JUPITER PRIME

Consulting • Training • Advisory

جوبيتر برايم للاستشارات والتدريب

COURSE BROCHURE

Industrial Facility Security Readiness Assessment Training Course

16 – 20 May 2027
Kuala Lumpur

Industrial Facility Security Readiness Assessment Training Course

Ref: 700_26193 **Date:** 16 – 20 May 2027 **Location:** Kuala Lumpur **Fees:** 4600 GBP

Industrial Facility Security Readiness Assessment is a 1-week training course for security managers, plant security supervisors and HSE managers, built around a security readiness assessment each participant completes for an industrial facility. Intrusion, sabotage, theft of hazardous materials and insider threats can halt production and trigger safety incidents within minutes. Jupiter Prime Training delivers this course for those who must prove a site is ready before an event tests it.

Why Industrial Facility Security Readiness Assessment Matters Now

Three pressures shape site security today: converging physical and digital threats that reach control rooms and gatehouses alike, insurers and corporate owners who ask for evidence of readiness rather than written procedures, and contractor-heavy workforces that widen insider exposure during shutdowns and expansions. Sites that measure readiness honestly close gaps before an intruder or incident finds them; those that rely on assumptions discover weaknesses during a crisis. The course links readiness findings to ISO 22361 crisis management guidelines and ISO 22301 business continuity planning.

Who Gains Most from Industrial Facility Security Readiness Assessment

- Security managers who own site protection strategy and guard force performance
- Plant security supervisors who run gatehouses, patrols and control room monitoring
- HSE managers who align security events with process safety and emergency response
- Facility managers who maintain fences, lighting, barriers and detection equipment
- Contract security coordinators who set duties and performance measures for guard providers

Results improve most when security, HSE and operations supervisors from one site attend together.

Industrial Facility Security Readiness Assessment Capabilities

Participants leave able to measure how prepared a plant really is against credible threats and to turn weak points into funded corrective actions.

- Assess credible threats and site vulnerabilities using structured scoring — site general manager
- Test perimeter, gate and access control layers against intrusion scenarios — operations director
- Design security drills that expose response times and communication gaps — emergency response team
- Calculate readiness indicators across people, procedures and equipment — corporate security
-

Specify gap closure actions with owners, cost bands and deadlines — capital approval committee
- Present a security readiness assessment with a prioritised improvement plan — plant leadership

Key Industrial Facility Security Readiness Assessment Terms

- Security Readiness — the measured ability of a site's people, procedures and equipment to detect, delay and respond to a security event.
- Threat Assessment — identifying who might target a facility, their intent and capability, and the assets most attractive to them.
- Vulnerability Assessment — examining physical, procedural and human weaknesses an adversary could exploit to reach critical assets.
- Defence in Depth — layered protection in which perimeter, access, detection and response measures back each other up.
- Readiness Indicator — a measurable signal, such as alarm response time or drill pass rate, showing how prepared a site is.
- Gap Closure Plan — a ranked list of corrective actions with owners, resources and target dates that addresses assessment findings.

Industrial Facility Security Readiness Assessment Day by Day

Day 1: Security Readiness Context for Industrial Sites

- Industrial Threat Landscape — Sabotage, Theft, Intrusion and Insider Risk
- Critical Asset Identification — Prioritising Control Rooms, Tank Farms and Substations
- Security Links to Crisis Management Under ISO 22361 — Escalation Paths
- Security and Process Safety Interfaces — Protecting Hazardous Inventories
- Readiness Assessment Scope Setting — Defining Boundaries and Assessment Teams

Day 2: Threat and Vulnerability Assessment

- Threat Actor Profiling — Matching Intent and Capability to Site Assets
- Vulnerability Walkdown Techniques — Recording Physical and Procedural Weaknesses
- Adversary Path Analysis — Estimating Detection and Delay Along Routes
- Insider Threat Indicators — Screening Contractors and Shift Access
- Risk Scoring Matrices — Ranking Scenarios by Likelihood and Consequence

Day 3: Perimeter, Access Control and Detection

- Perimeter Fencing, Lighting and Barriers — Judging Delay Effectiveness
- Gatehouse and Vehicle Search Procedures — Controlling Deliveries and Visitors
- Electronic Access Control and Credential Management — Closing Badge Gaps
- CCTV and Intrusion Detection Coverage — Mapping Blind Spots
- Security Control Room Operations — Alarm Handling and Dispatch Decisions

Day 4: Security Drills and Readiness Indicators

- Security Drill Design — Choosing Intrusion, Bomb Threat and Lockdown Scenarios
- Tabletop and Live Exercise Evaluation — Recording Response Timelines
- Readiness Indicator Selection — Measuring People, Procedures and Equipment
- Guard Force Performance Measures — Patrol Compliance and Post Orders
- Continuity Alignment Through ISO 22301 — Protecting Critical Production Activities

Day 5: Practising the Security Readiness Assessment

- Site Case Walkdown — Applying Vulnerability and Adversary Path Methods
- Readiness Scoring Exercise — Applying Indicators to a Plant Profile
- Drill Debrief Simulation — Applying Exercise Evaluation Findings
- Gap Closure Prioritisation — Ranking Corrective Actions and Owners
- Security Readiness Assessment — Final Presentation and Peer Challenge

Applying Industrial Facility Security Readiness Assessment After the Course

- Lead a vulnerability walkdown of one critical area of your plant using the adversary path method, then record detection and delay findings
- Run a short intrusion or lockdown drill and score it against the readiness indicators agreed in the course, feeding results into the gap closure plan

Industrial Facility Security Readiness Assessment Questions FAQ

What is Industrial Facility Security Readiness Assessment and why does it matter now?

It is the structured measurement of how prepared an industrial site is to detect, delay and respond to security threats. It matters now because physical, digital and insider threats increasingly converge on production sites.

Which roles gain most from Industrial Facility Security Readiness Assessment training?

Security managers, plant security supervisors, HSE managers, facility managers and contract security coordinators gain most, since each controls part of the site's protective layers.

How does Industrial Facility Security Readiness Assessment differ from a major emergency response course?

It focuses on preventing and detecting deliberate threats before they become incidents. An emergency response course covers controlling fires, releases and explosions once they occur.

What do you bring back from Industrial Facility Security Readiness Assessment training?

You bring back a security readiness assessment for an industrial facility, with scored findings and corrective actions, challenged by peers from petrochemical and power generation sites.

Industrial Facility Security Readiness Assessment: The Way Forward

The security readiness assessment first informs which protective layer receives investment and which drills run next. Security managers, HSE leads and plant directors use it during budget rounds and after incidents. Once the first corrective actions are complete, repeat the walkdown and drills, because shutdowns, new contractors and plant modifications quietly reopen gaps that earlier scores showed as closed.