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

Updated on 11/13/2026

Sign Up

PECB Lead AI Risk Manager Certification Training

5 days (35 hours)

Overview

AI risk management helps ensure safe use and supports the responsible adoption of artificial intelligence. The official PECB Lead AI Risk Manager certification validates skills in identifying, assessing, and mitigating risks, with a particular focus on biases and issues related to security, transparency, and ethics.

Our PECB Lead AI Risk Manager Certification Training will help you prepare for the exam while developing a structured approach to AI risk management tailored to your organization's specific challenges.

You will learn how to establish governance, create a risk register, and apply the NIST AI Risk Management Framework while taking into account the requirements of the EU AI Act as they apply to the relevant use cases.

Upon completion of the training, you will be able to select appropriate mitigation measures, prepare incident response plans, and monitor residual risks to inform business decisions.

This preparation combines practical case studies with reviews of the exam's five competency areas. It distinguishes between passing the exam and meeting the experience and ethical requirements necessary to obtain the certification.

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

Objectives

- Understand the concepts, approaches, and techniques of AI risk management within their organizational context
- Identify, analyze, and evaluate biases as well as risks related to security, transparency, and ethical risks
- Define mitigation strategies and incident response measures tailored to the identified risks
- Align the NIST AI Risk Management Framework with the applicable requirements of the EU AI Act as part of a governance approach
- Organize risk monitoring and the continuous improvement of the system
- Prepare for the five competency areas of the PECB Lead AI Risk Manager exam using scenario-based exercises

Target Audience

- Risk Manager
- AI Governance Manager
- Information Systems Security Manager
- Compliance Manager
- Data Scientist

Prerequisites

- Understanding of the fundamental concepts of artificial intelligence and its main applications
- General knowledge of organizational risk management principles
- Familiarity with the data lifecycle and AI systems in a corporate setting
- Ability to read technical materials in English to prepare for the exam

Technical Prerequisites

- Laptop running Windows 11 or macOS with permissions to install the necessary tools
- An up-to-date version of Google Chrome or Mozilla Firefox and a PDF reader
- Microsoft Excel or LibreOffice Calc spreadsheet software for risk registers and matrices
- Stable internet connection allowing access to materials and the PECB Exams app without network restrictions
- For the remote exam: an active myPECB account, a tested PECB Exams app, a webcam, a microphone, and a quiet, private space

Curriculum for our PECB Lead AI Risk Manager training

[Day 1 - Morning]

Fundamentals of AI Risk

- Overview of the PECB Lead AI Risk Manager Certification Training and presentation of the five exam domains
- Major AI systems, business applications, and lifecycle stages
- Distinction between threat, vulnerability, incident, consequence, and risk
- Characteristics of trustworthy AI and its impacts on individuals and organizations
- Hands-on Workshop: Describe an AI system and identify its benefits, limitations, and initial risk scenarios.

[Day 1 - Afternoon]

Reference Frameworks and Responsibilities

- GOVERN, MAP, MEASURE, and MANAGE functions of the NIST AI Risk Management Framework
- Interplay between voluntary frameworks, regulatory requirements, and internal policies
- The risk-based approach of the EU AI Act and classification of relevant use cases
- Issues of transparency, human oversight, and ethical accountability
- Hands-on Workshop: Linking the risks from the case study to the functions of the NIST AI RMF and identifying compliance issues to be addressed.

[Day 2 - Morning]

Organizational Context and Governance

- Defining the scope, objectives, and stakeholders of the AI risk program
- Inventory of AI systems, data, and vendor dependencies
- Allocation of roles and responsibilities among business units, technical teams, and control functions
- Defining risk appetite, evaluation criteria, and escalation rules
- Hands-on Workshop: Developing a scope document and a responsibility matrix for the AI risk management program.

[Day 2 - Afternoon]

Identification of AI-Related Risks

- Identification techniques using interviews, document analysis, and scenarios
- Risks of bias, discrimination, and poor data quality
- Security vulnerabilities, data breaches, and dependencies on third-party components
- Lack of explainability, misuse, and ethical implications
- Hands-on Workshop: Populating a risk registry with the causes, events, consequences, and owners associated with the case study.

[Day 3 - Morning]

Risk Analysis and Assessment

- Analysis of Likelihood, Severity, and Exposed Populations
- Selection of qualitative and quantitative methods based on available data
- Review of existing controls, uncertainties, and measurement limits
- Prioritization of inherent and residual risks based on acceptance criteria
- Hands-on workshop: Evaluate multiple scenarios, develop a criticality matrix, and justify treatment priorities.

[Day 3 - Afternoon]

Risk Treatment and Mitigation

- Risk treatment options and trade-offs between reduction, avoidance, sharing, and acceptance
- Measures related to data, models, access, and authorized uses
- Controls for human oversight, transparency, and robustness
- Formalization of the risk treatment plan, responsible parties, and expected evidence of effectiveness
- Hands-on Workshop: Develop a mitigation plan and present a reasoned decision on the acceptance of residual risks.

[Day 4 - Morning]

Incident monitoring and response

- Definition of risk indicators, alert thresholds, and review frequencies
- Monitoring deviations, biases, and the effectiveness of control measures
- Organizing incident response, containment, and fallback solutions
- Event traceability, reporting, and notification requirements to be evaluated based on the context
- Hands-on Workshop: Simulate an incident involving an AI system and create a response sheet with escalation decisions.

[Day 4 - Afternoon]

Learning and Continuous Improvement

- Developing a training and awareness program tailored to at-risk profiles
- Leveraging feedback and analyzing the causes of incidents
- Evaluating the performance of the AI risk management program
- Governance reviews, corrective actions, and updating the risk register
- Hands-on Workshop: Developing a dashboard and an improvement roadmap based on the results of the case study.

[Day 5 - Morning]

Review and exam preparation

- Summary of the five competency areas and identification of concepts to reinforce
- Review of scenario-based questions and identification of key factors
- Justification of choices regarding governance, risk analysis, and risk management
- Time management and use of reference materials in accordance with exam rules
- Hands-on workshop: Take a timed mock exam, then analyze the answers and areas for improvement.

[Day 5 - Afternoon]

Exam and Certification Pathway

- Verification of exam conditions, identity, and exam environment
- Review of confidentiality rules and authorized resources
- Take the three-hour PECB Lead AI Risk Manager exam according to the scheduled session
- Distinction between passing the exam, applying for certification, and experience requirements
- Hands-on workshop: Prepare a list of the supporting documents required for the certification application, without discussing the confidential content of the exam.

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 professional 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% 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 used to verify that participants have successfully acquired

of 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