ISO/IEC 27001 Foundation : 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-foundation/.

QUESTION 1

Hollis & Brandt Accountants demande à ses employés de bureau de ranger les documents papier des clients et de verrouiller leur écran d'ordinateur chaque fois qu'ils quittent leur poste. Quel thème de l'Annexe A contient la mesure de sécurité de l'information exigeant ces deux règles ?

A. Personnes

B. Physique

C. Technologique

QUESTION 2

Une équipe SMSI fixe un objectif visant à instaurer une culture dans laquelle le personnel signale sans crainte les erreurs de sécurité, et ne trouve aucun moyen réalisable de le mesurer. Lequel de ces éléments le paragraphe 6.2 exige-t-il malgré tout pour cet objectif ?

A. Approbation à titre d'exception par la direction

B. Une justification enregistrée dans la DdA

C. Surveillance de sa progression dans le temps

QUESTION 3

Un organisme informe l'ensemble du personnel de sa nouvelle politique de sécurité et fait suivre à son équipe pare-feu une formation certifiante du fournisseur, dont il conserve les certificats. Quel paragraphe de l'ISO/IEC 27001:2022 couvre la formation de l'équipe ?

A. Paragraphe 7.2 Compétences

B. Paragraphe 7.4 Communication

C. Paragraphe 7.3 Sensibilisation

QUESTION 4

Le système de gestion documentaire d'une entreprise ajoute une balise masquée « Restreint » aux propriétés de chaque fichier, afin que sa passerelle de messagerie puisse empêcher automatiquement la sortie de ces fichiers. Quelle mesure de sécurité de l'information l'ajout de la balise met-il en œuvre ?

A. Mesure 5.12 Classification des informations

B. Mesure 5.13 Marquage des informations

C. Mesure 5.14 Transfert des informations

QUESTION 5

Un organisme prévoit de transférer sa base de données clients vers un nouveau fournisseur d'hébergement le trimestre prochain. Quel paragraphe de l'ISO/IEC 27001:2022 exige qu'une appréciation des risques soit réalisée en raison de cette modification ?

A. Paragraphe 6.3 Planification des modifications

B. Paragraphe 6.1.2 Appréciation des risques de sécurité de l'information

C. Paragraphe 8.2 Appréciation des risques de sécurité de l'information

QUESTION 6

Lors d'une coupure de courant, les serveurs continuent de fonctionner grâce à un groupe électrogène de secours, mais la climatisation de la salle des serveurs n'y est pas raccordée et s'arrête, si bien que les serveurs surchauffent. Quelle mesure de sécurité de l'information de l'Annexe A couvre le PLUS directement cette lacune ?

A. Services supports

B. Emplacement et protection du matériel

C. Maintenance du matériel

QUESTION 7

Un document indique qu'il convient de conserver des sauvegardes des informations, des logiciels et des systèmes et de les tester régulièrement conformément à la politique spécifique à une thématique portant sur la sauvegarde. De quel document s'agit-il ?

A. ISO/IEC 27003

B. Annexe A de l'ISO/IEC 27001

C. ISO/IEC 27002

QUESTION 8

La politique de sécurité de l'information d'une entreprise ne dit rien de la façon dont sont traitées les demandes d'exception à cette politique. Comment convient-il de qualifier cette lacune ?

A. Un écart aux lignes directrices de l'ISO/IEC 27002

B. Une non-conformité au paragraphe 5.2

C. Une non-conformité à la mesure 5.1 de l'Annexe A

QUESTION 9

Quelle exigence de l'ISO/IEC 27001 reflète le plus directement l'approche processus ?

A. Inclure les processus et leurs interactions dans le SMSI

B. Définir et appliquer un processus d'appréciation des risques

C. Prendre en compte les interfaces et dépendances pour le domaine d'application

QUESTION 10

Un rançongiciel ayant atteint un PC de bureau a chiffré tous les serveurs de l'entreprise en l'espace d'une heure. Chaque appareil pouvait se connecter directement à tous les autres appareils. Quelle mesure de sécurité de l'information aurait le PLUS directement limité l'étendue de sa propagation ?

A. Mesure 8.7 (protection contre les programmes malveillants (malware))

B. Mesure 8.22 (cloisonnement des réseaux)

C. Mesure 8.20 (sécurité des réseaux)

Réponses

Q1 Bonne réponse : **B.** Physique

L'Annexe A de l'ISO/IEC 27001:2022 classe les règles du bureau vide et de l'écran vide (mesure 7.7) dans le thème physique. Le fait que le personnel applique ces règles, ou qu'un logiciel puisse verrouiller les écrans, ne fait pas passer la mesure dans le thème personnes ni dans le thème technologique.

`Référence : ISO/IEC 27001:2022 Annexe A`

`Piège : T-01 Mesures qui se ressemblent`

Q2 Bonne réponse : **C.** Surveillance de sa progression dans le temps

Le paragraphe 6.2 indique que les objectifs de sécurité de l'information doivent être mesurables si c'est réalisable ; un objectif valable qui ne peut pas raisonnablement être mesuré est donc admis. Les autres exigences de l'article continuent de s'y appliquer, et la surveillance en fait partie. La surveillance consiste à suivre l'état d'avancement, ce qui ne dépend pas de l'existence d'un chiffre à communiquer.

