ISO/IEC 27001 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 27001:2022, ISO 19011:2018, ISO/IEC 27002:2022. 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-27001-lead-auditor/.

QUESTION 1

Trustingo Pagos est un prestataire de traitement des paiements par carte en Uruguay dont la plateforme d'autorisation fonctionne depuis une salle serveurs sécurisée, protégée par une double porte à contrôle d'accès par badge et un accueil sous surveillance, chaque entrée étant enregistrée dans un journal électronique des accès. Alors qu'il est accompagné à travers le site lors de l'étape 2, un auditeur observe un employé badger puis maintenir la porte intérieure ouverte pour un prestataire de maintenance situé quelques pas derrière, qui entre sans présenter de justificatif. Le guide accompagnateur remarque que le prestataire « est ici toutes les semaines et tout le monde le connaît ». Quelle est l'étape suivante la PLUS appropriée pour l'auditeur ?

A. Émettre une non-conformité mineure pour l'unique manquement de l'employé à la porte.

B. Vérifier dans le journal des accès les visites hebdomadaires du prestataire.

C. Émettre une non-conformité majeure pour l'entrée du prestataire sans justificatif.

D. Vérifier dans le journal des accès les autres entrées de l'employé.

QUESTION 2

Un responsable de l'équipe d'audit examine le programme d'audit interne d'un audité : chaque domaine est audité selon une rotation uniforme de 36 mois, ordonnée alphabétiquement par service. Au cours de l'année écoulée, deux incidents significatifs ont touché des processus relevant des Articles 8 et 9, et les derniers audits internes de ces domaines ont chacun soulevé des constats récurrents, mais la rotation reste inchangée. Comment le responsable de l'équipe d'audit devrait-il traiter le programme ?

A. Émettre une non-conformité, car la planification du programme doit refléter l'importance de chaque processus et les résultats des audits antérieurs, et une rotation alphabétique uniforme ne reflète aucun de ces deux éléments.

B. N'émettre aucun constat, car le paragraphe laisse l'intervalle à l'appréciation de l'organisme, et une rotation de 36 mois documentée, dotée de ressources et réalisée avec constance satisfait l'exigence d'intervalles planifiés qu'il énonce.

C. Consigner une observation, car la pondération du programme en fonction du risque et des résultats antérieurs est une recommandation tirée de l'ISO 19011 sur la gestion du programme, et un constat certifiable nécessite une exigence de l'ISO/IEC 27001 elle-même.

QUESTION 3

Devon Okafor audite Northwind Compliance. Pour satisfaire à la mesure relative à la révision indépendante, Northwind fait réviser chaque année par son Responsable de la sécurité de l'information l'approche globale de l'organisme en matière de gestion de la sécurité de l'information, et les résultats sont communiqués au propre supérieur hiérarchique de ce même Responsable de la sécurité de l'information, le Directeur des opérations informatiques, qui est propriétaire de la plupart des mesures révisées. Northwind soutient que le réviseur est de haut niveau, compétent et ne fait pas partie des équipes opérationnelles, et que la révision est donc indépendante. En appliquant à ce dispositif la mesure relative à la révision indépendante, que devrait conclure l'auditeur ?

A. Une opportunité d'amélioration relative à la mesure 5.35

B. Aucun constat : la mesure 5.35 est satisfaite

C. Une non-conformité à la mesure 5.35

QUESTION 4

Vous réalisez l'audit d'étape 2 de Brindhal Freight, un opérateur logistique au Portugal. Sa gestion documentée des accès privilégiés attribue à chaque administrateur une identité privilégiée personnelle, désactive les comptes génériques « root » et n'octroie des droits élevés qu'au moment voulu, pour des fenêtres de changement approuvées, à l'issue desquelles ces droits expirent automatiquement. La politique de contrôle d'accès et le registre des administrateurs autorisés sont complets et à jour, et le responsable de la sécurité de l'information confirme que l'outil de gestion des accès privilégiés (PAM) applique ces règles. Quelle action démontrerait le plus sûrement que la mesure de sécurité de l'information relative aux droits d'accès privilégiés fonctionne comme prévu et n'est pas seulement documentée ?

A. Échantillonner des sessions privilégiées et vérifier que chacune a été enregistrée intégralement et revue par un second administrateur.

B. Inspecter les paramètres de l'outil PAM et vérifier que les octrois nécessitent une approbation préalable et expirent avec leur fenêtre.

