



course : Cybersecurity Audit Essentials

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 digital era, cybersecurity threats and risks are constantly evolving and pose significant challenges to organizations across industries. Beyond financial or operational damages, cybersecurity incidents can lead to severe reputation loss, as seen in global cases such as Facebook and Cambridge Analytica.

To effectively address these challenges, organizations must conduct cybersecurity audits to identify vulnerabilities, assess risks, and implement corrective measures. This training course provides participants with the essential knowledge and practical tools to plan, perform, and evaluate cybersecurity audits in line with international standards and frameworks.

Course Objectives

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

- Perform risk analysis of IT security breaches
- Apply cybersecurity risk appraisal and risk management methods
- Understand and utilize ISO 27001 and COBIT 5 frameworks
- Gain knowledge of Information Security Management principles
- Apply best practices in crisis management and disaster recovery planning
- Conduct structured and effective cybersecurity audits

Target Audience

This course is designed for professionals across various roles, including:

- Risk Managers and Auditors
- Application and Product Designers
- Research and Marketing Specialists
- Statistical and Data Analysts
- Application Development and Data Research Personnel
- Technology and Telecommunications Engineers
- IT and Cybersecurity Professionals seeking audit expertise

Methodology

The course combines interactive lectures, case studies, group exercises, simulations, and software-based workshops. Emphasis will be on learning by doing through risk assessment activities, audit planning, and execution exercises. Tools such as free risk management and auditing software will be used to ensure practical, hands-on learning.

Course Outline

Day 1 – IT Security Evolution

- Categorizing physical and electronic risks
- Networking and communication technologies
- Computer systems design
- Legal and regulatory considerations
- Current threat and trend analysis
- Review and case study

Day 2 – Identifying and Responding to Data Breaches

- IPv6 configuration and risks
- DNS Security Extensions (DNSSEC)
- Crisis management planning
- Forensic and electronic investigations
- Business continuity response
- Review and case study

Day 3 – Preparing the Cybersecurity Audit Scope

- NIST Cybersecurity Framework
- Cyber incident response policy requirements
- COBIT 5 framework
- Developing an audit plan using NIST and COBIT 5
- Review and case study

Day 4 – Executing the Cybersecurity Audit

- Using BowTie method for cybersecurity risk management
- Applying AuditXP software for cybersecurity audits
- Creating audit questionnaires based on NIST and COBIT 5 frameworks
- Performing a cybersecurity audit on a sample entity
- Review and case study

Day 5 – Cybersecurity Audit Workshop

- Forming the audit team and setting the scope
- Executing the audit process

Reviewing audit findings
Preparing and presenting recommendations
Implementation strategies, monitoring, and continuous upgrade

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.