Industrial Security Readiness and Crisis Management Assessment Training Course

23 – 27 May 2027
Nairobi

AGILE LEADERS
Training Center

AGILE LEADERS
Training Center

Industrial Security Readiness and Crisis Management Assessment Training Course

Ref: 1310_196855 **Date:** 23 – 27 May 2027 **Location:** Nairobi **Fees:** 4500 Euro

Overview

Industrial Security Readiness and Crisis Management Assessment Training Course is a one-week advanced course for industrial security, crisis, facility, operations, resilience, and emergency-planning leaders who leave with an Industrial Security Readiness Assessment and Improvement Portfolio. Participants evaluate critical assets, physical and operational controls, command interfaces, communications, exercises, evidence, and corrective actions through a structured assurance approach. Agile Leaders Training Center frames industrial security readiness assessment as an evidence-led management discipline.

Who Should Attend

- Teams responsible for industrial physical security and access-control assurance
- Functions responsible for crisis command, escalation, and coordination
- Facility and operations groups responsible for critical assets and shutdown interfaces
- Resilience and emergency-planning teams responsible for preparedness evidence
- Assurance personnel responsible for exercises, findings, and corrective actions

The course assumes participants already support industrial security or crisis-preparedness decisions at work, and it excludes cybersecurity engineering, broad enterprise-risk design, legal interpretation, and general business-continuity planning.

Departments and Industries

The course supports departments and industries that must demonstrate security readiness around critical operations and assets.

- Industrial security, protective services, and facility management
- Operations, maintenance, and control-room functions
- Emergency management, resilience, and crisis communication
- Manufacturing, chemicals, energy, and utilities
- Transport, logistics, warehousing, and infrastructure services

Learning Objectives

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

- Evaluate industrial threat, vulnerability, and consequence context
- Build critical-asset and readiness-evidence matrices
- Analyze physical and operational security control performance
- Apply ISO 22320 role and coordination principles
- Use exercises to diagnose gaps and prioritize corrective actions
- Create a reassessment and readiness-assurance portfolio

Course Agenda

Day 1: Assessment Scope and Security Context

- Industrial Security Context and Assessment Charter
- Critical Asset and Essential Function Map
- Threat, Vulnerability, and Consequence Profile
- Security Readiness Criteria and Evidence Matrix
- Assessment Governance and Independence Protocol

Day 2: Physical and Operational Controls

- Perimeter, Access, and Security-Zone Assessment
- Visitor, Contractor, and Credential-Control Review
- Surveillance, Detection, and Alarm Capability Map
- Critical Operations and Safe-Shutdown Interface
- Security Equipment, Staffing, and Resource Register

Day 3: Crisis Command and Coordination

- ISO 22320 Incident-Management Role Structure
- Command, Control, and Decision-Authority Matrix
- Security, Safety, Operations, and Responder Interface
- Resource Mobilization and Mutual-Support Plan
- Escalation, Notification, and Situation-Reporting Protocol

Day 4: Exercises and Corrective Action

- Threat-Based Exercise Objective Design
- Scenario, Inject, and Evaluation Guide
- Crisis Communication and Information-Control Test
- After-Action Review and Capability-Gap Register
- Corrective Action and Improvement Tracking Plan

AGILE LEADERS
Training Center

Day 5: Security Readiness Assessment Practice

- Exercise: Critical Asset and Threat-Profile Review
- Exercise: Physical and Operational Control Evidence Test
- Exercise: Crisis Command and Communication Simulation
- Exercise: Capability-Gap Prioritization and Action Review
- Capstone Exercise: Industrial Security Readiness Assessment and Improvement Portfolio

Practical Exercises

The course uses suggested activities based on manufacturing, utility, logistics, and process-facility scenarios.

- Suggested activity: inspect a critical-asset map and test whether threat and vulnerability evidence supports the assessment scope.
- Suggested activity: trace an access-control and shutdown-interface exception through command, escalation, and situation reporting.
- Suggested activity: evaluate an exercise record and convert observed capability gaps into owned corrective actions.
- Suggested activity: defend a readiness rating using evidence, priorities, and a reassessment schedule.

FAQs

What is an industrial security readiness assessment?

An industrial security readiness assessment evaluates whether physical controls, operational interfaces, people, resources, command arrangements, communications, and exercises can support effective action during an industrial crisis.

How does industrial security readiness assessment support crisis management?

Industrial security readiness assessment identifies critical assets, tests control evidence, clarifies decision authority, examines coordination, and tracks corrective actions before weaknesses undermine crisis response.

Who suits industrial security readiness assessment training and what does it assume?

Industrial security readiness assessment training suits managers and specialists responsible for security, facilities, operations, resilience, crises, or emergency planning. It assumes experience supporting preparedness or operational decisions.

AGILE LEADERS
Training Center

How does industrial security readiness assessment differ from cybersecurity or business continuity training?

Industrial security readiness assessment focuses on physical and operational protection, crisis command, coordination, exercises, and evidence. Cybersecurity training protects digital systems, while business continuity training addresses broader service recovery and continuity arrangements.

What evidence supports an industrial security readiness rating?

Industrial security readiness ratings use asset maps, threat profiles, control records, role matrices, resource registers, exercise observations, communication tests, gap registers, corrective-action records, and reassessment results.

Conclusion

The course integrates industrial security context, critical assets, control evidence, crisis command, communications, exercises, and corrective action. Participants take back an Industrial Security Readiness Assessment and Improvement Portfolio containing criteria, maps, matrices, registers, protocols, evaluation records, and action plans. The portfolio supports defensible readiness ratings, clearer priorities, assigned improvements, and repeatable assurance.