+33 (0)1 48 10 09 46
formation@ambient-it.net
140 Avenue Jean Lolive 93500 Pantin - France

Updated on 10/27/2026

Sign Up

ISO/IEC 27090 Lead Implementer Certification Training

5 days (35 hours)

Overview

ISO/IEC 27090:2026 provides an overview of the threats specific to artificial intelligence systems, their consequences, and the means to detect and mitigate them. Its recommendations cover the entire AI lifecycle, from design to decommissioning, including updates and model retraining.

Our ISO/IEC 27090 Lead Implementer Certification Training prepares you for the individual AI Security (ISO/IEC 27090:2026) Lead Implementer (ITC-230) certification issued by ITCERTS, which assesses advanced knowledge of AI security.

You will learn how to integrate ISO/IEC 27090 with ISO/IEC 42001 for AI management, ISO/IEC 27001 for information security management, and ISO/IEC 27002 for security measures.

Using an AI system as a common thread, you will analyze scenarios involving the compromise of data, models, and generative interfaces. You will examine their consequences, detection possibilities, and appropriate mitigation measures, taking into account their limitations and interactions.

Upon completion of the training, you will be able to develop a security plan and contribute to the risk assessment and treatment within your ISMS, in accordance with clauses 6.1.2 and 6.1.3 of ISO/IEC 27001. The workshops will allow you to test security controls, justify your choices, and document residual risks.

The preparation aligns with the exam objectives published by ITCERTS and combines case studies, a French–English glossary, quizzes, and a practice exam.

This training is based on ISO/IEC 27090:2026 and puts its recommendations into practice through AI security scenarios.

Objectives

- Identify the complementary roles of ISO/IEC 27090, 42001, 27001, and 27002
- Analyze threats, compromise scenarios, and their consequences throughout the entire AI lifecycle
- Inform the assessment and management of ISMS risks based on threats specific to AI systems
- Select and implement detection and mitigation measures tailored to data, models, and interfaces
- Verify the effectiveness of safeguards, analyze their interactions, and document residual risks
- Organize monitoring, incident response, and the reassessment of safeguards
- Prepare for the ITC-230 exam using practical case studies, practice questions, and an educational mock exam

Target Audience

- Cybersecurity Architect
- Information Systems Security Manager
- ISMS Manager or Cybersecurity Risk Management Consultant
- Machine Learning Engineer
- MLOps Engineer
- AI Security Consultant

Prerequisites

- Experience in cybersecurity and a basic understanding of risk management
- Understanding of the fundamentals of machine learning, training, and inference
- Proficiency in technical English for preparing for and taking the exam in English

Technical Requirements

- Computer running Windows 11 or Ubuntu 24.04 LTS with a quad-core processor and at least 8 GB of RAM for course activities
- Up-to-date Firefox or Chrome browser and PDF reader
- Stable internet connection allowing access to the learning platform and remote labs

Curriculum for our ISO/IEC 27090 Lead Implementer Training

[Day 1 - Morning]

Standard framework, relationship between standards, and scope of security measures

- Positioning of ISO/IEC 27090:2026: Understanding threats specific to AI systems, their consequences, detection, and mitigation
- Complementarity of standards: ISO/IEC 42001 for AI management, ISO/IEC 27001 for information security management, and ISO/IEC 27002 for security controls
- Distinction between the recommendations of ISO/IEC 27090 (a catalog of measures), the requirements of a management system, and individual certification
- Terminology related to AI systems, data, models, and learning, including the creation a French–English glossary
- Breakdown of the lifecycle, from design to decommissioning, and presentation of the objectives for preparing for the ITC-230 exam
- Hands-on workshop: Mapping a core AI system, its critical assets, and the responsibilities associated with each phase, then identify the contributions of the four standards.

[Day 1 - Afternoon]

Governance, threat modeling, and risk assessment

- Aligning AI governance with the information security management system and risk management responsibilities
- Identifying adversaries, access capabilities, exposed assets, and trust boundaries
- Using ISO/IEC 27090 as a source of threat scenarios for risk assessment—ISO/IEC 27001 §6.1.2
- Analysis of the impact on confidentiality, integrity, and availability; assessment of plausibility, and prioritization based on the organization’s criteria
- Application of Zero Trust and defense-in-depth principles to AI architectures
- Hands-on workshop: Develop a threat model and an initial risk register for the core system, then justify their prioritization through contextualized questions.

[Day 2 - Morning]

Data Threats and Securing the Learning Process

- Analysis of data provenance, transformations, and access rights
- Data poisoning scenarios, introduction of backdoors, and their impact on system behavior
- Anomaly detection, classification of contamination signals, and limitations of detection
- Selection of mitigation measures: integrity checks, source validation, and separation of datasets
- Protection of data collected in production before its reuse for retraining
- Hands-on workshop: Analyze a corrupted dataset, identify possible consequences, and set up a set of pre-training checks, then test your understanding with a quiz.

