Auditing and Securing AI: Cyberthreats, Ethics, Compliance

Duration: 4 days
Audience: Professionnel TI

Who is this training for?

Executives and teams responsible for technology, compliance, security, and AI projects.

Training objectives

- Analyze the differences between traditional IT audits and artificial intelligence-specific audits.
- Classify and distinguish the types of AI audits (technical, ethical, compliance) according to their characteristics.
- Use the major standards (ISO/IEC 42001, NIST AI RMF, MITRE ATT&CK, TRiSM) to structure and carry out an AI audit.
- Plan and carry out a complete AI audit by following the key steps: preparation, collection of evidence, analysis, restitution.
- Develop a customized checklist and implement internal practices to ensure the continuity of AI audits.

Summary

This training offers a complete program to master audits applied to artificial intelligence (AI). It allows participants to understand the specifics of AI audits, explore key compliance frameworks, and develop a practical methodology for effectively auditing AI systems.

Course outline

Week 1: Audit Fundamentals

Definition and role of auditing in IT and cybersecurity

- Discover the specificities, steps and main challenges related to artificial intelligence audits to ensure the compliance and security of digital systems.

Copyright © 2026 AFI by Edgenda inc.

Week 2: Typology and use cases of AI audits

Discover the different types of AI audits

- Technical (model, data, security), ethical (bias, transparency, fairness) and governance and compliance. Explore use cases: regulatory validation, bias reduction, and risk management.

Week 3: AI audit standards & methodology

Overview of the main standards for AI

- ISO/IEC 42001 for AI systems management, NIST AI Risk Management Framework, MITRE ATT&CK applied to AI, TRiSM (Trust, Risk & Security Management) and responsible AI principles.

Week 4: Practical application & audit simulation

Discover the AI audit methodology

- Planning, evidence collection, analysis and restitution. Learn how to map risks, define controls, develop an AI checklist, and assess the compliance of an AI project through a case study.

Approach and methodology

This course adopts a progressive and methodological approach, combining conceptual presentations, reference analyses and practical scenarios. The learning is centered on the realization of AI audits through case studies, making it possible to mobilize recognized executives and apply a structured approach. The progression aims to develop concrete skills in risk assessment, compliance and governance of artificial intelligence systems.

Prerequisites

- Basic knowledge of IT and cybersecurity.
- Notions about artificial intelligence.
- Experience in compliance, security or technology projects.

Recommendations

Copyright © 2026 AFI by Edgenda inc.

Review : the basics of cybersecurity the fundamental concepts of AI

Familiarize yourself with : governance and compliance issues

Identify your needs : management of risks related to AI audit and control of AI systems ethical and regulatory framework

Copyright © 2026 AFI by Edgenda inc.