C. Inspecter les paramètres de l'outil PAM et vérifier qu'ils enregistrent chaque session pour revue par un second administrateur.

D. Échantillonner des changements réalisés et vérifier que chaque octroi utilisé a été approuvé au préalable et a expiré avec sa fenêtre.

QUESTION 5

Marcus Patel audite la gestion des vulnérabilités techniques chez Kestrel Financial Services. L'organisme effectue chaque semaine un balayage de vulnérabilités authentifié sur l'ensemble de son parc de serveurs et corrige les constats critiques dans un délai convenu, des tickets en apportant la preuve. Lorsque Marcus demande l'inventaire des actifs sur lequel s'appuie le programme de balayage, le directeur des opérations informatiques reconnaît qu'il n'existe aucun inventaire tenu à jour des logiciels et des systèmes : le balayage se contente de parcourir les plages d'adresses IP qui répondent. Plusieurs charges de travail en nuage sont créées et détruites chaque jour et ne sont jamais dans le périmètre lorsque le balayage hebdomadaire s'exécute. Quel est le constat le plus approprié que l'auditeur puisse formuler ?

A. Aucun constat : la mesure 8.8 est satisfaite

B. Une opportunité d'amélioration relative à la mesure 8.8

C. Une non-conformité à la mesure 8.8

QUESTION 6

Dans une entreprise de 40 personnes, vous examinez le programme d'audit interne. Le dirigeant propriétaire a audité les domaines des finances et des ressources humaines ; le responsable informatique a audité tous les domaines de mesures techniques, y compris la configuration du réseau et les restaurations de sauvegardes qu'il administre lui-même au quotidien. Les deux auditeurs sont formés, les enregistrements sont complets, les constats ont été communiqués à la direction et le programme respecte le calendrier. Quel est le constat le plus défendable concernant ce dispositif d'audit interne ?

A. Une opportunité d'amélioration portant sur les audits des domaines des finances et des ressources humaines

B. Une non-conformité au paragraphe 9.2.2 portant sur les audits des domaines techniques

C. Une opportunité d'amélioration portant sur les audits des domaines techniques

D. Une non-conformité au paragraphe 9.2.2 portant sur les audits des domaines des finances et des ressources humaines

QUESTION 7

Brightmoor Health Analytics, un bureau de traitement de données en Nouvelle-Zélande, est fier de son programme de surveillance. Des tableaux de bord recueillent la latence des correctifs, le nombre d'échecs de connexion, les taux de clic des simulations d'hameçonnage et les volumes de tickets, actualisés quotidiennement et archivés mensuellement ; l'audité présente douze mois d'indicateurs conservés comme preuve que son SMSI porte l'amélioration continue. Lorsque vous demandez comment ces chiffres sont utilisés, le responsable de la sécurité répond qu'ils sont collectés et stockés afin d'être « disponibles si quelqu'un les demande ». Vous ne trouvez aucun enregistrement attestant que quiconque ait interprété ces chiffres, les ait comparés aux objectifs du SMSI ou ait agi sur ce qu'ils révélaient. Quel énoncé caractérise LE MIEUX l'écart que l'auditeur devrait consigner ?

A. Les chiffres sont collectés et conservés, mais personne ne les analyse ni ne les évalue.

B. Les chiffres sont analysés et évalués, mais aucune information documentée ne le montre.

C. Les chiffres sont collectés et conservés, mais aucune action corrective n'en découle.

D. Une action corrective découle des chiffres, mais aucune information documentée ne le montre.

QUESTION 8

Halcyon Risk Advisory s'appuie sur une norme de durcissement émise par un fournisseur externe pour configurer ses serveurs ; le personnel la considère comme faisant autorité et la suit quotidiennement. La déléguée à la protection des données, Maren Holloway, maintient une gestion stricte des versions, des règles d'accès et une durée de conservation pour les documents rédigés par l'entreprise, mais indique que le document du fournisseur est laissé exactement tel que reçu, sans identification interne ni suivi des modifications car, étant externe, il relève de la responsabilité du fournisseur de le maîtriser, et non de celle de Halcyon. Quelle position d'audit reflète le mieux le paragraphe 7.5.3 de l'ISO/IEC 27001:2022 concernant le document fourni par le fournisseur ?

