

€ TRAINING

Effective Modern Security Management and
Operations





Effective Modern Security Management and Operations

Introduction:

Effective modern security management and operations focus on integrating advanced strategies and technologies to protect organizational assets. This approach emphasizes proactive risk assessment, streamlined processes, and adaptive measures to ensure safety, resilience, and operational efficiency. This training program encompasses comprehensive understanding and application of cutting-edge security protocols, technologies, and methodologies. It cultivates a proactive mindset and fosters continuous improvement in security operations.

Program Objectives:

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

- Develop and perform effective security risk management frameworks to ensure comprehensive protection.
- Identify and address key challenges faced by security teams, including staffing, motivation, and threat assessments.
- Manage and operate advanced access control systems, including CCTV and electronic surveillance techniques.
- Execute security planning, including emergency response strategies, resource management, and investigative techniques.
- Integrate information security with physical security measures, ensuring a balanced and effective security management system.

Targeted Audience:

- Security Managers and Supervisors.
- Security Officers and Staff.
- Risk Management Professionals.
- Facility Managers.
- Safety and Security Consultants.
- IT and Information Security Professionals.

Program Outlines:

Unit 1:

Security Risk Management Framework:

- Security Risk Management.
- Loss prevention techniques.
- Security Surveillance.
- Security Management framework - Working the system.
- Key Concepts in Physical Security Resource Management.
- Building and Perimeter Security.

Unit 2:

Addressing Issues Faced by Security:

- Determining job requirements and recruitment criteria - Who makes a Good Security Officer.
- Motivating staff and providing feedback.
- Deploying, briefing, and supervising staff.
- How to assess staff performance.
- Understanding primary threats to physical security.
- Techniques of conducting Risk RA and Vulnerability SVA Assessments.

Unit 3:

Access Control and Physical Monitoring:

- Electronic Intruder Detection.
- Security Contingency Planning.
- Physical Security Asset Acquisition.
- CCTV Operations.
- Operation and Maintenance of Physical Security Resources.
- Situational Awareness.

Unit 4:

Overview of Security Planning and Investigations

- Security and Emergency Planning documentation.
- Responding to major security emergencies.
- Security Policies and Procedures.
- Defining Proposed Resource Outcomes and Cost-Effectiveness.
- Considering Life-Cycle, Warranty, and Preventive Maintenance.
- Industry Investigation Techniques.

Unit 5:

Information Security:

- Finding the balance between public facilitation and security measures.
- Security Management Systems SeMS.
- Close Protection Basics.
- Determining Resource Support.
- Physical Security/Information Technology Integration.