



Critical Infrastructure Protection, Facility Security & Crisis Management

9 – 13 November 2026
Kuala Lumpur

Critical Infrastructure Protection, Facility Security & Crisis Management

Ref: 808_161399 **Date:** 9 – 13 November 2026 **Location:** Kuala Lumpur **Fees:** 5200 Euro

Course Overview

A five-day practical course integrating critical infrastructure protection, facility security, emergency preparedness, crisis command, and business continuity. Participants apply CISA, FEMA, OSHA, and international practices to protect people, assets, information, and essential operations.

Target Audience

Security, facility, infrastructure, SOC, intelligence, emergency, crisis, risk, continuity, HSE, and operations professionals.

Targeted Organizational Departments

Security; Risk and Compliance; Emergency and Crisis Management; Facilities; Intelligence; Business Continuity; HSE; Government Coordination.

Targeted Industries

Government, defense, energy, utilities, transport, finance, data centers, telecoms, healthcare, manufacturing, logistics, education, and high-security facilities.

Course Offerings

- Assess threats, vulnerabilities, assets, and layered controls.
- Plan perimeter, access, surveillance, alarms, and readiness.
- Use intelligence, early warning, reporting, and secure handling.
- Coordinate authorities, evacuation, command, and crisis teams.
- Integrate continuity, recovery, exercises, and corrective action.

Training Methodology

Concise instruction, case studies, workshops, scenarios, and FEMA HSEEP-inspired tabletop exercises develop practical decisions, coordination, continuity, and after-action improvement.

Course Toolbox

- Risk, vulnerability, critical-asset, and security-plan tools
- Perimeter, access, CCTV, alarm, readiness, and escalation tools
- Threat, incident, information-handling, and emergency checklists
- ICS, evacuation, crisis-team, continuity, HSEEP, and review tools

Note: These tools and frameworks are introduced through guidance, demonstrations, examples, and practical discussions. Specialized security equipment, licensed software, and operational systems are not provided as part of the course.

Course Agenda - 5 Days

Day 1: Facility Protection

- Critical infrastructure protection
- Layered security
- Perimeter defense
- Access control
- Surveillance and alarms
- Asset and information protection
- **Reflection & Review:** Vulnerabilities and controls

Day 2: Planning and Risk

- Facility security plans
- Threat assessment
- Vulnerability priorities
- Readiness levels
- Governance and roles
- Risk mitigation
- **Reflection & Review:** Protection planning

Day 3: Intelligence and Coordination

- Threat intelligence
- Source verification
- Early warning
- Secure information handling
- Incident reporting
- Authority coordination
- **Reflection & Review:** Alerts and information sharing



Day 4: Response and Continuity

- Emergency plans
- Evacuation and shelter
- Fire and hazard response
- Incident command
- Business continuity
- Resource mobilization
- **Reflection & Review:** Response and recovery priorities

Day 5: Exercises and Evaluation

- Scenario design
- Access-breach exercise
- Suspicious-activity simulation
- Fire and evacuation exercise
- Disruption simulation
- After-action improvement
- **Reflection & Review:** Outcomes and corrective actions

FAQ

Are prerequisites required?

No formal qualification is required; relevant experience helps.

How long is the course?

Five days, normally four to five instructional hours daily.

What is integrated?

Preventive facility security with coordinated response, recovery, and continuity.

How This Course is Different from Other Similar Courses

It covers the complete protection cycle - safeguards, risk, intelligence, command, response, recovery, and improvement - through realistic scenarios and structured evaluation.