PECB Certified NIST Cybersecurity Consultant

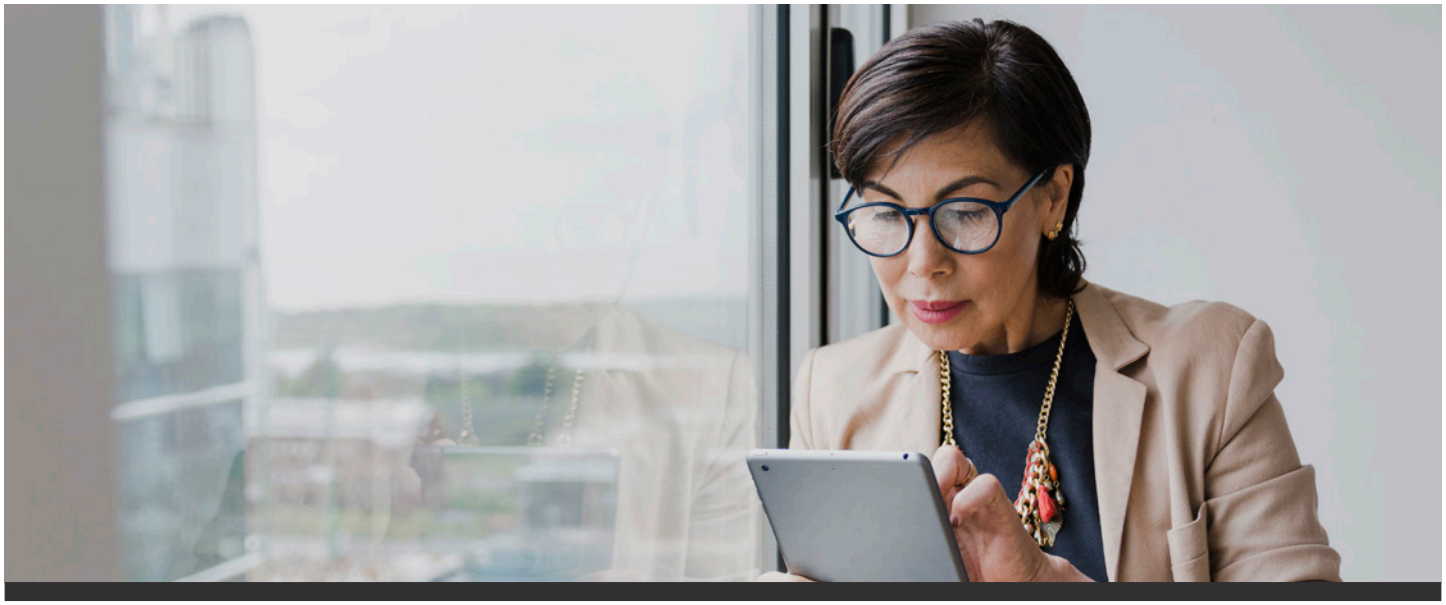
Gain expertise in applying NIST guidelines, managing security controls, employing risk management techniques, and designing a cybersecurity program aligned with organizational objectives and security needs.

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 Consultant" 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
- Consultants 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 structure
- Cybersecurity frameworks and standards
- Introduction to NIST and its role in cybersecurity
- Introduction to cybersecurity
- The organization and its context
- Cybersecurity program roles and responsibilities
- Cybersecurity policy

Day 2 | Risk management strategy and supply chain risk management

- Risk management strategy
- Supply chain risk management
- Asset management
- 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, 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 completion of this training course, participants will be able to:

- Discuss fundamental cybersecurity principles and concepts, including confidentiality, integrity, and availability, and how these principles are applied to protect information systems
- Explain key NIST publications, including NIST SP 800-12, NIST SP 800-53, the Risk Management Framework, NIST SP 800-171, and the NIST Cybersecurity Framework, and apply their guidance and requirements
- Implement a process to effectively monitor, assess, and manage security controls based on NIST publications
- Apply structured risk management techniques to identify, assess, and prioritize cybersecurity risks
- Develop risk mitigation strategies and implement risk treatment plans that align with NIST's risk management recommendations, ensuring a balanced approach to risk reduction and resource allocation
- Design a cybersecurity program that aligns with the organization's strategic goals and addresses specific security requirements

Examination

Duration: 3 hours

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

Domain 1 | Fundamental principles and concepts of cybersecurity

Domain 2 | Planning an organizational strategy in cybersecurity

Domain 3 | Implementing a cybersecurity program 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 successfully passing the exam, participants can apply for one of the credentials shown in the table below. Participants will receive the certificate once they comply with all the requirements related to the selected credential.

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

General information

- Certification and examination fees are included in the price of the training course.
- Participants will be provided with the training course material containing over 450 pages of explanatory information, examples, best practices, 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.
- In case you fail the exam, you are eligible to retake the exam within a 12-month period from the date the coupon code is received.