

Course : Operational Governance of AI—Defining Roles, Uses, Risks, and Controls

Design and deploy a compliant, manageable, and operational AI governance framework

Practical course - 3d - 21h00 - Ref. ODN

Price : 2220 CHF E.T.

NEW

The rise of generative and predictive AI, as well as AI agents, is transforming organizational practices while creating new challenges in risk management, compliance, and accountability. Faced with the growing requirements of the European AI Act, business, IT, risk, and compliance departments must implement appropriate governance frameworks that regulate AI usage while fostering innovation. This training course provides a comprehensive and immediately applicable methodology for building an operational AI governance framework.

Teaching objectives

At the end of the training, the participant will be able to:

- ✓ Identify the challenges, risks, and regulatory requirements applicable to generative, predictive, and agent-based AI systems
- ✓ Establish an AI governance framework by defining appropriate roles, responsibilities, committees, and decision-making processes
- ✓ Develop key AI governance frameworks: AI systems registry, usage policy, validation process, risk classification, and controls
- ✓ Implement a system for risk management, oversight, auditability, and AI incident management
- ✓ Develop a deployment roadmap and performance metrics to enable continuous improvement in AI governance

Intended audience

Executives and leaders in digital transformation, innovation leaders, AI leaders, CIOs, data governance leaders, CISOs, DPOs, compliance officers, risk managers, legal counsel, internal auditors, business unit leaders, and project managers involved in AI initiatives.

PARTICIPANTS

Executives and leaders in digital transformation, innovation leaders, AI leaders, CIOs, data governance leaders, CISOs, DPOs, compliance officers, risk managers, legal counsel, internal auditors, business unit leaders, and project managers involved in AI initiatives.

PREREQUISITES

Understand the fundamental concepts of artificial intelligence and its main applications in business.

TRAINER QUALIFICATIONS

The experts leading the training are specialists in the covered subjects. They have been approved by our instructional teams for both their professional knowledge and their teaching ability, for each course they teach. They have at least five to ten years of experience in their field and hold (or have held) decision-making positions in companies.

ASSESSMENT TERMS

The trainer evaluates each participant's academic progress throughout the training using multiple choice, scenarios, hands-on work and more. Participants also complete a placement test before and after the course to measure the skills they've developed.

Prerequisites

Understand the fundamental concepts of artificial intelligence and its main applications in business.

Practical details

Interactive presentations illustrated with real-world examples and lessons learned. A common thread running through the entire lifecycle of an AI governance framework. Individual assignments, pair exercises, and collaborative workshops in small groups. Reusable templates provided to participants: AI registry, RACI matrix, AI usage policy, risk classification grid, vendor evaluation grid, incident management procedure, governance dashboard, and roadmap.

Course schedule

1 Understanding the Challenges and Governance Framework of AI

- Identify the specific characteristics of generative AI, predictive AI, and agent-based AI, as well as their impacts on governance
- Analyze the strategic, organizational, technical, and regulatory issues related to the use of AI in business.
- Distinguish AI governance from data governance, cybersecurity, compliance, risk management, and project governance
- Assess the risks associated with AI systems: bias, data leaks, vendor lock-in, lack of traceability, and model drift, etc.
- Identify the key requirements of applicable standards and regulations, including the AI Act, the GDPR, and risk management frameworks

Hands-on work

Group case study based on a company that uses multiple generative and predictive AI systems. Working in small groups, participants map out use cases, identify stakeholders, assess associated risks, and determine governance issues. Findings are presented and consolidated during a plenary session.

2 Define AI Roles, Responsibilities, and Governance Bodies

- Identify the key stakeholders in AI governance: executive sponsor, CIO, CISO, DPO, vendors, etc.
- Building a RACI Matrix Tailored to the Lifecycle of AI Systems
- Define responsibilities for validation, oversight, monitoring, and risk management
- Establishing Governance Bodies: AI Committee, Risk Committee, Arbitration Committee, and Periodic Reviews
- Establish a formal escalation process that specifies the roles of approval, veto, review, arbitration, and ultimate responsibility

Hands-on work

Workshop on designing a target governance structure. Working in groups, participants develop a comprehensive RACI matrix, define the roles and responsibilities of the various stakeholders, and outline the functioning of an AI governance committee. Cross-group presentation and critical analysis of the proposed models.

