



Lead Cybersecurity Manager

Description

Organizations are facing increasingly complex and sophisticated cyberattacks. In light of this reality, the demand for skilled cybersecurity management professionals is more urgent than ever. Our **Lead Cybersecurity Manager PECB training** has been specifically designed to meet this critical need. By participating, you will gain the essential skills to implement, manage, and continuously improve an effective cybersecurity program, relying on international standards and best practices in the field.

This **cybersecurity training** goes beyond providing theoretical knowledge; it practically prepares participants to enhance the resilience and preparedness of their organization against cyber threats, making them key players in the evolving landscape of cybersecurity.

Course Content

Module 1: Introduction to Cybersecurity and Program Implementation

- Training course objectives and structure
- Standards and regulatory frameworks
- Fundamental concepts of cybersecurity
- Cybersecurity program
- The organization and its context
- Cybersecurity governance

Module 2: Roles, Responsibilities, and Risk Management

- Cybersecurity roles and responsibilities
- Asset management
- Risk management
- Attack mechanisms

Module 3: Cybersecurity Controls, Communication, and Training

- Cybersecurity controls
- Cybersecurity communication
- Awareness and training

Module 4: Incident Management, Monitoring, and Improvement

- ICT readiness in business continuity
- Cybersecurity incident management
- Testing in cybersecurity
- Measuring and reporting cybersecurity performance and metrics
- Continual improvement
- Closing of the training course

Module 5: Certification Exam Documentation

- Digital course material included

Exam

The "PECB Certified Lead Cybersecurity Manager" exam covers the following competency areas:

- Fundamental concepts of cybersecurity
- Initiation of the cybersecurity program and cybersecurity governance
- Defining roles and responsibilities in cybersecurity and risk management
- Selection of cybersecurity controls
- Establishment of cybersecurity communication and training programs
- Integration of the cybersecurity program into business continuity management and incident management
- Measuring performance and continuous improvement of the cybersecurity program

An exam voucher and a retake are included in the training price

- If you fail the exam on your first attempt, you have the opportunity to retake it once for free
- There is no need for a new exam voucher to retake the exam. The same voucher used for the first exam attempt is valid for the second attempt

Participant profiles

- Cybersecurity Managers
- IT Security Strategists
- IT and Security Specialists
- Compliance and Risk Managers
- Cybersecurity Decision-making Executives

Prerequisites

- Have basic knowledge and understanding of cybersecurity and its management

Objectives

- Understand the fundamental concepts of cybersecurity.
- Link ISO/IEC 27032 and the NIST cybersecurity framework to relevant standards.
- Master the operation of a cybersecurity program.
- Support the continuous improvement of the cybersecurity program.
- Apply effective methodologies for managing cybersecurity.

Description

Training Lead Cybersecurity Manager

Niveau

Fondamental

Classroom Registration Price (CHF)

4900

Virtual Classroom Registration Price (CHF)

4650

Duration (in Days)

5

Reference

CYF-02