FCMS CONSULTING

PECB

PECB Certified NIST Cybersecurity Professional

Gain expertise in applying NIST guidelines, managing security controls, employing risk management techniques, and designing a cybersecurity program aligned with organizational objectives and security needs.

Why should you attend?

In today's increasingly digital world, organizations face growing challenges in securing their information systems and ensuring compliance with regulatory standards. NIST publications such as NIST SP 800-12, NIST SP 800-53, NIST RMF, NIST SP 800-171, and the NIST Cybersecurity Framework offer comprehensive guidelines and best practices for establishing robust cybersecurity measures. Implementing these frameworks helps organizations enhance their cybersecurity posture, manage risks effectively, and maintain compliance with federal requirements.

Through in-depth guidance on NIST publications, participants learn to tackle complex security challenges, applying frameworks to build robust cybersecurity programs that align with organizational goals. The course also provides practical expertise to prevent, detect, and respond to cyber threats efficiently, integrating best practices and standards to create a cohesive security approach.

Upon completing the course, participants will be eligible to take the exam. Those who pass the exam will be awarded the globally recognized "PECB Certified NIST Cybersecurity Professional" credential.

Who should attend?

This training course is intended for:

- Executives or directors responsible for overseeing cybersecurity initiatives within their organizations
- System administrators and network engineers seeking a deeper understanding of security controls and risk management processes to adhere to NIST security standards
- Professionals involved in the development and implementation of cybersecurity programs
- Professionals and advisors who provide cybersecurity and compliance services, ensuring they stay up to date with the latest NIST frameworks and best practices
- Digital forensics and cybercrime investigators who need to understand the technical and regulatory aspects of cybersecurity frameworks to investigate and respond to security incidents comprehensively
- Individuals working in cybersecurity or information security who aim to enhance their understanding of NIST guidelines and develop practical skills in managing cybersecurity risks

Course agenda

Duration: 5 days

Day 1 | Introduction to NIST Cybersecurity standards and principles

- Training course objectives and structures
- Frameworks and standards for information security and cybersecurity
- Introduction to NIST and its role in cybersecurity
- Introduction to cybersecurity
- The organization and its context
- Roles, responsibilities, and authorities
- Cybersecurity policy

Day 2 | Risk management strategy and supply chain risk management

- Risk management strategy
- Supply chain risk management
- Asset management
- Risk assessment
- Improvement

Day 3 | Selecting security controls, awareness and training, and continuous monitoring

- Security control selection
- Awareness and training
- Security measures
- Security continuous monitoring

Day 4 | Cybersecurity incident management

- Incident management and analysis
- Incident response, mitigation, and reporting
- Incident recovery and lessons learned
- Closing of the training course

Day 5 | Certification Exam

Learning objectives

By the end of this training course, participants will be able to:

- Discuss the fundamental principles and concepts of cybersecurity
- Support compliance with key NIST publications, including NIST 800-12, NIST 800-53, NIST RMF, NIST 800-171, and the NIST CSF
- Assess and advise on security controls in alignment with NIST guidelines
- Provide guidance on cybersecurity risk management and incident management strategies
- Guide organizations in developing and optimizing cybersecurity programs

Examination

Duration: 3 hours

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

Domain 1 | **Fundamental principles and concepts of cybersecurity**

Domain 2 | **Planning an organizational strategy in cybersecurity**

Domain 3 | **Assessing and advising on cybersecurity programs and security controls**

Domain 4 | **Cybersecurity incident management**

Domain 5 | **Cybersecurity incident response**

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 in the table below. You will receive a certificate once you fulfill all the requirements of the selected credential.

Credential	Exam	Professional experience	Cybersecurity program experience	Other requirements
PECB Certified Provisional NIST Cybersecurity Professional	PECB Certified NIST Cybersecurity Professional exam	None	None	Signing the PECB Code of Ethics
PECB Certified NIST Cybersecurity Professional		5 years (2 in cybersecurity)	At least 300 hours	

General information

- Certificate and examination fees are included in the price of the training course.
- Participants will receive more than 450 pages of comprehensive training materials, including practical examples, exercises, and quizzes.
- Participants who have attended the training course will receive an attestation of course completion worth 31 CPD (Continuing Professional Development) credits.
- Candidates who have completed the training course with one of our partners and failed the first exam attempt are eligible to retake the exam for free within a 12-month period from the date the coupon code is received because the fee paid for the training course includes a first exam attempt and one retake. Otherwise, retake fees apply.