AI for Internal & IT Audit

Built for audit teams asked to assess AI systems they were never trained to test — delivered in person, hands-on with real techniques.

WHO IT'S FOR	FORMAT	LENGTH
Internal and IT audit teams, audit partners, and audit professionals.	In-house workshop	Full-day

What your team walks away with

Plan and run an audit of an AI system — its governance, its operation, and the tools to actually test it.

What you'll learn

- ✓ Build enough working knowledge of AI systems to ask the right questions without becoming a data scientist
- ✓ Plan an AI audit: set scope, identify the real risks and decide what evidence proves a control works
- ✓ Test AI controls across governance, data, the model itself and its outputs
- ✓ Audit third-party and embedded AI you didn't build by examining inputs, outputs and oversight
- ✓ Write up AI audit findings so they're clear, fair and actionable
- ✓ Reuse a structured AI audit work programme on the next system without starting over

Curriculum

01 What auditors need to understand about how AI systems work

- How AI and machine-learning systems behave, in terms an auditor needs
- The AI life cycle: data, training, deployment, monitoring, decommissioning
- Common failure modes: bias, drift, opaque decisions, data leakage
- Where AI risk sits inside existing governance and model-risk expectations
- Knowing enough to challenge a system without having to build one

02 Building an AI audit plan: scope, risks and evidence

- Scoping an AI audit: which systems, which decisions, which risks matter most
- Identifying the real risks rather than auditing everything equally
- Deciding what evidence would actually prove a control is working
- Mapping the audit to governance, data, model and output domains
- Planning fieldwork when the firm bought the model rather than built it

03 Testing AI controls — governance, data, model and output

- Testing governance: approvals, ownership, documentation and oversight
- Testing data: quality, sources, consent and representativeness
- Testing the model: validation, performance, bias and change control
- Testing outputs: monitoring, explainability and human review
- Practical techniques for gathering evidence on each

04 Auditing third-party and embedded AI you didn't build

- Auditing AI inside vendor tools you can't see inside
- Testing inputs and outputs when the model is a 'black box'
- Assessing the firm's oversight and contracts with the vendor
- What vendor assurance to demand, and how to verify it
- Where accountability stays with the firm even for bought-in AI

05 Common AI audit findings and how to write them up

- The findings that come up most often in AI audits
- Writing findings that are clear, fair and grounded in evidence
- Rating severity and framing realistic, actionable recommendations
- Explaining technical issues to non-technical stakeholders
- Avoiding findings that won't hold up under challenge

06 A reusable AI audit work programme for your team

- Turning the approach into a repeatable work programme
- Steps, test procedures and evidence requirements you can reuse
- Adapting the programme to different AI systems and risk levels
- Building an evidence and documentation trail by default
- Keeping the programme current as AI and expectations evolve

You keep

> A ready-to-run AI audit work programme.
