€TRAINING

Information Security Management

2 - 6 February 2025
Istanbul (Turkey)

Information Security Management

REF: B1578 DATE: 2 - 6 February 2025 Venue: Istanbul (Turkey) - Fee: 5850 Euro

Introduction:

This training program provides participants with essential knowledge and skills in information security management and cyber security. It empowers them to protect organizational assets, detect threats, and respond to security incidents effectively.

Program Objectives:

At the end of this program, participants will be able to:

- Understand the fundamental concepts of information security and cyber security.

- Identify and assess potential security threats and vulnerabilities.

- Implement security measures to protect information assets.

- Develop and manage security policies and procedures.

- Respond to and recover from security incidents.

Targeted Audience:

- IT Security Professionals.

- Network Administrators.

- Systems Administrators.

- IT Managers and Directors.

- Personnel responsible for managing or overseeing information security in an organization.

Program Outline:

Unit 1:

Introduction to Information Security:

- Overview of information security and cyber security concepts.

- Understanding the CIA triad Confidentiality, Integrity, Availability.

- Identifying types of threats and attacks malware, phishing, social engineering.

- Overview of security frameworks and standards ISO/IEC 27001, NIST.

- Implementing security policies and governance.

Unit 2:

Risk Management and Vulnerability Assessment:

- Understanding risk management concepts and processes.

- Conducting risk assessments and identifying vulnerabilities.

- Utilizing vulnerability assessment tools and techniques.

- Implementing risk mitigation strategies.

- Developing and maintaining a risk management plan.

Unit 3:

Implementing Security Controls:

- Introduction to security controls and their types.

- Implementing physical security measures.

- Utilizing technical controls firewalls, IDS/IPS, encryption.

- Applying administrative controls access control, security training.

- Monitoring and auditing security controls.

Unit 4:

Incident Response and Management:

- Understanding the incident response lifecycle.

- Developing an incident response plan.

- Identifying and analyzing security incidents.

- Implementing containment, eradication, and recovery measures.

- Conducting post-incident analysis and reporting.

Unit 5:

Security Operations and Continuous Improvement:

- Overview of security operations centers SOC.

- Implementing security monitoring and logging.

- Utilizing threat intelligence and analytics.

- Conducting regular security assessments and audits.

- Developing a culture of continuous improvement in security practices.