

Updated on 10/13/2026

[Sign Up](#)

ISO/IEC 42001 Lead Implementer Certification Training

4 days (28 hours)

Overview

The ISO/IEC 42001 Lead Implementer Certification training prepares you to design, implement, and improve an artificial intelligence management system compliant with the ISO/IEC 42001 standard. It guides you toward the official PECB Certified ISO/IEC 42001 Lead Implementer exam and the validation of advanced skills in AI governance.

This training will enable you to go beyond the principles of governance to master critical topics related to the implementation of an AI Management System (AIMS), from context analysis to preparation for the certification audit.

You will learn to interpret the requirements of the ISO/IEC 42001 standard and to define the scope, policy, roles, objectives, and documentation necessary for deploying a robust AI management system.

Upon completion of the training, you will be able to plan an implementation strategy, assess risks associated with AI systems, select appropriate control measures, and drive continuous improvement of the AIMS.

The training also prepares you for the official PECB Certified ISO/IEC 42001 Lead Implementer exam through role-playing exercises, contextualized multiple-choice questions, and a structured review of the assessed competency areas.

Like all our training courses, this one will introduce you to **the latest stable version** of the technology and its new features.

Objectives

- Interpret the requirements of an AIMS based on ISO/IEC 42001
- Plan and lead the implementation of an artificial intelligence management system
- Assess risks, define objectives, and prepare the statement of applicability
- Implement the controls, documentation, and operational processes of the AIMS
- Organize monitoring, internal audits, management reviews, and continuous improvement
- Prepare for the PECB Certified ISO/IEC 42001 Lead Implementer exam

Target Audience

- AI Governance Manager
- Artificial Intelligence Consultant
- Compliance Manager
- AI Project Manager
- Risk Management Manager

Prerequisites

- General knowledge of management systems
- Basic knowledge of artificial intelligence and AI projects
- General understanding of the ISO/IEC 42001 standard
- Experience in risk management, compliance, or governance

Technical Prerequisites

- Computer running Windows 10 or 11, macOS, or a recent Linux distribution
- A modern web browser, such as Google Chrome, Microsoft Edge, or Mozilla Firefox
- Stable internet connection allowing access to course materials and online assessments
- Webcam, microphone, and a quiet environment required for taking an online exam supervised

Curriculum for our ISO/IEC 42001 Lead Implementer training

[Day 1 - Morning]

Fundamentals of AIMS and the certification framework

- Positioning of ISO/IEC 42001 within the ecosystem of AI standards and regulatory frameworks
- Fundamental concepts of artificial intelligence, AI systems, machine learning, and risk levels
- Principles, objectives, and benefits of an AI management system (AIMS)
- Structure of the standard, clauses 4 through 10, and Annexes A, B, C, and D

- Subject areas, question logic, and expectations for the PECB Certified ISO/IEC 42001 Lead Implementer exam
- Hands-on workshop: mapping an AI use case and identifying its stakeholders, impacts, and its risk level

[Day 1 – Afternoon]

Launching the implementation process

- Approaches to implementing an AIMS and integration with existing management systems
- Management commitment, project approval, and definition of governance
- Roles, responsibilities, authorities, and competencies of the implementation team
- Development of the roadmap based on the IMS2 methodology and associated best practices
- Analysis of certification requirements and criteria for achieving the various PECB certification levels
- Hands-on workshop: developing an AIMS project charter with a sponsor, roles, milestones, deliverables, and success metrics

[Day 2 – Morning]

Context, scope, and planning for AIMS

- Analysis of the organizational context, internal and external challenges, and stakeholder requirements
- Defining the scope of the AIMS based on the relevant activities, products, data, models, and suppliers involved
- Assessment of the current state, gap analysis, and prioritization of compliance initiatives
- Development of the AI policy, measurable objectives, and implementation plan
- Management of resources, dependencies, skills, and planning documentation
- Hands-on workshop: defining the scope and conducting an ISO/IEC 42001 gap analysis for a fictitious organization

[Day 2 – Afternoon]

AI risks and statement of applicability

- Principles of AI risk management and integration into the overall risk management framework
- Identification of risks related to data, models, usage, bias, transparency, and security
- Risk assessment, mitigation, and acceptance based on consistent and traceable criteria
- Selection of control measures from Appendix A and justification of their applicability
- Design of the Statement of Applicability and the Risk Treatment Plan

- Hands-on workshop: Creating a risk register and a statement of applicability for a generative AI system

[Day 3 - Morning]

Deployment of control measures

- Design and implementation of AIMS controls tailored to the organization's risks and objectives
- Data governance, quality, provenance, preparation, and responsible use of
- Management of the AI systems lifecycle: development, validation, deployment, and evolution
- Management of vendors, third-party components, external models, and cloud services
- Management of documented information, evidence of compliance, traceability, and retention
- Hands-on workshop: Designing a control deployment plan for an internal chatbot

[Day 3 – Afternoon]

Operational functioning and adoption

- Planning and managing AI operations within the scope of AIMS
- Change management, incidents, model anomalies, and use case evolutions
- Internal and external communication regarding AI responsibilities, limitations, and authorized uses
- Skill development, team awareness, and human oversight
- Preparation for scenario-based questions, analysis of alternatives, and expected reasoning on the exam
- Hands-on workshop: Building an operational process for change and incident management for an AI service

[Day 4 – Morning]

Monitoring, internal auditing, and improvement

- Defining performance indicators, monitoring methods, measurement, analysis, and evaluation
- Internal audit program, preparation of evidence, findings, and follow-up on actions
- Organizing the management review and utilizing its input and output data
- Handling nonconformities, root cause analysis, and implementation of corrective actions
- Continuous improvement of AIMS, controls, and governance practices
- Hands-on workshop: preparing an AIMS dashboard and addressing a nonconformity identified during an internal audit

[Day 4 – Afternoon]

Preparing for the audit and certification

- Preparing for a certification audit: steps, expected evidence, and stakeholder engagement
- Comprehensive review of the six competency areas of the PECB exam
- Strategies for answering the 80 multiple-choice questions, including contextualized scenarios
- Time management, analysis of complex statements, and identification of distractors
- Passing requirements, required score, and steps to apply for official certification
- Hands-on workshop: taking a timed practice exam, reviewing answers, and creating a personalized study plan

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 industry 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 level across 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% Practical, 40% Theoretical. 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.