ISO/IEC 42001 Lead Auditor : 10 questions d'entraînement avec réponses

Dix questions de la banque de questions Mindset Prep, rédigées à partir des normes suivantes : ISO/IEC 42001:2023, ISO 19011:2018. Ce sont des questions d'entraînement originales, et non des questions de l'examen réel.

Dix questions, puis le corrigé avec la bonne réponse, son explication et la référence sur laquelle elle repose. Répondez aux dix avant de consulter les réponses.

Vous préférez une correction immédiate ? Les mêmes questions sont en ligne sur mindsetprep.com.au/fr/examen-blanc/iso-42001-lead-auditor/.

QUESTION 1

Lors de l'audit d'étape 2 d'un SMIA, l'audité présente son « évaluation de l'impact du système d'IA » pour un nouveau produit d'IA destiné aux clients. À l'examen, le document n'évalue que les risques financiers et de réputation que le produit pourrait faire peser sur l'organisme, notés selon la vraisemblance et l'impact et hiérarchisés en vue de leur traitement. Il ne traite pas des conséquences pour les personnes ou les communautés concernées par le système. Quelle est la conclusion la plus défendable à laquelle l'auditeur devrait parvenir ?

A. Une opportunité d'amélioration relative au paragraphe 6.3

B. Une opportunité d'amélioration relative au paragraphe 6.1.4

C. Une non-conformité au paragraphe 6.3

D. Une non-conformité au paragraphe 6.1.4

QUESTION 2

Un responsable d'équipe d'audit déclenche un audit de certification par tierce partie de Talveras, une entreprise dont la plateforme de recrutement par IA présélectionne les candidats à l'emploi. Lors du contact initial, l'audité remet sa déclaration du périmètre du SMIA, ainsi libellée : « tous les systèmes d'IA utilisés pour la présélection des candidats dans les bureaux de Londres et de Dublin ». Le responsable d'équipe convient à présent des objectifs, du champ et des critères de l'audit pour la mission. Alors que les termes de la mission sont convenus, le responsable de l'équipe d'audit doit confirmer les critères d'audit pour cet audit. Quelle option identifie correctement ce que sont les critères d'audit ?

A. Le résultat escompté que l'audit doit atteindre - pour Talveras, confirmer que le SMIA est conforme à la norme et efficacement mis en œuvre afin que la certification puisse être recommandée.

B. L'étendue et les limites de ce qui sera examiné - pour Talveras, les bureaux de Londres et de Dublin et les systèmes d'IA de présélection des candidats nommés dans la déclaration du périmètre du SMIA.

C. L'ensemble des exigences de référence auxquelles les preuves recueillies sont comparées - pour Talveras, l'ISO/IEC 42001:2023, la politique d'IA et la Déclaration d'Applicabilité de l'audité, et les exigences légales et réglementaires applicables.

D. La détermination de l'existence d'informations suffisantes, de la coopération de l'audité, du temps et des ressources - pour Talveras, la vérification effectuée avant que la mission ne soit autorisée à se poursuivre.

QUESTION 3

Lors d'un audit d'étape 2 du SMIA, l'audité Meridian Lending exploite sous licence un modèle d'IA tiers de notation de crédit, l'intègre à sa plateforme d'octroi de prêts et propose cette plateforme en tant que service à des banques partenaires. L'analyse du contexte réalisée par Meridian au titre du paragraphe 4.1 documente les enjeux externes et internes pertinents et consigne le rôle de l'organisme vis-à-vis des systèmes d'IA comme étant, simplement, « utilisateur d'IA ». Selon le scénario, quel est le fondement le PLUS approprié pour l'évaluation, par le responsable de l'équipe d'audit, de la détermination des rôles de Meridian au titre du paragraphe 4.1 ?

