JUPITER PRIME

Consulting • Training • Advisory

جوبيتر برايم للاستشارات والتدريب

COURSE BROCHURE

Advanced Security Planning and Integrated Asset Protection Course

jupiterprime.uk

info@jupiterprime.uk

Registered in the United Kingdom and Saudi Arabia

Advanced Security Planning and Integrated Asset Protection Course

Security Planning and Integrated Asset Protection is an advanced 2-week training course for security planners, asset protection managers and site security leads who must turn a design basis threat into a Strategic Security Plan tied to critical assets. New facilities, expansions and refurbishments now lock in protective choices for decades, so planning errors become expensive to reverse. Jupiter Prime Training offers this course to practitioners shaping protection before construction begins.

Why Security Planning and Integrated Asset Protection Matters Now

Three pressures shape security planning today: capital projects that fix protective requirements at concept stage, integrated platforms that merge access, video and intrusion data, and finance committees that compare proposals on whole-life cost. A site planned well receives proportionate protection built into its layout, while a site planned badly accumulates bolt-on measures, blind spots and maintenance bills. The course draws on ISO 22341 for Crime Prevention Through Environmental Design CPTED, the Enterprise Security Risk Management ESRM guideline for risk ownership and ISO 18788 for structuring security operations.

Who Gains Most from Security Planning and Integrated Asset Protection

- Security planners who write protective requirements for new builds and expansions
- Asset protection managers who decide which assets justify which level of protection
- Site security leads who must operate whatever the design teams install
- Facilities and engineering coordinators who integrate security into building services
- Capital project sponsors who approve security budgets and phasing

A project delivery group that sends its security planner, facilities engineer and future site security lead together gains most, because the people who specify, build and operate the protection agree its requirements before drawings are frozen.

Security Planning and Integrated Asset Protection Capabilities

Participants translate threat statements into layouts, specifications and phased budgets.

- Assess threats and vulnerabilities to set a design basis threat for each site — sponsors agreeing the protection level
- Design site layouts using CPTED surveillance, territoriality and access control principles — architects fixing the master plan
- Specify integrated access control, video and intrusion detection requirements — engineers preparing tender documents
- Calculate whole-life cost of protection options — finance committees approving budgets
- Weigh phased investment sequences against residual risk — project boards scheduling security works

- Communicate security requirements to design, operations and community stakeholders — planning approvals and handover

Key Security Planning and Integrated Asset Protection Terms

- Design basis threat — the adversaries, tactics and capabilities a site's protection is designed to defeat.
- Security master plan — a long-range plan that locates protective zones, routes, barriers and systems across a site.
- CPTED — Crime Prevention Through Environmental Design, shaping spaces so natural surveillance discourages crime.
- Standoff distance — the clear space kept between a protected building and the closest point a vehicle threat can reach.
- Physical security information management PSIM — software that combines alarms, video and access events into one operator view.
- Whole-life cost — the total cost of a protective measure across purchase, installation, operation, maintenance and replacement.

Security Planning and Integrated Asset Protection Day by Day

Day 1: Planning Context and Critical Assets

- Asset Criticality Registers — Ranking Facilities, Processes and People to Protect
- Security in the Project Lifecycle — Fixing Requirements at Concept Stage
- Stakeholder Requirements Capture — Balancing Operations, Visitors and Neighbours
- Planning Assumptions Log — Recording Constraints Before Design Starts
- Security Planning Brief — Defining Scope for the Design Team

Day 2: Threat and Vulnerability Assessment

- Design Basis Threat Statements — Setting the Adversary the Site Must Resist
- Threat Scenario Libraries — Covering Theft, Sabotage, Intrusion and Vehicle Attack
- Site Vulnerability Surveys — Recording Approaches, Sightlines and Weak Points
- Consequence Rating Tables — Linking Loss to Operational Impact
- Risk Ranking for Planning — Choosing Which Scenarios Drive Design

Day 3: Site Master Planning

- Security Zoning Hierarchies — Grading Public, Controlled and Restricted Areas
- Circulation and Route Planning — Separating Visitors, Staff and Deliveries
- Standoff and Setback Planning — Locating Buildings Against Vehicle Threats
- Perimeter Line Selection — Choosing Fence, Wall and Natural Boundaries
- Security Master Plan Drawings — Communicating Zones to Architects

