

PECB CERTIFIED ISO/IEC 27002

LEAD MANAGER

Duration: 5 days; Instructor-led | Virtual Instructor-led

WHAT WILL YOU LEARN

The ISO/IEC 27002 Lead Manager training course enables participants to develop the necessary knowledge and skills for supporting an organization in effectively determining, implementing, and managing information security controls. The training course provides information that will help participants interpret the ISO/IEC 27002 controls in the specific context of an organization.

The PECB ISO/IEC 27002 Lead Manager Certification demonstrates that you have acquired the necessary expertise for determining adequate information security controls needed to treat the risks identified by a risk assessment process. The training course is followed by an exam. If you pass, you can apply for the “PECB Certified ISO/IEC 27002 Lead Manager” credential.

COURSE OBJECTIVES

Upon successfully completing the training course, participants will be able to:

- Explain the fundamental concepts of information security, cybersecurity, and privacy based on ISO/IEC 27002
- Acknowledge the relationship between ISO/IEC 27001, ISO/IEC 27002, and other standards and regulatory frameworks
- Interpret the ISO/IEC 27002 information security controls in the specific context of an organization
- Support an organization in effectively determining, implementing, and managing information security controls based on ISO/IEC 27002
- Explain the approaches and techniques used for the implementation and effective management of information security controls

AUDIENCE

This training course is intended for:

- Managers or consultants seeking to enhance their knowledge regarding the implementation of information security controls in an ISMS based on ISO/IEC 27001
- Individuals responsible for maintaining information security, compliance, risk, or governance in an organization

- IT professionals or consultants seeking to enhance their knowledge in information security
- Members of an ISMS implementation or information security team

METHODOLOGY

This program will be conducted with interactive lectures, PowerPoint presentations, discussions, and practical exercises.

COURSE CONTENTS

Module 1: Introduction to ISO/IEC 27002

- Training course objectives and structure
- Standards and regulatory frameworks
- Fundamental concepts of information security, cybersecurity, and privacy
- Information security management system (ISMS) and ISO/IEC 27002
- Analysing the organization’s existing security architecture
- Understanding information security risks

Module 2: Roles and responsibilities, assets, policies, and people control

- Selection and design of controls
- Information security policies, procedures, and roles and responsibilities
- Information assets and access controls
- People control

Module 3: Physical controls and protection of information systems and networks

- Physical controls
- Operational security controls
- Protection of information systems and network controls

Module 4: Information security incident management and testing and monitoring of information security controls based on ISO/IEC 27002

- Supplier relationships and ICT supply chain
- Information security incident management
- Information security testing

- Monitoring information security controls
- Continual improvement
- Closing of the training course

Certification Exam