Formation
Certified ISO 27005 Risk Manager

CORRIGÉ DES EXERCICES

Attention : Le but de ce document est d'apporter une aide à la compréhension des exercices au candidat. Les réponses contenues dans ce corrigé ne sont que des exemples de réponses possibles, d'autres réponses peuvent être correctes dans certains cas.

Exercice 1 : Mythes et réalités – Gestion du risque

Pour chacun des énoncés suivants, veuillez déterminer si vous croyez qu'il est vrai ou faux et justifiez votre réponse :

1. Les organismes sont plus exposés au risque aujourd'hui qu'il y a 25 ans
Réponse : Généralement vrai: étant donné que les systèmes d'information sont plus complexes et interconnectés en particulier via différents réseaux, y compris Internet. La mondialisation et l'externalisation accrue sont également des facteurs qui ont contribué à accroître les facteurs de risque.

2) Un risque ne peut pas exister sans menace
Réponse : Bien qu'en théorie, un système ait des vulnérabilités, il n'y a pas de risques sans menaces qui peuvent exploiter ces vulnérabilités.

3) On peut prévoir la plupart des risques.
Réponse : Vrai et faux : On peut prédire la plupart des risques à partir de prévisions statistiques. D'un autre côté, on ne peut pas prédire exactement quel scénario de risque va se matérialiser. En outre, les sinistres avec un impact élevé et une faible probabilité sont difficiles à prédire. Par exemple, un organisme peut prédire qu'un tremblement de terre majeur peut se produire tous les 200 ans, mais il ne peut pas prédire la date exacte.

4) Le risque est avant tout une question de perception.
Réponse : Vrai et faux. Évidemment les risques sont une réalité tangible. Par contre, le manager de risque doit prendre en compte les perceptions du risque dans ses analyses. Les perceptions sont souvent différentes de la réalité objective des risques. Par exemple, les risques de vol d'identité lors de l'utilisation d'une carte de crédit sur internet sont moins élevés que par téléphone mais la perception du public est généralement l'inverse.

5) Il est possible d'éliminer complètement le risque.
Réponse : Faux, à moins d'éliminer l'activité à risque.
Par exemple, on peut éliminer le risque de fraude par carte de crédit en refusant de payer par carte de crédit.

6) Un bon gestionnaire sait prendre des risques.
Réponse : Vrai. Un bon gestionnaire prendra une décision sur la base des bénéfices attendus en tenant compte des risques encourus.

7) Une analyse de risque est toujours subjective.
Réponse : Vrai dans un contexte large. Même une analyse quantitative des risques.
Par exemple, la valeur qu'on donne à un actif est subjective, ainsi que la valeur calculée de l'impact sur les scénarios de risque.

8) Une analyse quantitative des risques fournit des résultats plus pertinents qu'une analyse qualitative.

Réponse : Faux. L'analyse quantitative donne souvent l'illusion de fournir des résultats plus pertinents. D'autre part, les données exprimées en termes monétaires facilitent la prise de décision des gestionnaires.

9) La culture du risque admet le droit à l'erreur.
Réponse : Vrai. La prise de décision comporte toujours un risque. Si quelqu'un punit un employé qui prend un risque calculé qui s'est avéré un choix malheureux, la prochaine fois qu'il verra une opportunité commerciale, il hésitera à prendre une décision.

10) Le risque peut être positif (opportunité) ou négatif (menace) pour un organisme.
Réponse : Vrai. Le risque est un terme neutre. Il représente une incertitude qui peut représenter une opportunité ou une menace pour un organisme.

1 Exercice 2 : Gestion des risques

Sur la base de votre opinion, veuillez décrire quels sont les trois plus importants avantages de la gestion des risques en sécurité de l'information et comment ces avantages peuvent-ils s'aligner sur la gestion des risques de l'entreprise ?

