ISO/IEC 27001 Lead Implementer : 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/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-implementer/.

QUESTION 1

L'équipe de mise en œuvre du SMSI de Kestrel Analytics a achevé son appréciation des risques, choisi des options de traitement pour chaque risque et déterminé les mesures de sécurité de l'information nécessaires, dont plusieurs proviennent d'un référentiel de sécurité du cloud plutôt que de l'ISO/IEC 27001. Le directeur de programme souhaite que le plan de traitement des risques soit déclaré achevé lors de la réunion du comité de pilotage de vendredi. Quelles étapes restantes le paragraphe 6.1.3 exige-t-il d'abord ?

A. Comparer les mesures déterminées avec l'Annexe A pour vérifier qu'aucune mesure nécessaire n'a été oubliée, produire une Déclaration d'Applicabilité justifiant les inclusions et les exclusions, et obtenir l'approbation du plan par la direction et l'acceptation formelle des risques résiduels au niveau du conseil d'administration.

B. Retravailler chaque mesure de sécurité de l'information issue du référentiel de sécurité du cloud afin qu'elle corresponde à une mesure de l'Annexe A, produire la Déclaration d'Applicabilité à partir de cette correspondance avec l'Annexe A, et faire confirmer par les propriétaires des risques que les mesures applicables de l'Annexe A sont toutes reprises dans le plan de traitement.

C. Comparer les mesures déterminées avec l'Annexe A pour vérifier qu'aucune mesure nécessaire n'a été oubliée, produire une Déclaration d'Applicabilité justifiant les inclusions et les exclusions, et obtenir l'approbation du plan et l'acceptation des risques résiduels par les propriétaires des risques.

QUESTION 2

Un implémenteur planifie l'activité opérationnelle de traitement des risques exigée pendant la phase de fonctionnement. Quel énoncé décrit correctement ce que ce paragraphe oblige l'organisme à faire ?

A. Produire la Déclaration d'Applicabilité et vérifier qu'aucune mesure nécessaire de l'Annexe A n'a été omise

B. Mettre en œuvre le plan de traitement des risques et conserver des informations documentées sur les résultats du traitement

C. Formuler le plan de traitement des risques et obtenir l'approbation des risques résiduels par les propriétaires du risque

QUESTION 3

Un fournisseur de services gérés de cinq personnes exploite le SMSI de plusieurs clients. Un ingénieur senior demande lui-même des modifications du pare-feu de production d'un client, puis approuve et déploie ces mêmes modifications, car aucun collègue ne possède les compétences réseau nécessaires pour examiner le travail. L'appréciation des risques signale cette concentration de tâches comme une source à forte vraisemblance de fraude ou d'erreur non détectée. Le responsable de la mise en œuvre doit décider comment la traiter tout en restant conforme. Quel traitement concilie le mieux le risque signalé avec les contraintes d'une petite équipe ?

A. Répartir les étapes de demande, d'approbation et de déploiement entre trois des cinq employés, même si un seul ingénieur possède les compétences en pare-feu nécessaires à l'examen.

B. Consigner l'acceptation du risque résiduel dans le registre des risques, puisqu'une équipe de cinq personnes ne peut pas séparer les tâches incompatibles et qu'aucune autre action n'est réalisable pour elle.

C. Transférer l'administration du pare-feu à un prestataire spécialisé externe afin que les tâches incompatibles de demande-approbation-déploiement soient assurées en dehors du personnel propre de l'organisme.

D. Conserver le rôle cumulé de l'ingénieur, mais ajouter une surveillance indépendante des journaux de modification du pare-feu ainsi qu'un examen documenté par l'encadrement de chaque déploiement en production.

QUESTION 4

Vous rédigez la Déclaration d'Applicabilité d'une société de logiciels dotée d'un siège social à Montreal et de deux bureaux régionaux de développement qui se connectent par VPN ; plusieurs développeurs travaillent également à domicile. Votre projet indique pour A.6.7 « Travail à distance » : « Non applicable - l'entreprise n'a pas de politique formelle de travail à domicile. » Le RSSI vous demande de confirmer cette décision d'applicabilité avant validation. Quelle est la manière la plus défendable de trancher la décision d'applicabilité de A.6.7 ?