[Day 2 – Afternoon]

Model Integrity and Supply Chain

- Analysis of direct model poisoning, unauthorized parameter modifications, and their consequences
- Identifying threats related to third-party models, dependencies, and components in the supply chain
- Implementation of secure development best practices and hardening of environments and delivery pipelines
- Secret management, separation of privileges, and protection of the model registry
- Detection of tampering, provenance verification, version traceability, and acceptance criteria for artifacts
- Hands-on workshop: Securing model promotion, blocking an artifact whose integrity cannot be established, and justifying the chosen protections based on training scenarios.

[Day 3 - Morning]

Model evasion and confidentiality

- Analysis of evasion attacks, input tampering during inference, and their consequences
- Scenarios involving model exfiltration and extraction through querying
- Distinction between membership inference and model inversion, depending on the attacker's objectives and the information exposed
- Detection of misuse, reduction of output exposure, and query control
- Selecting mitigation strategies and evaluating trade-offs between privacy, robustness, accuracy, and availability
- Hands-on workshop: Testing an isolated inference interface, comparing protections against evasion and extraction, then assess various attack scenarios in a reasoned quiz.

[Day 3 - Afternoon]

Security of generative interfaces

- Analysis of direct and indirect prompt injections, their exploitation conditions, and their consequences
- Detection of sensitive information leaks and control of model outputs
- Distinguishing between prompt injection and outputs containing injection payloads that could affect downstream components
- Separation of instructions from untrusted content in RAG architectures
- Restricting tools, validating actions, and limiting agent privileges, with an analysis of the limits of these protections
- Hands-on Workshop: Exploiting an indirect injection in a lab assistant, deploying and retest application safeguards, then justify security decisions.

[Day 4 - Morning]

Risk management, validation of safeguards, and interactions

- Using the recommendations of ISO/IEC 27090 to enhance risk treatment—ISO/IEC 27001 §6.1.3—and determine the necessary measures
- Aligning AI-specific safeguards with ISO/IEC 27002, comparing them with Annex A of ISO/IEC 27001 and providing justification in the statement of applicability
- Development of a matrix of threats, consequences, detection methods, and mitigation measures, including an analysis of complementarities, conflicts, and blind spots
- Definition of an authorized and reproducible red teaming protocol, measurement of effectiveness, and qualification of false positives and false negatives
- Assessment of residual risk, justification of trade-offs, and formalization of the treatment plan
- Hands-on workshop: Test multiple protections on the reference system, document their interactions, and complete a remediation plan accompanied by an excerpt from the statement of applicability.

[Day 4 - Afternoon]

AI Incident Monitoring and Response

- Designing logging for access, versions, entries, and sensitive events, while controlling data exposure in logs
- Detecting malicious behavior and distinguishing it from drift or degradation

- Defining alerts, thresholds, and incident qualification procedures
- Containment, preservation of evidence, and rollback to a controlled version
- Reassessment of risks and the effectiveness of safeguards during updates, retraining, and decommissioning operations
- Hands-on workshop: Handling a compromise incident, isolating affected components, preparing for a secure recovery, and updating the risk register based on lessons learned.

[Day 5 - Morning]

Integrated case study and targeted preparation

- Consolidation of the security plan across the entire lifecycle and integration of results into the ISMS
- Formalization of responsibilities, selected measures, evidence of controls, residual risks, and reassessment criteria
- Review of the scope, the French–English glossary, and the principles for implementing information security
- Training in classifying security breaches, analyzing their consequences, and selecting appropriate measures
- Analysis of proposed responses and justification of choices in scenario-based questions covering the published topics of the ITC-230 exam
- Hands-on workshop: Present a security proposal including the assessment and management , followed by a defense of the chosen security measures before a simulated committee.

[Day 5 - Afternoon]

Mock exam and preparation for the actual exam

- Summary of key points and review of common terminology confusion based on quizzes completed during the training
- Techniques for reading questions in English, analyzing scenarios, and managing time
- Overview of the exam structure
- Administrative and technical preparation for taking the official exam
- Practical workshop: Take the mock exam, analyze answers and results by subject area, then develop an individual study plan before taking the official exam.

Target Companies

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

Assessment upon enrollment

The assessment conducted upon enrollment complies with Qualiopi quality standards. Upon final enrollment, the learner receives a self-assessment questionnaire that allows us to evaluate their estimated proficiency with 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 monitoring and ensuring the smooth operation of the training session.

Teaching Methods

Hands-On Training: 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.

Training organization registered under number 11 75 54743 75. This registration does not constitute state accreditation.
© Ambient IT 2015-2026. All rights reserved. Paris, France - Switzerland - Belgium - Luxembourg