A. Une opportunité d'amélioration concernant le paragraphe 7.5.3

B. Aucun constat : le paragraphe 7.5.3 est respecté

C. Une non-conformité au paragraphe 7.5.3

QUESTION 9

Vous auditez Meridian Health Analytics. Sa Déclaration d'Applicabilité inclut la mesure de sécurité de l'information 5.18 (Droits d'accès), retenue pour garantir que les accès des partants sont supprimés rapidement. Les quatre dernières revues trimestrielles des droits d'accès sont documentées et validées par le propriétaire du système avec la mention « revu, aucun problème constaté ». Votre échantillon révèle trois partants, sortis il y a trois à cinq mois, qui détiennent toujours des comptes actifs sur la plateforme ; tous trois sont partis avant la revue la plus récente. Le propriétaire du système soutient que la mesure est conforme : la revue a lieu chaque trimestre et est validée exactement comme l'exige la politique de contrôle d'accès. Comment l'auditeur devrait-il répondre à la position du propriétaire du système ?

A. Émettre la non-conformité au titre du paragraphe 9.2 Audit interne, car la revue propre de l'organisme aurait toujours dû identifier les comptes et c'est donc la fonction d'audit interne elle-même qui n'a pas satisfait à l'exigence.

B. Consigner une observation plutôt qu'une non-conformité, puisque les comptes résiduels constituent un problème isolé de qualité des données et que les quatre enregistrements de revue validés sont des preuves objectives que la mesure relative aux droits d'accès fonctionne comme prévu.

C. Accepter que la mesure est conforme pour cette période : la revue des droits d'accès a été réalisée à la fréquence trimestrielle requise, et chacune des quatre dernières revues est documentée et validée par le propriétaire du système exactement comme le spécifie la politique de contrôle d'accès de l'organisme, ce qui constitue les preuves que la procédure a été conçue pour produire.

D. La conformité dépend du fait que la mesure atteigne son objectif, la suppression en temps opportun des accès des partants, et non du fait que la revue ait été planifiée et validée ; la revue n'a pas détecté trois partants qui ont conservé leurs accès, la mesure est donc inefficace et une non-conformité s'applique.

QUESTION 10

En examinant le traitement des risques dans une PME de logistique, vous trouvez une Déclaration d'Applicabilité qui liste chaque mesure de sécurité de l'information nécessaire avec la justification de son inclusion, un état de mise en œuvre indiqué pour chacune, et les raisons de chaque mesure de l'Annexe A exclue. Un plan de traitement des risques distinct existe et est réaliste. Cependant, le plan porte la mention de version « projet, en attente de validation », et vous ne trouvez aucun enregistrement indiquant que les propriétaires du risque l'ont approuvé ou ont accepté le risque résiduel. Quelle est la conclusion la plus défendable ?

A. Une non-conformité s'applique car on ne peut pas se fier à un projet de plan de traitement ; toute l'appréciation des risques doit donc être refaite avant que la Déclaration d'Applicabilité puisse être acceptée comme valide.

B. La Déclaration d'Applicabilité est complète, mais l'exigence relative au traitement des risques n'est pas satisfaite car les propriétaires du risque n'ont ni approuvé le plan ni accepté le risque résiduel.

C. L'exigence relative au traitement des risques est satisfaite, puisque la Déclaration d'Applicabilité contient les mesures de sécurité de l'information nécessaires, les justifications d'inclusion et d'exclusion, et l'état de mise en œuvre de chaque mesure.

D. Il s'agit d'une opportunité d'amélioration recommandant à l'entreprise de finaliser rapidement la validation, puisque les décisions de fond relatives au traitement ont été documentées et que le plan lui-même est réaliste et applicable.

Réponses

Q1 Bonne réponse : **B.** Vérifier dans le journal des accès les visites hebdomadaires du prestataire.

Un incident de talonnage observé est une piste, non une conclusion classée. Le prestataire est entré sans présenter de justificatif : la mesure d'accès physique par badge (mesure 7.2 de l'ISO/IEC 27001:2022, Les entrées physiques) a donc été contournée et son entrée est absente du journal électronique des accès. La classification d'une non-conformité (majeure = défaillance systémique ; mineure = manquement isolé) dépend de l'étendue, et l'ISO 19011:2018 recommande que les conclusions reposent sur des preuves vérifiables suffisantes. La remarque du guide laisse entendre que le prestataire est régulièrement admis, mais ne constitue pas une preuve vérifiée. Rechercher dans le journal les visites hebdomadaires que décrit le guide permet de l'éprouver ; les entrées par badge de l'employé lui-même ne le permettent pas, car elles ne montrent que les déplacements de l'employé. L'auditeur vérifie donc le journal avant de classer quoi que ce soit.

