JUPITER PRIME

Consulting • Training • Advisory

جوبيتر برايم للاستشارات والتدريب

COURSE BROCHURE

AI Vendor Risk and Third-Party Model Assurance Training Course

jupiterprime.uk

info@jupiterprime.uk

Registered in the United Kingdom and Saudi Arabia

AI Vendor Risk and Third-Party Model Assurance Training Course

AI Vendor Risk and Third-Party Model Assurance is a 1-week training course for risk, compliance and AI oversight leads who will assemble an AI Supplier Assurance File. Most organisations now run AI they did not build, yet remain accountable for its outcomes. Jupiter Prime Training treats AI Vendor Risk and Third-Party Model Assurance as proving that bought-in AI is controlled.

Why AI Vendor Risk and Third-Party Model Assurance Matters Now

Two pressures now meet at the supplier boundary. Providers add generative and predictive features to products already under contract, often without any fresh risk assessment. Boards and audit committees expect an inventory that shows every external model, its owner and its exposure. Organisations that control their AI suppliers can switch or pause with confidence; others inherit failures they cannot explain. The course rests on ISO/IEC 42001, the AI management system standard, and the NIST AI Risk Management Framework AI RMF.

Who Gains Most from AI Vendor Risk and Third-Party Model Assurance

- Professionals who maintain the register of AI risks and decide treatment for external models
- Specialists who map supplier controls against internal policy and management system clauses
- Officers who run onboarding questionnaires and due diligence for software and data suppliers
- Auditors who test whether evidence from providers supports the assurance claimed
- Advisers who prepare oversight committee papers on outsourced and embedded AI

An organisation gains most when its procurement, legal, information security and risk staff attend together, since each holds part of the clauses, tests and exit terms.

AI Vendor Risk and Third-Party Model Assurance Capabilities

Participants move from trusting supplier claims to holding testable evidence about each external model.

- Build an inventory of external and embedded models with owner, purpose and tier — oversight committees
- Assess supplier responses on training data, evaluation and incident history — onboarding decisions
- Specify contract clauses on model change notice, audit rights and data use — legal and procurement
- Test vendor evidence such as model cards and evaluation reports for sufficiency — internal audit
- Align supplier controls to ISO/IEC 42001 and NIST AI RMF functions — compliance leads
- Design monitoring triggers and exit plans for high-tier AI suppliers — risk owners

Key AI Vendor Risk and Third-Party Model Assurance Terms

- Third-party model — an AI model built, trained or hosted by an external provider and used inside an organisation's processes.
- Embedded AI feature — an AI capability added to purchased software, often without a separate purchase decision.
- Risk tiering — sorting AI suppliers into levels of scrutiny by impact on people, operations and reputation.
- Assurance evidence — documents, test results and attestations a supplier provides to show its controls operate.
- Model change notice — a contract duty requiring the provider to warn the buyer before retraining or replacing a model.
- Concentration exposure — reliance on one foundation model or provider across many business services at once.

AI Vendor Risk and Third-Party Model Assurance Day by Day

Day 1: The External AI Landscape

- Supply Chain Map of Foundation, Platform and Application Providers — Where Accountability Sits
- Embedded AI Feature Discovery in Existing Subscriptions — Hidden Exposure Decisions
- External Model Inventory Fields and Ownership — Committee Visibility Choices
- ISO/IEC 42001 Supplier Relationship Clauses — Management System Scope Decisions
- NIST AI RMF Third-Party Considerations — Framing Oversight Priorities

Day 2: Tiering and Due Diligence

- Impact-Based Risk Tiering Matrix — Depth of Scrutiny per Supplier
- AI Due Diligence Questionnaire Design — Onboarding Approval Criteria
- Training Data Provenance and Licence Checks — Intellectual Property Exposure
- Evaluation Report and Bias Testing Review — Accepting Supplier Performance Claims
- Security and Data Residency Questions for Hosted Models — Information Protection Choices

Day 3: Contracts and Control Mapping

- Model Change Notice and Retraining Clauses — Stability of Outcomes
- Audit Rights, Attestation and Evidence Delivery Terms — Assurance Access Decisions
- Supplier Control Mapping to Internal AI Policy — Gap Treatment Choices
- Liability, Incident Reporting and Service Credits — Allocating AI Failure Costs
- Exit, Portability and Model Substitution Plans — Switching Readiness

Day 4: Ongoing Monitoring and Oversight

- Key Risk Indicators for External Models — Escalation Thresholds for Owners
- Output Sampling and Drift Checks on Vendor Models — Continued Use Decisions
- Concentration Exposure Analysis Across Providers — Resilience and Diversification
- Supplier Incident Triage and Joint Response — Containment Choices
- Oversight Committee Reporting Pack — Board Assurance Messages

Day 5: Practising the AI Supplier Assurance File

- Tiering a Live Supplier Case from Banking — Applying the Day 2 Matrix
- Redlining a Healthcare AI Contract — Applying Day 3 Clauses
- Testing Vendor Evidence Against Mapped Controls — Internal Audit Sufficiency Judgement
- Monitoring Plan Walkthrough with Indicators — Applying Day 4 Thresholds
- AI Supplier Assurance File Completion — Committee Sign-Off Readiness

Applying AI Vendor Risk and Third-Party Model Assurance After the Course

- Run an embedded AI feature sweep across software subscriptions and tier each find in the external model inventory.
- Send the redesigned due diligence questionnaire to the two highest-tier AI suppliers and test their evidence.

AI Vendor Risk and Third-Party Model Assurance Questions FAQ

What is AI vendor risk and third-party model assurance, and why does it matter now?

It is the discipline of controlling AI models you buy rather than build. It matters now because suppliers add AI features quickly while you stay accountable for outcomes.

Which roles gain most from AI vendor risk and third-party model assurance training?

Risk, compliance and AI oversight leads gain most. Procurement, legal, security and internal audit staff also benefit.

How does AI vendor risk and third-party model assurance differ from a general AI oversight course?

It focuses on the supplier boundary. A general course covers policy and internal models broadly; this one concentrates on tiering, due diligence, contracts and evidence for external models.

What do you bring back from AI vendor risk and third-party model assurance training?

You bring back a completed supplier file for one real external model. It holds the risk tier, mapped controls, clause notes and a monitoring plan.

AI Vendor Risk and Third-Party Model Assurance: The Way Forward

The AI Supplier Assurance File gives the oversight committee one place to judge an external model. Its first use is deciding whether a high-tier supplier stays, changes terms or leaves, a call that risk owners, procurement and internal audit make together. After that first decision, revisit the tiering matrix, since supplier features change faster than contracts.