A. Indiquer A.6.7 comme applicable et la traiter par une nouvelle politique de travail à distance.

B. Indiquer A.6.7 comme non applicable, les bureaux régionaux étant des locaux de l'entreprise.

C. Indiquer A.6.7 comme applicable et consigner le VPN existant comme sa mise en œuvre.

D. Indiquer A.6.7 comme non applicable jusqu'à l'approbation d'une politique de travail à distance.

QUESTION 5

Meridian Legal est un cabinet d'avocats de taille moyenne doté d'un SMSI certifié en fonctionnement stabilisé. Sa procédure d'appréciation des risques indique que les appréciations sont réalisées chaque année en mars ; celle de cette année a été achevée il y a trois mois. En juin, le cabinet signe un contrat pour migrer l'intégralité de son système de gestion des dossiers et tous les documents des clients d'un serveur sur site vers une nouvelle plateforme SaaS, avec une mise en production prévue dans huit semaines. Le responsable du SMSI planifie la migration. En ce qui concerne l'appréciation des risques du SMSI, qu'exige le paragraphe 8.2 du responsable du SMSI au sujet de cette migration ?

A. Apprécier les risques de la bascule avant la mise en production ; ceux de la plateforme SaaS une fois en production

B. Apprécier les risques de la migration avant la mise en production ; maintenir le cycle de mars comme prévu

C. Maîtriser la migration comme une modification planifiée avant la mise en production ; ses risques en mars

D. Vérifier la sécurité du fournisseur SaaS avant la mise en production ; les risques de la migration en mars

QUESTION 6

Votre analyse du risque est terminée : vous prévoyez de réduire certains risques au moyen de mesures de sécurité de l'information, l'entreprise entend maintenir un risque à coût élevé et à faible vraisemblance, et vous en éviterez un en mettant hors service un service hérité. Un consultant en sécurité vous remet un tableur répertoriant les 93 mesures de l'Annexe A et déclare : « Voici votre traitement, mettez en œuvre chacune d'entre elles et vous serez couvert. » Le commanditaire du programme apprécie la simplicité et vous demande de procéder sur cette base. Quelle approche reflète le mieux les exigences de traitement des risques de l'ISO/IEC 27001:2022 ?

A. Procéder selon une partie du plan, en retenant une mesure du tableur pour chacun des risques.

B. Refuser le plan et laisser les résultats de l'analyse du risque fixer les mesures, sans vérification ultérieure.

C. Refuser le plan et conserver le tableur comme vérification une fois les mesures de chaque risque fixées.

D. Procéder selon le plan et conserver les résultats de l'analyse du risque comme vérification une fois ses mesures en place.

QUESTION 7

Marco, le responsable du SMSI, constitue le dossier de la revue de direction annuelle de l'entreprise avec la direction. Son projet d'ordre du jour couvre déjà : l'état d'avancement des actions décidées lors de la revue précédente, les modifications des enjeux internes et externes et des parties intéressées, les tendances de la performance (non-conformités et actions correctives, résultats de la surveillance et de la mesure, résultats d'audit et atteinte des objectifs), les retours d'information des parties intéressées et les opportunités d'amélioration continue. Un collègue qui relit l'ordre du jour indique qu'un élément d'entrée exigé par le paragraphe 9.3.2 manque encore. Quel élément Marco doit-il ajouter pour que les éléments d'entrée de la revue soient complets au titre du paragraphe 9.3.2 ?

A. Le résultat des appréciations des risques les plus récentes de l'organisme, ainsi que l'état d'avancement du plan de traitement de ces risques.

B. L'inventaire des actifs et la Déclaration d'Applicabilité, approuvés de nouveau par la direction au cours de la réunion.

C. La confirmation que les actions correctives reportées de la revue précédente sont désormais clôturées.

D. Les décisions documentées relatives aux modifications du SMSI que la revue conclut être nécessaires.

QUESTION 8

Une entreprise décide d'intégrer une filiale nouvellement acquise dans le domaine d'application du SMSI et, dans le même temps, d'assouplir ses critères d'acceptation des risques afin qu'une gamme plus large de risques puisse être acceptée sans remontée hiérarchique. Les deux décisions ont été approuvées sur le principe. Le responsable de la mise en œuvre doit décider comment mener à bien ces deux modifications au niveau du SMSI de manière maîtrisée. Comment convient-il de traiter ces modifications pour satisfaire à l'exigence de modification maîtrisée ?

