JUPITER PRIME

Consulting • Training • Advisory

جوبيتر برايم للاستشارات والتدريب

COURSE BROCHURE

AI Impact Assessment and Incident Handling Training Course

jupiterprime.uk

info@jupiterprime.uk

Registered in the United Kingdom and Saudi Arabia

AI Impact Assessment and Incident Handling Training Course

AI Impact Assessment and Incident Handling is a 1-week training course for compliance officers, risk managers and AI governance leads, built around one work product: an AI impact and incident dossier. Automated systems now decide on credit, claims, staffing and service access, so organisations must show they weighed the harm before launch and responded properly when something went wrong. Jupiter Prime Training delivers this course on AI Impact Assessment and Incident Handling.

Why AI Impact Assessment and Incident Handling Matters Now

Three groups now press on this field. Regulators and auditors ask for written evidence that fairness and transparency were tested, customers and staff challenge automated outcomes more often, and boards want to know which systems could cause serious harm. An organisation that handles this well launches systems with clear accountability and contains failures quickly; one that handles it badly faces complaints, suspended services and reputational damage. The course rests on ISO/IEC 42001 Artificial Intelligence Management System and the NIST AI Risk Management Framework AI RMF.

Who Gains Most from AI Impact Assessment and Incident Handling

- Compliance staff who sign off new automated decision systems
- Risk staff who classify system exposure and maintain control libraries
- AI oversight leads who chair ethics review panels
- Internal audit staff who test evidence behind AI controls
- Operational resilience staff who coordinate incident response

A second-line function sending compliance, risk and audit members together gains most.

AI Impact Assessment and Incident Handling Capabilities

Participants turn ethical principles into tiered assessments, evidence trails and response playbooks.

- Classify AI systems into risk tiers using intended purpose and affected groups — the approval panel
- Design an algorithmic impact assessment template with fairness and transparency tests — the system owner
- Specify accountability records that name decision owners and override rights — the board risk committee
- Test audit evidence against ISO/IEC 42001 control objectives — the internal auditor
- Build an AI incident severity scale and escalation path — the operational resilience lead
- Communicate post-incident findings to affected users and senior leaders — the chief compliance officer

Key AI Impact Assessment and Incident Handling Terms

- Algorithmic impact assessment — a structured review of who an automated system could harm, how, and which safeguards reduce it.
- Risk tier — a category that sets the depth of review a system receives according to its potential harm.
- Disparate outcome — a measurable difference in results between groups of people affected by the same automated decision.
- Model card — a short document describing a model's purpose, training data, performance limits and intended users.
- AI incident — an event where an AI system causes or nearly causes harm, unfair treatment or a serious error.
- Root cause review — an investigation that traces an incident to the data, model, process or human decision behind it.

AI Impact Assessment and Incident Handling Day by Day

Day 1: Ethical Principles and Accountability

- Fairness, Transparency and Accountability Principles — Translating Values into Tests
- ISO/IEC 42001 Management System Structure — Placing Assessments in Controls
- NIST AI RMF Govern, Map, Measure, Manage — Assigning Ownership
- Accountability Records and Override Rights — Naming Decision Owners
- Ethics Review Panel Charter — Escalation and Veto Powers

Day 2: Classifying and Assessing Impact

- Risk Tier Classification by Purpose and Affected Groups — Review Depth
- Algorithmic Impact Assessment Template — Questions Before Launch
- Disparate Outcome Testing — Accepting or Rejecting a Model
- Explainability Requirements by Tier — What Users Must Be Told
- Stakeholder Consultation Records — Including Affected People's Views

Day 3: Building Audit Evidence

- Model Cards and Data Sheets — Documenting Limits and Intended Use
- Control Testing Against ISO/IEC 42001 Objectives — Evidence Sufficiency
- Monitoring Logs and Drift Alerts — Proving Ongoing Oversight
- Third-Party Model Due Diligence — Supplier Evidence Requests
- Assurance Reporting to Board Committees — Residual Exposure Statements

Day 4: Handling AI Incidents

- AI Incident Severity Scale — Triggering Escalation and Suspension
- Containment Options for Faulty Models — Rollback, Throttle or Human Takeover
- Root Cause Review Method — Data, Model, Process or Decision
- Affected User Notification Wording — Remedy and Appeal Routes
- Lessons Log and Control Updates — Preventing Repeat Failures

Day 5: Practising the AI Impact and Incident Dossier

- Insurance Claims Triage Model Case — Applying Risk Tier Classification
- Public Transport Ticketing Fraud Detector Case — Applying Disparate Outcome Tests
- Credit Limit Model Failure Simulation — Applying Containment and Root Cause Steps
- Audit Evidence Walkthrough — Applying ISO/IEC 42001 Control Tests
- AI Impact and Incident Dossier Completion — Presenting Tiers, Evidence and Playbooks

Applying AI Impact Assessment and Incident Handling After the Course

- Classify every live AI system in one business unit into risk tiers and list missing impact assessments.
- Run a tabletop exercise of the AI incident severity scale with operations and communications staff.

AI Impact Assessment and Incident Handling Questions FAQ

What is AI Impact Assessment and Incident Handling and why does it matter now?

It is the practice of assessing the harm an AI system could cause before launch and responding in a controlled way when it fails. It matters now because auditors, regulators and affected people expect written proof of both.

Which roles gain most from AI Impact Assessment and Incident Handling training?

Compliance officers, risk managers and AI governance leads gain most, along with internal auditors and operational resilience staff.

How does AI Impact Assessment and Incident Handling differ from an AI governance strategy course?

It works at the level of individual systems rather than enterprise policy. A strategy course sets principles and structures; this one classifies systems, tests outcomes, gathers audit evidence and rehearses incident response.

What do you bring back from AI Impact Assessment and Incident Handling training?

You bring back a completed AI impact and incident dossier. It holds risk tiers, an assessment template, accountability records, an evidence checklist and an incident playbook ready for your own systems.

AI Impact Assessment and Incident Handling: The Way Forward

The AI impact and incident dossier first decides which systems need full assessment before their next release. Compliance, risk and audit leads use it to approve launches and brief board committees. After the first real incident or near miss, revisit the severity scale and containment options: actual response times usually show where escalation must move faster.