Référence : ISO 19011:2018 (approche fondée sur la preuve ; classification des non-conformités)

Piège : T-01 Preuves ou constatation

Q2 Bonne réponse : **A.** Émettre une non-conformité, car la planification du programme doit refléter l'importance de chaque processus et les résultats des audits antérieurs, et une rotation alphabétique uniforme ne reflète aucun de ces deux éléments.

L'obligation de prise en compte figure dans la norme certifiable elle-même : le paragraphe 9.2.2 exige que le programme d'audit tienne compte de l'importance des processus concernés et des résultats des audits précédents. Une rotation alphabétique de 36 mois laissée inchangée après des incidents significatifs et des constats récurrents ne satisfait ni l'un ni l'autre critère, de sorte qu'une non-conformité est justifiée. La fixation de la fréquence des audits est une partie du paragraphe, non la totalité de celui-ci, et l'obligation de prise en compte relève de l'ISO/IEC 27001 elle-même, et pas seulement des recommandations de l'ISO 19011.

Référence : ISO/IEC 27001:2022 paragraphe 9.2.2

Piège : T-02 « Doit » ou « il convient de »

Q3 Bonne réponse : **C.** Une non-conformité à la mesure 5.35

L'indépendance est ici structurelle, et pas seulement une question de compétence. Les préconisations de la mesure de sécurité de l'information indiquent qu'il convient que la révision soit effectuée par une personne indépendante du domaine faisant l'objet de la révision et extérieure à sa ligne hiérarchique, par exemple la fonction d'audit interne, un responsable indépendant ou un organisme externe spécialisé dans ce type de révision. Un responsable dont le propre supérieur hiérarchique est propriétaire de la plupart des mesures révisées se situe dans cette ligne hiérarchique et ne peut pas fournir cette appréciation indépendante, quelle que soit sa compétence. Comme la mesure 5.35 de l'Annexe A de l'ISO/IEC 27001 exige que l'approche fasse l'objet d'une révision indépendante, l'écart constitue une non-conformité plutôt qu'un point d'amélioration.

Référence : ISO/IEC 27002:2022 Mesure 5.35

Piège : T-03 Compétence ou indépendance

Q4 Bonne réponse : **D.** Échantillonner des changements réalisés et vérifier que chaque octroi utilisé a été approuvé au préalable et a expiré avec sa fenêtre.

Toutes les preuves d'audit n'ont pas le même poids : la documentation, le témoignage et les paramètres de l'outil établissent qu'une mesure de sécurité de l'information existe et est conçue ; seule la preuve de son action sur des événements réels établit qu'elle fonctionne. Ces événements doivent être ceux que la conception régit, ici des droits élevés octroyés au moment voulu pour des fenêtres de changement approuvées et expirant automatiquement. La mesure 8.2 de l'ISO/IEC 27002:2022 indique qu'il convient de maîtriser l'attribution des droits d'accès privilégiés au moyen d'un processus d'autorisation, et cite l'octroi d'un accès privilégié temporaire, limité à la fenêtre de temps nécessaire à la mise en œuvre des changements approuvés, parmi les dispositions à envisager. Tracer des changements réalisés jusqu'à l'accès utilisé, puis confirmer l'autorisation préalable et l'expiration, éprouve le fonctionnement lui-même. C'est l'approche fondée sur la preuve de l'ISO 19011:2018.

`Référence : ISO/IEC 27002:2022, mesure 8.2 (Droits d'accès privilégiés)`

`Piège : T-01 Preuves ou constatation`

Q5 Bonne réponse : **C.** Une non-conformité à la mesure 8.8

La gestion des vulnérabilités techniques ne se réduit pas au balayage et à l'application de correctifs. L'ISO/IEC 27002 présente un inventaire exact des actifs comme un préalable à une gestion efficace des vulnérabilités techniques. Ici, aucun inventaire n'est tenu à jour et les charges de travail en nuage éphémères n'entrent jamais dans le balayage : l'organisme ne peut donc pas démontrer qu'il gère leurs vulnérabilités. La mesure 8.8 de l'Annexe A de l'ISO/IEC 27001 exige que l'exposition aux vulnérabilités des systèmes d'information utilisés soit évaluée : il s'agit donc d'une non-conformité et non d'un point d'amélioration.

