
Frontline Security Operations Leadership: Guard Deployment, Post Orders and Escalation Course

1 – 5 November 2026
Kuala Lumpur





Frontline Security Operations Leadership: Guard Deployment, Post Orders and Escalation Course

Ref: 344_22165 **Date:** 1 – 5 November 2026 **Location:** Kuala Lumpur **Fees:** 4000 GBP

Programme Summary

Security operations leadership, covering guard deployment, post orders and escalation, is the subject of this five-day training course for security managers and heads of security operations, ending in a site security operating pack for one site. Guard forces are often run on habit, with post orders out of date and incidents escalated late. The programme moves from the risk basis of a security operation and diagnosis of coverage, through deployment and plan design, to escalation and performance review, then to a worked operating pack. Mars Training Centre UK delivers this programme in security operations leadership.

The Business Case

When supervisors cannot show where guards are, what they have been told to do and how an incident reaches a decision-maker, losses go unexplained and contractors cannot be challenged. Leaders who deploy from risk, keep post orders current and rehearse escalation can show owners what the guard budget buys.

- Incident Response Time: Shortens as escalation routes and decision points are agreed before an incident.
- Coverage Reliability: Improves as shift patterns and patrols are audited against the site risk register.
- Contractor Performance Control: Becomes measurable as post orders are written into guard requirements.

Principles and Evidence Base

- ISO 18788: Its requirements and guidance for operational planning and control, risk assessment and monitoring structure the programme from Session 1 to Session 4.
- Plan-Do-Check-Act cycle: This management system loop organises the review and improvement work of Session 4.
- Risk-based control: Setting deployment in proportion to assessed threat and vulnerability shapes the design work of Session 3.
- Human factors in vigilance: Evidence on fatigue and handover error informs the diagnosis in Session 2.

Intended Participants

- Security managers who deploy guard forces and answer for site coverage.
- Heads of security operations who set post orders, site plans and escalation rules.
- Shift and control room leaders who brief teams and manage incidents.
- Contract managers who specify and review guard services supplied by third parties.

The programme serves corporate campuses, port operators, healthcare providers and public venues.



Learning Outcomes

1. Participants will be able to evaluate the risk basis of a security operation against the planning and control expectations of ISO 18788.
2. Participants will be able to diagnose gaps in guard coverage, vigilance and handover on a live site.
3. Participants will be able to construct a risk-based deployment model and a set of post orders.
4. Participants will be able to design a site security plan with access rules.
5. Participants will be able to prioritise incidents and justify an escalation ladder for a site.
6. Participants will be able to justify a site security operating pack and its indicators to a head of security.

Programme Structure

Day 1: Security Operations Leadership and Risk Basis

What does a security operation owe the organisation, and how is its risk basis set?

- ISO 18788 Operational Planning and Control
- Site Threat and Vulnerability Register
- Security Mission and Authority Statement
- Use of Force and Duty of Care Limits
- Peer Review of Two Site Security Models

Day 2: Diagnosing Guard Force Capability and Coverage

Where do coverage, vigilance and supervision fall short on a live site?

- Post Coverage and Shift Pattern Audit
- Human Factors in Guard Vigilance
- Guard Competence and Training Matrix
- Patrol Route and Checkpoint Review
- Control Room Log and Handover Analysis

Day 3: Designing Deployment, Post Orders and Site Plans

How are guards deployed and instructed so that the site plan works in practice?

- Risk-Based Guard Deployment Model
- Post Order Drafting Template
- Site Security Plan Structure
- Access Control and Visitor Rules
- Contractor and Subcontractor Guard Requirements



Day 4: Escalation, Incident Control and Performance Review

How does an incident move from the post to a decision-maker, and how is the operation improved afterwards?

- Incident Escalation Ladder
- Shift Briefing and Debrief Protocol
- Incident Report and Evidence Handling
- Performance Indicator Dashboard
- Plan-Do-Check-Act Improvement Log

Day 5: Applying Security Operations Leadership to One Site

Is the site operating pack ready for a head of security to adopt?

- Applying the Session 2 Coverage Audit to the Chosen Site
- Testing Session 3 Deployment Against Risk
- Rehearsing the Session 4 Escalation Ladder
- Setting Review Indicators for the Site
- Completing the Site Security Operating Pack

Methodology

The programme is built around case analysis and structured exercises. Participants work in small teams on anonymised site records from campus, port and healthcare settings, audit shift logs, draft post orders and rehearse escalation.

- Suggested activity: Auditing a week of shift logs and listing coverage gaps.
- Suggested activity: Rewriting an out-of-date post order so that a new guard can act on it.
- Suggested activity: Walking an incident through the escalation ladder and timing handovers.

Capstone Output

Each participant completes a site security operating pack for one site. It holds a coverage audit summary, a deployment model, post orders, an escalation ladder and review indicators. It is used to brief shift leaders and instruct guard contractors.

Frequently Asked Questions

Is security operations leadership suitable for managers who have not led a guard force before?

Yes. Security operations leadership is set at managerial level and assumes familiarity with site security routines, not prior command of a guard force.



Which standard does security operations leadership rest on in this training?

Security operations leadership rests on ISO 18788 for operational planning, control and monitoring, with the Plan-Do-Check-Act cycle and risk-based deployment.

How is the operating pack from security operations leadership used at work?

You use the pack from security operations leadership to brief shift leaders, issue post orders and instruct guard contractors.

How does security operations leadership differ from a corporate security strategy programme?

Security operations leadership centres on guards, posts and incident escalation on a site, while a corporate security strategy programme centres on threat policy and governance.