JUPITER PRIME

Consulting • Training • Advisory

جوبيتر برايم للاستشارات والتدريب

COURSE BROCHURE

# Advanced Corporate Security Management Training Course

11 – 22 July 2027
Cairo

**jupiterprime.uk**

info@jupiterprime.uk

Registered in the United Kingdom and Saudi Arabia

# Advanced Corporate Security Management Training Course

**Ref:** 458_16557 **Date:** 11 – 22 July 2027 **Location:** Cairo **Fees:** 6000 GBP

Corporate Security Management is an advanced 2-week training course for security managers, corporate security heads and facility security leads who must turn scattered guarding arrangements into a Corporate Security Management Plan that executives approve and sites follow. Threats to people, premises and operations now change faster than annual security reviews, and boards expect security spending to be justified by risk. Jupiter Prime Training delivers this course for practitioners already running security functions.

## Why Corporate Security Management Matters Now

Three forces shape corporate security today: executives who want security framed in business risk terms, converged threats that move between physical sites, people and supply chains, and contracted guard forces whose performance must be proven rather than assumed. An organisation that manages security well protects continuity and reputation at a defensible cost, while one that manages it badly spends on visible measures that leave real exposure untouched. The course rests on the Enterprise Security Risk Management ESRM guideline, the ISO 18788 management system for security operations and ISO 22341 guidance on Crime Prevention Through Environmental Design CPTED.

## Who Gains Most from Corporate Security Management

- Heads of corporate security accountable for strategy and budget across sites
- Facility security leads responsible for protecting a campus, plant or headquarters
- Security risk specialists who assess threats for asset owners
- Guard force managers who oversee outsourced security providers
- Resilience leads who link security incidents to crisis arrangements

A corporate security function that sends its head, a site lead and its contract manager together gains most, because they can agree one security risk register and one set of performance measures for every site they protect.

## Corporate Security Management Capabilities

Participants move from running guarding rosters to directing security as a managed business function that asset owners can question and fund.

- Assess security risks to people, assets and operations using an ESRM cycle — asset owners accepting or treating each risk
- Design layered protection that combines deterrence, detection, delay and response — site leaders choosing investment priorities
- Specify security policies, standards and post orders that guards and staff can apply — executives approving the policy framework
- Build guard force contracts with measurable service levels and audit rights — procurement and finance selecting providers
- Calculate security performance indicators and present them as a dashboard — boards judging whether protection is adequate
- Test incident response and escalation through tabletop exercises — crisis teams confirming readiness

## Key Corporate Security Management Terms

- Enterprise Security Risk Management ESRM — a risk-based approach in which security partners with asset owners to assess and treat security risks.
- Layered protection — physical, procedural and human measures arranged in rings so an intruder must defeat several barriers.
- Security risk register — a controlled record of each security threat, the asset it affects, its rating, its owner and the agreed treatment.
- Post orders — written instructions for each guard post describing duties, patrols and actions in defined situations.
- Deter, detect, delay, respond — the four functions a physical protection system performs to stop an attack before harm occurs.
- Security performance indicator — a measured value that shows whether security arrangements work as intended.

## Corporate Security Management Day by Day

## Day 1: The Corporate Security Mandate

- Security Function Charter — Defining Scope Across People, Premises and Operations
- Organisational Placement of Security — Choosing Reporting Lines and Authority
- Stakeholder Mapping of Asset Owners — Agreeing Who Accepts Security Risk
- Converged Threat Landscape — Linking Physical, Personnel and Supply Chain Exposure
- Security Maturity Self-Assessment — Setting the Baseline for Improvement

## Day 2: Enterprise Security Risk Management

- ESRM Cycle — Partnering With Asset Owners on Risk Decisions
- Critical Asset Identification — Ranking What the Organisation Cannot Lose
- Threat Actor Profiling — Matching Intent and Capability to Targets
- Vulnerability Surveys — Recording Weaknesses Site by Site
- Risk Rating Matrices — Prioritising Treatment Against Risk Appetite

## Day 3: Security Policy and Governance

- Security Policy Hierarchy — Linking Policy, Standards and Procedures
- Post Orders and Site Instructions — Turning Policy Into Daily Duties
- Security Committee Terms of Reference — Allocating Oversight Responsibilities
- Policy Exception Handling — Recording Accepted Deviations and Owners
- ISO 18788 Management System Clauses — Structuring Security Operations Evidence