A. Planifier les deux comme des mises à jour du registre des risques et de la DdA

B. Planifier les deux comme des changements informatiques relevant de la procédure de gestion des changements

C. Planifier les deux comme des points de la prochaine revue de direction programmée

D. Planifier les deux comme des modifications du SMSI avant leur prise d'effet

QUESTION 9

Vous mettez en œuvre des mesures de sécurité de l'information pour la migration d'une charge de travail contenant des données clients vers une plateforme SaaS publique. Le fournisseur ne propose qu'un accord standard accepté d'un clic, dont les conditions sont figées et ne peuvent pas être négociées. Votre responsable soutient qu'une fois les données hébergées dans le nuage du fournisseur, la sécurité de l'information relève entièrement de la responsabilité du fournisseur et qu'il ne reste rien à faire pour le SMSI. Quelle est l'action la plus appropriée pour le responsable de la mise en œuvre au titre de la mesure 5.23 de l'ISO/IEC 27002:2022 ?

A. Déterminer les mesures qui nous incombent, puis examiner les conditions du fournisseur et faire accepter le risque résiduel.

B. Rechercher une assurance sur les mesures du fournisseur, puis exiger une clause de droit d'audit avant la migration.

C. Rechercher une assurance sur les mesures du fournisseur, puis examiner les conditions du fournisseur et faire accepter le risque résiduel.

D. Déterminer les mesures qui nous incombent, puis exiger une clause de droit d'audit avant la migration.

QUESTION 10

Le responsable de la mise en œuvre met en place la première appréciation des risques de sécurité de l'information de l'organisme. L'équipe prévoit d'organiser un atelier, de recenser par remue-méninges les risques pesant sur la confidentialité, l'intégrité et la disponibilité des informations incluses dans le domaine d'application, de noter la vraisemblance et l'impact de chaque risque sur une échelle de 1 à 5, de multiplier les deux pour obtenir un niveau de risque, puis de classer les résultats. Elle prévoit de ne déterminer que plus tard quels niveaux de risque l'organisme est prêt à tolérer, une fois que la direction aura examiné la liste classée. Selon le paragraphe 6.1.2, quelle exigence l'équipe a-t-elle le plus manifestement omis de satisfaire avant de réaliser cette appréciation ?

A. Utiliser une méthode de notation qui donne des résultats cohérents et comparables.

B. Identifier les risques pesant sur la confidentialité, l'intégrité et la disponibilité.

C. Définir les informations que l'appréciation doit couvrir.

D. Fixer les niveaux de risque que l'organisme est prêt à accepter.

Réponses

Q1 Bonne réponse : **C.** Comparer les mesures déterminées avec l'Annexe A pour vérifier qu'aucune mesure nécessaire n'a été oubliée, produire une Déclaration d'Applicabilité justifiant les inclusions et les exclusions, et obtenir l'approbation du plan et l'acceptation des risques résiduels par les propriétaires des risques.

Le paragraphe 6.1.3 achève le processus de traitement en trois temps : comparer les mesures déterminées avec l'Annexe A pour vérifier que rien de nécessaire n'a été omis, produire une Déclaration d'Applicabilité justifiant les inclusions et les exclusions, et faire approuver le plan de traitement et accepter les risques résiduels par les propriétaires des risques. Les mesures de sécurité de l'information peuvent provenir de n'importe quelle source ; les mesures issues d'un référentiel n'ont donc pas à être remises en correspondance avec l'Annexe A, et la validation revient aux propriétaires des risques, et non à la direction ou au conseil d'administration.

`Référence : ISO/IEC 27001:2022 paragraphe 6.1.3`

`Piège : T-01 Déclaration d'Applicabilité ou plan de traitement des risques`

Q2 Bonne réponse : **B.** Mettre en œuvre le plan de traitement des risques et conserver des informations documentées sur les résultats du traitement

Le paragraphe relatif au traitement en phase de fonctionnement porte sur l'exécution : mettre en œuvre le plan de traitement et conserver les résultats documentés. Formuler le plan, obtenir l'approbation des propriétaires du risque et produire la DdA sont autant d'activités de la phase de planification. Garder les deux phases distinctes évite d'attribuer des obligations de conception à l'étape de fonctionnement.

`Référence : ISO/IEC 27001:2022, paragraphe 8.3`

`Piège : T-02 Planification ou fonctionnement`

Q3 Bonne réponse : **D.** Conserver le rôle cumulé de l'ingénieur, mais ajouter une surveillance indépendante des journaux de modification du pare-feu ainsi qu'un examen documenté par l'encadrement de chaque déploiement en production.

