



Critical Infrastructure Protection and Resilience Course

5 – 9 September 2027
Nairobi

Critical Infrastructure Protection and Resilience Course

Ref: 550_142689 **Date:** 5 – 9 September 2027 **Location:** Nairobi **Fees:** 4500 Euro

Overview

Critical Infrastructure Protection and Resilience Course is a five-day intermediate course for security, continuity, risk, operations, cyber-physical, and emergency teams who leave with a Critical Infrastructure Protection Improvement Plan. Participants connect essential service criticality, threat and hazard analysis, dependency mapping, protective security controls, incident coordination, continuity and recovery priorities, and security assurance. The course addresses physical, digital, supply-chain, and operational exposure through traceable decisions and exercises. Agile Leaders Training Center frames critical infrastructure security around service resilience.

Who Should Attend

- Teams responsible for protecting essential services and critical assets
- Functions coordinating operational resilience, continuity, and emergency planning
- Personnel assessing enterprise, security, and cyber-physical risks
- Groups managing facilities, control environments, suppliers, and service dependencies
- Leaders overseeing incident coordination, recovery priorities, and security assurance

The course assumes participants can interpret risk, asset, incident, and continuity information, and it leaves out detailed engineering design, penetration testing, and sector licensing.

Departments and Industries

The course supports departments and industries responsible for critical infrastructure security and uninterrupted essential services.

- Corporate security, risk, resilience, and business continuity
- Operations, engineering, facilities, and asset management
- Cybersecurity, industrial control, emergency, and crisis teams
- Energy, water, transport, telecommunications, and healthcare
- Utilities, logistics, public infrastructure, and industrial production

Learning Objectives

By the end of this course, participants will be able to:



- Apply service criticality criteria to assets and functions
- Analyze threats, hazards, vulnerabilities, and cascading consequences
- Build dependency and interdependency maps for essential services
- Evaluate layered protective security controls and third-party exposure
- Prioritize incident, continuity, recovery, and information-sharing actions
- Develop a Critical Infrastructure Protection Improvement Plan

Course Agenda

Day 1: Criticality and Protection Context

- Essential Service Criticality Assessment Matrix
- Critical Asset and Function Register
- Protection Governance and Decision Rights Map
- NIST Cybersecurity Framework Function Alignment
- Security Assurance Scope and Evidence Catalogue

Day 2: Threats, Hazards and Dependencies

- All-Hazards Threat and Vulnerability Assessment
- Consequence and Service Disruption Scale
- Upstream and Downstream Dependency Map
- Interdependency and Cascading Failure Analysis
- Risk Scenario and Treatment Priority Matrix

Day 3: Layered Protection and Third Parties

- Physical and Cyber-Physical Interface Map
- Layered Protective Security Control Model
- Access, Monitoring, Detection, and Escalation Checklist
- Supply-Chain and Third-Party Exposure Register
- Control Ownership and Assurance Testing Schedule

Day 4: Incident Coordination and Resilience

- Incident Command and Coordination Structure
- Essential Service Continuity Priority Matrix
- Recovery Objective and Resource Dependency Table
- Cross-Organization Information-Sharing Protocol
- Exercise, After-Action, and Improvement Cycle



Day 5: Protection and Resilience Practice

- Exercise: Classify Essential Services and Critical Assets
- Exercise: Trace Dependencies and Cascading Disruptions
- Exercise: Select Layered Controls for a Cyber-Physical Scenario
- Exercise: Coordinate Incident, Continuity, and Recovery Decisions
- Capstone Exercise: Critical Infrastructure Protection Improvement Plan

Practical Exercises

The course uses suggested activities to convert critical infrastructure protection decisions into usable evidence.

- Suggested activity: classify services, assets, functions, consequences, and decision owners with a criticality matrix.
- Suggested activity: map upstream, downstream, and shared dependencies across energy, water, transport, and digital services.
- Suggested activity: evaluate physical, cyber-physical, supplier, detection, and escalation controls against a disruption scenario.
- Suggested activity: assemble incident, continuity, recovery, assurance, and improvement actions into a prioritized protection plan.

FAQs

Who suits the critical infrastructure protection course and what does it assume?

It suits personnel responsible for security, resilience, risk, operations, continuity, emergency planning, suppliers, or cyber-physical environments and assumes they can interpret basic asset, risk, incident, and continuity information.

How does critical infrastructure protection differ from a cybersecurity course?

Critical infrastructure protection integrates physical, personnel, cyber-physical, supplier, operational, continuity, and recovery controls, while a cybersecurity course usually concentrates on digital systems, information, and technical threats.

How are critical infrastructure dependencies assessed?

Dependencies are assessed by tracing the services, assets, utilities, data, suppliers, people, facilities, and decisions each function requires, then testing upstream, downstream, shared, and cascading effects under disruption scenarios.



How are protective security controls prioritized for essential services?

Protective controls are prioritized by service criticality, credible threat and hazard scenarios, vulnerabilities, consequences, existing safeguards, implementation dependencies, assurance evidence, and the time needed to sustain or recover essential delivery.

What belongs in a critical infrastructure improvement plan?

A critical infrastructure improvement plan records priority risks, control gaps, actions, owners, dependencies, resources, evidence, review points, incident lessons, continuity needs, and measurable completion conditions.

Conclusion

Participants take back a Critical Infrastructure Protection Improvement Plan linking critical services, dependencies, risks, controls, incident coordination, continuity, recovery, and assurance. It turns fragmented security information into owned and prioritized actions across operational and support teams. The plan supports resilient service decisions without replacing specialist engineering, technical testing, or statutory approval.