ISO 31000 Risk Manager : 10 questions d'entraînement avec réponses

Dix questions de la banque de questions Mindset Prep, rédigées à partir de la norme ISO 31000:2018. 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-31000-risk-manager/.

QUESTION 1

Un fabricant dispose d'excellents rapports sur les risques, à sens unique : dossiers trimestriels pour le conseil d'administration, tableaux de bord et registre tenu à jour. Pourtant, ses critères de risque ne reflètent toujours pas les réalités opérationnelles du terrain, et le personnel d'atelier applique les moyens de maîtrise de manière incohérente parce qu'il ne comprend pas les facteurs de risque sous-jacents. Le responsable des risques constate que les décisions continuent d'être prises sans les connaissances du terrain, et veut corriger la cause racine plutôt que les symptômes. Quel ajout au processus de management du risque répond le plus directement à cette lacune au regard de l'ISO 31000:2018 ?

A. Attribuer des responsabilités plus claires aux propriétaires des risques, afin que chaque moyen de maîtrise ait un propriétaire nommément désigné, qui réponde de son application cohérente et du compte rendu de son état.

B. Augmenter la fréquence et le niveau de détail des rapports existants sur les risques, afin que le personnel de terrain reçoive des informations plus complètes et plus opportunes sur les risques et sur les moyens de maîtrise qu'il est censé appliquer.

C. Ajouter une communication et une consultation bidirectionnelles tout au long de chaque étape, afin que le retour d'information des parties prenantes oriente des décisions telles que la définition des critères de risque et l'évaluation du risque, et que le personnel comprenne pourquoi des actions sont requises.

D. Renforcer la surveillance et la revue dans l'ensemble du processus, afin que l'application incohérente des moyens de maîtrise soit détectée plus tôt et corrigée dans le cadre du cycle de gestion de la performance avant que les écarts n'affectent les résultats.

QUESTION 2

Rivervale Health Services se préparait à lancer un service de dialyse de proximité. Avant de finaliser les critères de risque et l'appréciation du risque, le responsable des risques a réuni des médecins, du personnel infirmier de terrain, un groupe de représentants des patients et le régulateur du secteur, afin que leurs connaissances, leurs points de vue et leurs perceptions des risques du nouveau service soient recueillis pendant que l'appréciation était encore en cours d'élaboration. Plusieurs préoccupations soulevées par les représentants des patients, inconnues de l'équipe projet, ont sensiblement modifié la manière dont deux des risques ont été formulés. La décision du responsable des risques d'associer ces parties dès le début, afin que leurs perceptions façonnent l'appréciation, reflète le plus directement quel principe de l'ISO 31000 ?

A. Facteurs humains et culturels : le comportement humain et la culture influencent fortement tous les aspects du management du risque, en façonnant la manière dont les personnes, à chaque niveau et à chaque étape, perçoivent le risque, le jugent et y réagissent.

B. Inclusif : implication appropriée et en temps utile des parties prenantes afin que leurs connaissances, leurs points de vue et leurs perceptions soient pris en compte, ce qui améliore la sensibilisation et rend le management du risque plus éclairé.

C. Meilleure information disponible, éléments d'entrée tirés de données historiques et actuelles ainsi que d'attentes futures, les limites et les incertitudes de cette information étant explicitement prises en compte.

D. Communication et consultation : partager l'information avec les parties prenantes et recueillir leurs retours tout au long des étapes du management du risque, afin que différents points de vue soient pris en compte et qu'un sentiment d'appropriation se construise.

QUESTION 3

La direction de NnanTech veut disposer rapidement de critères de risque afin que les divisions puissent commencer à coter les risques de manière cohérente. Un consultant a rédigé une matrice cinq par cinq soignée, avec des bandes de vraisemblance chiffrées et des seuils d'impact financier, étalonnée sur les normes du secteur et prête à être déployée la semaine prochaine. Le conseil d'administration apprécie qu'elle paraisse rigoureuse et comparable à celle des pairs. Le responsable des risques, Devon, hésite, faisant observer que la direction ne s'est pas encore accordée sur le niveau et le type de risque que l'organisme est réellement prêt à prendre dans la poursuite de ses objectifs. Que convient-il que la direction fixe en premier pour que les critères soient solides ?

