PECB

Étude de cas

Extreme Adventure Tourse Inc.

FORMATION CERTIFIED ISO/IEC 27005
RISK MANAGER

Table des matières

I. Introduction et historique

Extreme Adventure Tours (EAT) a commencé ses opérations en mars 2003. Marc Leroux et son épouse, Isabelle Garnier ont fondé l'agence de voyages juste après leur retour d'une expédition dans le Sahara. Ces deux grands aventuriers voulaient établir un nouveau type d'agence de voyages. Depuis le tout début, EAT était axé principalement sur le marché du tourisme d'aventure extrême. Leurs forfaits les plus populaires sont la traversée du Sahara avec une caravane bédouine ou une expédition en canot avec des Amérindiens au Canada. EAT a loué ses locaux commerciaux dans un immeuble de bureaux situé au centre-ville.

Depuis sa création, l'agence de voyages a connu un succès commercial considérable en améliorant ainsi la visibilité de sa marque, non seulement localement mais aussi au niveau international. Considérant ce marché de niche, Marc et Isabelle ont rapidement décidé en 2005 de s'emparer du marché international en se concentrant sur la création d'un réseau de revendeurs et d'une agence de voyages virtuelle.

L'agence de voyages a connu une croissance impressionnante en signant des ententes de partenariat avec plusieurs autres agences de voyages. En moins de 18 mois, EAT a construit un réseau de 75 partenaires dans 20 pays. Avec un site Internet promotionnel créé en 2003, Extreme Adventure Tours a lancé son site de voyages transactionnel en mai 2006. Le directeur de la commercialisation est particulièrement fier d'avoir actuellement plus de 76 000 membres inscrits sur le site, ce qui représente une saine base de client.

Marc estime que l'Internet est l'instrument qui stimulera encore davantage la croissance de l'entreprise à un coût réduit, plutôt que d'avoir un réseau de succursales ouvertes à l'étranger. La création d'une agence de voyages virtuelle où les clients peuvent acheter tous les produits EAT en ligne permettra à EAT d'étendre son activité au niveau mondial. En outre, EAT s'attend à générer des recettes supplémentaires en ajoutant des guides personnalisés à sa gamme de produits, et par la vente d'espace publicitaire sur son site Web. Avoir une agence de voyages virtuelle réduira également le coût d'exploitation de ses agences « immobilières », puisqu'elles peuvent être fermées et leurs services sous-traités à des pigistes dans ces endroits respectifs. Enfin, pour des raisons administratives, l'élaboration d'un réseau intranet est cruciale. Ce site Web amélioré servira de passerelle intranet de l'EAT, qui servira de base à la nouvelle stratégie administrative et facilitera le partage de l'information entre ses partenaires, ses clients et le siège social.

Pour contrôler les coûts d'exploitation, EAT a choisi d'adopter un modèle d'entreprise virtuelle. La société sous-traite la plupart de ses opérations : site Web, centre d'appels, comptabilité, recouvrement de comptes en retard, recrutement de partenaires, marketing et publicité. Marc et Isabelle ont décidé de se concentrer sur les processus qui créent de la valeur, tels que la création de produits touristiques et

la gestion des partenaires. Par conséquent, le centre d'appels clients a été sous-traité à une société indienne, la recherche et la qualification de partenaires à une société américaine, et le développement du matériel marketing a été confié à diverses agences de publicité après un appel d'offres.

Le chiffre d'affaires de l'entreprise s'élève actuellement à 10 millions de dollars canadiens et elle ne compte que 15 employés à temps plein et 8 employés à temps partiel, qui travaillent principalement à domicile. Les guides touristiques sont des employés contractuels qui reçoivent des montants forfaitaires fixes tout compris. L'EAT dispose d'une base de données d'une centaine de guides préqualifiés potentiels. Chaque fois qu'une visite est confirmée, l'EAT l'affiche sur son intranet et les guides peuvent demander un contrat pour agir comme guide pour la visite.

L'expansion impressionnante de l'EAT a cependant été suivie de difficultés constantes. L'entreprise a connu des crises de croissance et Marc et Isabelle ont dû relever de nouveaux défis. La coordination des activités et le contrôle global de l'entreprise deviennent des transitions très perturbantes à gérer. Plusieurs incidents ont eu lieu récemment. Par exemple, certains partenaires se plaignent des erreurs dans les factures émises par EAT. En outre, certains clients n'ont pas reçu de réponse à leurs courriels, pendant plusieurs semaines.

