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

Mis à jour le 13/11/2026

S'inscrire

Formation Certification PECB Lead AI Risk Manager

5 jours (35 heures)

Présentation

Le management du risque lié à l'IA permet de sécuriser les usages et de soutenir une adoption responsable de l'intelligence artificielle. La certification officielle PECB Lead AI Risk Manager valorise les compétences en identification, évaluation et atténuation des risques, avec une attention particulière aux biais et aux enjeux de sécurité, de transparence et d'éthique.

Notre Formation Certification PECB Lead AI Risk Manager vous permettra de préparer l'examen tout en développant une démarche structurée de management du risque lié à l'IA adaptée aux enjeux de votre organisation.

Vous apprendrez à établir une gouvernance, à construire un registre des risques et à appliquer le NIST AI Risk Management Framework en tenant compte des exigences de l'EU AI Act selon les usages concernés.

À l'issue de la formation, vous serez en mesure de sélectionner des mesures d'atténuation pertinentes, de préparer la réponse aux incidents et de suivre les risques résiduels pour éclairer les décisions métier.

Cette préparation associe cas pratiques et révisions des cinq domaines de compétences de l'examen. Elle distingue la réussite à l'épreuve des conditions d'expérience et de déontologie nécessaires à l'obtention du titre.

Comme toutes nos formations, celle-ci vous présentera **la dernière version stable** de la technologie et ses nouveautés.

Objectifs

- Comprendre les concepts, les approches et les techniques du management du risque lié à l'IA dans leur contexte organisationnel
- Identifier, analyser et évaluer les biais ainsi que les risques de sécurité, de transparence et d'éthique
- Définir des stratégies d'atténuation et des mesures de réponse aux incidents adaptées aux risques identifiés
- Articuler le NIST AI Risk Management Framework avec les exigences applicables de l'EU AI Act dans une démarche de gouvernance
- Organiser la surveillance des risques et l'amélioration continue du dispositif
- Préparer les cinq domaines de compétences de l'examen PECB Lead AI Risk Manager à partir de mises en situation

Public visé

- Risk Manager
- Responsable gouvernance IA
- Responsable sécurité des systèmes d'information
- Responsable conformité
- Data Scientist

Pré-requis

- Compréhension des concepts fondamentaux de l'intelligence artificielle et de ses principaux usages
- Connaissance générale des principes de management du risque en organisation
- Familiarité avec le cycle de vie des données et des systèmes d'IA en entreprise
- Capacité à lire des supports techniques en anglais pour la préparation à l'examen

Pré-requis techniques

- Ordinateur portable sous Windows 11 ou macOS avec droits permettant l'installation des outils nécessaires
- Navigateur Google Chrome ou Mozilla Firefox à jour et lecteur de documents PDF
- Tableur Microsoft Excel ou LibreOffice Calc pour les registres et matrices de risques
- Connexion Internet stable permettant l'accès aux supports et à l'application PECB Exams sans blocage réseau
- Pour l'examen à distance, compte myPECB actif, application PECB Exams testée, webcam, microphone et espace individuel calme

Programme de notre formation PECB Lead AI Risk Manager

[Jour 1 - Matin]

Fondamentaux du risque lié à l’IA

- Positionnement de la Formation Certification PECB Lead AI Risk Manager et présentation des cinq domaines de l’examen
- Principaux systèmes d’IA, usages métier et étapes du cycle de vie
- Distinction entre menace, vulnérabilité, événement, conséquence et risque
- Caractéristiques d’une IA digne de confiance et impacts sur les personnes et les organisations
- Atelier pratique : Décrire un système d’IA et distinguer ses bénéfices, ses limites et ses premiers scénarios de risque.

[Jour 1 - Après-midi]

Cadres de référence et responsabilités

- Fonctions GOVERN, MAP, MEASURE et MANAGE du NIST AI Risk Management Framework
- Articulation entre cadre volontaire, exigences réglementaires et politiques internes
- Approche par les risques de l’EU AI Act et qualification des usages concernés
- Enjeux de transparence, de supervision humaine et de responsabilité éthique
- Atelier pratique : Relier les risques du cas fil rouge aux fonctions du NIST AI RMF et repérer les questions de conformité à examiner.

[Jour 2 - Matin]

Contexte organisationnel et gouvernance

- Définition du périmètre, des objectifs et des parties prenantes du programme de risques IA
- Inventaire des systèmes d’IA, des données et des dépendances fournisseurs
- Répartition des rôles et responsabilités entre métiers, équipes techniques et fonctions de contrôle
- Définition de l’appétence au risque, des critères d’évaluation et des règles d’escalade
- Atelier pratique : Construire une fiche de cadrage et une matrice de responsabilités pour le programme de management du risque IA.

