



ISO 27001 LEAD IMPLEMENTER CERTIFIED



I27001CLI Version 042021

CertiProf[®]

ISO 27001 Certified Lead Implementer I27001CLI

Syllabus V042021

Introduction	3
Learning Objectives	3
Certification Exam	3
Target Audience	3
Content	4



Introduction

This certification helps to understand and implement a global management system, based on an approach of business risks, to establish, implement, operate, monitor, review, maintain and improve information security.

It includes organizational structure, policies, plans, responsibilities, procedures, processes, and resources.

Learning Objectives

- Provide explanation and guidance on ISO / IEC 27001 based on ISO / IEC 27003: 2017 for the implementation of an Information Security Management System (ISMS)
- Ability to define business cases
- Ability to define and perform GAP analysis
- Understanding of the organization, its context, the needs and expectations of stakeholders
- Acquire knowledge about organizational hierarchies and policies
- Ability to plan and take actions to address risks and opportunities
- Planning and operational control
- Track, measure, analyze and evaluate performance

Certification Exam

- Format: Multiple choice
- Questions: 40
- Pass Score: 32/40 or 80 %
- Language: Spanish
- Duration: 60 minutes
- Open book: No
- Delivery: This examination is available online.
- Supervised: It will be at the discretion of the Partner

Target Audience

- People interested in expanding their knowledge in ISO / IEC 27001 based on ISO / IEC 27003: 2017 for the implementation of an Information Security Management System (ISMS)

Content

1. Introduction

- Introduction
- Information Security
- Information Security Management System
- ISO/IEC 27003:2017 Information Technology. Security Techniques
- ISO 27001: Administrative
- ISO 27001: Technical Controls
- Navigation Path

2. Business Case

- Business Case
- Parts of a Business Case

3. Diagnostic

- Diagnostic
- GAP Analysis Objectives
- How to Perform a GAP Analysis
- Maturity Model
- COBIT Maturity Model
- How to Perform a GAP Analysis

4. Context of the Organization

- Organizational Context
- Understanding the Organization and its Context
- External Issues
- Internal Issues
- Internal & External Issues
- Understanding Stakeholder Needs and Expectations
- Internal Stakeholders
- External Stakeholders
- ISMS Scope

5. Leadership

- Leadership
- Leadership & Commitment
- Policies
- Content of a Policy
- Information Security Policy
- I.S. Roles, Responsibilities and Authorities

6. Planning

- Planning
- Actions to Address Risks and Opportunities
- Risk Identification
- Risk Analysis
- Risk Assessment
- Risk Management

Declaration of Applicability
Information Security Objectives
Expression of Security Objectives

7. Support

Support
Resources
Competence
Awareness Raising
Communication
Documented Information

8. Operation

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

9. Performance Evaluation

Performance Evaluation
Monitoring, Measurement, Analysis and Evaluation
Internal Auditing
Management Review

10. Improvement

Improvement
Nonconformity and Corrective Action
Continuous Improvement

Structure: Business Case

Structure: Business Case

Methodology: ISMS Scope and Boundary

Define
ISMS Scope Definition Steps
Ellipse Method
Functional Structure Diagram
Physical Plant Diagram
Logical Plant Diagram

Methodology: Assets Management

Identification
Classification and Valuation
Analyze Information Assets

Methodology: Risk Management

Methodology: ISMS Policy

ISMS Policy Creation Steps
Internal Requirements
External Requirements
Requirements Relation

Revision & Delivery
Policy Writing
Matching Workshops