`Référence : ISO/IEC 27001:2022 Paragraphe 6.2`

`Piège : T-02 Exigence ou bonne pratique`

Q3 Bonne réponse : **A.** Paragraphe 7.2 Compétences

Une activité peut ressembler à une autre ; demandez-vous donc ce qu'elle accomplit. Développer les compétences dont un rôle a besoin, par la formation initiale, la formation professionnelle ou l'expérience, et conserver des preuves telles que des certificats, c'est la compétence au sens du paragraphe 7.2. Veiller à ce que les personnes connaissent la politique et leur rôle dans le SMSI, c'est la sensibilisation au sens du paragraphe 7.3, et planifier ce qui est communiqué, quand, avec qui et comment, c'est le paragraphe 7.4.

`Référence : ISO/IEC 27001:2022 paragraphe 7.2`

`Piège : T-03 Paragraphes voisins`

Q4 Bonne réponse : **B.** Mesure 5.13 Marquage des informations

La classification (mesure 5.12) détermine le niveau ; le marquage (mesure 5.13) appose ce niveau sur l'information afin qu'il puisse être reconnu. L'ISO/IEC 27002 inclut le soutien à l'automatisation dans l'objectif du marquage et recommande les métadonnées pour les informations numériques, afin que les systèmes puissent prendre des décisions en fonction du marquage.

`Référence : ISO/IEC 27002:2022 Mesure 5.13`

`Piège : T-01 Mesures qui se ressemblent`

Q5 Bonne réponse : **C.** Paragraphe 8.2 Appréciation des risques de sécurité de l'information

L'appréciation des risques apparaît deux fois dans l'ISO/IEC 27001:2022. Le paragraphe 6.1.2, qui relève de la planification, définit le processus et ses critères. Le paragraphe 8.2, qui relève du fonctionnement, exige que des appréciations soient réalisées à intervalles planifiés et chaque fois que des modifications significatives sont proposées ou surviennent, les résultats étant conservés sous forme d'information documentée. Un projet de transfert d'hébergement est précisément ce type de déclencheur.

`Référence : ISO/IEC 27001:2022 paragraphe 8.2`

`Piège : T-03 Paragraphes voisins`

Q6 Bonne réponse : **A.** Services supports

Les services supports ne se limitent pas à l'alimentation électrique des serveurs. L'ISO/IEC 27002 cite la ventilation et la climatisation aux côtés de l'électricité, de l'eau et des télécommunications. La mesure 7.11 de l'Annexe A exige que les moyens de traitement de l'information soient protégés contre les perturbations causées par des défaillances des services supports ; le refroidissement des serveurs a donc lui aussi besoin d'être protégé contre une coupure de courant.

`Référence : ISO/IEC 27002:2022 mesure 7.11`

`Piège : T-01 Mesures qui se ressemblent`

Q7 Bonne réponse : **C.** ISO/IEC 27002

La mesure de sécurité de l'information 8.13, « Sauvegarde des informations », est formulée de façon presque identique dans les deux documents ; c'est donc la forme verbale qui tranche. L'Annexe A de l'ISO/IEC 27001 l'énonce avec « doit », la formulation d'une exigence. L'ISO/IEC 27002 l'énonce avec « il convient de », la formulation propre aux lignes directrices. L'ISO/IEC 27003 fournit elle aussi des lignes directrices, mais elle porte sur les articles relatifs au SMSI, et non sur des mesures individuelles.

`Référence : ISO/IEC 27002:2022 Mesure 8.13`

`Piège : T-02 Exigence ou bonne pratique`

Q8 Bonne réponse : **A.** Un écart aux lignes directrices de l'ISO/IEC 27002

Le paragraphe 5.2 de l'ISO/IEC 27001 fixe les exigences relatives au contenu de la politique de sécurité de l'information, et le traitement des exceptions n'en fait pas partie. L'ISO/IEC 27002 recommande des énoncés supplémentaires, comme la façon dont les dérogations et les exceptions sont traitées, mais ses lignes directrices ne sont pas obligatoires. La lacune mérite d'être comblée, mais ce n'est pas une non-conformité.

`Référence : ISO/IEC 27002:2022 Mesure 5.1`

`Piège : T-02 Exigence ou bonne pratique`

Q9 Bonne réponse : **A.** Inclure les processus et leurs interactions dans le SMSI

L'approche processus considère un système de management comme un ensemble de processus dont les interactions sont identifiées et gérées. Le paragraphe 4.4 de l'ISO/IEC 27001 la reflète en exigeant que le SMSI inclue les processus nécessaires et leurs interactions. Les interfaces du domaine d'application (paragraphe 4.3) et le processus d'appréciation des risques (paragraphe 6.1.2) impliquent aussi des processus ou des activités, mais aucun des deux ne porte sur la manière dont les processus du SMSI s'articulent entre eux.

`Référence : ISO/IEC 27001:2022 paragraphe 4.4`

`Piège : T-03 Paragraphes voisins`

Q10 Bonne réponse : **B.** Mesure 8.22 (cloisonnement des réseaux)

Le rançongiciel s'est propagé aussi loin parce que rien ne s'interposait entre les PC de bureau et les serveurs. La mesure 8.22 de l'Annexe A exige que les groupes de services, d'utilisateurs et de systèmes soient maintenus séparés au sein des réseaux de l'organisme. L'ISO/IEC 27002 décrit la division d'un réseau en domaines, par exemple un domaine des postes de travail et un domaine des serveurs, le trafic entre eux étant contrôlé au niveau du périmètre.

Référence : ISO/IEC 27002:2022 Mesure 8.22

Piège : T-01 Mesures qui se ressemblent

Vous voulez toute la banque de questions ?

Mindset Prep propose plus de 3 050 questions pour sept examens 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.