`Référence : ISO/IEC 27002:2022, mesure 8.8`

`Piège : T-02 « Doit » ou « il convient de »`

Q6 Bonne réponse : **B.** Une non-conformité au paragraphe 9.2.2 portant sur les audits des domaines techniques

Un programme complet et bien mené échoue tout de même si un auditeur examine un domaine qu'il exploite. L'impartialité est un élément obligatoire de l'exigence d'audit interne ; il s'agit donc d'une non-conformité et non d'une opportunité d'amélioration, et elle porte sur les audits des domaines techniques, puisque rien dans la question ne montre que le dirigeant propriétaire effectue au quotidien des travaux relevant des finances ou des ressources humaines.

`Référence : ISO/IEC 27001:2022, paragraphe 9.2.2`

`Piège : T-03 Compétence ou indépendance`

Q7 Bonne réponse : **A.** Les chiffres sont collectés et conservés, mais personne ne les analyse ni ne les évalue.

L'écart, ici, c'est mesurer par opposition à évaluer. Le paragraphe 9.1 de l'ISO/IEC 27001:2022 ne s'arrête pas à la surveillance et à la mesure ; il exige également que les résultats soient analysés et évalués, et que la performance de sécurité de l'information et l'efficacité du SMSI soient évaluées. Des indicateurs collectés, conservés et laissés « disponibles si quelqu'un les demande » sont des preuves dormantes : l'étape « Vérifier » produit des résultats qui n'atteignent jamais l'étape « Agir », de sorte que rien n'alimente l'amélioration. Tenir des informations documentées à disposition comme preuves des résultats satisfait à une partie du paragraphe. Ce qui manque, c'est l'analyse et l'évaluation elles-mêmes, et non des informations documentées à leur sujet ; tant que personne n'interprète les chiffres, rien n'en ressort qu'une action corrective puisse traiter.

Référence : ISO/IEC 27001:2022, paragraphe 9.1 Surveillance, mesurages, analyse et évaluation

Piège : T-01 Preuves ou constatation

Q8 Bonne réponse : **C.** Une non-conformité au paragraphe 7.5.3

Le paragraphe 7.5.3 ne s'arrête pas aux documents rédigés par l'organisme. Les informations documentées d'origine extérieure que l'organisme juge nécessaires à la planification et au fonctionnement du SMSI doivent être identifiées comme il convient et maîtrisées. Une norme de durcissement émise par un fournisseur que l'équipe suit quotidiennement entre exactement dans ce cas ; la laisser non maîtrisée au motif qu'elle vient de l'extérieur laisse une exigence non satisfaite : une non-conformité, et non un point d'amélioration.

Référence : ISO/IEC 27001:2022, paragraphe 7.5.3

Piège : T-02 « Doit » ou « il convient de »

Q9 Bonne réponse : **D.** La conformité dépend du fait que la mesure atteigne son objectif, la suppression en temps opportun des accès des partants, et non du fait que la revue ait été planifiée et validée ; la revue n'a pas détecté trois partants qui ont conservé leurs accès, la mesure est donc inefficace et une non-conformité s'applique.

La conformité s'apprécie à l'aune d'un seul critère : l'objectif de la mesure, et non l'exhaustivité de l'enregistrement de l'activité. L'Annexe A 5.18 de l'ISO/IEC 27001:2022 exige que les droits d'accès soient attribués, revus, modifiés et supprimés afin que l'accès reste autorisé conformément aux exigences métier, y compris la suppression en temps opportun des accès des partants. Trois partants ont conservé des comptes actifs malgré une revue validée : l'objectif n'est donc pas atteint et une non-conformité s'applique ; les validations attestent seulement que la revue a eu lieu.

Référence : ISO/IEC 27002:2022 Mesure 5.18 (droits d'accès ; suppression en temps opportun des accès des partants)

Piège : T-01 Preuves ou constatation

Q10 Bonne réponse : **B.** La Déclaration d'Applicabilité est complète, mais l'exigence relative au traitement des risques n'est pas satisfaite car les propriétaires du risque n'ont ni approuvé le plan ni accepté le risque résiduel.

Une Déclaration d'Applicabilité complète ne suffit pas à elle seule à satisfaire l'exigence relative au traitement des risques. L'approbation du plan par les propriétaires du risque et l'acceptation du risque résiduel sont des éléments de sortie obligatoires distincts, absents ici ; une non-conformité est donc établie, plutôt qu'une opportunité d'amélioration ou une nouvelle appréciation inutile.

Référence : ISO/IEC 27001:2022 Paragraphe 6.1.3

Piège : T-02 « Doit » ou « il convient de »

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.