Day 4: CPTED and Environmental Design

- Natural Surveillance Principles From ISO 22341 — Opening Sightlines Across Spaces
- Territorial Reinforcement — Signalling Ownership Through Landscaping and Edges
- Lighting Design for Security — Supporting Identification at Night
- Landscaping and Street Furniture Choices — Removing Concealment Opportunities
- CPTED Design Reviews — Testing Drawings Before Approval

Day 5: Barriers and Building Hardening

- Hostile Vehicle Mitigation Layouts — Placing Bollards, Planters and Gates
- Building Envelope Protection — Selecting Doors, Glazing and Wall Ratings
- Delay Calculations — Matching Barrier Times to Guard Response
- Secure Rooms and Vaults — Protecting High-Value Assets Inside Buildings
- Mail and Loading Bay Screening Areas — Isolating Inbound Threats

Day 6: Integrated Security Systems

- Access Control Zoning — Mapping Credentials to Security Zones
- Video Surveillance Specifications — Defining Detect, Observe and Identify Views
- Intrusion Detection Layering — Combining Perimeter and Internal Sensors
- PSIM Platform Requirements — Uniting Alarms Into One Operator View
- Network and Power Resilience for Security Systems — Avoiding Single Points of Failure

Day 7: Procurement and Commissioning

- Security Specification Writing — Turning Requirements Into Tender Clauses
- Vendor Evaluation Matrices — Comparing System Bids Fairly
- Factory and Site Acceptance Tests — Proving Systems Before Handover
- Commissioning Records and As-Built Documents — Preparing for Operation
- Handover to Operations — Transferring Systems to Site Security Teams

Day 8: Security Budgeting and Investment

- Whole-Life Cost Models — Comparing Capital and Running Costs
- Staffing Versus Technology Trade-Offs — Choosing the Protection Mix
- Phased Capital Plans — Sequencing Works Against Residual Risk
- Cost-Benefit Arguments for Protection — Presenting Value to Finance Committees
- Maintenance and Refresh Budgets — Keeping Systems Effective Over Time

Day 9: Plan Integration and Resilience

- Emergency Egress Versus Security Conflicts — Reconciling Life Safety and Access
- Business Continuity Interfaces — Protecting Recovery Sites and Critical Spares
- Operational Security Procedures — Aligning Post Duties With the Design
- ISO 18788 Planning Elements — Structuring Objectives, Resources and Controls
- Plan Verification Exercises — Walking Scenarios Through the Proposed Layout

Day 10: Practising the Strategic Security Plan

- Applying the Design Basis Threat — Confirming Scenarios for a Chosen Site
- Applying the Security Master Plan — Presenting Zones, Routes and Barriers
- Applying Integrated System Requirements — Linking Sensors to Response
- Applying Whole-Life Cost Models — Justifying the Phased Budget
- Strategic Security Plan — Linking Protective Measures to Critical Assets

Applying Security Planning and Integrated Asset Protection After the Course

- Lead a design basis threat session for a planned facility or expansion, producing agreed threat scenarios and protection levels for the design team.
- Run a CPTED and standoff review of current site drawings and issue a marked-up security master plan with recommended changes to the project sponsor.

Security Planning and Integrated Asset Protection Questions FAQ

What is security planning and integrated asset protection and why does it matter now?

Security planning and integrated asset protection designs barriers, layouts and systems around critical assets before facilities are built or changed. It matters now because capital projects fix protective choices for decades and late changes are costly.

Which roles gain most from security planning and integrated asset protection training?

Security planners, asset protection managers and site security leads gain most from security planning and integrated asset protection training.

How does security planning and integrated asset protection differ from a corporate security management course?

Security planning and integrated asset protection focuses on design: threats, layouts, CPTED, barriers, systems and budgets for a site. A corporate security management course focuses on running an established security function, its policies, guard forces and performance reporting.

What do you bring back from security planning and integrated asset protection training?

You bring back a Strategic Security Plan for a real or planned site. It links a design basis threat to zones, barriers, systems and a phased budget.

Security Planning and Integrated Asset Protection: The Way Forward

The Strategic Security Plan first informs which protective requirements enter the design brief and which are phased for later investment. Security planners, engineers and sponsors use it to coordinate drawings, tenders and budgets. After the first design review, revisit the design basis threat against what operations teams observe, whether at a logistics hub or a university campus, so the plan stays proportionate to real exposure.