A. Aucun écart : la licence du modèle fait d'« utilisateur d'IA » la bonne mention pour Meridian.

B. Un écart : le service de plateforme proposé aux banques partenaires ajoute un rôle qu'omet « utilisateur d'IA ».

C. Aucun écart : le service de plateforme proposé aux banques partenaires relève du paragraphe 4.2.

D. Un écart : la licence du modèle fait du rôle unique de Meridian celui de client d'IA, et non d'utilisateur d'IA.

QUESTION 4

Un audité a déployé un vaste système de contenu fondé sur l'IA générative qui exige une puissance de calcul considérable pour l'entraînement et le réentraînement. Au cours de l'audit d'étape 2, l'auditeur examine l'évaluation documentée de l'impact du système d'IA. Celle-ci traite de façon approfondie les impacts sur les utilisateurs individuels et les groupes concernés : équité, respect de la vie privée et bien-être psychologique. L'auditeur relève que l'évaluation n'aborde ni l'empreinte environnementale de l'entraînement de modèles à grande échelle ni la possibilité que le système contribue à une désinformation à grande échelle. Le responsable du SMIA répond : « nous avons évalué les impacts sur les personnes et les groupes, comme l'exige la norme ». À l'encontre de quelle mesure le constat de l'auditeur est-il formulé le plus exactement ?

A. Annexe A.5.5 (Évaluation des impacts sociétaux des systèmes d'IA), parce que des impacts sociétaux tels que l'empreinte environnementale et la désinformation n'ont pas été évalués.

B. Annexe A.5.4 (Évaluation de l'impact du système d'IA sur des personnes ou groupes de personnes), parce que l'évaluation de l'impact est incomplète.

C. Annexe A.4.5 (Ressources système et informatiques), parce que l'impact environnemental de la puissance de calcul n'est pas documenté.

D. Paragraphe 6.1.2 (Appréciation des risques liés à l'IA), parce que l'appréciation des risques à l'échelle de l'organisme est incomplète.

QUESTION 5

Un audit tierce partie du SMIA porte sur les 30 modèles d'IA déployés d'une fintech. Douze modèles pilotent des décisions de crédit automatisées qui affectent des individus ; les dix-huit autres sont des outils d'efficacité interne (par exemple l'acheminement de documents) dont l'impact sur les individus est négligeable. Le temps d'audit permet d'examiner en profondeur huit modèles environ. Parmi les huit modèles de crédit à fort impact que l'auditeur échantillonne, l'évaluation de l'impact du système d'IA (paragraphe 6.1.4) d'un modèle n'a jamais été réalisée avant le déploiement. En appliquant une approche par les risques à l'échantillonnage et aux preuves, quelle est la meilleure conduite à tenir ?

A. Maintenir l'échantillon pondéré vers les modèles de crédit et consigner une opportunité d'amélioration.

B. Réaffecter une partie de l'échantillon aux outils internes et émettre une non-conformité dès maintenant.

C. Réaffecter une partie de l'échantillon aux outils internes et consigner une opportunité d'amélioration.

D. Maintenir l'échantillon pondéré vers les modèles de crédit et émettre une non-conformité dès maintenant.

QUESTION 6

Une entreprise de logiciels dispose d'un conseil d'éthique de l'IA permanent, composé de membres seniors des fonctions juridique, ingénierie et produit. Il se réunit chaque mois, examine les nouvelles fonctionnalités d'IA, et sa charte, ses procès-verbaux et les feuilles de présence sont tous bien documentés. L'auditeur confirme que le conseil fonctionne réellement. Cependant, lorsque l'auditeur demande qui détient l'autorité attribuée pour s'assurer que le système de management de l'IA est conforme à la norme et pour rendre compte de la performance du SMIA à la direction, le personnel désigne vaguement « le conseil collectivement », et aucun enregistrement ne montre que la direction a attribué ces deux responsabilités à un rôle défini. Compte tenu du conseil d'éthique actif et bien documenté, quelle est la position la plus défendable de l'auditeur ?