A. Quels risques prendre ou ne pas prendre, et dans quelle mesure pour chacun

B. Qui détient l'autorité et la redevabilité sur les critères de risque

C. La manière dont les conséquences et la vraisemblance seront définies et mesurées

QUESTION 4

Meridian Freight, un opérateur logistique, mettait en place son processus de management du risque pour l'année à venir. Avant qu'aucun risque n'ait été identifié ou analysé, le directeur des risques a travaillé avec le conseil d'administration pour convenir de déclarations écrites précisant le montant des pertes financières que l'organisme était prêt à absorber par événement, les catégories de conséquences en matière de sécurité qui étaient inacceptables, et la manière dont la vraisemblance et les conséquences seraient mesurées. Ces déclarations étaient alignées sur les objectifs de l'organisme et sur ses politiques déclarées. Quelle étape du processus de management du risque de l'ISO 31000:2018 le directeur des risques réalise-t-il ?

A. Établir le contexte externe et interne, l'environnement dans lequel l'organisme poursuit ses objectifs.

B. Réaliser l'évaluation du risque, en comparant les risques analysés aux seuils de l'organisme pour décider lesquels nécessitent un traitement.

C. Mener l'analyse du risque pour comprendre le niveau de chaque risque à partir de ses conséquences et de sa vraisemblance.

D. Définir les critères de risque au regard desquels l'importance du risque est évaluée.

QUESTION 5

Quatre mois avant son entrée en vigueur, un régulateur a annoncé une règle de localisation des données touchant directement les dispositifs d'infogérance cloud d'une entreprise. L'entreprise mettait à jour son registre des risques selon un cycle annuel fixe, et la prochaine mise à jour prévue n'aurait lieu que neuf mois plus tard. Le responsable des risques a demandé à l'équipe d'ajouter et d'apprécier immédiatement le nouveau risque réglementaire, de réattribuer la responsabilité de ce risque et de réviser les plans de traitement concernés, plutôt que d'attendre le cycle annuel. Quel principe de l'ISO 31000:2018 le responsable des risques met-il avant tout en application ?

A. Dynamique : le management du risque répond en temps voulu aux changements du contexte de l'organisme.

B. Amélioration continue : le cadre organisationnel est amélioré au fil du temps grâce aux enseignements que l'organisme tire de son expérience.

C. Meilleure information disponible : le registre reflète l'information réglementaire du moment, dont l'origine est établie et qui est tenue à jour.

D. Surveillance et revue : une surveillance et une revue continues maintiennent le registre des risques à jour tout au long du processus.

QUESTION 6

Aldermere, une coopérative d'épicerie régionale, conduit l'identification du risque pour une nouvelle gamme de produits sous marque propre. Le responsable des risques recense les ruptures d'approvisionnement chez les producteurs sous contrat, mais propose de laisser deux éléments hors du registre : une sécheresse régionale prolongée, au motif que la météo échappe au contrôle de la coopérative, et l'atteinte à la promesse de marque « cultivé localement », au motif qu'elle ne peut pas être exprimée en dollars. En application du paragraphe 6.4.2 de l'ISO 31000:2018, comment le responsable des risques devrait-il traiter ces deux exclusions proposées ?

A. Maintenir les deux exclusions et en consigner les raisons à l'intention des décideurs.

B. Renoncer aux deux exclusions et consigner les deux éléments dans le registre.

C. Renoncer à l'exclusion liée à la promesse de marque et consigner pourquoi la sécheresse reste hors du registre.

D. Renoncer à l'exclusion liée à la sécheresse et consigner pourquoi la promesse de marque reste hors du registre.

QUESTION 7

Une entreprise de logistique traite un risque de perturbation de la chaîne d'approvisionnement en recourant à un double approvisionnement pour un composant critique. Une fois le dispositif en place, le propriétaire du risque apprécie le risque traité au regard des critères de risque de l'entreprise et constate que l'exposition résiduelle se situe toujours au-dessus du niveau que le conseil d'administration a fixé comme tolérable. Le traitement a fonctionné comme prévu et n'a introduit aucun nouveau problème ; le risque de perturbation était simplement trop important pour qu'une seule mesure suffise à le réduire. Le propriétaire du risque a documenté l'exposition résiduelle, informé le conseil d'administration et planifié une revue. Dans le cadre du processus de traitement du risque, que devrait faire le propriétaire du risque au sujet de cette exposition résiduelle ?