II. Site Web – Développement

Pour le développement du site Web et du nouveau système, EAT a lancé plusieurs appels d'offres, avant de retenir les services de Web Transit, une société de conseil reconnue dans le domaine du commerce électronique, avec une excellente réputation. Web Transit est également l'entreprise qui a présenté l'offre la plus basse.

La première étape de la mission de Web Transit était de développer un Intranet à des fins administratives et d'y intégrer, entre autres, le nouveau système comptable. L'objectif de la première étape est d'améliorer la communication entre les partenaires, les guides touristiques associés, les consultants et le siège social en assurant la consultation à distance des bases de données et des rapports financiers. L'intranet permet également la saisie à distance d'informations telles que les notes de frais et les feuilles de présence pour accélérer le traitement, et ce, à moindre coût.

La deuxième étape comprenait la transformation du site Web promotionnel en un site Web axé sur les transactions pour héberger la nouvelle agence de voyages virtuelle. L'EAT a automatisé et simplifié le nombre maximum de ses opérations

grâce aux paiements électroniques et a partiellement intégré la gestion électronique des documents (GED).

III. Site Web – Organisation mondiale

Compte tenu des changements qui se sont produits au sein de l'organisme, l'utilisation d'Internet représente une composante essentielle des opérations commerciales d'EAT.

Dans un premier temps, les clients potentiels consultent le site Web d'EAT pour obtenir des informations sur les différents produits et services offerts, ainsi que des informations générales sur l'entreprise.

Le client qui souhaite commander ou consulter un guide de voyage personnalisé doit d'abord s'inscrire sur le site Web. Pour ce faire, le client remplit un formulaire électronique en indiquant son nom, ses coordonnées, une adresse e-mail et les détails de sa carte de crédit. Cette information est obligatoire. Le client doit également saisir des informations personnelles telles que l'âge, le sexe, les domaines d'intérêt, des préférences de destination, etc.

Le client doit ensuite choisir un code d'utilisateur et un mot de passe contenant au moins huit caractères qui, pour des raisons de sécurité, doit être saisi deux fois. Avant de valider l'enregistrement du client, le système effectue une recherche dans la base de données pour s'assurer que le code utilisateur n'est pas déjà utilisé. Le système communique également avec l'entreprise émettrice de la carte pour valider les informations fournies par le client. L'ensemble du processus ne prend que quelques minutes.

En remplissant le formulaire d'inscription, le client accepte de recevoir un bulletin électronique d'EAT et toute autre information promotionnelle par e-mail. Il autorise également EAT à partager cette information avec ses partenaires commerciaux qui pourront l'utiliser à des fins promotionnelles. Toutefois, EAT s'engage à toujours garder confidentielles les informations de la carte de crédit.

Dès que l'enregistrement du client est accepté, l'information est entrée dans la base de données d'EAT. Ensuite, le client peut accéder au site en utilisant son code d'utilisateur. Lorsque le client accède au site avec ce code d'utilisateur, le site peut être adapté pour mieux répondre aux besoins du client. Par exemple, il peut demander à EAT d'envoyer des notifications sur les nouveaux forfaits en Asie dès qu'ils sont affichés sur le site. Le client peut également modifier les informations personnelles saisies lors de l'inscription. La communication des informations

confidentielles des clients (code d'utilisateur et mot de passe, informations personnelles, etc.) par l'intermédiaire du site Web se fait en utilisant le protocole de transmission SSL (*Secure Socket Layer*).

Pour chaque produit acheté, le client doit saisir le nom et les coordonnées de la personne (ou les personnes) pour lesquels l'achat est effectué (p. ex., nom et adresse du passager pour un billet d'avion). Ceci est exigé parce que chaque billet d'avion, forfait, etc. doit afficher le nom d'un individu, qui peut être différent de celui de la personne qui passe la commande. Par défaut, le système suggère le nom et les coordonnées du client enregistré. À tout moment, le client peut retourner à la page précédente et apporter les changements nécessaires.

