€TRAINING

Integrated Security Management

15 - 19 June 2025
Istanbul (Turkey)

Integrated Security Management

REF: Y2037 DATE: 15 - 19 June 2025 Venue: Istanbul (Turkey) - Fee: 5850 Euro

Introduction:

Integrated Security Management combines the protection of physical, digital, and personnel assets into a unified and strategic approach. This training program equips professionals with advanced skills to design, implement, and manage security frameworks that address multi-faceted threats in modern organizations. Participants will explore innovative strategies, risk mitigation techniques, and coordinated systems to enhance organizational resilience and operational continuity.

Program Objectives:

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

- Develop and conduct integrated security strategies tailored to organizational needs.
- Conduct thorough risk assessments and prioritize mitigation measures.
- Align physical and digital security operations within a unified framework.
- Respond to and resolve security incidents effectively.
- Ensure compliance with security regulations and standards.

Targeted Audience:

- Security and risk management professionals.
- IT security officers and compliance specialists.
- Facility and operations managers.
- Corporate governance and executive leadership.
- Professionals involved in organizational safety and resilience.

Program Outline:

Unit 1:

Foundations of Integrated Security:

- The evolution of security threats and the need for integration.
- Key components of physical, digital, and human security.

- Frameworks for aligning security with organizational objectives.
- Principles of governance in integrated security systems.
- Assessing the effectiveness of existing security measures.

Unit 2:

Advanced Risk Assessment and Analysis:

- Identifying and evaluating multi-layered risks.
- Tools and methodologies for comprehensive risk assessments.
- Integrating data analytics into threat detection processes.
- Evaluating vulnerabilities in interconnected systems.
- Developing prioritized risk mitigation plans.

Unit 3:

Strategic Security Framework Implementation:

- How to design cohesive security systems for physical and digital environments.
- Leveraging emerging technologies in security operations.
- Establishing protocols for monitoring and incident detection.
- Importance of coordinating security measures across departments and stakeholders.
- Ensuring seamless integration with existing infrastructure.

Unit 4:

Incident Management and Recovery Strategies:

- Crafting detailed incident response plans.
- Effective investigation techniques and resolving breaches to minimize impact.
- Ensuring business continuity during and after security events.
- Evaluating recovery efforts to enhance future preparedness.
- Communication protocols for internal and external stakeholders.

Unit 5:

Regulatory Compliance and Governance in Security:

- Navigating global security regulations and standards.
- Integrating compliance requirements into security frameworks.
- Ensuring accountability in security governance structures.
- The role of conducting audits to verify compliance and identify gaps.
- Maintaining alignment with legal and ethical considerations.