JUPITER PRIME

Consulting • Training • Advisory

جوبيتر برايم للاستشارات والتدريب

COURSE BROCHURE

AI Cyber Risk and Operational Resilience for Leaders Training Course

jupiterprime.uk

info@jupiterprime.uk

Registered in the United Kingdom and Saudi Arabia

AI Cyber Risk and Operational Resilience for Leaders Training Course

AI Cyber Risk and Operational Resilience is a 1-week training course for non-technical leaders, risk owners and operations managers, who leave with an AI Cyber Resilience Board Brief. Attackers now use machine learning to scale phishing, voice cloning and reconnaissance, while defenders adopt it in detection, so leaders must judge both sides. Jupiter Prime Training delivers this course on AI cyber risk and operational resilience.

Why AI Cyber Risk and Operational Resilience Matters Now

Three forces shape the subject: generative models that make deepfake calls and tailored lures cheap, boards that expect important business services to stay within tolerable disruption, and suppliers that embed machine learning in products the organisation cannot inspect. Leaders who handle this well protect the right services first; those who do not discover their tolerances during an outage. The course rests on the NIST Cybersecurity Framework 2.0 NIST CSF 2.0, including its Govern function.

Who Gains Most from AI Cyber Risk and Operational Resilience

- Business service owners who answer for keeping customer-facing operations running during disruption
- Risk owners who rate cyber exposure and approve treatment choices for their area
- Operations managers who run recovery tasks, workarounds and manual fallbacks
- Executive sponsors of automation and machine learning initiatives who accept their residual risk
- Committee members who scrutinise resilience reports and challenge investment cases

A leadership group sending service, risk and operations leads together gains most, leaving with one shared view of tolerances.

AI Cyber Risk and Operational Resilience Capabilities

Participants turn machine-driven threats into service-level choices.

- Assess how deepfakes, automated phishing and model manipulation could reach critical services — risk owners setting priorities
- Weigh the benefits and limits of machine learning in detection and response tools — investment committees
- Specify impact tolerances for important business services — executive approval of recovery priorities
- Design severe but plausible disruption scenarios for resilience testing — operations managers and service owners
- Test third-party and supplier dependencies for hidden algorithmic exposure — procurement and vendor owners
-

Communicate resilience posture and remediation needs in plain terms — the board and audit committee

Key AI Cyber Risk and Operational Resilience Terms

- Operational resilience — the ability of an organisation to prevent, adapt to, respond to and recover from disruption.
- Impact tolerance — the maximum level of disruption to an important business service, often a time limit, the organisation will accept.
- Important business service — a service whose failure would cause intolerable harm to customers, the organisation or the wider market.
- Deepfake — synthetic audio, image or video created by machine learning to impersonate a real person.
- Adversarial machine learning — techniques that manipulate model inputs or training data so that an AI system produces wrong outputs.
- Severe but plausible scenario — a demanding yet realistic disruption used to test whether services stay within tolerance.

AI Cyber Risk and Operational Resilience Day by Day

Day 1: The AI-Shaped Threat Landscape

- Generative AI Attack Patterns — Gauging Exposure of Executives and Staff
- Deepfake Voice and Video Fraud Cases — Hardening Payment Authorisation Steps
- Automated Reconnaissance and Phishing at Scale — Prioritising Awareness Spending
- Model Poisoning and Prompt Injection Basics — Questioning Vendor AI Claims
- Banking and Healthcare Incident Contrasts — Learning From Recent Service Failures

Day 2: AI on the Defender's Side

- Machine Learning Detection in Security Operations — Setting Realistic Expectations
- Alert Triage Automation — Balancing Speed Against False Positives
- NIST CSF 2.0 Govern Function — Assigning Leadership Accountability for Cyber Risk
- AI Use Inventory — Revealing Shadow Models Across Business Units
- Supplier Algorithm Dependency Map — Exposing Concentration and Lock-In Risk

Day 3: Important Services and Impact Tolerances

- Service Identification Criteria — Choosing Which Operations Truly Matter
- End-to-End Service Mapping — Tracing People, Systems and Suppliers
- Impact Tolerance Setting — Converting Harm Into Maximum Outage Times
- Recovery Workarounds and Manual Fallbacks — Funding Proportionate Continuity Options
- Tolerance Breach Escalation Paths — Deciding Who Acts and When

Day 4: Testing Resilience Under Pressure

- Severe but Plausible Scenario Design — Stretching Assumptions Without Fantasy
- Tabletop Exercise With a Deepfake Trigger — Rehearsing Executive Decisions
- Ransomware and Data Integrity Scenarios — Comparing Restore Choices
- Exercise Findings Log — Ranking Vulnerabilities for Remediation Funding
- Crisis Communication Protocol — Informing Customers, Staff and Partners

Day 5: Practising the AI Cyber Resilience Board Brief

- Threat Exposure Summary — Applying Day One Attack Patterns to Own Services
- Tolerance Statement Review — Applying Service Maps to Approval Requests
- Exercise Results Narrative — Applying Test Findings to Remediation Asks
- Resilience Metrics Dashboard — Selecting Indicators the Board Can Track
- AI Cyber Resilience Board Brief — Completing Threats, Tolerances and Remediation Plan

Applying AI Cyber Risk and Operational Resilience After the Course

- Run a one-hour tabletop on a deepfake payment request, recording gaps in authorisation steps.
- Map one important business service end to end and propose an impact tolerance.

AI Cyber Risk and Operational Resilience Questions FAQ

What is AI cyber risk and operational resilience, and why does it matter now?

It is judging how machine learning changes cyber threats while keeping critical services within tolerable disruption. It matters now because cheap generative tools let attackers impersonate executives and scale fraud faster than traditional controls adapt.

Which roles gain most from AI cyber risk and operational resilience training?

Service owners, risk owners and operations managers gain most. They take the decisions on tolerances, recovery funding and supplier dependencies.

How does AI cyber risk and operational resilience differ from a technical incident response course?

It works at the level of services, tolerances and board decisions rather than forensic tools or log analysis. A technical response course trains analysts to contain an intrusion; this subject prepares leaders to decide what must keep running.

What do you bring back from AI cyber risk and operational resilience training?

You bring back an AI Cyber Resilience Board Brief. It summarises machine-driven threats to your services, proposed impact tolerances, exercise findings and the remediation you need approved.

AI Cyber Risk and Operational Resilience: The Way Forward

The AI Cyber Resilience Board Brief first informs which important business services receive recovery investment. Service owners, risk owners and the executive committee use it to approve tolerances and track remediation. After its first exercise cycle, the threat exposure summary is worth revisiting, because attacker use of generative tools shifts quickly.