Enfin, le client doit saisir le code CCV de la carte de crédit. EAT est relié, via Internet, aux sociétés émettrices de carte de crédit et reçoit un numéro d'autorisation. Une confirmation de paiement indiquant le numéro de commande du client s'affiche sur l'écran. Le client est invité à imprimer ce document. Le processus est très rapide. Le système d'EAT est programmé pour transférer les paiements du compte commercial au compte actuel et pour saisir le revenu des ventes à la date de départ du client.

En dépit de l'automatisation de l'ensemble du processus, EAT veut s'assurer qu'ils maintiennent un haut niveau de qualité du service pour sa clientèle. Pour commencer, les clients peuvent accéder à une section « Foire aux questions » où ils peuvent trouver des réponses à des questions qui sont d'intérêt plus élevé pour eux. Deuxièmement, ils peuvent envoyer leurs questions ou commentaires par courriel à EAT et obtenir une réponse dans les 24 heures. Enfin, le service client peut être joint à tout moment et gratuitement par l'intermédiaire du centre d'appels en Inde.

IV. Organisation technique et services d'information

Le système de prise de commande et le système d'administration Web sont des versions personnalisées de programmes propriétaires spécialement développés par Web Transit pour le commerce électronique dans le domaine des voyages. EAT n'a pas accès à la version source des programmes et systèmes, et tous les changements doivent être effectués par Web Transit.

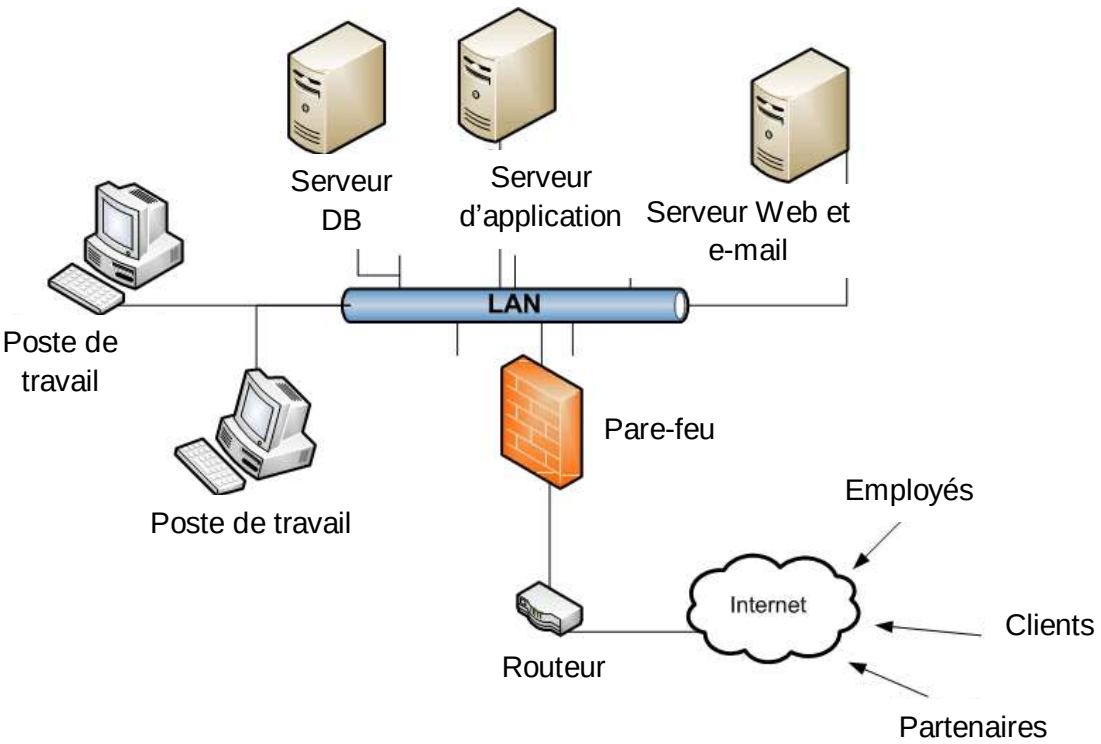
Le service d'information est assisté par un webmestre et un administrateur réseau. L'administrateur réseau est responsable de la maintenance de tous les systèmes d'information et du réseau, de la gestion de la sécurité, de l'administration des bases de données, de la gestion des incidents et du support aux employés. Le webmestre

s'occupe essentiellement de la mise à jour du contenu du site Web et de l'assistance à l'administrateur réseau avec le support aux utilisateurs des employés.