A. Émettre une non-conformité au titre du paragraphe 9.3

B. Émettre une non-conformité au titre de la mesure A.3.2

C. Émettre une non-conformité au titre du paragraphe 5.3

D. Émettre une non-conformité au titre du paragraphe 5.1

QUESTION 7

Lors de l'audit d'étape 2 du prêteur à la consommation LumenScore, l'équipe confirme l'existence d'une évaluation de l'impact menée dans le cadre du SMIA pour le modèle de notation de crédit en production. Les journaux d'exploitation révèlent un second modèle, non annoncé : un challenger qui reçoit discrètement environ dix pour cent des demandeurs réels et dont les scores prennent, pour ceux-ci, la décision d'octroi effective. Aucune évaluation de l'impact n'a été réalisée pour ce modèle. Le responsable MLOps affirme que le challenger est un pilote interne maîtrisé, non officiellement mis en production, et qu'il sera documenté une fois promu ; jusque-là, soutient l'audité, les pilotes échappent à l'exigence d'information documentée. En tant que responsable d'audit, quelle est la position LA PLUS défendable à adopter au sujet du modèle challenger ?

A. Émettre une non-conformité au regard du paragraphe 8.2 pour le modèle challenger.

B. Émettre une non-conformité au regard du paragraphe 8.4 pour le modèle challenger.

C. Accepter le statut de pilote et examiner le challenger une fois qu'il aura été promu.

QUESTION 8

Vantage Health AI a été certifiée ISO/IEC 42001 l'an dernier. Depuis, elle a déployé un nouveau système d'IA majeur, un modèle de triage clinique, qui constitue un changement significatif de son SMIA. Un auditeur planifie le premier audit de surveillance du cycle de certification. Lors de l'audit de certification initial, une non-conformité mineure concernant les évaluations de l'impact des systèmes d'IA avait été relevée et sa correction acceptée. Quelle approche reflète le mieux la finalité et le périmètre de cet audit de surveillance ?

A. Échantillonner le SMIA et l'action corrective antérieure, en considérant le modèle de triage comme faisant partie du périmètre.

B. Réauditer chaque article et chaque mesure de l'Annexe A, en considérant le modèle de triage comme faisant partie du périmètre.

C. Échantillonner le SMIA et l'action corrective antérieure, en considérant le modèle de triage comme ne faisant pas encore partie du périmètre.

D. Réauditer chaque article et chaque mesure de l'Annexe A, en considérant le modèle de triage comme ne faisant pas encore partie du périmètre.

QUESTION 9

Renji Stenmark audite Granitepath AI Logistics, dont le système d'IA de routage associe un modèle tiers, des données d'entraînement d'origine externe et un code d'intégration développé en interne. Le responsable de la conformité présente les contrats de fourniture du modèle et des données, qui contiennent chacun des clauses de responsabilité et de garantie, et explique que ceux-ci déterminent qui répond de quoi. Granitepath ne tient donc aucun enregistrement propre indiquant quelle partie est responsable de quel volet du cycle de vie du système d'IA. D'après le scénario, quelle réponse correspond le mieux à ce que les recommandations relatives à l'attribution des responsabilités attendent réellement de Granitepath ?

A. Un enregistrement de l'attribution est attendu, mais il faut qu'il couvre les travaux d'intégration internes que Granitepath maîtrise directement ; les responsabilités relatives au modèle acquis et aux données d'entraînement relèvent de leurs fournisseurs, à qui il appartient de les définir et de les documenter.

B. Les recommandations attendent que Granitepath documente elle-même toutes les parties intervenant tout au long du cycle de vie du système d'IA et leurs responsabilités respectives, de sorte que l'absence d'enregistrement de l'attribution constitue un écart, quelles que soient les attributions prévues par les contrats.

C. Comme chaque élément d'origine externe est couvert par un contrat comportant des clauses de responsabilité et de garantie, la responsabilité est réglée par les recommandations relatives aux relations avec les fournisseurs, et un enregistrement distinct de l'attribution ferait double emploi avec le dossier d'achat.