La séparation des tâches est un principe à appliquer dans la mesure où cela est possible et réalisable, et non une règle absolue. Il convient que les petits organismes qui ne peuvent pas séparer entièrement les tâches incompatibles envisagent des mesures de sécurité de l'information compensatoires (surveillance, pistes d'audit, supervision par l'encadrement) plutôt que d'accepter le risque sans traitement ou de simuler une séparation.

`Référence : ISO/IEC 27002:2022 Mesure 5.3`

`Piège : T-03 Réduire, maintenir, éviter ou partager`

Q4 Bonne réponse : **A.** Indiquer A.6.7 comme applicable et la traiter par une nouvelle politique de travail à distance.

La mesure 6.7 de l'ISO/IEC 27002:2022 indique que le travail à distance a lieu chaque fois que le personnel travaille depuis un lieu situé hors des locaux de l'organisme et accède à des informations sous quelque forme que ce soit. Les bureaux régionaux sont des locaux de l'organisme, mais les développeurs travaillant à domicile correspondent à cette définition ; le risque que traite la mesure de sécurité de l'information existe donc et A.6.7 est applicable. L'applicabilité est déterminée par le profil de risque, et non par l'existence préalable d'une politique - la politique manquante est précisément le traitement (une politique spécifique à une thématique portant sur le travail à distance), et le paragraphe 6.1.3 de l'ISO/IEC 27001 exige que la DdA contienne les mesures nécessaires, la justification de leur inclusion et l'indication de leur mise en œuvre ou non. Exclure une mesure dont le risque est présent, ou la consigner comme mise en œuvre avant que ses dispositions ne couvrent les personnes travaillant à distance, donne une image inexacte du contexte de l'organisme.

Référence : ISO/IEC 27002:2022 Mesure 6.7

Piège : T-01 Déclaration d'Applicabilité ou plan de traitement des risques

---

Q5 Bonne réponse : **B.** Apprécier les risques de la migration avant la mise en production ; maintenir le cycle de mars comme prévu

Le paragraphe 8.2 stipule que l'organisme « doit réaliser des appréciations des risques de sécurité de l'information à des intervalles planifiés ou lorsque des modifications significatives sont proposées ou se produisent, en tenant compte des critères établis en 6.1.2 a) », et « doit conserver des informations documentées sur les résultats ». Deux déclencheurs indépendants s'appliquent : l'intervalle annuel de mars en est un ; une migration, proposée à l'échelle du cabinet, du système central de gestion des dossiers et des données des clients est l'autre. Comme le paragraphe est déclenché par des modifications « proposées », et pas seulement par celles qui se sont produites, l'appréciation est due maintenant, avant la mise en production, afin que ses résultats puissent orienter la manière dont la migration est menée et que la transition de huit semaines ne reste pas sans appréciation.

Référence : ISO/IEC 27001:2022 paragraphe 8.2

Piège : T-02 Planification ou fonctionnement

Q6 Bonne réponse : **C.** Refuser le plan et conserver le tableur comme vérification une fois les mesures de chaque risque fixées.

Le traitement des risques est guidé par l'appréciation des risques, et non par un catalogue de mesures de sécurité de l'information. En vertu du 6.1.3, l'organisme (a) choisit une option de traitement appropriée pour chaque risque en tenant compte des résultats de l'appréciation, réduire, maintenir, éviter ou partager selon le risque, puis (b) détermine toutes les mesures nécessaires à la mise en œuvre de ces options, en s'appuyant sur toute source appropriée (NOTE 1), et seulement ensuite (c) compare cet ensemble déterminé à l'Annexe A afin de vérifier qu'aucune mesure nécessaire n'a été omise (NOTE 2). L'Annexe A est un filet de sécurité d'exhaustivité, et non une obligation de mettre en œuvre les 93 mesures (ce qui réfute l'argumentaire du consultant), ni la seule source admissible (NOTE 1, NOTE 3). La comparaison du 6.1.3 c) est elle-même une exigence qui ne peut pas être omise, et ses résultats sous-tendent les justifications d'exclusion dans la Déclaration d'Applicabilité (6.1.3 d).

Référence : ISO/IEC 27001:2022 paragraphe 6.1.3

Piège : T-03 Réduire, maintenir, éviter ou partager

Q7 Bonne réponse : **A.** Le résultat des appréciations des risques les plus récentes de l'organisme, ainsi que l'état d'avancement du plan de traitement de ces risques.

