

Préparation à la certification d'auditeur

APERÇU GRATUIT

Auditer un système de management de l'intelligence artificielle

Ce que l'épreuve mesure, et comment on y répond · ISO/IEC 42001:2023 et ISO 19011:2026

Référence APERCU-AI-AUD Version 1.0 Statut Projet



HEMC

HUB ENGINEERING
MANAGEMENT CONSULTING

Sommaire

Ce que contient le produit complet.....	1
Extrait de la partie 1, le cours.....	1
Extrait de la partie 2, l'épreuve blanche.....	2
Extrait de la partie 3, le corrigé commenté.....	3
Et ensuite.....	3

Ce que contient le produit complet

Cet aperçu est gratuit. Il ne contient pas d'extraits tronqués mais un exemplaire complet de chacune des trois parties : le premier chapitre du cours en entier, une question de l'épreuve avec son espace de réponse, et le corrigé de cette même question.

- Partie 1, le cours : ce que l'épreuve mesure, les sept principes d'audit, ce qui n'existe que dans ISO/IEC 42001, la rédaction d'un constat et la méthode de réponse.
- Partie 2, l'épreuve blanche : seize questions, quatre sections, 90 points, deux heures, espaces de réponse inclus.
- Partie 3, le corrigé commenté : la réponse attendue élément par élément, le barème, ce que cherche le correcteur et les erreurs fréquentes.

Extrait de la partie 1, le cours

1. Ce que l'épreuve mesure

Une épreuve écrite d'auditeur ne mesure pas ce que vous savez de la norme. Elle mesure trois choses, et une seule d'entre elles est de la connaissance.

- Lire une consigne et y répondre exactement. C'est la moitié des points perdus, et cela n'a aucun rapport avec l'intelligence artificielle.
- Relier une observation de terrain à une exigence précise, avec son numéro de clause ou de mesure.
- Écrire un constat qu'un audité peut contester et qui tiendra quand même.

Le reste, l'apprentissage des clauses, sert de vocabulaire. Un candidat qui récite l'Annexe A et qui ne sait pas faire ces trois choses échoue.

Ce qui rend l'épreuve 42001 différente des autres

La quasi-totalité des candidats arrive d'un autre référentiel, le plus souvent l'ISO/IEC 27001. C'est un avantage sur la forme, la structure de haut niveau étant la même, et un piège sur le fond. Trois réflexes de sécurité de l'information produisent ici des constats faux :

- Traiter l'appréciation des risques comme le seul dispositif d'analyse. L'ISO/IEC 42001 en exige DEUX, distincts, et l'un alimente l'autre.
- Chercher un actif à protéger. Ici l'objet du soin n'est pas seulement l'organisme : ce sont aussi les personnes et les sociétés sur lesquelles le système d'IA produit des effets.
- Prendre l'Annexe A pour une liste à cocher. La norme dit le contraire, en toutes lettres, et nous verrons où.

Un correcteur repère un candidat « 27001 déguisé » en deux questions. Le chapitre 6 de ce cours est écrit pour cela.

Le format des questions

Les épreuves d'auditeur mélangent quatre familles de questions, dans des proportions qui varient selon le schéma. Ce cahier les couvre toutes les quatre.

Famille	Ce qui est demandé	Ce qui fait perdre les points
Connaissance	Restituer une exigence, une définition, un rôle	Répondre juste sur le fond sans citer la clause
Application	Rattacher une situation à une exigence	Citer la bonne idée et la mauvaise clause
Jugement	Décider : écart, piste, ou rien	Qualifier en écart ce qui n'est qu'une observation
Rédaction	Écrire le constat lui-même	Un constat sans preuve, ou une preuve sans exigence

Extrait de la partie 2, l'épreuve blanche

Question 2.2 · 5 points

Un assureur santé achète un système d'IA d'aide à la tarification auprès d'un éditeur. Il déclare n'être qu'utilisateur et estime que les obligations pèsent sur l'éditeur. Citez cinq preuves que vous demandez pour vérifier cette position.

Votre réponse :

Extrait de la partie 3, le corrigé commenté

Élément attendu	Points
La détermination documentée de ses rôles vis-à-vis de ce système (4.1), et ce que son domaine d'application en dit (4.3).	1
La répartition documentée des responsabilités entre l'organisme, l'éditeur et les autres tiers (A.10.2).	1
Le processus qui garantit que l'usage des services et produits du fournisseur s'aligne sur son approche responsable (A.10.3).	1
L'évaluation d'impact du système tel qu'il est DÉPLOYÉ chez lui, dans son contexte technique, sociétal et juridique (6.1.4, 8.4).	1
Ce qu'il obtient et vérifie du fournisseur sur la qualité et la provenance des données, et la documentation technique reçue (A.7.4, A.7.5, A.6.2.7).	1
Le respect de l'usage prévu du système et de sa documentation d'accompagnement (A.9.4).	1

Ce que cherche le correcteur

Que le candidat refuse la position de l'audité SANS la contredire frontalement : être utilisateur ne dispense de rien, cela change seulement la nature des preuves.

Erreurs fréquentes

- Demander le code du modèle ou les jeux d'apprentissage de l'éditeur : ce n'est ni proportionné ni exigé de l'utilisateur.
- Conclure directement à l'écart : la question demande des preuves à collecter, pas un constat.

Et ensuite

Le produit complet réunit les trois parties dans les quatre langues. La licence couvre l'usage individuel ; pour un usage en salle ou par plusieurs personnes, écrivez à contact@hem-consulting.com.