Facility and Asset Physical Security Management Course

30 May – 3 June 2027
Nairobi

AGILE LEADERS
Training Center

AGILE LEADERS
Training Center

Facility and Asset Physical Security Management Course

Ref: 998_175888 **Date:** 30 May – 3 June 2027 **Location:** Nairobi **Fees:** 4500 Euro

Overview

Facility and Asset Physical Security Management Course is a one-week advanced course for physical security managers, facilities leaders, asset protection teams, security operations supervisors, risk managers, and site managers. Participants develop an Integrated Facility Security Plan that connects asset criticality, threat and vulnerability assessment, layered protection, access control, detection, guard operations, incident response, assurance, and performance review. Agile Leaders Training Center develops practical capability in facility and asset physical security management.

Who Should Attend

- Physical security managers responsible for protection strategy, controls, and assurance
- Facilities and site leaders accountable for buildings, equipment, people, and operations
- Asset protection and security operations teams managing daily protective measures
- Risk and resilience professionals coordinating security, incidents, and continuity
- Contract and supplier managers overseeing guards, technology, and maintenance services

The course assumes participants already hold operational or managerial responsibility for facilities, assets, risk, security systems, or protective services. It leaves out entry-level guarding instruction, weapons training, and certification examination preparation.

Departments and Industries

The course supports organizations that require controlled access, dependable detection, coordinated response, and evidence-based protection of people and assets.

- Facilities, workplace, property, and corporate real estate
- Security, asset protection, risk, resilience, and business continuity
- Energy, utilities, manufacturing, logistics, and transport facilities
- Healthcare, education, hospitality, retail, and public facilities
- Data centers, telecommunications, warehouses, and corporate campuses
- Government, infrastructure, engineering, and outsourced security services

Learning Objectives

By the end of this course, participants will be able to:

- Prioritize facilities and assets using criticality, threat, vulnerability, and consequence evidence
- Conduct a structured physical security risk assessment and site security survey
- Design layered facility security across perimeter, zones, entries, and critical rooms
- Specify access, surveillance, intrusion detection, lighting, and control-room requirements
- Coordinate guard operations, incidents, continuity interfaces, suppliers, and maintenance
- Build measures, tests, corrective actions, and an Integrated Facility Security Plan

AGILE LEADERS
Training Center

Course Agenda

Day 1: Governance, Assets, Threats, and Site Assessment

- Facility Asset and Criticality Register
- Threat, Vulnerability, and Consequence Assessment
- Physical Security Risk and Treatment Matrix
- Security Roles and Decision-Rights Map
- Site Security Survey and Evidence Log

Day 2: Layered Protection, Perimeter, and Access

- Layered Protection and Security-Zone Model
- Perimeter Barrier and Entry-Control Plan
- Pedestrian, Vehicle, and Delivery Screening Map
- Visitor and Contractor Access Workflow
- Key, Credential, and Privilege Control Register

AGILE LEADERS
Training Center

Day 3: Detection, Surveillance, and Control Rooms

- Security Lighting Coverage Assessment
- Video Surveillance Purpose and Camera Plan
- Intrusion Detection and Alarm-Zone Map
- Security Control Room Event and Escalation Protocol
- Security System Testing and Maintenance Schedule

Day 4: Guard Operations, Incidents, and Assurance

- Guard Post, Patrol, and Response Plan
- Incident Classification and Notification Matrix
- Evidence Preservation and Handover Checklist
- Emergency and Business Continuity Interface Map
- Security Supplier Performance and Assurance Scorecard

Day 5: Facility Physical Security Simulation

- Exercise: Threat and Vulnerability Prioritization
- Exercise: Perimeter and Access Control Breach
- Exercise: Alarm, Control Room, and Guard Response
- Exercise: Incident, Continuity, and Supplier Tradeoff
- Capstone Exercise: Integrated Facility Security Plan

AGILE LEADERS
Training Center

Practical Exercises

The course uses suggested activities that connect protection decisions with facility conditions, asset value, threats, operating needs, system performance, and response capability.

- Suggested activity: complete a physical security risk assessment for a representative facility
- Suggested activity: map a layered facility security design from perimeter to critical asset
- Suggested activity: test access, alarm, control-room, and guard-response handoffs
- Suggested activity: assemble an Integrated Facility Security Plan and assurance schedule

FAQs

Who suits facility and asset physical security management training?

Facility and asset physical security management training suits experienced personnel responsible for facilities, protection programs, asset security, site operations, risk, resilience, control rooms, guarding contracts, or security technology. Participants should understand their organization's sites and operating priorities.

What does a physical security risk assessment examine?

A physical security risk assessment identifies important people, property, information, equipment, and operations; considers credible threats; examines vulnerabilities and existing controls; evaluates consequences and response capability; and prioritizes proportionate treatments with accountable owners.

How does layered facility security work?

Layered facility security places coordinated deterrence, detection, delay, access, and response measures from the wider site and perimeter through controlled zones to the asset. Each layer should support the next without creating unmanaged operational or safety risks.

What should a site security survey record?

A site security survey should record boundaries, approaches, entrances, vehicle and pedestrian flows, deliveries, visitors, critical rooms, keys and credentials, lighting, surveillance, alarms, control-room arrangements, guard deployment, emergency interfaces, defects, evidence, and recommended actions.

AGILE LEADERS
Training Center

How should security systems and suppliers be assured?

Assurance should define performance requirements, acceptance tests, inspection and maintenance schedules, alarm and response tests, fault escalation, service levels, evidence retention, supplier reviews, corrective actions, and measures that connect control performance with current risks.

What belongs in an Integrated Facility Security Plan?

An Integrated Facility Security Plan should connect asset priorities, threats, vulnerabilities, protection layers, access rules, technology, guarding, incidents, continuity, suppliers, maintenance, testing, metrics, ownership, resources, review triggers, and a controlled improvement roadmap.

Conclusion

Participants leave with an Integrated Facility Security Plan grounded in asset criticality, site evidence, layered protection, operational controls, coordinated response, testing, suppliers, and measurable assurance. The plan gives security and facilities leaders a practical basis for proportionate investment, reliable operations, and continuous review as threats, assets, and operating conditions change.