Les avantages de la gestion des risques liés à la sécurité de l'information incluent :

- ☑ Accroître la probabilité d'atteindre les objectifs
- ☑ Encourager un management proactif
- ☑ Prendre conscience de la nécessité d'identifier et de traiter les risques à travers tout l'organisme
- ☑ Améliorer l'identification des opportunités et des menaces
- ☑ Se conformer aux exigences légales et réglementaires pertinentes et aux normes internationales
- ☑ Améliorer la gouvernance
- ☑ Accroître l'assurance et la confiance des parties prenantes
- ☑ Établir une base fiable pour la prise de décision et la planification

Exercice 3 : Ressources

Après avoir connu une croissance rapide de leur entreprise, la direction de Voyage Extrême est soudainement préoccupée par les aspects de contrôle et de sécurité, d'autant plus qu'il y a eu quelques incidents de sécurité dernièrement. La direction de l'entreprise hésite toutefois à mettre en œuvre un programme de gestion des risques car elle ne sait pas si l'entreprise peut se le permettre en termes de coût. Veuillez identifier les ressources dont Voyage Extrême aurait besoin pour effectuer un exercice adéquat de gestion des risques. Veuillez évaluer plusieurs options pour l'entreprise avec les couts associés.

1) Exemples de ressources financières :

Ressources financières pour payer les salaires des employés responsables de la gestion des risques

Ressources financières pour payer les honoraires des consultants chargés d'aider à la mise en œuvre de la gestion des risques

Ressources financières pour l'équipement (voir catégorie suivante)

2) Exemples de ressources matérielles :

Matériel liés au travail des employés chargés de la gestion des risques (ordinateurs, systèmes d'opération, logiciels, etc.)

Matériel de support (serveurs). Logiciels de support (logiciels de gestion documentaires).

Logiciels de gestion des risques

3) Exemples de ressources humaines :

Employés expérimentés en gestion des risques

Consultants expérimentés en gestion des risques

Formations en gestion de risques

Exercice 4 : Etablir le contexte

Après avoir connu une croissance rapide de leur entreprise, la direction de Voyage Extrême est soudainement préoccupée par les aspects de contrôle et de sécurité, d'autant plus qu'il y a eu quelques incidents de sécurité dernièrement. Comme ils vous connaissent bien et qu'ils savent que vous êtes des experts en gestion des risques, ils vous confient la mission de préparer leur gestion des risques afin de les aider à mieux comprendre leur situation actuelle et à identifier les mesures de sécurité susceptibles d'améliorer la situation.
La première étape de votre mandat consiste à établir le contexte de la gestion des risques. Le président ne sait pas trop comment il convient de formuler les objectifs et le domaine d'application de la gestion des risques. Cela lui semble du jargon de spécialistes. Il veut que vous lui proposiez une version qu'il approuvera.
En outre, en vous basant sur l'information contenue dans l'étude de cas, identifiez les sources des exigences de conformité pour cet organisme

1) Principaux objectifs de gestion des risques
Réponse :

- Comprendre la nature et la source des incidents actuels afin de pouvoir corriger la situation
- Conserver leur image de marque en tant qu'innovateur dans leur domaine d'activité
- Assurer la disponibilité du site Web et des transactions en ligne
- Assurer l'intégrité des informations internes à l'organisme liées aux opérations (facturations, liste de clients, etc.)
- Protéger la confidentialité des informations personnelles des clients
- Identifier et gérer les risques avec les partenaires externes

2) Critères d'évaluation des risques
Réponse :
Tous les risques répondant à l'un des critères suivants doivent être priorisés :

- Possibilité d'actions en justice
- Indisponibilité du site Web pour une période de plus d'une heure
- Possibilité d'une fuite d'information des informations des clients
- Possibilité de fraude

3) Sources d'exigences
Réponse :

- Sources d'exigence 1 : Lois et règlements sur la protection du consommateur
  Enjeux : Fournir des informations exactes aux consommateurs et respect des engagements de la politique de vente (politique de remboursement, confidentialité, etc.)
- Sources d'exigence 2 : Règlements de l'association des sociétés de cartes de crédit
  Enjeux : respecter le code de sécurité pour les transactions en lignes de l'association des sociétés émettrices de cartes de crédit.
- Sources d'exigence 3 : Contrats de vente avec les clients

Enjeux : Respect des clauses du contrat de vente de voyage

Exercice 5 : Identification des actifs

Quels seraient selon vous les 6 actifs les plus importants pour l'entreprise Voyage Extrême ? Expliquez pourquoi il s'agit des actifs ayant le plus de valeur pour l'organisme. Veuillez justifier votre réponse et identifier si ce sont des actifs primordiaux ou des actifs en support.

Actif 1 : Site Web d'information
Justification : Le site Web de l'entreprise est le principal outil marketing de l'organisme.