Le paragraphe 9.3.2 énumère les éléments d'entrée qu'une revue de direction doit prendre en compte : a) l'état d'avancement des actions décidées précédemment ; b) les modifications des enjeux internes et externes ; c) les modifications des besoins et attentes des parties intéressées ; d) les retours d'information et les tendances relatifs à la performance de la sécurité de l'information ; e) les retours d'information des parties intéressées ; f) les résultats de l'appréciation des risques et l'état d'avancement du plan de traitement des risques ; g) les opportunités d'amélioration continue. Le projet de Marco couvre a), b), c), d), e) et g) : la seule lacune est donc f), la vision des risques. L'élément d'entrée a) est l'état d'avancement des actions décidées lors des revues précédentes, et non la preuve qu'elles sont clôturées ; les décisions relatives aux modifications du SMSI sont des résultats de la revue au titre du paragraphe 9.3.3, et non des éléments d'entrée de celle-ci ; et ni l'inventaire des actifs ni une nouvelle approbation de la Déclaration d'Applicabilité, qui est produite au titre du paragraphe 6.1.3 d), ne figurent parmi les éléments d'entrée énumérés.

Référence : ISO/IEC 27001:2022, paragraphe 9.3.2

Piège : T-01 Déclaration d'Applicabilité ou plan de traitement des risques

---

Q8 Bonne réponse : **D.** Planifier les deux comme des modifications du SMSI avant leur prise d'effet

Ce qui compte ici, c'est de savoir quelle exigence relative aux modifications s'applique. Le domaine d'application et les critères d'acceptation des risques sont des éléments du système de management ; le paragraphe 6.3 s'applique donc : la modification doit être réalisée de manière planifiée. La mesure de sécurité de l'information portant sur la gestion technique des changements vise les systèmes d'information, pas le SMSI, et ni le report à la revue de direction ni la modification des enregistrements en aval ne satisfait à la modification planifiée.

Référence : ISO/IEC 27001:2022 Paragraphe 6.3

Piège : T-02 Planification ou fonctionnement

Q9 Bonne réponse : **A.** Déterminer les mesures qui nous incombent, puis examiner les conditions du fournisseur et faire accepter le risque résiduel.

Un accord figé et non négociable ne lève pas les responsabilités du client. La mesure de sécurité de l'information 5.23 de l'ISO/IEC 27002:2022 relève que l'usage de l'informatique en nuage peut impliquer une responsabilité partagée et indique qu'il est essentiel que les responsabilités des deux parties soient définies et mises en œuvre de manière appropriée ; parmi les éléments qu'il convient que l'organisme définisse figurent les mesures de sécurité gérées par le fournisseur et celles qu'il gère lui-même en tant que client. L'obtention d'une assurance sur les mesures du fournisseur figure également dans la liste, mais ne tranche pas la question de savoir qui exploite quelles mesures. Bien que les accords de service en nuage soient souvent prédéfinis et non ouverts à la négociation, il convient néanmoins que l'organisme les examine au regard de ses exigences de confidentialité, d'intégrité, de disponibilité et de traitement de l'information, qu'il réalise une appréciation des risques pertinente et que le risque résiduel soit identifié et accepté par la direction appropriée.

Référence : ISO/IEC 27002:2022, mesure de sécurité de l'information 5.23

Piège : T-03 Réduire, maintenir, éviter ou partager

Q10 Bonne réponse : **D.** Fixer les niveaux de risque que l'organisme est prêt à accepter.

Le paragraphe 6.1.2(a) exige que le processus d'appréciation des risques établisse et tienne à jour des critères de risque de sécurité de l'information comprenant (1) les critères d'acceptation des risques et (2) les critères de réalisation des appréciations des risques. Ils sont fondamentaux : 6.1.2(e)(1) évalue les risques en comparant les résultats de l'analyse à ces critères, puis les classe par ordre de priorité en vue de leur traitement. Déterminer quels niveaux de risque sont tolérables seulement après le classement des risques inverse cet ordre exigé. Deux autres éléments du plan tiennent : l'équipe identifie les risques pesant sur la confidentialité, l'intégrité et la disponibilité des informations incluses dans le domaine d'application (6.1.2(c)(1)), et le paragraphe est neutre quant à la méthode, à condition que des appréciations répétées soient cohérentes, valides et comparables (6.1.2(b)) ; un modèle fondé sur le produit de la vraisemblance et de l'impact est donc acceptable.

Référence : ISO/IEC 27001:2022 paragraphe 6.1.2

Piège : T-02 Planification ou fonctionnement

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.