SCANDINAVIAN ACADEMY
For Training and Development

Mobile : +46700414979 | Mobile : +46700414979 | phone : +46114759991
Email : info.en@scandinavianacademy.net | Web site : https://scandinavianacademy.net/en
location : Sweden - Norrköping - Timmermansgatan100 | P.O.BOX : 60359

Course: Corporate Physical & Field Security Management

Code	City	Hotel	Start	End	Price	Language - Hours
SM-939	Kuala Lumpur (Malaysia)	Hotel Meeting Room	2026-11-09	2026-11-13	4450 €	En - 25

Program Introduction

Corporate environments today face increasingly complex security threats, including theft and fraud, workplace violence, insider threats, civil unrest, and corporate espionage. These risks directly impact business continuity, executive safety, corporate reputation, and regulatory compliance.

According to ASIS International, modern corporate security must adopt the Enterprise Security Risk Management (ESRM) approach to align security strategy with business objectives. In addition, International Organization for Standardization through ISO 31000 emphasizes the importance of structured risk management frameworks to identify, assess, and mitigate organizational risks systematically.

This 5-Day Intensive Program provides a structured and practical framework for managing corporate physical and field security. It integrates risk management, access control systems, executive movement protection, incident management, crisis response, and strategic security leadership. The program combines theory with applied workshops and simulations tailored to real corporate environments.

General Objective

To equip participants with the knowledge and practical tools required to design, manage, and enhance an integrated corporate physical and field security framework that protects assets, executives, facilities, and corporate reputation while supporting

business continuity.

Training Objectives

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

- Analyze the corporate security risk landscape and identify priority threats.
- Apply the risk formula (Threat × Vulnerability × Impact) in corporate environments.
- Conduct a Physical Security Vulnerability Assessment (PSVA).
- Design layered physical security models for corporate facilities.
- Develop effective access control and visitor management systems.
- Design CCTV and tracking strategies aligned with corporate security needs.
- Establish and structure a Security Operations Center (SOC).
- Develop executive movement and journey management protocols.
- Plan response strategies for civil unrest and urban disruption.
- Write legally defensible and objective incident reports.
- Analyze incident trends and develop security performance KPIs.
- Develop corporate security policies and Standard Operating Procedures (SOPs).
- Integrate security into Business Continuity Planning (BCP).
- Justify security investments based on risk mitigation and operational impact.
- Demonstrate leadership in managing corporate security teams and crisis situations.

Target Audience

This program is designed for:

- Corporate Security Managers and Directors
- Physical Security Supervisors
- Facility and Asset Managers

- Risk and Compliance Officers
- Business Continuity Professionals
- Security Operations Center (SOC) personnel
- Executive Protection teams in corporate environments
- Contract security management professionals

Course Outline

DAY 1 – Corporate Risk & Physical Security Foundations

Corporate Security Risk Landscape

- Corporate threat categories:
  - Theft & fraud
  - Workplace violence
  - Insider threats
  - Civil unrest & protests
  - Corporate espionage
- Reputational risk & business impact
- Duty of care obligations

Corporate Security Risk Management Framework

- Risk formula: Threat × Vulnerability × Impact
- Enterprise Security Risk Management (ESRM) principles
- Risk appetite in corporate settings
- Risk registers & prioritization

Physical Security Layers in Corporate Facilities

- Layered security model:
  - Perimeter

    - Access control
    - Internal zoning
    - Critical asset protection
- Crime Prevention Through Environmental Design (CPTED)
- Corporate campus vs high-rise building security

Building Security Vulnerability Assessment

- Conducting a Physical Security Vulnerability Assessment (PSVA)
- Entry point mapping
- Guard post effectiveness
- Lighting, barriers, and sightlines
- Identifying single points of failure

Workshop

- Conduct a mock corporate HQ security assessment
- Identify top 10 vulnerabilities
- Develop mitigation recommendations

DAY 2 – Access Control, Surveillance & Tracking Systems

Corporate Access Control Systems

- Badge systems & smart cards
- Biometric systems (corporate application)
- Visitor management protocols
- Contractor/vendor access control
- Key & master key management

CCTV & Surveillance Strategy

- Camera placement strategy (not just coverage)