V. Architecture des systèmes d'information et description du réseau

EAT utilise trois serveurs Web qui fonctionnent sous le système d'exploitation Windows 10, dont Microsoft IIS (Internet Information Services). Un serveur héberge les bases de données, un autre héberge toutes les applications, le système de prise de commande et le système de comptabilité, et le troisième est dédié à la gestion du site Web et des courriels.

Les stations de travail sont équipées avec des micro-ordinateurs IBM. Ceux-ci comprennent une série d'applications de base telles que le traitement de texte, le tableur, etc. De plus, ils sont tous reliés à un réseau local (LAN). Un routeur assure une connexion permanente à partir du réseau LAN à l'Internet.



VI. Annexe A : Processus de gestion du changement

Extreme Adventure Tours n'effectue pas de programmation interne. Web Transit, avec lequel un contrat de maintenance a été signé après l'élaboration et la mise en

œuvre du site transactionnel, est toujours appelée pour développer un nouveau système ou modifier les programmes ou applications existants. Des modifications mineures ont été apportées depuis la mise en service du nouveau système, en particulier pour corriger certains problèmes liés à la facturation de compte pour les taxes applicables.

La personne responsable des services d'information et de technologie de l'information doit examiner toute demande de changement reliée au système de prise de commande. À la suite d'une demande, il évalue les besoins de l'entreprise, si tout est acceptable approuve la demande, puis envoie à l'analyste de Web Transit une demande de modification formelle. Dans les 48 heures, Web Transit doit répondre à la demande de changement en indiquant la date de développement et la date prévue de mise en service.

Cependant, les techniciens d'Extreme Adventure Tours peuvent créer et modifier des rapports générés par le système et apporter des modifications dans la base de données. Ils peuvent également modifier l'apparence et l'organisation générale du site Web sans affecter le système de prise de commande. Lorsqu'ils reçoivent une demande de changement, ils demandent habituellement l'autorisation du directeur des services d'information et de technologie de l'information avant d'apporter les modifications demandées et de les mettre en service. Le technicien effectue quelques tests standards dans un environnement distinct avant de mettre les modifications en service.

Certaines modifications sont routinières et se font sans l'approbation du directeur des services d'information et de technologie de l'information. C'est le cas des modifications apportées au site Web afin d'ajouter une publicité, des mises à jour de la base de données, des ajouts de nouveaux produits et des modifications des prix.

Toutes les demandes de changements concernant le contenu du site Web sont adressées directement au webmestre de l'entreprise. Il s'occupe d'apporter les modifications aux textes présents sur le site Web.

Afin de rendre opérationnelles les modifications, les systèmes, le site Web et les bases de données sont mis à jour quotidiennement entre 4 h et 5 h du matin, quand le niveau d'activité est au plus bas. Cela entraîne un arrêt temporaire du service pendant au plus une heure, mais cet arrêt peut aussi durer à peine dix minutes. Un message apparaît alors à l'écran afin d'aviser le visiteur que le site est « en maintenance ». On profite de cet arrêt du système pour effectuer une copie de sauvegarde du contenu des trois différents serveurs.

PECB

Exercices

FORMATION CERTIFIED ISO/IEC 27005 RISK MANAGER

Exercice 1 : Mythes et réalités – Gestion des risques

Pour chacun des énoncés suivants, indiquez si vous pensez qu'ils sont vrais ou faux et justifiez votre réponse :

1. Les organismes sont davantage exposés aux risques aujourd'hui qu'il y a cinq ans.

.....

.....

.....

.....

2. Un risque ne peut exister sans une menace.

.....

.....

.....

.....

3. La plupart des risques peuvent être prévus.

.....

.....

.....

.....

4. Le risque est principalement une question de perception.

.....

.....

.....

.....

5. Il est possible d'éliminer entièrement le risque.

.....

.....

.....

6. Un bon gestionnaire sait comment prendre des risques.

.....

.....

.....

.....

7. Une analyse de risque est toujours subjective en fonction de son contexte, des seuils d'acceptation, etc.

.....

.....

.....

.....

8. Une analyse quantitative du risque fournit des résultats plus pertinents qu'une analyse qualitative.

.....

.....

.....

.....

9. La culture de l'appréciation des risques reconnaît le droit à l'erreur.

.....

.....

.....

.....

