CYBER SECURITY RISK ASSESSMENT & MANAGEMENT



London - UK
07 - Dec 2026 - 11 - Dec 2026
$6,000

GENTEX®
TRAINING CENTER

GENTEX Training Center LLC | Orlando - FL, USA
Info@gentextraining.com

Introduction

In today's ever-evolving digital landscape, cyber threats pose a constant challenge to organizations of all sizes. A proactive approach to cyber security risk assessment and management is essential to safeguarding sensitive data, protecting critical infrastructure, and ensuring business continuity. This intensive five-day program, offered by Gentex Training Center, equips participants with the knowledge and practical skills needed to effectively assess cyber security risks, develop robust mitigation strategies, and implement a comprehensive risk management framework. Through a comprehensive exploration of key risk assessment methodologies, industry best practices, and practical exercises, participants gain the ability to identify vulnerabilities, prioritize risks, and build a strong cyber security posture within their organizations.

Cyber Security Risk Assessment & Management Course Objectives:

- Master the core principles of cyber security risk assessment and management.
- Understand the cyber threat landscape and the various types of cyberattacks organizations face.
- Identify and analyze cyber security vulnerabilities within an organization's IT infrastructure and data systems.
- Apply industry-standard risk assessment methodologies to evaluate the likelihood and impact of cyber threats.
- Develop a comprehensive risk management plan to prioritize risks, allocate resources, and implement mitigation strategies.
- Explore best practices for incident response, disaster recovery, and business continuity planning in the event of a cyberattack.
- Utilize relevant legal and regulatory frameworks related to cyber security risk management.

GENTEX® TRAINING CENTER

- Analyze real-world case studies of successful and unsuccessful cyber security risk management practices.
- Formulate a personalized action plan to assess and manage cyber security risks within your organization.

Course Methodology

This interactive program utilizes a participant-centric approach. It blends lectures from cyber security experts, interactive workshops, real-world case studies, group discussions, and practical exercises. Participants actively engage in conducting risk assessments, developing risk management plans, simulating incident response scenarios, and crafting action plans to address specific cyber security risks within their organizations. Through experiential learning, participants gain the practical skills and theoretical knowledge needed to become cyber security risk management champions within their organizations, ensuring a more secure and resilient digital environment.

Who Should Take This Course

- IT security professionals, system administrators, and network engineers seeking to enhance their cyber security risk assessment and management skills.
- Business managers, project managers, and decision-makers responsible for protecting organizational assets and mitigating cyber security risks.
- Compliance officers and risk management professionals seeking to integrate cyber security considerations into their overall risk management frameworks.
- Anyone interested in understanding and contributing to building a strong cyber security posture for their organization.

LEARN BOLD. **LEAD BEYOND**
GENTEX Training Center LLC | Orlando - FL, USA
Info@gentextraining.com

Cyber Security Risk Assessment & Management Course Outline:

Day 1: Understanding the Threats: Identifying Cyber Security Vulnerabilities

- Demystifying Cyber Security Risk: Core Concepts, Threat Landscape, and Types of Cyberattacks

- Identifying and Analyzing Vulnerabilities: Network Infrastructure, Data Systems, and Human Factors

Day 2: Assessing the Risks: Industry-Standard Risk Assessment Methodologies

- Exploring Risk Assessment Methodologies: FMEA (Failure Mode and Effect Analysis), NIST CSF (National Institute of Standards and Technology Cybersecurity Framework)

- Conducting Risk Assessments and Evaluating Likelihood and Impact of Cyber Threats

Day 3: Building a Robust Defense: Developing a Comprehensive Risk Management Plan

- Prioritizing Risks and Allocating Resources: Developing a Risk Management Plan with Mitigation Strategies

- Implementing Controls: Technical, Administrative, and Physical Safeguards to Address Vulnerabilities

GENTEX® TRAINING CENTER

GENTEX Training Center LLC | Orlando - FL, USA
Info@gentextraining.com

Day 4: Beyond the Breach: Incident Response, Disaster Recovery, and Business Continuity

- Planning for the Unexpected: Developing an Incident Response Plan and Disaster Recovery Strategy
- Ensuring Business Continuity: Minimizing Downtime and Maintaining Critical Operations After a Cyberattack

Day 5: Building a Secure Future: Legal Considerations, Best Practices, and Action Planning

- Understanding Legal and Regulatory Frameworks Related to Cyber Security
- Exploring Best Practices for Ongoing Risk Management and Continuous Improvement
- Formulating a Personalized Action Plan to Implement Cyber Security Risk Assessment & Management within Your Organization

Conclusion

By successfully completing this comprehensive program offered by Gentex Training Center, participants gain the knowledge and practical skills needed to navigate the complex world of cyber security risk assessment and management. They will be equipped to identify and address potential security breaches, prioritize cyber risks effectively, and contribute to building a strong and resilient cyber security posture within their organizations. This enhanced knowledge empowers them to become proactive defenders in the fight against cyber threats, safeguarding valuable assets and ensuring business continuity in today's digital age.

GENTEX® TRAINING CENTER

GENTEX Training Center LLC | Orlando - FL, USA
Info@gentextraining.com

FAQs

Q1 What is the Cyber Security Risk Assessment & Management course about?

The Cyber Security Risk Assessment & Management course focuses on identifying, analyzing, and managing cyber security risks. It covers cyber threats, vulnerabilities, risk assessment methodologies, mitigation strategies, incident response, disaster recovery, business continuity, and legal and regulatory considerations related to cyber security.

Q2 What are the key benefits of the Cyber Security Risk Assessment & Management course?

The course helps participants identify vulnerabilities, assess the likelihood and impact of cyber threats, prioritize risks, and develop effective mitigation plans. It also strengthens organizational resilience by addressing incident response, disaster recovery, business continuity, and ongoing cyber security risk management.

Q3 What skills will I gain from the Cyber Security Risk Assessment & Management course?

Participants will gain Cyber Security Risk Assessment, Vulnerability Analysis, Risk Management Planning, and Incident Response and Business Continuity skills. These capabilities support effective risk evaluation, vulnerability identification, mitigation planning, incident preparedness, and maintaining critical operations following cyber security incidents.

GENTEX® TRAINING CENTER

GENTEX Training Center LLC | Orlando - FL, USA
Info@gentextraining.com

Q4 What tools, methods, or standards are covered in the Cyber Security Risk Assessment & Management course?

The course covers FMEA (Failure Mode and Effect Analysis) and the NIST CSF (National Institute of Standards and Technology Cybersecurity Framework) as risk assessment methodologies. It also addresses technical, administrative, and physical controls, incident response planning, disaster recovery, and business continuity strategies.

Q5 How is the Cyber Security Risk Assessment & Management course applied in real-world practice?

The course applies risk management through practical risk assessments, risk management plan development, incident response simulations, real-world case studies, and action planning. Participants practice identifying vulnerabilities, evaluating cyber threats, prioritizing risks, implementing safeguards, and preparing organizations to maintain operations after cyberattacks.