QUESTION 10

VeridicAI vend aux employeurs un modèle de présélection pour le recrutement. Lors de l'étape 2, le responsable d'équipe examine l'évaluation de l'impact du système d'IA. Elle couvre les conséquences pour les employeurs qui achètent l'outil, chacune reprise dans le registre des risques avec un propriétaire et un plan de traitement. Elle n'examine ni la situation juridique ni les perspectives de vie des candidats que le modèle note, ni aucun effet différencié selon les groupes protégés. Le responsable de la gouvernance de l'IA affirme que l'évaluation de l'impact et l'appréciation des risques sont délibérément maintenues cohérentes, que chaque impact a été reporté dans le registre et traité, et que le processus est donc complet et clos. Le responsable de l'équipe d'audit détermine comment qualifier cet écart. Quelle réponse est la PLUS défendable ?

A. N'enregistrer aucun constat : l'évaluation et le registre sont cohérents et clos.

B. Relever une non-conformité au paragraphe 6.1.3 portant sur le plan de traitement des risques.

C. Relever une non-conformité au paragraphe 6.1.4 portant sur l'évaluation de l'impact.

Réponses

Q1 Bonne réponse : **D.** Une non-conformité au paragraphe 6.1.4

Les conséquences qui importent ici sont celles supportées à l'extérieur de l'organisme. Le paragraphe 6.1.4 de l'ISO/IEC 42001:2023 exige une évaluation de l'impact du système d'IA qui détermine les conséquences potentielles du déploiement, de l'utilisation prévue et de la mauvaise utilisation prévisible d'un système d'IA pour les individus ou groupes d'individus et pour les sociétés, ces résultats étant pris en compte dans l'appréciation des risques liés à l'IA du paragraphe 6.1.2. Le document présenté comme cette évaluation ne note que les risques financiers et de réputation pour l'organisme ; il laisse donc cette détermination inaccomplie. Une exigence n'est pas satisfaite, ce qui en fait une non-conformité au paragraphe 6.1.4 plutôt qu'un point d'amélioration.

Référence : ISO/IEC 42001:2023 Paragraphe 6.1.4

Piège : T-01 Appréciation des risques ou évaluation de l'impact

---

Q2 Bonne réponse : **C.** L'ensemble des exigences de référence auxquelles les preuves recueillies sont comparées - pour Talveras, l'ISO/IEC 42001:2023, la politique d'IA et la Déclaration d'Applicabilité de l'audité, et les exigences légales et réglementaires applicables.

Les critères d'audit sont aisément confondus avec les autres points arrêtés au déclenchement de l'audit : le champ de l'audit, la faisabilité et les objectifs. Les critères sont les exigences de référence auxquelles les preuves objectives sont comparées (ISO 19011:2018), et le terme 3.18 de l'ISO/IEC 42001:2023 renvoie à l'ISO 19011 pour « critères d'audit » et « preuves d'audit » ; cette définition régit donc cet audit de certification 42001. Les critères sont par conséquent la norme normative ainsi que les informations documentées propres au SMIA de l'audité et les exigences légales applicables.

Référence : ISO 19011:2018 (déclenchement de l'audit)

Piège : T-02 Périmètre du SMIA ou périmètre du système d'IA

Q3 Bonne réponse : **B.** Un écart : le service de plateforme proposé aux banques partenaires ajoute un rôle qu'omet « utilisateur d'IA ».

Le paragraphe 4.1 exige que l'organisme prenne en compte la finalité prévue des systèmes d'IA qu'il développe, fournit ou utilise, et qu'il détermine ses rôles vis-à-vis de ceux-ci ; la norme énumère des rôles possibles (fournisseur d'IA, producteur d'IA, client d'IA, partenaire d'IA, sujet d'IA, autorités compétentes) et un organisme peut en cumuler plusieurs simultanément. Meridian est client d'IA de l'éditeur du modèle et, parce qu'il propose un service fondé sur l'IA à des banques partenaires, également fournisseur/partenaire d'IA. L'enregistrement d'un rôle unique d'« utilisateur d'IA » laisse donc la détermination du contexte incomplète. Identifier les banques partenaires comme parties intéressées au titre du paragraphe 4.2 ne règle pas la question du propre rôle de Meridian vis-à-vis d'elles.