A. Demander au conseil d'administration de réexaminer le niveau tolérable qu'il a fixé pour ce risque.

B. Remplacer le double approvisionnement par une autre option de traitement.

C. Sélectionner un traitement complémentaire à appliquer en parallèle du double approvisionnement.

D. Laisser l'exposition en l'état et la maintenir sous revue continue.

QUESTION 8

Thandi Krause, responsable des risques de l'entreprise chez Currentline Power Distribution, réserve deux jours tous les six mois à un exercice qu'elle tient à l'écart des revues du registre que son équipe mène déjà. Elle recueille des preuves de ce que le comité exécutif a réellement tiré du programme de risques au cours de la période, compare l'état actuel du programme avec ce qu'il était censé avoir produit à ce stade, et se forge une opinion à l'intention du conseil d'administration sur une seule question : le programme de risques mis en place par l'entreprise il y a deux ans justifie-t-il toujours sa place dans le soutien aux décisions stratégiques ? Elle ne recote aucun risque et ne propose encore aucune refonte. Quelle activité de l'ISO 31000 Thandi réalise-t-elle ?

A. Évaluation du risque - comparer les résultats de l'analyse du risque aux critères de risque de l'organisme afin de décider si une action supplémentaire est requise pour un risque donné

B. Évaluation du cadre organisationnel de management du risque - juger périodiquement si les dispositions mises en place pour soutenir la prise de décision atteignent toujours ce pour quoi elles ont été établies

C. Surveillance et revue au sein du processus de management du risque - vérifier périodiquement que les appréciations restent à jour et que les traitements continuent de fonctionner à mesure que le contexte de l'organisme évolue

QUESTION 9

Une entreprise de logistique a mené un essai saisonnier de livraison par drone au-dessus d'un port côtier très fréquenté. L'analyse du risque a montré que les drones créaient, au-dessus du port, un risque de collision en vol qui dépassait les critères de risque de l'entreprise. Après avoir pesé les options, le propriétaire du risque a décidé de mettre fin complètement à l'essai de livraison par drone et de revenir au service de livraison routière existant de l'entreprise. Laquelle des sept options de traitement du risque de l'ISO 31000 la décision du propriétaire du risque représente-t-elle ?

A. Éliminer la source de risque

B. Partager le risque

C. Modifier la vraisemblance

D. Éviter le risque

QUESTION 10

La direction d'une entreprise de logistique adopte l'ISO 31000 et souhaite démontrer de façon tangible son leadership et son engagement. Elle a déjà délégué les travaux d'identification du risque et d'analyse du risque à une équipe risque de deuxième ligne nouvellement constituée. Le conseil d'administration a demandé à l'équipe dirigeante de désigner une action, réalisée par la direction elle-même, qui démontre son leadership et son engagement avant la prochaine revue trimestrielle. Quelle action démontre le plus directement le leadership et l'engagement tels que décrits dans l'ISO 31000:2018, paragraphe 5.2 ?

A. Confirmer que les systèmes de management du risque sont mis en œuvre dans l'ensemble de l'organisme et fonctionnent efficacement.

B. Animer les ateliers au cours desquels le personnel identifie les risques afin que l'organisme puisse constituer et tenir à jour son registre des risques.

C. Publier une politique établissant l'approche de management du risque de l'organisme et allouer les ressources nécessaires au management du risque.

D. Réaliser des analyses SWOT et PEST du contexte opérationnel afin de cartographier les forces, les faiblesses et les pressions externes de l'organisme.

Réponses

Q1 Bonne réponse : **C.** Ajouter une communication et une consultation bidirectionnelles tout au long de chaque étape, afin que le retour d'information des parties prenantes oriente des décisions telles que la définition des critères de risque et l'évaluation du risque, et que le personnel comprenne pourquoi des actions sont requises.

Le paragraphe 6.2 indique que la communication et la consultation ont pour objectif d'aider les parties prenantes à comprendre le risque et les fondements des décisions, que la communication favorise la sensibilisation tandis que la consultation permet d'obtenir un retour d'information pour appuyer la prise de décision, et qu'il convient que l'une et l'autre aient lieu au sein de toutes les étapes du processus et tout au long de celles-ci, en garantissant que les différents points de vue sont pris en compte lors de la définition des critères de risque et de l'évaluation des risques, et en développant l'inclusion et l'appropriation. Le fabricant dispose déjà de rapports solides vers l'extérieur ; ce qui lui manque, c'est la boucle de consultation entrante et bidirectionnelle ; ajouter la consultation tout au long de chaque étape est donc la solution. Multiplier les rapports (paragraphe 6.7), renforcer la surveillance (paragraphe 6.6) et clarifier la propriété des risques (paragraphe 5.4.3) sont autant de leviers légitimes, mais chacun cible une étape différente et laisse sans réponse la boucle de retour d'information manquante.

`Référence : ISO 31000:2018 paragraphe 6.2`

`Piège : T-01 Quelle étape du processus ?`

Q2 Bonne réponse : **B.** Inclusif : implication appropriée et en temps utile des parties prenantes afin que leurs connaissances, leurs points de vue et leurs perceptions soient pris en compte, ce qui améliore la sensibilisation et rend le management du risque plus éclairé.