[Jour 2 - Après-midi]

Identification des risques liés à l’IA

- Techniques d’identification par entretiens, analyse documentaire et scénarios
- Risques de biais, de discrimination et de qualité insuffisante des données
- Vulnérabilités de sécurité, fuites de données et dépendances aux composants tiers
- Défauts d’explicabilité, usages détournés et conséquences éthiques
- Atelier pratique : Alimenter un registre des risques avec les causes, événements, conséquences et propriétaires associés au cas fil rouge.

[Jour 3 - Matin]

Analyse et évaluation des risques

- Analyse de la vraisemblance, de la gravité et des populations exposées
- Choix des méthodes qualitatives et quantitatives selon les données disponibles
- Examen des contrôles existants, des incertitudes et des limites de mesure
- Hiérarchisation des risques inhérents et résiduels selon les critères d’acceptation
- Atelier pratique : Évaluer plusieurs scénarios, établir une matrice de criticité et justifier les priorités de traitement.

[Jour 3 - Après-midi]

Traitement et atténuation des risques

- Options de traitement du risque et arbitrages entre réduction, évitement, partage et acceptation
- Mesures sur les données, les modèles, les accès et les usages autorisés
- Contrôles de supervision humaine, de transparence et de robustesse
- Formalisation du plan de traitement, des responsables et des preuves d’efficacité attendues
- Atelier pratique : Élaborer un plan d’atténuation et présenter une décision motivée sur l’acceptation des risques résiduels.

[Jour 4 - Matin]

Surveillance et réponse aux incidents

- Définition des indicateurs de risque, des seuils d’alerte et des fréquences de revue
- Surveillance des dérives, des biais et de l’efficacité des mesures de maîtrise
- Organisation de la réponse aux incidents, du confinement et des solutions de repli
- Traçabilité des événements, reporting et obligations de notification à examiner selon le contexte
- Atelier pratique : Simuler un incident impliquant un système d’IA et produire une fiche de réponse avec décisions d’escalade.

[Jour 4 - Après-midi]

Apprentissage et amélioration continue

- Construction d’un programme de formation et de sensibilisation adapté aux profils exposés
- Exploitation des retours d’expérience et analyse des causes des incidents
- Évaluation de la performance du programme de management du risque IA
- Revues de gouvernance, actions correctives et actualisation du registre des risques
- Atelier pratique : Construire un tableau de bord et une feuille de route d’amélioration à partir des résultats du cas fil rouge.

[Jour 5 - Matin]

Révisions et entraînement à l’examen

- Synthèse des cinq domaines de compétences et repérage des notions à consolider
- Lecture des questions de mise en situation et identification des éléments déterminants
- Justification des choix de gouvernance, d’analyse et de traitement des risques
- Gestion du temps et utilisation des supports selon les règles de l’examen
- Atelier pratique : Réaliser une évaluation blanche chronométrée puis analyser les réponses et les axes de progression.

[Jour 5 - Après-midi]

Examen et parcours de certification

- Vérification des conditions de passage, de l’identité et de l’environnement d’examen
- Rappel des règles de confidentialité et des ressources autorisées
- Passage de l’examen PECB Lead AI Risk Manager pendant trois heures selon la session planifiée
- Distinction entre réussite à l’examen, demande de certification et conditions d’expérience
- Atelier pratique : Préparer une liste des justificatifs nécessaires au dossier de certification, sans revenir sur le contenu confidentiel de l’épreuve.

Sociétés concernées

Cette formation s’adresse à la fois aux particuliers ainsi qu’aux entreprises, petites ou grandes, souhaitant former ses équipes à une nouvelle technologie informatique avancée ou bien à acquérir des connaissances métiers spécifiques ou des méthodes modernes.

Positionnement à l'entrée en formation

Le positionnement à l'entrée en formation respecte les critères qualité Qualiopi. Dès son inscription définitive, l'apprenant reçoit un questionnaire d’auto-évaluation nous permettant d’apprécier son niveau estimé sur différents types de technologies, ses attentes et objectifs personnels quant à la formation à venir, dans les limites imposées par le format sélectionné. Ce questionnaire nous permet également d’anticiper certaines difficultés de connexion ou de sécurité interne en entreprise (intraentreprise ou classe virtuelle) qui pourraient être problématiques pour le suivi et le bon déroulement de la session de formation.

Méthodes pédagogiques

Stage Pratique : 60% Pratique, 40% Théorie. Support de la formation distribué au format numérique à tous les participants.

Organisation

Le cours alterne les apports théoriques du formateur soutenus par des exemples et des séances de réflexions, et de travail en groupe.

Validation

À la fin de la session, un questionnaire à choix multiples permet de vérifier l’acquisition correcte

des compétences.

Sanction

Une attestation sera remise à chaque stagiaire qui aura suivi la totalité de la formation.

Organisme de formation enregistré sous le numéro 11 75 54743 75. Cet enregistrement ne vaut pas agrément de l'État.
© Ambient IT 2015-2026. Tous droits réservés. Paris, France - Suisse - Belgique - Luxembourg