Actif 2 : site transactionnel
Justification: Le site transactionnel prend en charge la procédure d'achat de voyages organisés

Actif 3 : Intranet des guides touristiques
Justification : Supporte les transactions liées à l'organisation des voyages et aux communications avec les guides.

Actif 4 : Base de données des membres inscrits
Justification: Les 76000 membres inscrits sont des clients potentiels qualifiés et représentent un revenu lors de la revente de la liste.

Actif 5 : Les deux propriétaires (actif de support)
Justification : Ce sont eux qui créent des forfaits touristiques originaux et innovateurs.

Actif 6: Processus d'affaires: processus de vente en ligne
Justification: l'ensemble du processus de prise de commandes se fait via le site Web de l'entreprise.

Exercice 6 : Identification des menaces, vulnérabilités et impacts

Veuillez identifier au moins deux scénarios de menaces et de vulnérabilités associés aux actifs suivants et indiquer les impacts potentiels et si les risques affecteraient la confidentialité, l'intégrité et/ou la disponibilité.

Complétez la matrice de risque et préparez-vous à discuter vos réponses après l'exercice :

- Processus comptable
- Informations personnelles des clients
- L'équipe de guides touristiques

Réponse : Plusieurs scénarios de réponse sont possibles. Il est important de s'assurer que les menaces, les vulnérabilités et les impacts identifiés sont conformes.

Actif 1 : Processus comptable

Scénario de risque	Menace	Vulnérabilité	Impacts	C	I	A
#1	Pirate, ancien employé	De nombreuses personnes ont accès aux données comptables; système d'authentification faible ; le système est accessible par internet ; pas de revue des privilèges associés au contrôle d'accès ; les données ne sont pas cryptées	Vol d'identité d'un client ou d'un employé de l'entreprise	X		
#2	Erreur de saisie d'un employé	Manque de contrôle lors de la saisie des données dans le système comptable ; Il n'y a pas de processus de validation des données saisies dans le système comptable	Base de données de comptabilité contenant des données corrompues		X	
#3	Les employés ne suivent pas les procédures internes de sauvegarde	Il n'y a pas de processus automatique de sauvegarde pour les données comptables	Perte de données due à un incident de sécurité		X	X

Actif 2 : Informations personnelles des clients

Scénario de risque	Menace	Vulnérabilité	Impacts	C	I	A
#1	Pirate, ancien employé	De nombreuses personnes ont accès aux données personnelles des clients ; le système d'authentification sur le site web est faible ; le système est accessible par internet ; pas de piste d'audit sur la base de données ; les données ne sont pas cryptées	Vol d'identité d'un client	X		

#2	Les clients qui saisissent leurs propres informations sur le site web sont responsables de les tenir à jour	Il n'y a pas de contrôle lorsque les données sont saisies ; il n'y a pas de processus de validation des données ; les clients ne mettent pas à jour leurs données	La base de clients contient des données corrompues		X	
#3	Déni de service (attaque d'un pirate informatique sur le site web)	Absence d'un mécanisme de protection contre le déni de service	Site web non disponible			X

Actif 3 : L'équipe des guides touristiques

Scénario de risque	Menace	Vulnérabilité	Impacts	C	I	A
#1	Guide touristique malveillant	Le guide travaille en même temps pour des entreprises concurrentes ; il n'y a pas d'accord de non divulgation ; il n'y a pas de contrôle lors du processus d'embauche (vérification des qualifications, des références, entrevues, etc.)	Vol et divulgation d'informations stratégiques aux concurrents ; perte de revenus causée par l'utilisation frauduleuse des informations volées	X		
#2	Guide touristique incompétent	Il n'y a pas de contrôle lors du processus d'embauche (vérification des qualifications, des références, entrevues, etc.). Il n'y a pas de supervision de la direction ; il n'y a pas de validation des transactions des guides sur l'intranet	Données corrompues des guides de touristes contenus dans les bases de données liées à l'Intranet		X	
#3	Erreur d'un guide touristique	Il n'y a pas de formation sur l'utilisation d'intranet et sur les processus internes de l'organisme	Données corrompues des guides de touristes contenues dans les bases de données liées à intranet		X	

Exercice 7: feuille de calcul des risques des actifs informationnels

Le formateur va diviser la classe en petits groupes. Pour chaque groupe, sélectionnez un actif informationnel critique dans l'Étude de cas et remplissez la feuille de calcul 10 - feuille de calcul des risques des actifs informationnels.