L'Article 4 d) Inclusif est l'implication appropriée et en temps utile des parties prenantes afin que leurs connaissances, leurs points de vue et leurs perceptions soient pris en compte, ce qui améliore la sensibilisation et conduit à un management du risque éclairé, exactement ce que le responsable a obtenu en réunissant les parties concernées avant la finalisation des critères de risque et de l'appréciation. La communication et la consultation constituent l'activité du processus (paragraphe 6.2) mettant en pratique le caractère inclusif, mais ne figurent pas parmi les principes de l'Article 4 que la question demande. Les Facteurs humains et culturels (Article 4 g), influence comportementale et culturelle) et la Meilleure information disponible (Article 4 f), éléments d'entrée de données et leurs limites) sont également des principes de l'Article 4, mais les éléments précis du scénario ne les étayent pas.

`Référence : ISO 31000:2018, Article 4 d), Inclusif`

`Piège : T-02 Principe, cadre organisationnel ou processus`

Q3 Bonne réponse : **A.** Quels risques prendre ou ne pas prendre, et dans quelle mesure pour chacun

Les critères de risque expriment le niveau et le type de risque qu'un organisme est disposé à prendre au regard de ses objectifs ; la direction doit donc fixer cet appétit en premier. Une matrice étalonnée sur les pairs peut paraître rigoureuse, mais tant que l'appétit n'est pas défini, les seuils n'ont aucune signification pour cet organisme.

`Référence : ISO 31000:2018, paragraphe 5.2`

`Piège : T-03 Risque, conséquence ou vraisemblance`

Q4 Bonne réponse : **D.** Définir les critères de risque au regard desquels l'importance du risque est évaluée.

Tout repose sur la chronologie : l'étalon est en cours de création, et non d'application. Le paragraphe 6.3.4 de l'ISO 31000:2018 définit les critères de risque comme l'ampleur et le type de risque que l'organisme peut ou non prendre au regard de ses objectifs, ainsi que les critères utilisés pour évaluer l'importance du risque ; ils sont fixés au début de l'appréciation du risque, en cohérence avec les objectifs et les politiques, et reflètent la manière dont les conséquences et la vraisemblance seront mesurées. Convenir des seuils de tolérance aux pertes, des catégories de conséquences inacceptables et de la base de mesure avant qu'aucun risque n'existe à apprécier correspond précisément à cette activité.

`Référence : ISO 31000:2018 paragraphe 6.3.4`

`Piège : T-01 Quelle étape du processus ?`

Q5 Bonne réponse : **A.** Dynamique : le management du risque répond en temps voulu aux changements du contexte de l'organisme.

Le principe e) Dynamique énonce que les risques peuvent apparaître, changer ou disparaître à mesure que le contexte externe et interne d'un organisme évolue, et que le management du risque anticipe, détecte, prend acte de ces changements et y répond de manière appropriée et en temps voulu.
Une règle de localisation des données nouvellement annoncée constitue un changement du contexte externe ; ajouter, apprécier et traiter ce risque hors cycle plutôt que d'attendre la mise à jour annuelle constitue précisément cette réponse en temps voulu. La surveillance et la revue (paragraphe 6.6) constituent l'étape du processus qui détecterait ce changement, et non un principe. Le principe Amélioration continue porte sur l'amélioration du cadre organisationnel fondée sur l'apprentissage, et le principe Meilleure information disponible porte sur l'origine et l'actualité des informations utilisées ; ni l'un ni l'autre ne décrit le jugement de réactivité dont il s'agit ici.

`Référence : ISO 31000:2018, Article 4 (Principes), principe e) Dynamique`

`Piège : T-02 Principe, cadre organisationnel ou processus`

Q6 Bonne réponse : **B.** Renoncer aux deux exclusions et consigner les deux éléments dans le registre.

Le paragraphe 6.4.2 indique qu'il convient que l'organisme identifie les risques, que leurs sources soient ou non sous son contrôle, et cite les « sources de risque tangibles et intangibles » parmi les facteurs à prendre en compte, en ajoutant que les résultats peuvent avoir des « conséquences tangibles ou intangibles ». Aucun des deux motifs du responsable des risques ne justifie de laisser un élément de côté au stade de l'identification, et en consigner les raisons n'y change rien. La sécheresse échappe au contrôle de la coopérative, mais le paragraphe 6.5.2 énumère tout de même des options de traitement telles que la modification des conséquences ou le partage du risque. Même si l'atteinte à la promesse de marque « cultivé localement » ne peut pas être exprimée en dollars, le paragraphe 6.4.3 indique que les techniques d'analyse peuvent être qualitatives. Il convient donc d'identifier les deux éléments.

