

NIST CYBERSECURITY LEAD IMPLEMENTER
TRAINING AND CERTIFICATION

WISELEARNER

WHAT IS NIST?

- The Certified NIST Cybersecurity Lead Implementer program equips professionals with the expertise to apply NIST frameworks and guidelines to strengthen organizational cybersecurity and resilience.
- This certification focuses on developing cybersecurity strategies, conducting risk assessments, selecting appropriate security controls, and establishing effective incident management and response processes. Participants learn to design, implement, and maintain cybersecurity programs aligned with organizational objectives, regulatory requirements, and industry best practices.
- Through practical, framework-based learning, professionals develop the skills to manage cybersecurity risks, evaluate control effectiveness, implement continuous monitoring, and respond to evolving threats. The program prepares them to lead cybersecurity initiatives, enhance organizational resilience, and support the ongoing improvement of security practices.

BENEFIT OF NIST

- Recognition as a certified professional in NIST cybersecurity implementation.
- Comprehensive knowledge of NIST frameworks and standards, including SP 800-12, SP 800-53, RMF, SP 800-171, and the Cybersecurity Framework (CSF).
- Practical skills in risk management, security control selection, and incident response.
- Strengthened organizational compliance with applicable federal, regulatory, and industry requirements.
- Enhanced ability to lead cybersecurity programs and mitigate risks effectively.
- Improved capability to identify vulnerabilities, assess threats, and prioritize risk mitigation measures.
- Expertise in developing and implementing risk-based cybersecurity strategies.
- Enhanced understanding of cybersecurity governance, policies, and organizational security responsibilities.
- Improved preparedness to detect, analyze, contain, and recover from cybersecurity incidents.



WHO SHOULD ATTEND?

- Executives and directors responsible for cybersecurity governance, risk oversight, and strategic decision-making.
- System administrators and network engineers involved in securing IT infrastructure and implementing security controls.
- Cybersecurity professionals responsible for developing, managing, and implementing organizational cybersecurity programs.
- Advisors and consultants providing cybersecurity, risk management, and compliance services.
- Digital forensics specialists and cybercrime investigators involved in security incident analysis and investigation.
- Information security practitioners seeking to strengthen their expertise in NIST frameworks and cybersecurity implementation.
- IT managers and security team leaders overseeing information security operations and risk mitigation initiatives.
- Risk management professionals involved in identifying, assessing, and treating cybersecurity risks.

LEARNING OBJECTIVES

- Understand NIST Frameworks: Explain the fundamental principles, standards, and guidelines used to establish and improve organizational cybersecurity programs.
- Develop Cybersecurity Strategies: Define cybersecurity objectives, establish implementation priorities, and align security initiatives with organizational requirements.
- Conduct Cybersecurity Risk Assessments: Identify critical assets, evaluate threats and vulnerabilities, assess risks, and determine appropriate risk treatment measures.
- Implement Security Controls: Select, apply, and evaluate suitable cybersecurity controls based on organizational risks and applicable NIST guidance.
- Assess Cybersecurity Programs: Evaluate existing security practices, identify control gaps, and recommend improvements to strengthen the organization's security posture.
- Establish Incident Management Processes: Develop structured procedures for incident identification, classification, reporting, documentation, and coordination.
- Strengthen Incident Response Capabilities: Apply appropriate approaches to incident detection, analysis, containment, eradication, recovery, and post-incident review.



COURSE CONTENTS

Module 1: Fundamental Principles and Concepts of Cybersecurity

- Introduction to cybersecurity principles and terminology
- Cybersecurity threats, vulnerabilities, and risks
- Information security objectives and organizational security needs
- Introduction to NIST frameworks, standards, and publications
- Overview of the NIST Cybersecurity Framework and Risk Management Framework

Module 2: Planning an Organizational Cybersecurity Strategy

- Understanding organizational cybersecurity requirements
- Establishing cybersecurity objectives and priorities
- Developing a risk-based cybersecurity strategy
- Identifying critical assets and assessing cybersecurity risks
- Defining security policies, roles, and responsibilities
- Planning security controls and implementation activities

Module 3: Assessing and Advising on Cybersecurity Programs and Security Controls

- Identifying security gaps and areas for improvement
- Selecting and implementing appropriate security controls
- Understanding NIST SP 800-53 and SP 800-171 guidance
- Risk assessment and security control evaluation
- Security documentation, reporting, and implementation planning
- Monitoring control effectiveness and supporting compliance objectives

Module 4: Cybersecurity Incident Management

- Establishing an incident management framework
- Identifying and classifying cybersecurity incidents
- Defining incident management roles and responsibilities
- Incident reporting, documentation, and communication
- Coordinating incident management activities
- Integrating incident management with organizational risk management

Module 5: Cybersecurity Incident Responsey

- Developing and maintaining incident response procedures
- Incident detection, analysis, and prioritization
- Containment, eradication, and recovery
- Incident response coordination and stakeholder communication
- Post-incident analysis and lessons learned
- Continuous improvement of incident response capabilities



CERTIFICATION

- Exam Mode: Online
- Exam Duration: 90 Minutes
- Exam Format: Multiple-Choice Questions (MCQs)
- Number of Questions: 50
- Passing Score: 70% (35 out of 50)