Information and General Principles Information Security

The Management System

Critical Success Factors of an ISMS

Benefits of the ISMS Family of Standards

### 3. Terms and Definitions (See supplement N°1 Glossary 27001)

Structure of ISO/IEC 27001 Deming Cycle PDCA and ISMS

### 4. Organizational Context

Understanding the Organization and its Context

Workshop: Determine the context of the organization using a SWOT analysis matrix

Understanding Stakeholder Needs and Expectations

Determining the Scope of the Information Security Management System

Information Security Management System

Workshop: Defining the Scope of the ISMS

### 5. Leadership

Leadership and commitment

Policy

Roles, Responsibilities, and Authorities in the Organization

### 6. Planning

Actions to Address Risks and Opportunities

Structure of the ISO 31000 Risk Management Standard - Guidelines Workshop: Defining the

Statement of Applicability for 5 Controls of Annex A  
Information Security Objectives and Planning for their Achievement Workshop: Defining Information Security Objectives

## **7. Support**

Resources Competence Awareness Communication  
Documented Information

## **8. Operation**

Operational Planning and Control  
Information Security Risk Assessment  
Information Security Risk Management  
Risk Assessment and Management

## **9. Performance Evaluation**

Monitoring, Measurement, Analysis, and Evaluation  
Internal Audit  
Audit  
Management Review

## **10. Improvement**

Non-conformity and corrective actions Continuous improvement  
Annex 1: Terms and Definitions  
Workshop: Review of Information Security Terms and Definitions  
Analysis and study of a list of 90 key terms related to the ISO 27000 series and information security, defined in the context of information security management systems.

## **Conclusions**