SMCE
Service Management
Center of Excellence

PECB

PECB Certified ISO/IEC 27032
Lead Cybersecurity Manager

Master the implementation and management of a Cybersecurity Program based on ISO/IEC 27032

Why should you take this training course?

In the era of digital transformation, with almost everything being done digitally from education, to business, to communication, cybersecurity has never been more important! One should not forget that as technology advances, so do malicious threats and attacks. As a result, there is an ever growing need for cybersecurity professionals, competent to protect people's data.

ISO/IEC 27032 Lead Cybersecurity Manager training course enables you to acquire the expertise and competence needed to support an organization in implementing and managing a cybersecurity program based on ISO/IEC 27032 and NIST Cybersecurity Framework. During this training course, you will gain a comprehensive knowledge of cybersecurity, the relationship between cybersecurity and other types of IT security, and the different stakeholders' role in cybersecurity.

Why is this course more desirable than the others?

This course is an amalgamation of ISO/IEC 27032 and the NIST Cybersecurity Framework. The course not only elaborates the theoretical information provided in the aforementioned documents, but gives you practical advice based on real-life experience.

The development of this course is the result of strenuous work by PECB's network of experts and course developers.

After mastering all the necessary concepts of cybersecurity, you can sit for the exam and apply for a "PECB Certified ISO/IEC 27032 Lead Cybersecurity Manager" credential. By holding this credential, you will be able to demonstrate that you have the practical knowledge and professional capabilities to support and lead a team in managing cybersecurity. By obtaining your certification, you showcase a certain skill level which will display added value not only to your professional career but to your organization as well. This can help you stand out from the crowd and increase your earning potential.

What will the certification allow you to do?

Certification is the formal recognition and proof of knowledge which carries an important weight when you are entering the labor market, or when you want to advance in your career. Due to the technological advancements and the complexity of cyberattacks, the demand for information security professionals continues to grow.

PECB issues certifications that have international recognition, thus leading to more employment opportunities for you or making you even more competitive in an already fast-developing job market.

Who should attend this training course?

- Cybersecurity professionals
- Information Security experts
- Professionals seeking to manage a cybersecurity program
- Individuals responsible to develop a cybersecurity program
- IT specialists
- Information Technology expert advisors
- IT professionals looking to enhance their technical skills and knowledge

Course agenda

Duration: 5 days

Day 1 | Introduction to Cybersecurity and related concepts as recommended by ISO/IEC 27032

- Course objectives and structure
- Standards and regulatory frameworks
- Fundamental concepts in cybersecurity
- Cybersecurity program
- Initiating a cybersecurity program
- Analyzing the organization
- Leadership

Day 2 | Cybersecurity policies, risk management and attack mechanisms

- Cybersecurity policies
- Cybersecurity risk management
- Attack mechanisms

Day 3 | Cybersecurity controls, information sharing and coordination

- Cybersecurity controls
- Information sharing and coordination
- Training and awareness program

Day 4 | Incident management, monitoring and continuous improvement

- Business continuity
- Cybersecurity incident management
- Cybersecurity incident response and recovery
- Testing in Cybersecurity
- Performance measurement
- Continuous improvement
- Closing the training

Day 5 | Certification Exam

Learning objectives

- Acquire a comprehensive understanding of the elements and operations of a Cybersecurity Program in conformance with ISO/IEC 27032 and NIST Cybersecurity Framework
- Acknowledge the correlation between ISO/IEC 27032, NIST Cybersecurity Framework, and other standards and operating frameworks
- Master the concepts, approaches, standards, methods, and techniques used to effectively set up, implement, and manage a cybersecurity program within an organization
- Learn how to interpret the guidelines of ISO/IEC 27032 in the specific context of an organization
- Master the necessary expertise to plan, implement, manage, control and maintain a cybersecurity program as specified in ISO/IEC 27032 and NIST Cybersecurity Framework
- Acquire the necessary expertise to advise an organization on the best practices for managing cybersecurity

Examination

Duration: 3 hours

The "PECB Certified ISO/IEC 27032 Lead Cybersecurity Manager" exam meets the requirements of the PECB Examination and Certification Programme (ECP). The exam covers the following competency domains:

Domain 1 | Fundamental principles and concepts of cybersecurity

Domain 2 | Roles and responsibilities of stakeholders

Domain 3 | Cybersecurity Risk Management

Domain 4 | Attack mechanisms and cybersecurity controls

Domain 5 | Information sharing and coordination

Domain 6 | Integrating cybersecurity program in Business Continuity Management (BCM)

Domain 7 | Cybersecurity incident management and performance measurement

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 successfully completing the exam, you can apply for the credentials shown on the table below. You will receive a certificate once you comply with all the requirements related to the selected credential. For more information about ISO/IEC 27032 certifications and the PECB certification process, please refer to the Certification Rules and Policies.

Credential	Exam	Professional experience	CSMS project experience	Other requirements
PECB Certified ISO/IEC 27032 Provisional Cybersecurity Manager	PECB Certified ISO/IEC 27032 Lead Cybersecurity Manager Exam or equivalent	None	None	Signing the PECB Code of Ethics
PECB Certified ISO/IEC 27032 Cybersecurity Manager	PECB Certified ISO/IEC 27032 Lead Cybersecurity Manager Exam or equivalent	**Two years:** One year of work experience in cybersecurity	Cybersecurity activities: a total of 200 hours	Signing the PECB Code of Ethics
PECB Certified ISO/IEC 27032 Lead Cybersecurity Manager	PECB Certified ISO/IEC 27032 Lead Cybersecurity Manager Exam or equivalent	**Five years:** Two years of work experience in cybersecurity	Cybersecurity activities: a total of 300 hours	Signing the PECB Code of Ethics
PECB Certified ISO/IEC 27032 Senior Lead Cybersecurity Manager	PECB Certified ISO/IEC 27032 Lead Cybersecurity Manager Exam or equivalent	**Ten years:** Seven years of work experience in cybersecurity	Cybersecurity activities: a total of 1,000 hours	Signing the PECB Code of Ethics

Note: *PECB certified individuals who possess Lead Implementer and Lead Auditor credentials are qualified for the respective PECB Master credential, given that they have taken four additional Foundation exams related to this scheme. More detailed information about the Foundation exams and the Master credential requirements can be found here.*

General information

- Certification and examination fees are included in the price of the training course
- Training material containing over 400 pages of information and practical examples will be distributed
- An Attestation of Course Completion worth 31 CPD (Continuing Professional Development) credits will be issued to all candidates who have attended the training course
- In case you do not pass the exam, you can retake it within 12 months following the initial attempt for free