

ENTERPRISE PROGRAM BRIEF

AI Governance and Assurance in Practice

Create an operational governance approach for business AI use cases. Participants build an inventory, assess context and risk, assign control owners, review evaluation evidence, and practise an approval and incident tabletop using a synthetic enterprise case.

VNode ITes

VAI-206

Coming soon

DURATION
16 hours

LEVEL
Beginner to Intermediate

FORMAT
Private cohort

AUDIENCE PROFILE

Built for these roles

AI programme managers, governance and risk practitioners, technical leads, architects, product owners, and responsible AI champions.

OVERVIEW

Executive overview

Create an operational governance approach for business AI use cases. Participants build an inventory, assess context and risk, assign control owners, review evaluation evidence, and practise an approval and incident tabletop using a synthetic enterprise case.

READINESS

Prerequisites

- Basic AI literacy and familiarity with enterprise processes, data ownership, and risk concepts. Coding is not required. Sector-specific or jurisdiction-specific legal interpretation requires qualified review outside this course.

PROGRAM OUTCOMES

Capabilities your teams will gain

- Create an AI inventory with accountable ownership.
- Assess use-case context and relevant risks.
- Map risks to implementable controls and evidence.
- Review release and ongoing-monitoring responsibilities.
- Run an incident and exception review with clear decisions.

ENTERPRISE CUSTOMIZATION

Enterprise customization

Tailor this program to your organization's priorities: Build practical AI inventories controls and review evidence across the lifecycle

- 2 learning days of 8 hours, or 4 sessions of 4 hours. Learning hours exclude breaks and include module exercises and capstone time. Setup is completed before the course.

CURRICULUM

Curriculum roadmap

1

MODULE 1 · 2 PROPOSED HOURS

AI lifecycle and governance responsibilities

Governance makes decision ownership and control evidence explicit. Define the business owner, technical owner, data owner, risk reviewer, and incident responsibilities for each use case. Distinguish a framework for risk management from a legal compliance determination.

- AI use cases and lifecycle boundaries
- Accountability and review forums
- Framework context and legal-review boundaries

Planned lab: Map ownership for three enterprise AI use cases.

Expected output: Accountability matrix and governance scope.

2 MODULE 2 · 2 PROPOSED HOURS

Inventory and intake

An inventory should capture what the system does, who uses it, what information it accesses, and which external services it depends on. A list of model names alone does not support an operational review.

- Use-case inventory and intended use
- Data and third-party dependencies
- Intake and change triggers

Planned lab: Create an inventory record for a support assistant, an HR drafting tool, and an invoice triage workflow.

Expected output: Inventory and intake form.

3 MODULE 3 · 3 PROPOSED HOURS

Risk assessment and control selection

Risk depends on use, impact, access, and operating conditions. Select controls that change behaviour or provide decision evidence. Assign each control an owner and a method for checking whether it works.

- Context and impact assessment
- Privacy, security, quality, and oversight risks
- Control owner and evidence mapping

Planned lab: Build a risk register and control matrix for the synthetic support application.

Expected output: Risk assessment and control matrix.

4 MODULE 4 · 3 PROPOSED HOURS

Assurance and release evidence

Assurance reviews whether the evidence supports the proposed use. Check evaluation coverage, access tests, approval boundaries, source provenance, and operations readiness. A green aggregate metric should not hide a blocking failure.

- Evidence standards and review criteria
- Evaluation and security reports
- Exceptions and conditional approval

Planned lab: Review a deliberately incomplete evidence pack and issue an approval, conditional approval, or hold decision.

Expected output: Assurance checklist and reasoned review decision.

5 MODULE 5 · 2 PROPOSED HOURS

Operational monitoring and change

AI systems and their contexts change after release. Define review triggers for new sources, model changes, expanded users, and incidents. Keep the inventory and evidence aligned with the version actually in use.

- Monitoring owners and review triggers
- Model/source/use changes
- Retention and documentation responsibilities

Planned lab: Draft a change and periodic-review process with clear escalation responsibilities.

Expected output: Change-control and monitoring plan.

6 MODULE 6 · 2 PROPOSED HOURS

Incident and exception tabletop

An incident response needs clear roles, a contained workflow, and evidence for restart. Exceptions should be time-bounded and owned rather than silently accepted. Document the decision and follow-up actions.

- Incident identification and containment
- Exception expiry and risk acceptance
- Restart criteria and learning actions

Planned lab: Run a tabletop for a restricted-source disclosure in a synthetic assistant.

Expected output: Incident record and corrective-action list.

7

MODULE 7 · 2 PROPOSED HOURS

Governance capstone

Bring the inventory, risk assessment, control evidence, and operating responsibilities together. Present a justified decision for a specific use case and identify what remains outside the evidence available.

- Governance evidence index
- Decision and ownership presentation
- Follow-up plan

Planned lab: Present a complete governance review for one synthetic AI use case to a mock review panel.

Expected output: Governance pack and next-review plan.

CAPSTONE

Capstone

A governance and assurance pack for an enterprise AI assistant, including inventory, risks, controls, evidence review, and an incident tabletop.

ASSESSMENT

Assessment

Inventory and ownership 25%; risk/control mapping 30%; evidence review 30%; incident and decision communication 15%. The work must not confuse framework alignment with legal certification.

DELIVERABLES

Participant deliverables

- AI inventory and ownership matrix
- Risk and control register
- Assurance checklist and decision record
- Change and incident review plan

SCOPE

Scope boundaries

Legal advice, accredited auditor qualification, ISO certification preparation, and a guarantee of compliance with any jurisdiction. **Delivery options:** 2 learning days of 8 hours, or 4 sessions of 4 hours. Learning hours exclude breaks and include module exercises and capstone time. Setup is completed before the course.

DELIVERY

Delivery options

2 learning days of 8 hours, or 4 sessions of 4 hours. Learning hours exclude breaks and include module exercises and capstone time. Setup is completed before the course. Proposed hours exclude breaks and are subject to pilot validation.

PRIVATE DELIVERY

Plan a private cohort for your team

Scope delivery format, role mix, and rollout timeline with our solutions team.

[Plan Private Delivery](#)[Book advisory call](#)