



course : Cybersecurity and Enterprise Resilience

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

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



Course Overview

The Cybersecurity and Enterprise Resilience Training Course is designed to empower professionals with the knowledge and skills to address today's growing cyber threats. As organizations rely heavily on digital systems and data, the ability to anticipate, manage, and respond to cyber risks has become critical. This program provides a comprehensive approach, combining strategic, technical, and managerial perspectives to strengthen enterprise resilience and ensure effective protection of sensitive information assets.

Course Objectives

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

Recognize and classify different types of cybersecurity threats and vulnerabilities

Develop effective response and mitigation strategies against cyber risks

Integrate security considerations into IT systems and organizational processes

Apply best practices in planning, monitoring, and controlling systems security

Understand the legal, regulatory, and compliance frameworks for cybersecurity and data protection

Target Audience

This program is suitable for a wide range of professionals, including:

Business managers and department heads in public and private organizations

IT professionals, developers, and system administrators

Risk management and compliance officers

Digital business strategists and entrepreneurs

Professionals seeking to enhance their cybersecurity awareness and resilience capabilities

Methodology

The course employs a mix of interactive lectures, real-world case studies, scenario analysis, group exercises, and discussions. Practical examples will ensure participants gain not only theoretical knowledge but also the ability to apply concepts to real organizational challenges.

Course Outline

Day 1 – Cybersecurity Foundations and Enterprise Resilience

Cybersecurity in modern organizations
Threat landscape and attack methods
The concept of enterprise resilience
Security risks in IT and BYOD environments
Introduction to resilience frameworks

Day 2 – Threats, Impacts, and Risk Assessments

Analyzing types of threats and vulnerabilities
Security risk assessment frameworks
Impacts of cyberattacks on organizations
Case studies of major cyber incidents
Tools for effective risk identification

Day 3 – Security Frameworks, Policies, and Regulations

Legislation and policies for data security
Regulatory frameworks: national, European, and international
Industry standards and compliance requirements
Corporate responsibility and governance in cybersecurity
Developing security strategies and policies

Day 4 – Emerging Technologies and Critical Infrastructure

Cybersecurity in critical infrastructure
Protection of data (small and big data)
Autonomous systems, IoT, blockchain, and AI vulnerabilities
Governance and standards for IT systems
Use cases from public and private sectors

Day 5 – Cyber Risk Management and Future Challenges

Cyber risk management principles and practices
Business continuity and disaster recovery planning
Scenarios and simulation exercises for cyber resilience
Designing secure systems and data protection strategies
Preparing organizations for emerging cyber challenges

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.