CONCEPT

Security Management and Asset Protection: Physical Security, Integrated Systems and Guarding

1 – 5 February 2027
London - Central London four-star



Security Management and Asset Protection: Physical Security, Integrated Systems and Guarding

Ref: 154_10206 **Date:** 1 – 5 February 2027 **Location:** London - Central London four-star **Fees:** 25300 SAR

Introduction:

Security management fails quietly when guard posts, cameras, card readers and alarms are bought one at a time, never tied to a documented threat picture, and never tested against how an intruder would actually approach a site. Theft, unauthorised entry, sabotage and workplace violence then exploit the gaps between them. This Core Concept course gives security managers and supervisors a structured method to assess risk to people and physical assets, design layered protection, run guarding operations and measure performance. Each participant produces a Site Security Survey and Asset Protection Plan for a facility of their own.

Course Objectives:

- Conduct a security risk assessment that rates threat, vulnerability and consequence for the critical assets of a site using ISO 31000 principles
- Draft a security policy, organisation chart and post orders that define who protects what, when and how
- Design layered physical protection using the deter, detect, delay and respond model and CPTED principles
- Specify access control, CCTV and intrusion detection so that they operate as one integrated security system monitored from a control room
- Manage in-house and contracted guard forces through post orders, patrol plans, supervision checks and service level agreements
- Plan security incident reporting, internal investigations and security KPIs, and audit the security programme against its own policy

Target Audience:

- Managers responsible for the security function of a corporate campus, plant, hospital, hotel or retail estate
- Supervisors who lead guard shifts, control room operators and patrol teams
- Facility and property managers accountable for perimeter, building access and asset loss
- Contract managers who oversee outsourced security providers and their service levels
- Project and engineering leads who specify and commission electronic security systems
- Loss prevention and asset protection leads who investigate theft, fraud and shrinkage on site

Course Outline:

Day 1: Security Management Foundations and Security Risk Assessment

- Asset Identification and Criticality Ranking for People, Property and Operations
- Threat Assessment: Criminal, Insider, Activist and Hostile Reconnaissance Profiles
- Vulnerability Rating Against the Deter, Detect, Delay and Respond Model
- Consequence and Likelihood Scoring in an ISO 31000 Security Risk Register
- Security Survey Checklist and Current-State Baseline of a Site

Day 2: Security Policy, Organisation and Physical Protection Design

- Security Policy Statement, Roles and Reporting Lines for the Security Function
- Post Orders and Standard Operating Procedures for Security Posts
- Crime Prevention Through Environmental Design CPTED: Natural Surveillance, Territoriality and Access
- Perimeter Protection: Fencing, Vehicle Barriers, Gates and Security Lighting
- Protection-in-Depth Zoning from Outer Perimeter to Restricted Asset Rooms

Day 3: Integrated Security Systems: Access Control, CCTV and Intrusion Detection

- Electronic Access Control: Credentials, Card Readers, Biometrics and Anti-Passback Rules
- Visitor, Contractor and Vehicle Management Procedures at Entry Points
- CCTV Camera Placement for Detection, Recognition and Identification Views
- Intrusion Detection Sensors: Perimeter, Motion, Door Contact and Glass-Break Devices
- Security Control Room Layout, Alarm Handling Flow and Integration Matrix

Day 4: Guarding Operations, Investigations and Special Protection Cases

- Guard Force Sizing, Patrol Route Planning and Supervisory Checks
- Contracted Security Service Level Agreements and Provider Performance Reviews
- Security Incident Reporting, Evidence Preservation and Internal Investigation Interviews
- Critical Facility Protection: Utilities, Data Halls, Warehouses and Cash Handling Areas
- Executive Protection and Business Travel Security Planning at Overview Level

Day 5: Site Security Walkthrough and Asset Protection Plan

- Guided Inspection Walkthrough: Perimeter and Entry Point Vulnerability Scoring
- Guided Inspection Walkthrough: Control Room, Camera Coverage and Alarm Response Test
- Security KPI Dashboard: Incident Rates, Response Times and Patrol Compliance
- Security Programme Audit Checklist and Corrective Action Log
- Site Security Survey and Asset Protection Plan Build and Peer Review

Skills You Will Gain:

- Security Risk Assessment
- Security Survey Technique
- Layered Protection Design
- CPTED Application
- Integrated Security System Specification
- Guard Force Management
- Security Incident Investigation
- Security Performance Measurement

Why Attend This Course:

- Return with a Site Security Survey and Asset Protection Plan for a facility you are responsible for
- Justify security spending to management with a risk register that links each control to a rated threat
- Find the gaps between guarding, cameras, access control and alarms that single-system reviews overlook
- Compare security arrangements with peers from industrial, commercial, healthcare and hospitality sites

Conclusion:

Physical security works when people, procedures and technology are designed together around a clear view of what needs protecting and from whom. The course moves from asset and threat assessment through policy, CPTED and layered protection, to access control, CCTV and intrusion detection working as one integrated system, then to guarding, contracted security, investigations and critical facility protection. The final day applies it all in inspection walkthroughs and produces a Site Security Survey and Asset Protection Plan, with KPIs and an audit checklist to keep it under review.