JUPITER PRIME

Consulting • Training • Advisory

جوبيتر برايم للاستشارات والتدريب

COURSE BROCHURE

Critical Infrastructure Risk and Risk-Based Auditing Training Course

3 – 7 May 2027
Rome

Critical Infrastructure Risk and Risk-Based Auditing Training Course

Ref: 3237_123203 **Date:** 3 – 7 May 2027 **Location:** Rome **Fees:** 6200 GBP

Critical Infrastructure Risk and Risk-Based Auditing is a 1-week training course for owners, operators and auditors of energy, water, transport and communications assets, built around a critical infrastructure risk-based audit plan. Essential services now face linked cyber, physical, supplier and insider hazards, and one failed asset can cascade to others. Jupiter Prime Training offers this critical infrastructure risk course.

Why Critical Infrastructure Risk and Risk-Based Auditing Matters Now

Three pressures shape this field: control systems now connect to corporate networks, supply chains for spares reach across many vendors, and the public expects essential services to run through storms and attacks. An operator that maps its hazards on an all-hazards basis and audits its controls where failure would hurt most can show boards real assurance; one that does not finds weak controls during an incident. The course rests on internationally recognised risk management guidelines and on the three lines model of assurance.

Who Gains Most from Critical Infrastructure Risk and Risk-Based Auditing

- Owning hazard registers for grids, pipelines, treatment plants or telecoms networks
- Running control rooms and deciding how operations continue after a loss
- Planning internal audits of operational and security controls
- Vetting contractors, suppliers and staff with sensitive site access
- Reporting hazard exposure and assurance results to boards

The strongest gains come when an asset owner sends risk, security and audit staff together to agree hazard ratings and audit priorities.

Critical Infrastructure Risk and Risk-Based Auditing Capabilities

These outcomes join hazards at essential-service assets to the audit work that tests their controls.

- Assess cyber, physical, natural and insider hazards to an essential service — the asset owner deciding protection priorities
- Map dependencies between energy, water, transport and communications assets — continuity leads planning for cascading outages
- Specify supply chain and personnel security controls — procurement and security managers
- Build a risk-weighted audit universe and annual audit cycle — the head of audit allocating audit days
- Test control design and operating effectiveness at operational sites — the audit committee relying on assurance
- Communicate findings and remediation actions plainly — executives approving investment

Key Critical Infrastructure Risk and Risk-Based Auditing Terms

- Critical infrastructure — assets, systems and networks whose loss would seriously disrupt essential services, public safety or economic activity.
- All-hazards approach — planning that treats natural, accidental, cyber, physical and deliberate human threats together.
- Interdependency — a link where the failure of one service disrupts another, such as power loss halting water pumping.
- Audit universe — the full list of auditable units, processes and controls from which a risk-based audit cycle is chosen.
- Residual risk — the exposure that remains after existing controls are applied.
- Operational technology — the control systems, sensors and field devices that run physical processes.

Critical Infrastructure Risk and Risk-Based Auditing Day by Day

Day 1: Essential Services and the Hazard Landscape

- Essential Service Mapping — Which Functions Society Cannot Lose For Long
- Sector Interdependency Diagrams — How Power Loss Spreads To Water And Telecoms
- All-Hazards Threat Catalogue — Natural, Technical, Cyber And Deliberate Events Together
- Single Points Of Failure Review — Where One Asset Halts A Whole Network
- Risk Appetite For Service Interruption — Tolerable Outage Duration And Public Impact

Day 2: Physical, Cyber and Insider Hazards

- Site Perimeter And Access Control Assessment — Protecting Substations, Pumping Stations And Depots
- Operational Technology Exposure Review — Remote Access Paths Into Control Systems
- Personnel Vetting And Trusted Insider Controls — Who Holds Sensitive Site Access
- Supplier And Spare Parts Dependency Analysis — Concentration In Critical Vendor Base
- Likelihood And Consequence Scoring Matrix — Ranking Hazards For Protection Investment

Day 3: Controls, Resilience and Recovery

- Layered Protection Design — Deter, Detect, Delay And Respond Measures
- Contract Security Clauses — Holding Vendors To Access And Patching Duties
- Continuity And Restoration Plans — Priority Order For Bringing Services Back
- Incident Escalation Routes — Linking Control Rooms, Security Teams And Executives
- Exercise And Drill Scenarios — Testing Recovery Against Realistic Combined Events

Day 4: Risk-Based Audit Planning and Fieldwork

- Three Lines Assurance Mapping — Avoiding Gaps And Overlap Between Assurance Providers
- Risk-Weighted Audit Universe — Choosing Which Sites And Controls To Audit
- Control Design Walkthroughs — Judging Whether A Safeguard Could Ever Work
- Operating Effectiveness Sampling — Evidence That Controls Work Day After Day
- Finding Rating Criteria — Separating Critical Weaknesses From Minor Lapses

Day 5: Practising the Critical Infrastructure Audit Plan

- Hazard Profile Drafting For A Water Utility Case — Applying All-Hazards Scoring
- Telecoms Supplier Access Audit Simulation — Testing Personnel And Vendor Controls
- Audit Report And Board Summary Writing — Turning Findings Into Funded Actions
- Remediation Tracking Log — Owners, Deadlines And Follow-Up Testing Rules
- Critical Infrastructure Risk-Based Audit Plan — Completing The Participant's Own Cycle

Applying Critical Infrastructure Risk and Risk-Based Auditing After the Course

- Lead interdependency mapping for one essential service and log its single points of failure.
- Re-rank the audit cycle so highest-consequence sites are tested first.

Critical Infrastructure Risk and Risk-Based Auditing Questions FAQ

What is critical infrastructure risk and risk-based auditing, and why does it matter now?

It is identifying hazards to essential services and auditing the controls where failure hurts most. It matters now because connected control systems and long supply chains raise the chance that one weakness interrupts an essential service.

Which roles gain most from critical infrastructure risk and risk-based auditing?

Operations risk leads, security managers, continuity planners and internal auditors at asset owners gain most. You gain whether you rate hazards, design controls or test them.

How does a critical infrastructure risk and risk-based auditing course differ from a general enterprise risk course?

It focuses on assets that deliver essential services and on auditing their protection. You work with interdependencies, control systems, insider access and site security.

What do you bring back from critical infrastructure risk and risk-based auditing?

You bring back a draft audit plan ranked by hazard consequence for your own assets. It comes with a hazard scoring matrix, an assurance map and a remediation tracking log.

Critical Infrastructure Risk and Risk-Based Auditing: The Way Forward

The critical infrastructure risk-based audit plan first informs which sites and supplier access arrangements are tested next. Heads of audit, asset owners and security leads use it to agree priorities and defend audit days. After its first cycle, revisit the interdependency map, because new connections between services shift where consequences sit.