10. Le risque peut être positif (opportunité) ou négatif (menace) pour un organisme.

.....

.....

Exercice 2 : Gestion des risques

Décrivez ce que vous considérez comme les trois avantages les plus importants de la gestion des risques en sécurité de l'information et comment ils peuvent s'aligner sur le management du risque d'entreprise.

Exercice 3 : Ressources

Après avoir connu une croissance rapide, la direction d'Extreme Adventure Tours est soudainement préoccupée par les aspects de contrôle et de sécurité, surtout depuis qu'il y a eu quelques incidents de sécurité récemment. La gestion de l'organisme hésite encore à mettre en œuvre la gestion des risques parce qu'ils ne savent pas s'ils peuvent se le permettre. Identifier les ressources dont Extreme Adventure Tours aurait besoin pour effectuer un exercice adéquat de gestion des risques. Évaluez plusieurs options avec les coûts associés.

1. Ressources financières

.....

.....

.....

.....

.....

2. Ressources matérielles

.....

.....

.....

.....

.....

3. Ressources humaines

.....

.....

.....

.....

.....

Exercice 4 : Établir le contexte

Après avoir connu une croissance rapide, la direction d'Extreme Adventure Tours est soudainement préoccupée par les aspects de contrôle et de sécurité, surtout depuis qu'il y a eu

récemment quelques incidents de sécurité. Parce qu'ils vous connaissent bien et qu'ils savent que vous êtes des experts en gestion des risques, ils vous mandatent pour les aider à mieux comprendre leur situation actuelle et à identifier les mesures de sécurité qui pourraient améliorer la situation.

La première étape de votre mission consiste à établir le contexte de gestion des risques d'EAT. Le président ne sait pas comment il devrait formuler les objectifs et le périmètre de gestion des risques. Pour lui, cela semble un jargon de spécialistes. Il veut que vous rédigiez une version qu'il approuvera.

Sur la base des informations contenues dans l'étude de cas, abordez les trois points suivants, en proposant une déclaration ou une position initiale pour chacun :

1. Principaux objectifs pour la gestion des risques

.....

.....

.....

.....

.....

2. Critères d'évaluation du risque

.....

.....

.....

.....

.....

3. Sources d'exigences de conformité

   Exigence de conformité source 1

.....

.....

.....

.....

.....

Exigence de conformité source 2

.....

.....

.....

.....

.....

Exigence de conformité source 3

.....

.....

.....

.....

.....

Exercice 5 : Identification des actifs

Quels sont, selon vous, les quatre actifs les plus importants d'Extreme Adventure Tours ? Donnez une justification pour chaque réponse et indiquez s'il s'agit d'actifs primordiaux ou d'actifs en support.

Actif 1

.....

.....

Actif primordial ☐ Actif en support ☐

Justification

.....

.....

.....

.....

Actif 2

.....

.....

Actif primordial ☐ Actif en support ☐

Justification

.....

.....

.....

.....

Actif 3

.....

.....

Actif primordial ☐ Actif en support ☐

Justification

.....

.....

.....

.....

Actif 4

.....

.....

Actif primordial ☐ Actif en support ☐

Justification

.....

.....

.....

.....

Exercice 6 : Identification des menaces, vulnérabilités et impacts

Identifiez au moins deux scénarios de menaces et vulnérabilités associés à l'actif et indiquer les impacts potentiels. Précisez si le risque aurait une incidence sur la confidentialité, l'intégrité et la disponibilité.

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

- Processus de comptabilité
- Informations personnelles des clients
- Équipe des guides touristiques

Actif 1 : Processus de comptabilité						
Scénarios de risques	**Menace**	**Vulnérabilité**	**Impacts**	**C**	**I**	**D**
1						
2						

Actif 2 : Informations personnelles des clients

Scénarios de risques	Menace	Vulnérabilité	Impacts	C	I	D
Actif 3 : Équipe des guides touristiques						
1						
2						

Scénarios de risques	Menace	Vulnérabilité	Impacts	C	I	D
#1				X		
#2					X	

Exercice 7 : Feuille de travail sur le risque lié aux actifs informationnels

En petits groupes, sélectionnez un actif d'information critique dans l'étude de cas et remplissez la feuille de travail 10 - Feuille de travail sur le risque lié à l'actif informationnel.

