

AGENTIC AI GOVERNANCE AND CONTROL



GENTEX[®]
TRAINING CENTER



Introduction

Agentic AI Governance and Control Training Course prepares technology, risk, and governance professionals to govern AI agents that plan and act with autonomy. Participants work through agentic AI fundamentals and architecture, agent autonomy levels and decision boundaries, the AI governance frameworks including the NIST AI RMF and ISO/IEC 42001, agent risk assessment and control design, human oversight and escalation models, accountability and auditability, and monitoring, incident response, and assurance as one connected discipline. The programme links the decisions an AI agent takes with the human accountability that must remain. As a result, learners gain a practical command of agentic AI governance. Furthermore, the course strengthens control judgement, oversight design, and technology risk literacy.

Agentic AI Governance and Control Course Objectives

- Explain agentic AI concepts, architecture, and autonomy levels.
- Apply the NIST AI RMF and ISO/IEC 42001 to agentic systems.
- Apply AI governance structures, policies, and accountability models.
- Apply agent risk assessment covering autonomy, data, and tool access.
- Apply control design: permissions, guardrails, and sandboxing.
- Apply human-in-the-loop and human-on-the-loop oversight models.
- Apply prompt, tool, and agent identity controls and audit logging.
- Apply model evaluation, testing, and red teaming for agents.
- Apply monitoring, incident response, and escalation procedures.
- Apply agent registries, documentation, and AI assurance reporting.

Course Methodology

- Interactive sessions built on agentic AI governance and control cases.

LEARN BOLD. LEAD BEYOND

GENTEX Training Center LLC | Orlando - FL, USA
Info@gentextraining.com



- Workshops on autonomy mapping, risk assessment, and control design.
- Group exercises on oversight models, escalation, and incident scenarios.
- Hands-on practice with control matrices, agent registers, and audit logs.
- Simulation of an AI governance board review and an agent incident.
- Facilitator coaching and peer review on personal AI governance plans.

Who Should Take This Course

- AI governance and technology risk professionals.
- CIOs, CTOs, and digital transformation leaders.
- Risk, compliance, and internal audit staff covering AI.
- Data scientists and ML engineers with governance duties.
- Information security and data protection officers.
- Consultants advising on AI governance and control frameworks.

Agentic AI Governance and Control Course Outlines

Day 1: Agentic AI Fundamentals and Architecture

- Generative AI, LLM agents, and agentic behaviour.
- Agent architecture: models, memory, tools, and orchestration.
- Autonomy levels and degrees of decision latitude.
- Multi-agent systems and delegation patterns.
- Capability, limitation, and failure mode awareness.
- Regulatory landscape and emerging AI obligations.
- Case discussion: an agent that acted correctly and harmfully.





Day 2: AI Governance Frameworks and Structures

- NIST AI Risk Management Framework and its functions.
- ISO/IEC 42001 AI management system requirements.
- OECD AI principles and sector regulatory expectations.
- AI governance structures, councils, and accountability.
- AI policy, use case intake, and approval gates.
- The three lines model applied to AI risk.
- Workshop: mapping an agentic AI governance structure.

Day 3: Agent Risk Assessment and Control Design

- Agent risk assessment: autonomy, data, and tool exposure.
- Data governance, privacy, and data leakage risk.
- Tool and API access risk and permission scoping.
- Control design: guardrails, sandboxing, and rate limits.
- Least privilege, identity, and credential management for agents.
- Human approval thresholds and transaction limits.
- Exercise: designing controls for a high-autonomy agent.

Day 4: Oversight, Testing, and Incident Response

- Human-in-the-loop and human-on-the-loop models.
- Escalation design, override, and kill-switch capability.
- Prompt, tool, and agent identity audit logging.
- Model evaluation, testing, and red teaming.
- Bias, hallucination, and drift monitoring.

LEARN BOLD. LEAD BEYOND

GENTEX Training Center LLC | Orlando - FL, USA
Info@gentextraining.com



- AI incident response, containment, and disclosure.
- Simulation: responding to an agent incident and escalating it.

Day 5: Assurance, Documentation, and Reporting

- Agent registries and inventory documentation.
- Model cards, system documentation, and decision records.
- AI assurance approaches and internal audit over AI.
- Third-party and model supplier risk management.
- AI governance reporting to the board and regulators.
- Continuous improvement and AI governance maturity.
- Capstone: presenting an agentic AI governance and control framework.

Conclusion

By successfully completing Agentic AI Governance and Control, participants will gain a practical command of agentic AI concepts and autonomy levels, AI governance frameworks including the NIST AI RMF and ISO/IEC 42001, agent risk assessment and control design, human oversight and escalation models, and monitoring, assurance and AI governance reporting. They will acquire skills in AI governance structuring, agent risk assessment, control and oversight design, and AI assurance reporting that keep autonomous systems accountable. Gentex Training Center designs the programme to help professionals govern agentic AI with confidence.

FAQs for the Agentic AI Governance and Control course





Q1 What is the "Agentic AI Governance and Control" course about?

It prepares technology, risk, and governance professionals to govern AI agents that plan and act with autonomy. The course spans agentic AI fundamentals and architecture, AI governance frameworks and structures, agent risk assessment and control design, oversight, testing and incident response, and assurance, documentation and reporting.

Q2 What are the key benefits of the "Agentic AI Governance and Control" course?

You gain a practical command of agentic AI governance that links the decisions an AI agent takes with the human accountability that must remain. The course improves autonomy mapping and governance structuring, strengthens control design across permissions and guardrails, sharpens oversight and incident response practice, and gives you AI assurance and regulatory reporting that keeps autonomous systems accountable.

Q3 What skills will I gain from the "Agentic AI Governance and Control" course?

You will develop four core skills: AI governance framework application with the NIST AI RMF and ISO/IEC 42001, agent autonomy mapping and risk assessment, agent control design with oversight, escalation and incident response, and AI assurance, documentation and governance reporting.



Q4 What tools, methods, or standards are covered in the "Agentic AI Governance and Control" course?

The course covers generative AI, LLM agents and agentic behaviour, agent architecture across models, memory, tools and orchestration, autonomy levels and degrees of decision latitude, multi-agent systems and delegation patterns, capability, limitation and failure mode awareness, the regulatory landscape and emerging AI obligations, the NIST AI Risk Management Framework and its functions, ISO/IEC 42001 AI management system requirements, OECD AI principles and sector regulatory expectations, AI governance structures, councils and accountability, AI policy, use case intake and approval gates, the three lines model applied to AI risk, agent risk assessment across autonomy, data and tool exposure, data governance, privacy and data leakage risk, tool and API access risk and permission scoping, control design with guardrails, sandboxing and rate limits, least privilege, identity and credential management for agents, human approval thresholds and transaction limits, human-in-the-loop and human-on-the-loop models, escalation design, override and kill-switch capability, prompt, tool and agent identity audit logging, model evaluation, testing and red teaming, bias, hallucination and drift monitoring, AI incident response, containment and disclosure, agent registries and inventory documentation, model cards, system documentation and decision records, AI assurance approaches and internal audit over AI, third-party and model supplier risk management, and AI governance reporting to the board and regulators.



Q5 How is the "Agentic AI Governance and Control" course applied in real-world practice?

Participants apply it to real work such as mapping an agentic AI governance structure, assessing autonomy and tool exposure risk for an agent, designing controls for a high-autonomy agent, defining escalation and kill-switch procedures, reviewing agent audit logs, running an agent red teaming exercise, documenting an agent in the registry, and presenting an AI governance framework to the board. The same methods support AI incident response and assurance over third-party models.