Counter-Terrorism Preparedness and Response Management Training Course for Security Leaders

31 October – 4 November 2027
Kuala Lumpur

Counter-Terrorism Preparedness and Response Management Training Course for Security Leaders

Ref: 2481_88570 **Date:** 31 October – 4 November 2027 **Location:** Kuala Lumpur **Fees:** 4000 GBP

Programme Summary

Counter-terrorism preparedness and response management is the subject of this one-week training course for security leaders at managerial level, ending in an organisational terrorism preparedness and response plan. Organisations that host the public, run critical services or employ staff in higher-risk locations must show that they have assessed the threat, protected people and assets proportionately and prepared to respond and recover. The programme moves from threat awareness to risk assessment, protective planning, incident response and recovery. Mars Training Centre UK delivers this programme on counter-terrorism preparedness and response management.

The Business Case

A terrorist incident affecting staff, visitors or operations tests every part of an organisation at once: security, safety, communications, leadership and continuity. Organisations that have rehearsed decisions in advance protect people better, restore services sooner and face less reputational damage. Preparedness is also increasingly expected by boards, insurers, partners and the public, who want evidence that reasonable steps were taken.

- Exposure of people and assets, reduced through proportionate protective measures based on assessed threat
- Time to an effective response, shortened by clear roles, alerting and rehearsed decisions
- Service recovery time, improved by linking security plans to continuity and welfare arrangements

Principles and Evidence Base

- The prevent, protect, prepare and respond logic common to public counter-terrorism strategies structures the programme from threat awareness to recovery.
- Risk management principles of likelihood, impact and proportionate treatment are applied to terrorism scenarios and protective decisions.
- Layered protective security, or defence in depth, guides how physical, personnel and information measures combine.
- Incident command and crisis management models shape roles, escalation and decision-making during a response.

Intended Participants

- Leading security for sites, venues, campuses or estates that receive staff and the public
- Owning security risk assessments and recommending protective investment to senior management
- Coordinating emergency, crisis or continuity arrangements with public responders and partners
- Briefing executives and boards on threat, exposure and preparedness

The programme suits security, risk and resilience functions in government, energy and utilities, transport, hospitality, retail and healthcare.

Learning Outcomes

1. Participants will be able to interpret threat information and assess its relevance to their organisation.
2. Participants will be able to construct a terrorism risk assessment for a site or operation.
3. Participants will be able to prioritise proportionate protective security measures across people, places and information.
4. Participants will be able to design alerting, response and escalation arrangements for a terrorist incident.
5. Participants will be able to evaluate recovery, welfare and communication needs after an incident.
6. Participants will be able to justify a counter-terrorism preparedness plan to senior decision-makers.

Programme Structure

Day 1: Counter-Terrorism Threat Awareness

How do global and domestic terrorism threats translate into risk for an organisation?

- Terrorism Threat Landscape and Trends
- Radicalisation Pathways and Early Warning Signs
- Threat Levels and Intelligence Sources
- Prevent, Protect, Prepare and Respond Logic
- Organisational Roles in Counter-Terrorism

Day 2: Terrorism Risk Assessment

How is terrorism risk to a site or operation assessed and ranked?

- Asset and Crowded Place Identification
- Attack Scenario Selection for Planning
- Vulnerability Assessment Methods
- Likelihood and Impact Rating
- Security Risk Register and Treatment Options

Day 3: Protective Security Planning

Which proportionate measures protect people, places and information?

- Layered Protective Security Design
- Hostile Reconnaissance Deterrence and Detection
- Personnel Security and Insider Risk
- Security Culture and Staff Awareness
- Protective Investment Business Cases

Day 4: Incident Response and Recovery

How does an organisation respond to and recover from a terrorist incident?

- Alerting, Invacuation and Evacuation Decisions
- Incident Command Roles and Escalation
- Liaison with Emergency Services
- Crisis Communications and Media Handling
- Staff Welfare and Business Recovery

Day 5: Applying the Preparedness Plan

How are the earlier sessions combined into a tested organisational plan?

- Tabletop Exercise on a Multi-Site Scenario
- Exercise Debrief and Lessons Identified
- Plan Maintenance and Review Cycle
- Executive Briefing on Preparedness Gaps
- Completing the Terrorism Preparedness and Response Plan

Methodology

The programme combines case analysis of published incident reviews with structured exercises and a facilitated tabletop simulation. Cases are drawn from transport, hospitality and public venues so that participants compare different operating contexts. Each session adds a section to the capstone plan, reviewed by peers.

- Suggested activity: rank three attack scenarios for a sample venue using a likelihood and impact matrix
- Suggested activity: map protective layers for a site and identify gaps
- Suggested activity: run the first hour of an incident as an incident command team

Capstone Output

Each participant completes a terrorism preparedness and response plan for one site or operation. It contains a threat summary, a risk assessment, a set of prioritised protective measures, response roles and alerting arrangements, and a recovery and exercise schedule. It serves as the basis for management approval and the next live exercise.

Frequently Asked Questions

Is counter-terrorism preparedness training suitable for managers new to security?

It suits managers who already hold security, risk or resilience responsibilities. It assumes familiarity with basic risk assessment but no prior counter-terrorism experience.

Which models does counter-terrorism preparedness and response management rest on?

It rests on the prevent, protect, prepare and respond logic, risk management principles, layered protective security and incident command and crisis management models.

How is the counter-terrorism preparedness plan used at work?

You use it to seek approval for protective measures, assign response roles, brief executives and plan the next exercise with partners and emergency services.

How does counter-terrorism preparedness differ from general crisis management training?

General crisis management covers all hazards. This programme focuses on terrorism threat, risk assessment and protective security, then links them to response and recovery.