# PECB

BEYOND RECOGNITION



## PECB Certified Lead Cybersecurity Manager

**Master the ability to implement and manage a cybersecurity program based on industry best practices.**

## Why should you attend?

Organizations nowadays are affected by the ever-evolving digital landscape and constantly face new threats and complex and sophisticated cyberattacks. There is a pressing need for skilled individuals capable of effectively managing and implementing robust cybersecurity programs to counter these threats. Our Lead Cybersecurity Manager training course has been developed to address this need.

By attending the PECB Certified Lead Cybersecurity Manager, participants will learn the fundamental cybersecurity concepts, strategies, methodologies, and techniques utilized to effectively establish and manage a cybersecurity program based on the guidance of international standards and industry best practices for cybersecurity.

Additionally, this training course empowers participants to enhance their organization's readiness and resilience against cyber threats. Participants will be well-prepared to support their organization's ongoing cybersecurity efforts and make valuable contributions in today's ever-evolving cybersecurity landscape.

## Who should attend?

This training course is intended for:

➤ Managers and leaders involved in cybersecurity management
➤ Individuals tasked with the practical implementation of cybersecurity strategies and measures
➤ IT and security professionals seeking to advance their careers and contribute more effectively to cybersecurity efforts
➤ Professionals responsible for managing cybersecurity risk and compliance within organizations
➤ C-suite executives playing a crucial role in decision-making processes related to cybersecurity

## Course agenda                                          Duration: 5 days

**Day 1** | **Introduction to cybersecurity and initiation of a cybersecurity program implementation**

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

**Day 2** | **Cybersecurity roles and responsibilities, risk management, and attack mechanisms**

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

**Day 3** | **Cybersecurity controls, communication, and awareness and training**

➤ Cybersecurity controls
➤ Cybersecurity communication
➤ Awareness and training

**Day 4** | **Cybersecurity incident management, monitoring, and continual 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