Référence : ISO/IEC 42001:2023 paragraphe 4.1

Piège : T-03 Rôles vis-à-vis de l'IA ou rôles du système de management

---

Q4 Bonne réponse : **A.** Annexe A.5.5 (Évaluation des impacts sociétaux des systèmes d'IA), parce que des impacts sociétaux tels que l'empreinte environnementale et la désinformation n'ont pas été évalués.

A.5 exige que l'organisme évalue les impacts du système d'IA tout au long du cycle de vie, en séparant la perspective individuelle (A.5.4, personnes ou groupes de personnes) de la perspective sociétale (A.5.5, impacts sociétaux). B.5.5 cite la durabilité environnementale et la désinformation parmi les impacts sociétaux. L'audité a traité la dimension A.5.4 mais a omis A.5.5 ; le constat relève donc de A.5.5. Le détail environnemental est un leurre délibéré vers A.4.5, dont les recommandations B.4.5 mentionnent effectivement l'impact environnemental du matériel, mais A.4.5 porte sur la documentation des ressources informatiques, non sur l'évaluation des conséquences sociétales. L'évaluation de l'impact (conséquences pour les personnes et les sociétés) ne doit pas non plus être confondue avec l'appréciation des risques liés à l'IA à l'échelle de l'organisme du paragraphe 6.1.2, qui concerne les risques pesant sur les objectifs d'IA de l'organisme.

`Référence : ISO/IEC 42001:2023, Annexe A.5.5 (avec B.5.5)`

`Piège : T-01 Appréciation des risques ou évaluation de l'impact`

Q5 Bonne réponse : **D.** Maintenir l'échantillon pondéré vers les modèles de crédit et émettre une non-conformité dès maintenant.

Un échantillon pondéré par les risques peut prouver certaines choses et pas d'autres. L'ISO 19011:2018 et l'approche par les risques orientent l'échantillonnage fondé sur le jugement vers les éléments présentant le risque le plus élevé, les douze modèles de crédit qui affectent des individus, et non vers une couverture égale ou statistiquement représentative. Les preuves issues d'un échantillon sont asymétriques : une défaillance étaye un constat et peut indiquer une étendue plus large, mais un échantillon conforme ne prouve jamais la conformité de la population. Une évaluation de l'impact du système d'IA jamais réalisée (ISO/IEC 42001:2023, paragraphe 6.1.4) est un non-respect vérifiable, c'est-à-dire une non-conformité : elle est donc émise et la conclusion porte le risque résiduel.

`Référence : ISO 19011:2018`

`Piège : T-02 Périmètre du SMIA ou périmètre du système d'IA`

Q6 Bonne réponse : **C.** Émettre une non-conformité au titre du paragraphe 5.3

L'exigence en cause porte sur l'attribution spécifique, par la direction, de la responsabilité et de l'autorité pour deux points nommés (la conformité du SMIA et le compte rendu de la performance du SMIA), et non sur une répartition générale des rôles, sur le leadership et l'engagement, ni sur la revue de direction. Un conseil d'éthique actif atteste une activité, mais pas cette attribution, et l'écart se situe dans le paragraphe 5.3, et non dans la mesure de l'Annexe A relative aux rôles.

`Référence : ISO/IEC 42001:2023 Paragraphe 5.3`

`Piège : T-03 Rôles vis-à-vis de l'IA ou rôles du système de management`

Q7 Bonne réponse : **B.** Émettre une non-conformité au regard du paragraphe 8.4 pour le modèle challenger.

La lecture défendable repose sur le fond plutôt que sur l'étiquette. Le paragraphe 8.4 exige des évaluations de l'impact du système d'IA, réalisées conformément au paragraphe 6.1.4, lorsque des changements significatifs sont proposés, et le challenger décide déjà de l'octroi réel de crédit pour environ dix pour cent des demandeurs sans qu'aucune n'ait été réalisée. Le qualifier de pilote ne suspend pas cette obligation. Les éléments de preuve portent sur l'absence d'évaluation de l'impact ; rien de ce qui a été constaté ne montre qu'il manque une appréciation des risques liés à l'IA au titre du paragraphe 8.2. Celui qui bachote s'attache au moment où l'information documentée doit exister ; un responsable d'audit s'attache à la question de savoir si des personnes réelles sont affectées dès maintenant.