Réponse: plusieurs réponses sont possibles. Veuillez tenir compte des questions suivantes lors du remplissage de la feuille de calcul 10.

(1) Les participants ont-ils identifié tous les acteurs?

(2) Les participants ont-ils identifié tous les moyens?

(3) Ceux-ci doivent être soigneusement identifiés, car ils sont utiles pour identifier les vulnérabilités (ISO 27001)

(4) Cela aidera à comprendre l'impact

(5) Exigences de sécurité - considérer la confidentialité, l'intégrité, la disponibilité

(6) L'évaluation des probabilités est-elle réaliste? En cas de doute, les participants devraient-ils adopter une probabilité plus élevée ou plus faible? Des moyens inférieurs signifient qu'il est possible de sous-estimer le risque et donc de ne pas suffisamment être couvert. Des moyens plus élevés peuvent signifie que le risque peut être surestimé et qu'on peut dépenser trop de ressources pour le couvrir.

(7) Il convient d'identifier la conséquence la plus probable.

(8) Les participants devront justifier la valeur qu'ils ont attribuée. La clé ici est de faire en sorte que tous ces différents domaines d'impact soient comparables.

(9) Les participants doivent justifier pourquoi ils ont choisi l'atténuation des risques spécifiques:

Accepter le risque: seulement si le risque est trop coûteux à traiter.

Reporter le risque: ne doit être utilisé que si la décision ne peut être prise maintenant. Le formateur doit mettre l'accent sur le fait qu'un report de risque peut signifier qu'il

existe un risque inacceptable qui reste sans traitement. Si le risque se matérialise alors qu'il est différé lors du report, le gestionnaire des risques pourrait avoir des problèmes.

Transférer le risque: seulement si cela revient moins cher et plus facile que d'atténuer le risque

Atténuer le risque: Il convient de l'utiliser pour tous les risques qui n'ont pas été acceptés/reportés ou transférés.

<table>
<tr><td colspan="2">Allegro - Feuille de calcul</td><td colspan="4">FEUILLE DE CALCUL DES RISQUES DES ACTIFS</td></tr>
<tr><td rowspan="9">Risque de l'actif informationnel</td><td rowspan="8">Menace</td><td>Actif informationnel</td><td colspan="4"></td></tr>
<tr><td>Domaine de préoccupation</td><td colspan="4"></td></tr>
<tr><td colspan="2">(1) Acteur
Qui exploiterait le domaine de préoccupation ou de menace?</td><td colspan="4"></td></tr>
<tr><td colspan="2">(2) Moyens
Comment l'acteur le fera-t-il? Que ferait-il?</td><td colspan="4"></td></tr>
<tr><td colspan="2">(3) Motif
Quelle est la raison de l'acteur pour le faire?</td><td colspan="4"></td></tr>
<tr><td colspan="2">(4) Résultat
Quel serait l'effet qui en résulterait sur l'actif informationnel?</td><td colspan="4">❑ Divulgation ❑ Destruction
❑ Modification ❑ Interruption</td></tr>
<tr><td colspan="2">(5) Exigences de sécurité
Comment les exigences de sécurité de l'actif informationnel seraient-elles enfreintes?</td><td colspan="4"></td></tr>
<tr><td colspan="2">(6) Probabilité
Quelle est la vraisemblance que ce scénario de menace puisse se produire?</td><td>❑ Élevée</td><td>❑ Moyenne</td><td colspan="2">❑ Faible</td></tr>
<tr><td colspan="3">(7) Conséquences
Quelles sont les conséquences pour l'organisme ou le propriétaire de l'actif informationnel en raison du résultat et de l'infraction des exigences de sécurité?</td><td colspan="3">(8) Gravité
Quelle est la gravité de ces conséquences pour l'organisme ou le propriétaire de l'actif par</td></tr>
</table>

		domaine impacté?		
		Domaine impacté	**Valeur**	**Score**
		Réputation et confiance du client		
		Financier		
		Productivité		
		Sécurité et santé		
		Amendes et pénalités		
		Domaine d'impact défini par l'utilisateur		
		Score de risque relatif		

Exercice 8 : Évaluation quantitative des risques

1) Des données évaluées à 25000 $ sont stockées sur le serveur Z. Lors de l'analyse des menaces et des vulnérabilités, on a estimé qu'un virus endommagerait 80% des données stockées sur le serveur Z. La probabilité que le serveur Z soit infecté par un virus est estimée à une fois sur 10 ans. Calculez la Perte Unique Anticipée (Single-Loss Expectancy) et la Perte Annuelle Anticipée (Annualized Loss Expectancy).

