MAESTRO CONSULTANTS

SECURITY PLANNING & OPERATIONS

COURSE OUTLINE 2025

Contact Us On :

Tel : +971 7 2042072 |

Email: training@maestrouae.net

Website: www.maestrouae.net

TRAINING TITLE

SECURITY PLANNING & OPERATIONS

VENUE

Dubai, UAE

DURATION

5 Days

DATES

02nd-06th Feb 2026

PRICE

$5,250 per attendee including training material/handouts, morning/afternoon coffee breaks and Lunch.

TRAINING INTRODUCTION

In today's world of increasing complexity, threats to personnel, assets, and infrastructure can arise from a wide range of sources — physical breaches, insider threats, civil unrest, terrorism, or even cyber-physical attacks. For critical sectors like energy, manufacturing, logistics, and public infrastructure, security is no longer just a support function; it is a key component of organizational resilience and operational continuity.

This 5-day course, *"Security Planning & Operations,"* is designed to equip professionals with practical, risk-based skills to plan, implement, and manage effective security programs. It covers the full lifecycle of security operations — from threat assessment and system design to daily operations, incident response, and long-term strategic planning.

TRAINING OBJECTIVES

- Identify and assess physical, operational, and emerging security threats
- Develop and implement risk-informed security plans and procedures
- Design and manage layered physical protection systems and access control
- Lead incident response efforts and conduct post-incident investigations
- Align security functions with organizational strategy, compliance, and crisis preparedness

TRAINING AUDIENCE

Security managers, site supervisors, emergency planners, risk professionals, facilities managers, and personnel involved in corporate or field-level security operations

TRAINING OUTLINE

Day 1: Fundamentals of Security Management

Objective: Build a foundational understanding of security principles, threats, and governance frameworks.

- Introduction to Security Management
  - Purpose and scope of security planning
  - Key terms: threat, vulnerability, risk, deterrence
- Understanding the Threat Landscape
  - Physical threats (intrusion, theft, sabotage)
  - Human threats (insider threats, workplace violence)
  - Emerging threats (cyber-physical, terrorism, civil unrest)
- Legal, Regulatory & Ethical Considerations
  - Duty of care, use of force, privacy, and surveillance laws
  - International security standards (ASIS, ISO 18788, ISO 28000)

Day 2: Security Risk Assessment & Planning

Objective: Equip participants with risk-based approaches to develop security plans.

- Security Risk Assessment Techniques
  - Risk matrices, asset identification, likelihood vs. impact
  - Security audits and vulnerability analysis
- Developing a Security Plan
  - Components of a security master plan

    - Aligning with business continuity and crisis management
- Security Policies, Procedures & SOPs
    - Writing effective protocols and incident response guidelines
    - Training, drills, and communication strategies

Day 3: Physical Security Systems & Access Control

Objective: Understand and design integrated physical protection systems.

- Physical Security Layers
    - Deterrence, detection, delay, response
    - Perimeter security, barriers, fencing, lighting
- Access Control & Surveillance Technologies
    - Card access, biometrics, visitor management
    - CCTV, intrusion detection systems, control room operations
- Security System Integration & Maintenance
    - Linking physical and electronic systems
    - System testing, redundancy, and fail-safes

Day 4: Security Operations & Incident Response

Objective: Develop practical skills in managing day-to-day operations and responding to incidents.

- Managing Security Teams and Contracts
    - Roles of guards, supervisors, and control room operators
    - Outsourcing vs. in-house security, KPIs, and SLA management
- Incident Management & Emergency Response
    - Incident categories and escalation levels
    - Coordination with emergency services and internal stakeholders
- Investigation & Reporting

    - Scene control, evidence handling, post-incident analysis
    - Writing actionable security reports

Day 5: Strategic Security Planning & Future Trends

Objective: Align security operations with organizational goals and prepare for emerging challenges.

- Strategic Security Program Development
    - Security governance, leadership, and budgeting
    - KPIs and continuous improvement frameworks
- Security in a Digital World
    - Cybersecurity basics for physical security professionals
    - Convergence of cyber and physical threats (e.g., drones, AI surveillance)
- Business Continuity & Crisis Leadership
    - Integrating security with crisis management and emergency planning
    - Communication during security events

TRAINING CERTIFICATE

MAESTRO CONSULTANTS Certificate of Completion for delegates who attend and complete the training course

METHODOLOGY

Our courses are highly interactive, typically taking a case study approach that we have found to be an effective method of fostering discussions and transferring knowledge. Participants will learn by active participation during the program through the use of individual exercises, questionnaires, team exercises, training videos and discussions of “real life” issues in their organizations.
The material has been designed to enable delegates to apply all of the material with immediate effect back in the workplace.