TEACHING AIDS AND TECHNICAL RESOURCES

- The main teaching aids and instructional methods used in the training are audiovisual aids, documentation and course material, hands-on application exercises and corrected exercises for practical training courses, case studies and coverage of real cases for training seminars.
- At the end of each course or seminar, ORSYS provides participants with a course evaluation questionnaire that is analysed by our instructional teams.
- A check-in sheet for each half-day of attendance is provided at the end of the training, along with a course completion certificate if the trainee attended the entire session.

TERMS AND DEADLINES

Registration must be completed 24 hours before the start of the training.

ACCESSIBILITY FOR PEOPLE WITH DISABILITIES

Do you need special accessibility accommodations? Contact Mrs. Fosse, Disability Manager, at psh-accueil@orsys.fr to review your request and its feasibility.

3 Develop policies, processes, and controls for the use of AI

- Develop a policy for the responsible use of AI that addresses business, regulatory, and ethical requirements
- Establish a specific policy governing the use of generative AI: prohibited data, permitted uses, human validation, etc.
- Create a registry of AI systems that includes use cases, purposes, owners, data used, vendors, etc.
- Define a process for validating and approving AI applications
- Implement a Shadow AI management framework: detection, reporting, awareness-raising, oversight, and remediation

Hands-on work

Overarching Theme. Participants gradually develop a comprehensive AI registry, define a policy for the use of generative AI, and establish a process for validating AI projects. Work is conducted in pairs, followed by a group consolidation session to produce a model that can be directly applied in a business setting.

4 Implement AI risk management, controls, and compliance

- Mapping risks throughout the lifecycle of AI systems: scoping, design, testing, validation, etc.
- Classify AI systems based on their level of criticality and risk
- Define preventive, detective, and corrective controls appropriate for different uses
- Implement mechanisms for human oversight, traceability, and auditability
- Prepare the compliance and supporting documentation required for audits and regulatory inspections

Hands-on work

Scenario. Based on the case study, participants will develop a risk classification matrix, define applicable controls (human validation, data review, bias testing, logging, access control, supplier audit), and create an AI risk map. Group debriefing and comparison of the selected approaches.

5 Oversee AI providers and manage incidents

- Assess the risks associated with suppliers and external AI solutions
- Develop a supplier evaluation framework that incorporates security, privacy, data location, etc.
- Define the procedures for monitoring and periodically reviewing AI suppliers
- Establish an AI incident management procedure
- Organize the handling of incidents related to critical errors, data breaches, model deviations, etc.

Hands-on work

Group case study. Participants evaluate several AI providers using a structured analysis grid and then design an incident management procedure that includes mechanisms for detection, escalation, investigation, remediation, and lessons learned.

6 Developing an AI Governance Roadmap and Driving Its Continuous

Improvement

- Assess the organization's level of maturity in AI governance
- Define a phased approach: identify use cases, create an AI registry, formalize roles, etc.
- Building an AI Governance Dashboard
- Define performance metrics: identified use cases, validation rates, AI incidents, document compliance, etc.
- Organize periodic reviews and the process for continuous improvement of the system

Hands-on work

Summary Workshop. Each participant develops an AI governance roadmap tailored to their organization. Using the case study as a guide, they define priorities, deliverables, responsibilities, monitoring metrics, and deployment milestones. The session concludes with a final presentation and an exchange of best practices among participants.

This programme is an original creation, developed by the teaching teams at ORSYS Formation. Any reproduction, representation, adaptation or use, in whole or in part, without the prior written authorisation of ORSYS, is strictly prohibited. ORSYS reserves the right to take any action necessary to protect its intellectual property rights.

Dates and locations

REMOTE CLASS

2026 : 7 Dec.

2027 : 15 Mar., 28 June, 4 Oct., 13 Dec.