
Critical Infrastructure Resilience: Risk Assessment, Continuity and Crisis Leadership Course

17 – 21 January 2027
Kuala Lumpur





Critical Infrastructure Resilience: Risk Assessment, Continuity and Crisis Leadership Course

Ref: 284_20124 **Date:** 17 – 21 January 2027 **Location:** Kuala Lumpur **Fees:** 4000 GBP

Programme Summary

Critical infrastructure resilience is the subject of this one-week training course for senior officials, asset owners and continuity leaders at strategic level, ending in a critical infrastructure resilience plan for one essential service. Energy, water, transport and communications services depend on one another, and a failure in one spreads quickly to the others. The approach moves from identifying critical assets and dependencies, through risk assessment and protective measures, to continuity planning and crisis leadership. Mars Training Centre UK delivers this programme in critical infrastructure resilience.

The Business Case

When essential services fail, the cost falls on citizens, regulators and the organisations that depend on them. Organisations that know which assets matter most, how services depend on each other and who decides during a disruption can limit the harm and restore service sooner.

- Service Disruption Time: Falls as recovery priorities, alternative arrangements and tested continuity plans are agreed in advance.
- Unmanaged Risk Exposure: Reduces as threats, vulnerabilities and dependencies are assessed and ranked consistently.
- Decision Speed in Incidents: Improves as roles, escalation routes and communication lines are rehearsed.

Principles and Evidence Base

- ISO 31000: Its risk management process structures the identification, analysis and evaluation work in Sessions 2 and 3.
- ISO 22301: Its business continuity management requirements shape the impact analysis and recovery strategies in Session 4.
- Critical Entities Resilience Directive: Its sequence of identifying critical entities, assessing risk, taking resilience measures and reporting incidents guides the programme logic from Session 1 to Session 5.

Intended Participants

- Officials who set policy or standards for the protection of essential services.
- Asset owners and operators who are accountable for the continuity of a critical service.
- Risk, security and emergency planning leaders who coordinate protective measures.
- Continuity and crisis managers who lead the response when services are disrupted.

The programme serves government ministries, utilities, transport operators and telecommunications providers.



Learning Outcomes

1. Participants will be able to classify the assets and services that are critical to a national or sector function.
2. Participants will be able to construct a dependency map that shows how failures spread between sectors.
3. Participants will be able to evaluate threats and vulnerabilities and rank the resulting risks.
4. Participants will be able to prioritise protective and resilience measures against cost and consequence.
5. Participants will be able to design continuity and recovery arrangements for an essential service.
6. Participants will be able to justify a critical infrastructure resilience plan to a board or ministry.

Programme Structure

Day 1: Critical Infrastructure Resilience Foundations

Which assets and services are critical, and who is accountable for them?

- Criteria for Criticality of Assets and Services
- Sector and Cross-Sector Responsibility Map
- Resilience Directive Logic for Critical Entities
- Public and Private Ownership Roles
- Case Review of Two Service Failures

Day 2: Dependencies and Risk Assessment

How do failures spread, and how is exposure measured and ranked?

- Interdependency Mapping Across Energy, Water, Transport and Communications
- ISO 31000 Risk Identification and Analysis
- Threat and Hazard Register
- Vulnerability and Single Point of Failure Review
- Consequence Scoring and Risk Matrix

Day 3: Protective Measures and Resilience Design

Which measures reduce risk most for the cost and effort involved?

- Layered Protection of Physical and Digital Assets
- Redundancy and Alternative Supply Options
- Supplier and Contractor Risk Controls
- Cost and Consequence Prioritisation Grid
- Public and Private Information Sharing Arrangements



Day 4: Continuity Planning and Crisis Leadership

How is service restored, and who decides during a disruption?

- ISO 22301 Business Impact Analysis
- Recovery Time and Priority Schedule
- Crisis Command Structure and Escalation Routes
- Incident Communication Plan for Public and Partners
- Rehearsal Design and Lessons Capture

Day 5: Applying Critical Infrastructure Resilience to an Essential Service

Is the resilience plan ready for a board or ministry to approve?

- Applying the Session 1 Criticality Criteria to the Chosen Service
- Testing the Session 2 Dependency Map and Risk Ranking
- Checking Session 3 Measures Against Cost and Consequence
- Stress-Testing the Session 4 Continuity and Command Arrangements
- Completing the Critical Infrastructure Resilience Plan

Methodology

The programme is built around simulation and structured exercises. Participants work with an anonymised essential service, build the dependency map and risk ranking in small teams, and then respond to a staged disruption that develops over several hours. No technical engineering background is required.

- Suggested activity: Mapping the dependencies of a regional water treatment and distribution service.
- Suggested activity: Ranking the risks to a port or airport using a shared matrix.
- Suggested activity: Leading a staged power and communications outage from the first alert to recovery.

Capstone Output

Each participant completes a critical infrastructure resilience plan for one essential service. It contains a criticality statement, a dependency map, a ranked risk register, a set of protective measures, a continuity and recovery schedule and a crisis command outline. It is used to brief a board or ministry and to guide the next review of protective and continuity arrangements.



Frequently Asked Questions

Is critical infrastructure resilience training suitable for officials without an engineering background?

Yes. Critical infrastructure resilience training is set at strategic level and assumes responsibility for policy, operations or risk in an essential service, not engineering or cybersecurity expertise.

Which standards does critical infrastructure resilience rest on in this programme?

Critical infrastructure resilience rests on ISO 31000 for risk management, ISO 22301 for business continuity and the logic of the Critical Entities Resilience Directive for identifying and protecting critical entities.

How is the critical infrastructure resilience plan used at work?

You use the critical infrastructure resilience plan to brief a board or ministry, set protective priorities and guide continuity and crisis arrangements for the service.

How does critical infrastructure resilience differ from general cybersecurity training?

Critical infrastructure resilience covers physical and digital assets, dependencies, continuity and crisis leadership, while cybersecurity training concentrates on technical controls.