



course : Cyber Security Risk Assessment Training

City : Kuala Lumpur
Start Date : 2025-11-24
Period : 1 Week

Hotel : Kuala Lumpur
End Date : 2025-11-28
Price : 3950 \$

HighPoint Training and Management Consultancy
هاي بوينت للتدريب والاستشارات الإدارية

info@highpointtc.com ✉
www.Highpointtc.com 🌐
UAE - Dubai 📍
+971 50 360 6133 📞

Course Overview

In today's fast-paced digital environment, cyber threats are increasingly sophisticated and pervasive, affecting organizations across all sectors. Protecting sensitive information, ensuring business continuity, and maintaining stakeholder trust are critical priorities for every organization.

This Cyber Security Risk Management training course provides a comprehensive framework to proactively identify vulnerabilities, assess potential risks, and implement effective security measures. Participants will gain practical insights into threat detection, risk assessment, incident response, and regulatory compliance, enabling them to safeguard digital assets and enhance organizational resilience.

Course Objectives

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

- Understand the fundamentals of cyber security risk management
- Identify and assess potential cyber threats and vulnerabilities
- Develop and implement effective cyber security strategies and policies
- Execute risk assessment techniques to prioritize cyber risks
- Implement encryption, authentication, and access control measures
- Plan and execute incident response procedures to mitigate cyber incidents
- Ensure compliance with relevant regulations and standards
- Educate employees and stakeholders on cyber security best practices
- Collaborate with cross-functional teams to address cyber security challenges
- Monitor and respond to real-time cyber threats

Target Audience

This course is designed for professionals responsible for the security of digital assets, including:

- IT Managers and Professionals
- Cyber Security Analysts
- Risk Management Professionals
- Chief Information Security Officers (CISOs)
- Compliance Officers
- Business Executives and Managers
- Information Security Officers

Network Administrators

Methodology

The course combines interactive lectures, hands-on exercises, case studies, and group discussions to ensure maximum comprehension and practical application. Participants will "learn by doing," applying risk assessment, mitigation, and incident response strategies to simulated real-world scenarios.

Course Outline

Day 1 – Introduction to Cyber Security Risk Management

Understanding Cyber Security and Its Importance

Evolution of Cyber Threats and Attack Vectors

Cyber Security Risk Management Frameworks

Case Study: Real-world cyber incidents

Day 2 – Identifying and Assessing Cyber Risks

Types of Cyber Security Threats

Vulnerability Assessment and Penetration Testing

Risk Assessment Methodologies and Prioritization

Hands-on Exercises: Risk identification and evaluation

Day 3 – Developing Cyber Security Strategies and Controls

Security Policies and Procedures

Security by Design Principles

Security Awareness Training

Implementing Controls: Encryption, Authentication, Access Management

Day 4 – Incident Response, Recovery, and Compliance

Incident Response Planning and Execution

Business Continuity and Disaster Recovery

Legal and Regulatory Considerations (GDPR, HIPAA, etc.)

International Standards and Frameworks (ISO 27001, NIST)

Day 5 – Collaboration, Monitoring, and Emerging Threats

Cross-Functional Collaboration and Communication

Real-Time Threat Monitoring and Threat Intelligence

Building a Culture of Cyber Security

Emerging Technologies, Predictive Analytics, and Future Trends

Final Discussion, Q&A, and Course Wrap-Up

Certificates

On successful completion of this training course, HighPoint Certificate will be awarded to the delegates. Continuing Professional Education credits (CPE): In accordance with the standards of the National Registry of CPE Sponsors, one CPE credit is granted per 50 minutes of attendance.