- Monitoring room best practices
- Evidence retention policies
- Privacy considerations in corporate settings

Tracking Technologies for Corporate Security

- GPS fleet tracking systems
- Executive vehicle tracking
- Asset tracking (RFID)
- Lone worker tracking apps
- Geofencing alerts

Security Operations Center (SOC)

- SOC structure in corporate environments
- Alarm monitoring & escalation procedures
- Incident logging platforms
- Integration of CCTV + access + tracking

Practical Exercise

- Design a corporate SOC layout
- Create alarm escalation flowchart
- Develop tracking policy for executives

DAY 3 – Movement Security, Civil Unrest & Executive Protection

Movement Risk in Urban & Unrest Environments

- Route risk assessments
- Intelligence gathering (open-source & local)
- Safe travel protocols for executives
- Protest mapping & avoidance

- Curfew & emergency regulation awareness

Journey Management Planning (Corporate Context)

- Pre-trip risk assessment checklist
- Travel approval systems
- Check-in protocols
- Safe hotel selection criteria
- Emergency contacts structure

Corporate Convoy & Secure Transport Basics

- When convoys are necessary (corporate context)
- Vehicle spacing & communications
- Breakdown protocols
- Emergency rerouting
- Low-profile movement strategy

Executive/VIP Protection in Corporate Settings

- Advance security planning
- Site advance checklist
- Secure arrival/departure procedures
- Protective formations (low-visibility approach)
- Board meeting & shareholder event security

Simulation

- Scenario: Executive trapped due to sudden civil unrest
- Participants develop extraction plan
- Group debrief & risk evaluation

DAY 4 – Incident Management, Reporting & Crisis Response

Corporate Incident Classification

- Security incidents vs safety incidents
- Near-miss reporting
- Workplace violence indicators
- Threatening communications

Writing Effective Incident Reports

- Objective reporting techniques
- Legal defensibility
- Evidence documentation
- Digital incident management systems

Incident Tracking & Trend Analysis

- Security dashboards
- KPI tracking (response times, incident frequency)
- Pattern identification
- Intelligence sharing within corporation

Crisis Response in Corporate Environment

- Active shooter awareness
- Bomb threat procedures
- Civil unrest spillover response
- Lockdown vs evacuation decision-making
- Media & communication coordination

Practical Exercise

- Write full incident report from scenario
- Conduct trend analysis

- Present corrective actions

DAY 5 – Strategic Corporate Security Leadership

Corporate Security Policy Development

- Security policy structure
- SOP development
- Guard force post orders
- Executive protection policy

Business Continuity & Security Integration

- Business Continuity Planning (BCP)
- Crisis management teams
- Coordination with HR, Legal, IT
- Duty of care compliance

Security Audits & Continuous Improvement

- Internal security audits
- Red teaming concepts (corporate)
- Lessons learned integration
- Budget justification for security upgrades

Leadership in Corporate Security

- Decision-making under pressure
- Managing contract security teams
- Ethical considerations
- Managing security during labor unrest

The Scandinavian Academy for Training and Development adopts the latest scientific and professional methodologies in training and human resource development, aiming to enhance the efficiency of individuals and organizations. Training programs are delivered through a comprehensive approach that includes:

- Theoretical lectures supported by PowerPoint presentations and visual materials (videos and short films).
- Scientific evaluation of participants before and after the program to measure progress and knowledge acquisition.
- Brainstorming sessions and practical role-playing to simulate real-life scenarios.
- Case studies tailored to align with the training content and participants work nature.
- Assessment tests conducted at the end of the program to evaluate the achievement of training objectives.

Each participant receives the training material (both theoretical and practical) in printed form and saved on a CD or flash drive. Detailed reports, including attendance records, final results, and overall program evaluations, are also provided.

Training materials are prepared professionally by a team of experts and specialists in various fields. At the end of the program, participants are awarded a professional attendance certificate, signed and accredited by the Scandinavian Academy for Training and Development.

Program Timings:

- 9:00 AM to 2:00 PM in Arab cities.
- 10:00 AM to 3:00 PM in European and Asian cities.

The program includes:

- A daily Coffee Break provided during the sessions to ensure participants comfort.