Réponse:

Perte Unique Anticipée (SLE) = 25 000 $ (AV) X 0,8 (EF) = 20 000 $

Perte Annuelle Anticipée (ALE) = 20 000 $ (SLE) X 0,1 (ARO) = 2 000 $

2) Calculer la valeur d'une mesure de contrôle pour une pompe à eau d'un coût total (installation plus entretien) de 1000€ réduisant la perte annuelle de 6000€ à 4000€.

Réponse:

Valeur de la mesure de contrôle = (ALE avant - ALE après - coût de maintenance annuel de la mesure de contrôle)

Valeur de la mesure de contrôle = 6 000 $ - 4 000 $ - 1 000 $ = 1 000 $

3) L'organisme envisage de changer les clés USB de ses employés par des clés USB à protection biométrique. Sachant que la valeur moyenne des informations stockées sur une clé USB est de 2000€ et que l'organisme a un niveau d'acceptation du risque de 1000€, quel est le facteur d'exposition minimum pour que la mesure de contrôle soit rentable ?

Réponse: 0,5

Valeur X Facteur d'exposition (EF) = niveau d'acceptation du risque

2 000 $ X 0,5 = 1 000 $

4) Une mesure de sécurité est rentable jusqu'à ce que sa valeur soit égale a zéro. Sachant qu'une mesure de sécurité visant à protéger l'accès coute 5000€ et que la nouvelle perte après mise en œuvre de la mesure de sécurité est de 5000€, calculez la valeur minimale de l'actif à protéger pour que la mesure soit rentable. Le facteur d'exposition et le taux annuel d'occurrence sont tous deux égaux à 10%.

Réponse:

Valeur de la mesure de sécurité = $ 0 +

Coût de maintenance annuel de la mesure de sécurité = 5 000 $

ALE après = $ 5.000 $

EF et ARO = 0,1

Valeur du contrôle = (ALE avant - ALE après - coût de maintenance annuel du contrôle)

$ 0 = X - $ 5,000 - $ 5,000

X = 10 000 $

10 000 $ = Valeur de l'actif (AV) X 0,1 (EF, Facteur d'exposition) X 0,1 (ARO)

Valeur de l'actif = 1 000 000 $

Exercice 9 : Options de traitement du risque

Suite à l'analyse de risque, vous avez identifié que 0,5% des transactions électroniques (chiffre d'affaires de 10 millions) effectuées par cartes de crédit sur le site Web de Voyage Extrême sont de nature frauduleuse et que 70% de ces transactions proviennent de 6 pays.

La direction de Voyage Extrême veut prendre une décision pour le traitement de ce risque. Veuillez lui préparer une note exécutive expliquant les 4 choix d'options possibles pour traiter ce risque.

Réponse :

Option 1 : acceptation du risque
Il convient que l'organisme calcule les pertes sur une base périodique et prévoit une réserve financière nécessaire. La direction doit être informée des risques et les accepter officiellement.

Option 2 : réduction des risques
L'organisme peut mettre en place des contrôles pour diminuer les risques de fraudes. Par exemple, rappeler les clients qui ont passé une commande dans les six pays concernés avant d'accepter la transaction à validée.

Option 3 : Transfert des risques
L'organisme peut prendre une assurance contre les fraudes. En outre, il peut externaliser le processus de paiement à une entreprise externe.

Option 4 : évitement des risques
L'organisme peut décider de ne plus accepter les paiements par cartes de crédit pour les clients des six pays concernés et n'accepter que les paiements par virement bancaire.

Exercice 10: Communication des risques

À partir des scénarios de l'exercice 6, veuillez indiquer à quelles parties prenantes internes et externes vous communiqueriez les risques que vous avez identifiés. Indiquez également comment vous effectuez cette communication.

1. Parties prenantes internes

Tous les employés, par courrier électronique, sessions de formation et de sensibilisation, rapports mensuels.

2. Parties prenantes externes

Les clients, les médias, les organismes de réglementation, à travers les bulletins d'information, les courriels, les rapports de performance.