**Day 5** | **Certification Exam**
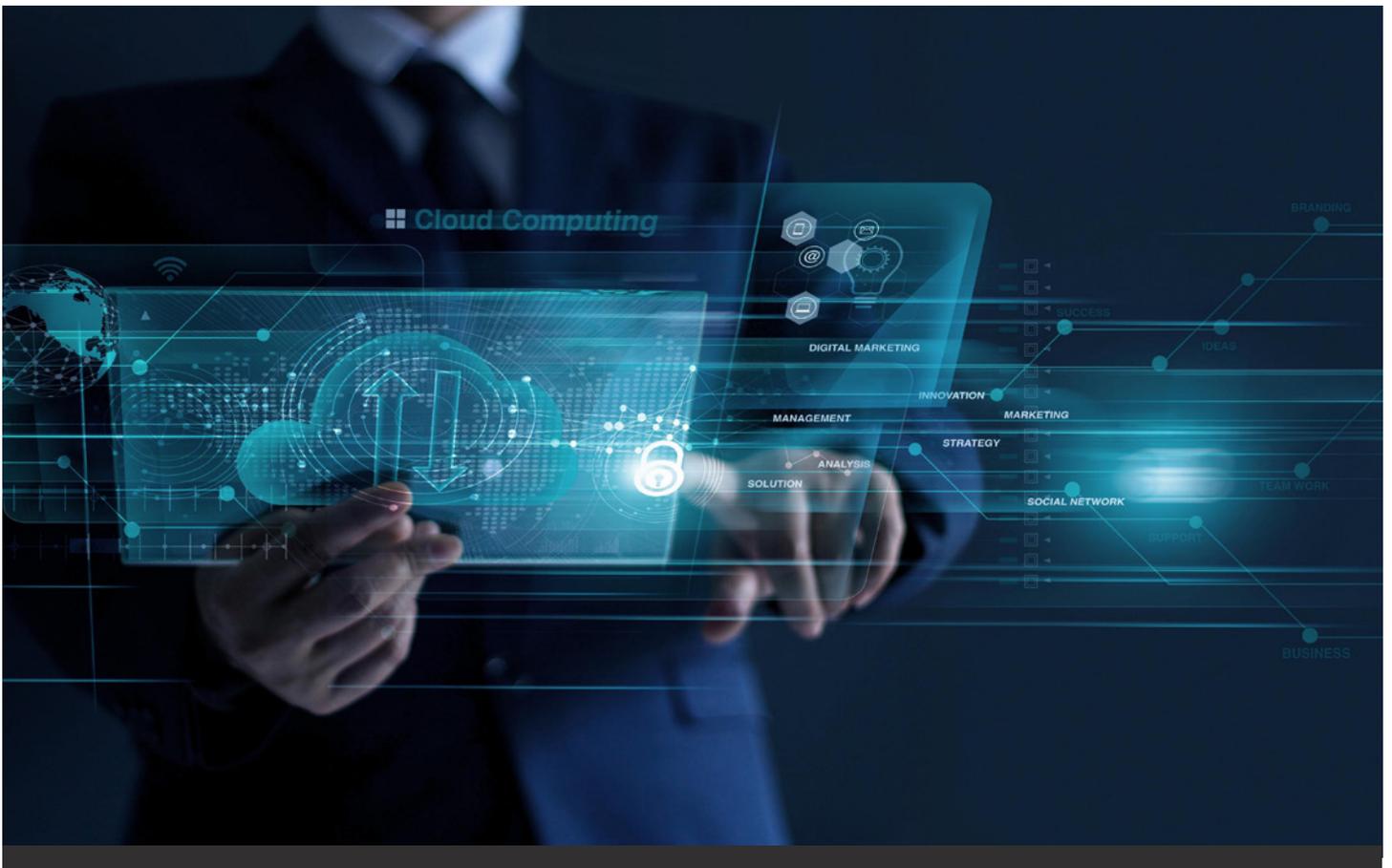
# Learning objectives

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

➤ Explain the fundamental concepts, strategies, methodologies, and techniques employed to implement and manage a cybersecurity program

➤ Explain the relationship between ISO/IEC 27032, NIST Cybersecurity Framework, and other relevant standards and frameworks

➤ Comprehend the operation of a cybersecurity program and its components

➤ Support an organization in operating, maintaining, and continually improving their cybersecurity program

# Examination

**Duration: 3 hours**

The "PECB Certified Lead Cybersecurity Manager" exam fully meets all the requirements of the PECB Examination and Certification Program (ECP). It covers the following competency domains:

**Domain 1** | Fundamental concepts of cybersecurity

**Domain 2** | Initiating the cybersecurity program and cybersecurity governance

**Domain 3** | Defining cybersecurity roles and responsibilities and managing risks

**Domain 4** | Selecting cybersecurity controls

**Domain 5** | Establishing cybersecurity communication and training programs

**Domain 6** | Integrating the cybersecurity program in business continuity management and incident management

**Domain 7** | Measuring the performance of and continually improving the cybersecurity program

For specific information about exam type, languages available, and other details, please visit the List of PECB Exams and the Examination Rules and Policies.

# Certification

After passing the exam, you can apply for one of the credentials shown on the table below. You will receive a certificate once you fulfill all the requirements of the selected credential.

| Professional Credential | Education | Exam | Professional experience | Experience in cybersecurity programs | Other requirements |
|---|---|---|---|---|---|
| **PECB Certified Provisional Cybersecurity Manager** | At least secondary education | PECB Certified Lead Manager Exam | None | None | Signing the PECB Code of Ethics |
| **PECB Certified Cybersecurity Manager** | | | 2 years (1 in cybersecurity) | 200 hours | |
| **PECB Certified Lead Cybersecurity Manager** | | | 5 years (2 in cybersecurity) | 300 hours | |
| **PECB Certified Senior Lead Cybersecurity Manager** | | | 10 years (7 in cybersecurity) | 1.000 hours | |

For more information about cybersecurity certifications and the PECB Certification process, please refer to Certification Rules and Policies.

# General information

➤ Certification and examination fees are included in the price of the training course.

➤ Participants will receive comprehensive training materials, compromising more than 400 pages of content, including practical examples, exercises, and quizzes.

➤ An attestation of course completion worth 31 CPD (Continuing Professional Development) credits will be issued to participants who have attended the training course.

➤ Candidates who complete the training but do not pass the exam can retake the exam at no additional cost within a 12-month period from the initial exam date.

For more information, please contact us at marketing@pecb.com or visit www.pecb.com.