Référence : ISO/IEC 42001:2023, paragraphe 8.4

Piège : T-01 Appréciation des risques ou évaluation de l'impact

---

Q8 Bonne réponse : **A.** Échantillonner le SMIA et l'action corrective antérieure, en considérant le modèle de triage comme faisant partie du périmètre.

Selon l'ISO/IEC 17021-1, qui fixe des exigences pour les organismes de certification, un audit de surveillance a une fonction définie au sein du cycle de certification : une confirmation partielle, fondée sur l'échantillonnage, que le SMIA reste conforme et demeure efficace. Il couvre les éléments obligatoires (notamment audit interne, revue de direction, actions sur les non-conformités antérieures, changements, usage des marques), l'efficacité de l'action corrective antérieure et tout changement significatif. C'est pourquoi le déploiement du nouveau modèle de triage clinique est échantillonné, y compris son appréciation des risques liés à l'IA, son évaluation de l'impact et ses mesures ; le paragraphe 8.2 de l'ISO/IEC 42001:2023 exige une appréciation des risques liés à l'IA lorsque des changements significatifs sont proposés ou surviennent, et le paragraphe 8.4 une évaluation de l'impact lorsque des changements significatifs sont proposés.

Référence : ISO/IEC 42001:2023 paragraphes 8.2 et 8.4

Piège : T-02 Périmètre du SMIA ou périmètre du système d'IA

Q9 Bonne réponse : **B.** Les recommandations attendent que Granitepath documente elle-même toutes les parties intervenant tout au long du cycle de vie du système d'IA et leurs responsabilités respectives, de sorte que l'absence d'enregistrement de l'attribution constitue un écart, quelles que soient les attributions prévues par les contrats.

Attribuer les responsabilités signifie que l'organisme documente lui-même qui répond de chaque volet du cycle de vie du système d'IA pour l'ensemble des parties - fournisseur de données, fournisseur de modèle et intégrateur interne. Les contrats répartissent la responsabilité juridique entre deux signataires ; ils alimentent cette cartographie sans s'y substituer, et l'approvisionnement externe ne réduit pas la cartographie à la part interne. L'absence d'enregistrement constitue un écart, quel que soit celui qui a construit le modèle.

Référence : ISO/IEC 42001:2023 Mesure A.10.2

Piège : T-03 Rôles vis-à-vis de l'IA ou rôles du système de management

---

Q10 Bonne réponse : **C.** Relever une non-conformité au paragraphe 6.1.4 portant sur l'évaluation de l'impact.

L'évaluation de l'impact du système d'IA et l'appréciation des risques liés à l'IA répondent à des questions différentes. L'appréciation des risques (paragraphe 6.1.2) identifie les risques qui favorisent ou empêchent l'atteinte des objectifs de l'organisme en matière d'IA, et peut s'appuyer sur l'évaluation de l'impact pour apprécier leurs conséquences ; l'évaluation de l'impact (paragraphe 6.1.4) doit déterminer les conséquences potentielles pour les individus ou les groupes d'individus, ou les deux, et pour les sociétés - ici, les candidats que le modèle note, y compris les effets selon les groupes démographiques. Omettre ces conséquences constitue donc une lacune de l'évaluation de l'impact elle-même, et non du traitement des risques qui en a fidèlement repris les résultats. Reporter les impacts dans le registre des risques est une bonne pratique, mais ne remplace pas l'analyse des personnes que le système affecte.

Référence : ISO/IEC 42001:2023 Annexe B.5.2

Piège : T-01 Appréciation des risques ou évaluation de l'impact

---

Vous voulez toute la banque de questions ?

Mindset Prep propose plus de 2 500 questions pour cinq certifications PECB, chacune avec une explication, et fait revenir les questions que vous manquez. Commencez par un essai gratuit de 3 jours.

Commencer l'essai gratuit de 3 jours

app.mindsetprep.com.au/start

Mindset Prep est indépendante de PECB, qui ne la cautionne pas.