`Référence : ISO 31000:2018, paragraphe 6.4.2`

`Piège : T-03 Risque, conséquence ou vraisemblance`

Q7 Bonne réponse : **C.** Sélectionner un traitement complémentaire à appliquer en parallèle du double approvisionnement.

Le traitement du risque est itératif : après la mise en œuvre d'une option, le propriétaire juge si le risque résiduel est acceptable au regard des critères et, s'il ne l'est pas, un traitement complémentaire s'ensuit. Ici, l'exposition dépasse toujours le niveau tolérable fixé par le conseil d'administration ; le propriétaire revient donc à la sélection des options. Le double approvisionnement a fonctionné comme prévu et le risque était simplement trop important pour qu'une seule mesure suffise à le réduire ; on lui adjoint donc une option complémentaire au lieu de le remplacer, les options de traitement ne s'excluant pas nécessairement mutuellement. Documenter, informer et planifier une revue maintiennent la visibilité du risque résiduel, mais consigner et revoir, à eux seuls, conviennent aux cas où aucune option de traitement n'est disponible ou ne modifie suffisamment le risque, et non à un reliquat simplement trop important pour une seule mesure.

`Référence : ISO 31000:2018, Paragraphe 6.5`

`Piège : T-01 Quelle étape du processus ?`

Q8 Bonne réponse : **B.** Évaluation du cadre organisationnel de management du risque - juger périodiquement si les dispositions mises en place pour soutenir la prise de décision atteignent toujours ce pour quoi elles ont été établies

Deux frontières tranchent la question. L'évaluation du cadre organisationnel (paragraphe 5.6) mesure périodiquement le cadre au regard de sa finalité et des résultats attendus, et juge s'il reste adapté - c'est l'exercice de Thandi. La surveillance et la revue au sein du processus portent sur les risques, les appréciations et les traitements, auxquels elle ne touche délibérément pas ; l'évaluation du risque compare des risques individuels aux critères, ce qu'elle ne fait jamais. L'homonymie est le piège : « évaluation » désigne à la fois une activité du cadre organisationnel et une étape du processus, et seul l'objet évalué permet de les distinguer.

`Référence : ISO 31000:2018 paragraphe 5.6`

`Piège : T-02 Principe, cadre organisationnel ou processus`

Q9 Bonne réponse : **D.** Éviter le risque

Le paragraphe 6.5.2 énumère sept options de traitement du risque, qui ne s'excluent pas nécessairement mutuellement. La première consiste à éviter le risque « en décidant de ne pas démarrer ou de ne pas poursuivre l'activité porteuse du risque ». Le propriétaire du risque a mis fin complètement à l'essai de livraison par drone ; les vols à l'origine du risque de collision n'ont donc plus lieu : c'est un évitement. Aucun drone ne survole plus le port et la possibilité d'une collision disparaît, mais ces deux effets découlent de l'arrêt de l'activité, et non d'un traitement appliqué à des vols qui se poursuivent. Revenir au service de livraison routière propre à l'entreprise ne confie le risque à aucune autre partie ; rien n'est donc partagé.

`Référence : ISO 31000:2018 Paragraphe 6.5.2`

`Piège : T-03 Risque, conséquence ou vraisemblance`

Q10 Bonne réponse : **C.** Publier une politique établissant l'approche de management du risque de l'organisme et allouer les ressources nécessaires au management du risque.

Le paragraphe 5.2 de l'ISO 31000:2018 décrit la manière dont la direction et les organes de surveillance démontrent leur leadership et leur engagement : l'adaptation et la mise en œuvre de tous les composants du cadre organisationnel, la publication d'une déclaration ou d'une politique établissant une approche du management du risque, l'assurance que les ressources nécessaires sont allouées au management du risque, et l'attribution de l'autorité, de la responsabilité et de l'obligation de rendre compte. L'acte qui compte est la publication de la politique, et non sa rédaction : un spécialiste du risque tel qu'un directeur des risques (CRO) peut la rédiger, mais sa publication et l'allocation des ressources sont réalisées par la direction elle-même. Les travaux d'identification et d'analyse délégués, ainsi que l'analyse du contexte, sont des activités de processus et de conception, et non cette démonstration.

Référence : ISO 31000:2018, paragraphe 5.2

Piège : T-02 Principe, cadre organisationnel ou processus

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.