## Day 4: Layered Physical Protection

- Deter, Detect, Delay, Respond Model — Sequencing Protective Measures
- Perimeter and Building Envelope Hardening — Choosing Barrier Standards
- CPTED Principles From ISO 22341 — Shaping Spaces to Discourage Crime
- Protection Zoning — Matching Controls to Asset Criticality
- Adversary Path Analysis — Testing Whether Delay Exceeds Response Time

## Day 5: Electronic Security Systems

- Access Control Architecture — Managing Credentials and Zone Permissions
- Video Surveillance Coverage Plans — Placing Cameras for Identification
- Intrusion Detection Selection — Balancing Sensitivity and Nuisance Alarms
- Security Control Room Design — Organising Alarm Handling and Dispatch
- System Integration and Maintenance Regimes — Keeping Technology Reliable

## Day 6: Managing the Guard Force

- In-House Versus Contracted Guarding — Weighing Control, Cost and Flexibility
- Security Service Specifications — Writing Duties Providers Can Price
- Service Level Agreements — Setting Measurable Guarding Standards
- Guard Selection, Vetting and Training Plans — Raising Officer Competence
- Contractor Performance Audits — Deciding on Remedy or Replacement

## Day 7: Personnel and Insider Risk

- Pre-Employment Screening Levels — Matching Checks to Role Sensitivity
- Insider Threat Indicators — Spotting Behaviour That Warrants Attention
- Visitor and Contractor Management — Controlling Temporary Access
- Executive Protection Assessments — Sizing Protective Arrangements for Leaders
- Travel Security Briefings — Preparing Staff for Higher-Risk Destinations

## Day 8: Incident Response and Investigations

- Security Incident Classification — Triggering the Right Level of Response
- Escalation and Notification Protocols — Linking Security to Crisis Teams
- Evidence Preservation at Scenes — Supporting Later Investigation
- Internal Investigation Planning — Scoping Interviews and Records
- Tabletop Exercises for Security Scenarios — Testing Plans Before Real Events

## Day 9: Measuring Security Performance

- Security Performance Indicators — Choosing Leading and Lagging Measures
- Security Audits and Inspections — Verifying Controls Against Policy
- Return on Security Investment Arguments — Framing Spend as Risk Reduction
- Board Security Dashboards — Reporting Posture in Business Language
- Continual Improvement Reviews — Feeding Lessons Into the Risk Register

## Day 10: Practising the Corporate Security Management Plan

- Applying the ESRM Risk Register — Setting Priorities for a Chosen Site
- Applying Layered Protection Design — Specifying Barriers, Systems and Guards
- Applying Guard Force Service Levels — Defining Contractor Expectations
- Applying Performance Indicators — Agreeing the Dashboard for Executives
- Corporate Security Management Plan — Presenting Risks, Measures, Owners and Budget

## Applying Corporate Security Management After the Course

- Lead an ESRM risk assessment of one critical site with its asset owners, producing a rated security risk register with agreed treatments and owners.
- Run a performance audit of the guard force contract against new service levels and present the findings with a remedy plan to procurement and the site leader.

## Corporate Security Management Questions FAQ

### What is corporate security management and why does it matter now?

Corporate security management is the discipline of protecting an organisation's people, premises and operations through risk-based policy, layered protection and managed guard forces. It matters now because threats change quickly and executives expect every security measure to be justified by risk.

### Which roles gain most from corporate security management training?

Heads of corporate security, facility security leads and security risk specialists gain most from corporate security management training. Guard force contract managers also benefit.

### How does advanced corporate security management differ from a cybersecurity leadership course?

Advanced corporate security management deals with physical, personnel and operational protection: barriers, guard forces, access control and site incidents. A cybersecurity leadership course focuses on networks, data and digital threats, so the two complement each other without overlapping.

## What do you bring back from corporate security management training?

You bring back a Corporate Security Management Plan for a real site or organisation. It sets out rated risks, layered measures, service levels and owners for executive approval.

## Corporate Security Management: The Way Forward

The Corporate Security Management Plan first informs which protective measures an executive committee funds and in what order. Security heads, site leads and contract managers use it to coordinate guarding, systems and policy changes. After its first quarter in use, revisit the risk ratings against recorded incidents and audit findings, in an energy plant or a hospital campus alike, so the plan keeps pace with real exposure.