

CERTIFIED LEAD CYBERSECURITY MANAGER

TRAINING AND CERTIFICATION

WISELEARNER

WHAT IS CERTIFIED LEAD CYBERSECURITY MANAGER?

- Goal of the Lead Cybersecurity Manager training course appears to be preparing individuals to take on leadership roles in cybersecurity, ensuring they are well-equipped to protect organizations from cyber threats and manage the complexities of a cybersecurity program.

BENEFITS OF CERTIFIED LEAD CYBERSECURITY MANAGER

- Comprehensive security posture: Leads the development and implementation of a comprehensive cybersecurity strategy.
- Risk mitigation: Conducts risk assessments and implements measures.
- Incident response excellence: Establishes and oversees incident response plans, enabling the organization to respond effectively to cybersecurity incidents, minimize damage, and recover quickly.
- Regulatory compliance: Ensures compliance with relevant laws, regulations, and industry standards, reducing legal and financial risks associated with non-compliance.
- Leadership and team effectiveness: Provides strong leadership to the cybersecurity team, fostering a culture of security awareness and professionalism. This contributes to a more effective and motivated cybersecurity workforce.
- Strategic alignment: Aligns cybersecurity initiatives with overall business strategies, demonstrating the value of cybersecurity as an integral part of the organization's success.
- Resource allocation and budget management: Effectively allocates resources and manages the cybersecurity budget, optimizing investments to address the most critical areas of risk and vulnerability.
- Vendor management and technology integration: Oversees relationships with cybersecurity vendors, ensuring that the organization adopts and integrates cutting-edge security technologies and solutions.
- Communication with stakeholders: Communicates cybersecurity risks, strategies, and initiatives to executive leadership, board members, and other stakeholders, facilitating informed decision-making.



WHO SHOULD ATTEND?

- Experienced cybersecurity practitioners who aspire to move into managerial positions.
- IT and security pofessionals.
- Managers and leaders in cybersecurity who are progressively moving into leadership positions.
- Individuals Implementing cybersecurity strategies.
- Professionals from various Industries such as finance, healthcare, manufacturing, or any sector handling sensitive data.

LEARNING OBJECTIVES

The learning objectives for a Certified Lead Cybersecurity Manager (CLCM) certification program typically encompass a range of knowledge, skills, and competencies related to effectively leading and managing cybersecurity within an organization. Following topics are covered:

- Understanding cybersecurity fundamentals
- Legal and regulatory compliance
- Governance and leadership
- Risk management
- Information security management systems (ISMS)
- Incident response and management
- Security policies and procedures
- Security awareness and training
- Security controls and technologies
- Security monitoring and surveillance
- Business continuity and disaster recovery
- Cybersecurity metrics and reporting



COURSE CONTENT

Introduction to Cybersecurity Management:

- Overview of cybersecurity concepts and principles
- Importance of cybersecurity in modern organizations
- Role of a cybersecurity manager in an organization

Legal and Regulatory Framework:

- Understanding relevant cybersecurity laws and regulations
- Compliance requirements and implications
- Data protection and privacy considerations

Cybersecurity Governance:

- Establishing and maintaining a cybersecurity governance framework
- Roles and responsibilities of key stakeholders
- Board-level considerations for cybersecurity

Cybersecurity Risk Management:

- Identifying and assessing cybersecurity risks
- Risk mitigation and management strategies
- Developing a risk management plan

Information Security Management Systems (ISMS):

- Overview of ISMS frameworks (e.g., ISO/IEC 27001)
- Implementing and managing an ISMS
- Certification and audit processes

Incident Response and Management:

- Developing an incident response plan
- Managing and responding to cybersecurity incidents
- Post-incident analysis and improvement

CERTIFICATION

- Exam Duration - 3 Hours
- Exam Pattern - Multiple choice question
- Exam Pass Mark - 70%
- Exam Result - Participant can expect exam result in 2 working days

WISELEARNER