Commentaires du formateur :

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

Allegro - Feuille de travail 10	FEUILLE DE TRAVAIL SUR LE RISQUE LIE AUX ACTIFS D'INFORMATION

Risque lié à l'actif informationnel	**Menace**	Actifs informationnels				
		Domaine de préoccupation				
		(1) Acteur *Qui pourrait exploiter le domaine de préoccupation ou menace ?*				
		(2) Moyens *Comment l'acteur s'y prendrait-il ? Que feraient-ils?*				
		(3) Motif *Quelle est la raison de l'acteur pour le faire ?*				
		(4) Résultat *Quel serait l'effet sur l'actif informationnel ?*	❑ **Divulgation** ❑ **Modification**	❑ **Destruction** ❑ **Interruption**		
		(5) Exigences en matière de sécurité *Comment les exigences en matière de sécurité de l'actif informationnel seraient-elles violées ?*				
		(6) Probabilité *Quelle est la probabilité que ce scénario de menace pourrait se produire?*	❑ **Élevée**	❑ **Moyenne**	❑ **Faible**	
	(7) Conséquences *Quelles sont les conséquences pour l'organisme ou le propriétaire de l'actif informationnel à la suite du résultat et de la violation des exigences en matière de sécurité ?*		(8) Gravité *Quelle est la gravité de ces conséquences pour l'organisme ou le propriétaire des actifs, par zone d'impact ?*			
			Zone d'impact	**Valeur**	**Score**	
			Réputation et confiance des clients			
			Finances			
			Productivité			
			Sécurité et santé			
			Amendes et pénalités légales			
			Zone d'impact définie par l'utilisateur			
					Résultat de risque relatif	

Exercice 8 : Appréciation quantitative des risques

1. Des données d'une valeur de 25 000 $ sont stockées sur le serveur Z. Dans l'analyse des menaces et des vulnérabilités, on a estimé que 80 % des données stockées sur le

serveur Z pourraient être endommagées par un virus. La probabilité que le serveur Z soit infecté par un virus est estimée à une fois tous les 10 ans. Calculez l'estimation de perte unique et l'estimation de perte annualisée.

.....

.....

.....

.....

.....

2. Calculez la valeur d'une mesure pour une pompe à eau à un coût total (installation et entretien) de 1 000 $, ce qui réduit la perte annuelle de 6 000 $ à 4 000 $.

.....

.....

.....

.....

.....

3. EAT prévoit de remplacer les clés USB de ses employés par des clés dotées d'une protection biométrique. Étant donné que la valeur moyenne de l'information stockée sur une clé USB est de 2 000 $ et que l'organisme accepte un niveau de risque de 1 000 $, quel est le facteur d'exposition minimal pour que le contrôle (c'est-à-dire les clés USB compatibles biométriques) soit efficace en termes de coûts ?

.....

.....

.....

.....

.....

4. Une mesure de sécurité est rentable jusqu'à ce que sa valeur soit égale à zéro. Étant donné qu'une mesure de sécurité pour la protection des accès coûte 5 000 $ et que la nouvelle perte après la mise en œuvre de la mesure de sécurité est de 5 000 $, calculez la valeur minimale de l'actif devant être protégé pour que la mesure soit rentable. Le facteur d'exposition et le taux annuel d'occurrence sont à 10 %.

.....

.....

.....

.....

.....

Exercice 9 : Options de traitement du risque

Après l'analyse de risque, vous avez identifié que 0,5 % des transactions électroniques (chiffre d'affaires de 10 millions de dollars) par carte de crédit sur le site Web d'Extreme Adventure Tours sont de nature frauduleuse et que 70 % de ces transactions proviennent de 6 pays spécifiques.

Le président d'Extreme Adventure Tours veut prendre une décision pour le traitement de ces risques. Préparez un résumé expliquant le choix de quatre options possibles pour faire face à ce risque.

Option 1 :

.....

.....

.....

.....

.....

.....

.....

.....

.....

Option 2 :

.....

.....

.....

.....

.....

.....

.....

.....

Option 3 :

.....

.....

.....

.....

.....

.....

.....

.....

Option 4 :

.....

.....

.....

.....

.....

.....

.....

Exercice 10 : Communication des risques

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

1. Parties prenantes internes

.....

.....

.....

.....

.....

.....

.....

.....

2. Parties prenantes externes

.....

.....

.....

.....

.....

.....

.....