Corporate Security Leadership: Threat Assessment, Protection and Response Course

6 – 10 December 2026
Manama

Corporate Security Leadership: Threat Assessment, Protection and Response Course

Ref: 135_15077 **Date:** 6 – 10 December 2026 **Location:** Manama **Fees:** 4300 GBP

Programme Summary

Corporate security leadership, threat assessment, protection and response is a one-week training course for heads of corporate and facility security at advanced level, culminating in a site security strategy and operating plan. Security functions are often judged on guard hours and camera counts rather than on how well they reduce credible threats to people, assets and operations. The approach moves from threat and risk assessment to protective design, then to security operations, incident response and performance management. Mars Training Centre UK delivers this programme in corporate security leadership and threat assessment.

The Business Case

When protective measures are bought without a threat assessment, organisations overspend on visible controls, leave real vulnerabilities open and struggle to justify the security budget. Untested response plans turn minor incidents into losses and reputational damage. A risk-based security programme lets leaders show the board what each measure protects and why.

- Security Risk Exposure: Falls as credible threats are assessed and matched with layered, tested controls.
- Security Cost Effectiveness: Improves as spending on guarding and technology follows risk priority.
- Incident Impact: Reduces as detection, escalation and response are rehearsed and measured.

Principles and Evidence Base

- ISO 18788 Security Operations Management System: Structures the planning, control and evaluation of security operations in Session 3 and Session 5.
- ISO 31000 Risk Management: Provides the risk assessment and treatment logic applied to security threats in Session 1.
- Deter, Detect, Delay, Respond Model: Shapes the layered protective design evaluated in Session 2.
- Crime Prevention Through Environmental Design CPTED: Guides site layout, lighting, natural surveillance and territorial measures in Session 2.

Intended Participants

- Leaders accountable for the protection of people, sites and assets across an organisation.
- Managers who direct guard forces, contractors and security control rooms.
- Heads of facilities who specify access control and electronic security systems.
- Leaders who coordinate security incident response with emergency and crisis teams.

The programme serves energy and utilities, government facilities, banking and hospitality.

Learning Outcomes

1. Participants will be able to construct a security threat and vulnerability assessment for a site.
2. Participants will be able to evaluate protective designs using layered deter, detect, delay and respond principles.
3. Participants will be able to specify access control and electronic security requirements that match assessed risks.
4. Participants will be able to design guard force and security operations centre procedures with clear escalation.
5. Participants will be able to diagnose weaknesses in security incident response and investigation practice.
6. Participants will be able to justify a security operating plan and performance metrics to senior management.

Programme Structure

Day 1: Corporate Security Threat Assessment

Which threats matter most to the organisation, and how vulnerable is each site?

- Corporate Security Mandate and Governance Structure
- Threat Identification and Adversary Profiling
- Asset Criticality and Consequence Ranking
- Vulnerability Survey Methods and Site Walkdowns
- ISO 31000 Security Risk Register and Treatment Options

Day 2: Protective Design and Physical Security

How are layered physical measures designed so that intruders are detected and delayed before harm occurs?

- Deter, Detect, Delay, Respond and Defence in Depth
- CPTED Principles for Layout, Lighting and Natural Surveillance
- Perimeter, Barrier and Vehicle Mitigation Measures
- Access Control, Identity Management and Visitor Processes
- CCTV, Intrusion Detection and System Integration Requirements

Day 3: Security Operations Management

How are people, procedures and the control room organised to deliver protection every shift?

- ISO 18788 Operational Planning and Control
- Guard Force Deployment, Post Orders and Patrol Design
- Security Operations Centre Roles, Alarms and Escalation
- Contract Security Provider Selection and Oversight
- Personnel Security and Insider Threat Controls

Day 4: Security Incident Response and Investigations

How does the security function respond to, investigate and learn from incidents?

- Security Incident Classification and Response Plans
- Bomb Threat, Intrusion and Workplace Violence Procedures
- Interface with Emergency, Crisis and Business Continuity Teams
- Internal Investigation Process and Evidence Handling
- Post-Incident Review and Lessons Learned

Day 5: Security Performance and Operating Plan

How are threats, controls and operations combined into one plan that management can approve?

- Security Performance Metrics and Assurance Reporting
- Applied Threat Assessment for a Participant Site
- Applied Protective Layer Review Against Assessed Threats
- Applied Control Room and Response Procedure Test
- Site Security Strategy and Operating Plan Completion

Methodology

The programme relies on case analysis of security incidents across energy, government and commercial sites, with structured exercises and tabletop simulation. Participants assess threats, critique protective layouts, test control room escalation and run an incident response scenario.

- Suggested activity: Conducting a vulnerability walkdown of a sample facility plan.
- Suggested activity: Redesigning a perimeter and access layout using CPTED principles.
- Suggested activity: Running a tabletop exercise for an intrusion during a night shift.

Capstone Output

Each participant completes a site security strategy and operating plan. It sets out the threat assessment, prioritised risks, protective layers, technology and guarding requirements, control room procedures, incident response arrangements and performance metrics, ready for approval by senior management.

Frequently Asked Questions

Is corporate security leadership training suitable for managers new to a head of security role?

Yes, if you already manage security or facilities teams. It assumes operational security experience, but no prior training in threat assessment or security management systems.

Which standards support corporate security leadership and threat assessment?

It draws on ISO 18788 for security operations management, ISO 31000 for risk management, the deter, detect, delay, respond model and crime prevention through environmental design.

How is the corporate security operating plan used at work?

You can use it to justify security priorities and budgets to senior management, brief guard providers and track performance.

How does corporate security leadership differ from cybersecurity management programmes?

It addresses physical, personnel and operational security of people, sites and assets, rather than the protection of networks, systems and data.