

Updated on 10/13/2026

Sign Up

AI Governance Professional Certification Training

2 days (14 hours)

Overview

The AI Governance Professional Certification Training prepares you for the official Artificial Intelligence Governance Professional (AIGP) certification and equips you with the essential knowledge to govern reliable, responsible, and compliant artificial intelligence systems.

This course helps you prepare for the IAPP's AIGP exam, which is designed to assess your understanding of AI systems, their impacts, and the governance practices needed to ensure security, trust, and risk management.

You will learn how to structure an AI governance approach, define appropriate roles, policies, and controls, and then assess risks related to data, models, uses, and automated decisions throughout the entire lifecycle.

The program covers applicable regulatory frameworks and standards, including the GDPR, the EU AI Act, and risk management frameworks. You will also study the governance of the design, training, deployment, monitoring, and maintenance of AI systems.

Upon completion of the training, you will be able to effectively prepare for the official exam, analyze certification scenarios, and contribute to the implementation of responsible AI within your organization.

Like all our training courses, this one will introduce you to **the latest stable version** of the AI Governance Professional technology [\(1.27.2\)](#) and its new features.

Objectives

- Master the knowledge areas assessed by the Artificial Intelligence Governance Professional (AIGP) certification
- Identify the risks, impacts, and trust principles applicable to artificial intelligence systems
- Structure an AI governance program covering roles, policies, controls, and processes
- Apply the requirements of the GDPR, the EU AI Act, and key standards to AI use cases
- Evaluate the governance of the design, deployment, and operational monitoring of an AI system
- Answer exam-style questions and develop a strategy for preparing for certification

Target Audience

- AI Manager
- Data Protection Officer
- Compliance Manager
- Data Scientist
- Cybersecurity Manager

Prerequisites

- General knowledge of artificial intelligence systems and their use cases
- Experience with risk management, compliance, or data protection issues
- Knowledge of the key principles of the GDPR or an equivalent regulatory framework
- Ability to analyze business processes and governance scenarios

Technical Requirements

- Laptop with at least 8 GB of RAM and a recent processor
- Stable internet connection allowing access to training resources and collaborative tools
- A recent browser, such as Google Chrome or Microsoft Edge (up to date)
- Office suite compatible with PDF documents and presentation files

Curriculum for our AI Governance Professional Training

[Day 1 - Morning]

Fundamentals of AI and Responsible Governance

- Overview of the Artificial Intelligence Governance Professional (AIGP) certification, exam structure, and preparation methods

- Key concepts in artificial intelligence, machine learning, generative models, and autonomous systems
- The lifecycle of an AI system, from requirement definition to model retirement or replacement
- Understanding the 6 capabilities of the ITIL AI Capability Model: creation, curation, clarification, cognition, communication, and coordination
- Socio-technical impacts, risks of bias, discrimination, opacity, privacy violations, and security risks
- Principles of trustworthy AI: transparency, explainability, robustness, fairness, human oversight, and accountability
- Mapping the risks associated with the various AI capabilities and creating a heatmap of risks by capability
- Hands-on workshop: Analyze a generative AI use case, identify its stakeholders, impacts, and risks, then create a risk heatmap based on the capabilities used

[Day 1 – Afternoon]

Legal frameworks, standards, and risk management

- The relationship between AI governance, data protection, cybersecurity, compliance, ethics, and business continuity
- Application of GDPR principles to AI systems, purposes, data minimization, lawfulness, and impact assessments
- Key elements of the EU AI Act, risk-based approach, obligations of stakeholders, and requirements for high-risk systems
- Overview of standards, frameworks, and governance tools, including risk management and AI management
- Methods for identifying, assessing, addressing, and monitoring risks associated with an AI system
- Assessing risks using a probability × impact matrix and defining criticality and response levels
- Implement preventive, detective, and corrective controls tailored to the risks, uses, and the AI system's lifecycle
- Hands-on workshop: Build a probability × impact matrix and define preventive, detective, and corrective controls for a decision-support tool incorporating an AI model

[Day 2 – Morning]

Govern the development and adoption of AI systems

- Organizing an AI governance program: roles, responsibilities, committees, policies, and escalation mechanisms
- Design governance, requirements definition, documentation, traceability, and validation of business objectives
- Management of training and test data, quality, provenance, representativeness, usage rights, and data protection
- Model evaluation, performance testing, fairness, robustness, security, red teaming, and acceptance criteria

- Integrating AI governance requirements into DevOps and PRINCE2 project management practices: responsibilities, controls, validation milestones, and evidence
- Preparation for production deployment, model documentation, evidence of controls, and of suppliers
- Mapping stakeholders, their expectations, their influence, and their level of exposure to AI applications
- Organizing communication and transparency with users, supporting teams, and develop the skills needed for adoption
- Identify and manage “Shadow AI,” define authorized uses, and track metrics for adoption, understanding, and trust
- Hands-on workshop: Develop an adoption and stakeholder engagement plan for the deployment of an AI system

[Day 2 – Afternoon]

Deployment, resilience, monitoring, and preparation for review

- Deployment decision, analysis of the usage context, proportionality, human oversight, and communication with users
- Defining human supervision mechanisms, takeover conditions, and the levels of autonomy granted to the AI system
- Plan for fallback and rollback mechanisms in the event of unexpected behavior, performance degradation, or uncontrolled risk
- Implement observability for AI systems: logging, metrics, alerts, data drift and model drift, and risk indicators
- Organize AI incident management, alert escalation, root cause analysis, and the implementation of corrective measures
- Prepare for business continuity in the event of a failure, unavailability, or change in an AI model or service provider
- Continuous monitoring, risk reassessment, maintenance, evolution, and decommissioning of the system
- Hands-on workshop: Build a resilience plan for an AI use case that includes human oversight, observability, incident management, fallback, and supplier continuity
- Review of the AIGP framework domains, reading of scenarios, and strategies for responding to multiple-choice questions
- Exam preparation, time management, identifying common pitfalls, and prioritizing study topics

Target Audience

This training is intended for both individuals and companies—large or small—seeking to train their teams in new, advanced IT technologies or to acquire specific domain knowledge or modern methodologies.

Entry-Level Assessment

The pre-training assessment complies with Qualiopi quality standards. Upon final registration, the learner receives a self-assessment questionnaire that allows us to evaluate their estimated proficiency in various types of technologies, as well as their expectations and personal goals for the upcoming training, within the limits imposed by the selected format. This

questionnaire also allows us to anticipate certain connection or internal security issues within the company (intra-company or virtual classroom) that could pose challenges for the monitoring and smooth operation of the training session.

Teaching Methods

Hands-On Course: 60% Hands-On, 40% Theory. Training materials distributed in digital format to all participants.

Organization

The course alternates between theoretical input from the instructor—supported by examples and reflection sessions—and group work.

Assessment

At the end of the session, a multiple-choice quiz is administered to verify that participants have successfully acquired the skills.

Certification

A certificate will be issued to each trainee who has completed the entire training program.