# Formation Certifiée ISO/CEI 27005 Risk Manager



# **EXERCICES**





## Exercice 1 : Mythes et réalités – Gestion des risques

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
Un risque ne peut exister sans une menace
3. La plupart des risques peuvent être prévus
4. Le risque est avant tout une question de perception
5. Il est possible d'éliminer complètement le risque.
6. Un bon gestionnaire sait prendre des risques.



Formation certifiée ISO/CEI 27005 Risk Manager Exercices © 2017 PECB

7. Une analyse des risques est toujours subjective.
8. Une analyse quantitative des risques fournit des résultats plus pertinents qu'une analyse
qualitative.
O. La guitura du riagua admet la drait à l'arrour
9. La culture du risque admet le droit à l'erreur.
10. Le risque peut être positif (opportunité) ou négatif (menace) pour un organisme.



### **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.

Avantage 1)
Comment cet avantage s'aligne sur la gestion des risques de l'entreprise?
Avantage 2)
Comment cet avantage s'aligne sur la gestion des risques de l'entreprise?
Avantage 3)
Comment cet avantage s'aligne sur la gestion des risques de l'entreprise?



#### **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) Ressources financières
2) Ressources matérielles
3) Ressources humaines



#### Exercice 4 : Établir 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, veuillez:

- Proposer les principaux objectifs de la gestion des risques;
- Proposer des critères d'évaluation des risques ;
- Identifier les sources des exigences de conformité pour cette organisation.

1) Principaux objectifs de gestion des risques de Voyage Extrême								
2) Critères d'évaluation des risques								
3) Sources des exigences								





Source d'exigence 1 :	• •
Enjeux :	
	••
Source d'exigence 2 :	
Enjeux :	
Source d'exigence 3 :	
Enjeux :	



#### **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:		
	·	
Explication :		
Actif 2:		
	·	
Explication :		
Actif 3:		
	·	
Explication :		
Actif 4:		
	Actif primordial □	Actif en support
Explication :		



#### 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



Exercice 6 : Scénarios de risque

cénario isque	Menace	Vulnérabilité	Impacts	С	ı	[
#1						
#2						ł
12						

www.pecb.com Page 10 of 20

Page **11** of **20** 



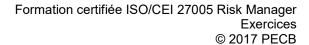
cénario risque	Menace	Vulnérabilité	Impacts	С	ı	D
#1						
#2						

www.pecb.com



Actif 3 : L'équipe des guides touristiques									
Scénario risque	Menace	Vulnérabilité	Impacts	С	ı	D			
#1									
#2									

www.pecb.com Page 12 of 20



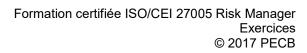


#### Exercice 7: feuille de calcul des risques des actifs informationnels

1) 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.

Comm	nentaire	es du tuteur:						
Alleg	ro - Fe	uille de calcul 10	FEUILLE DE CAL	.CUL	DES RISC	QUES DES	ACTI	FS INFORMATIONNELS
		Actif informationnel						
nnel		Domaine de préoccupation						
atio		(1) Acteur						
nform	<b>9</b> 3	Qui exploiterait le d préoccupation ou d						
ctif i	Menace	(2) Moyens						
Risque de l'actif informationnel	Z	Comment l'acter Que ferait-il?	ur le fera-t-il?					
		(3) Motif Quelle est la raison le faire?	de l'acteur pour					
		(4) Résultat  Quel serait l'effet que sur l'actif information			Divulga Modific			Destruction Interruption

sur l'actif informationnel?



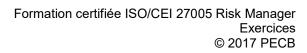


	(5) Exigences de sécurité  Comment les exigences de sécurité de l'actif informationnel seraient- elles enfreintes?						
	(6) Probabilité  Quelle est la vraisemblance que ce scénario de menace puisse se produire?	□ Élevée	☐ Moyenne	□ F	aible		
Quelle: proprié	onséquences s sont les conséquences pour l'organis étaire de l'actif informationnel en raison fraction des exigences de sécurité?		(8) Gravité  Quelle est la gravité de ces conséquences pour l'organisme o propriétaire de l'actif par 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 risqu	ue 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).
2) Calculer la valeur d'une mesure de contrôle pour une pompe à eau d'un coût total (installation
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€.
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€.
plus entretien) de 1000€ réduisant la perte annuelle de 6000€ à 4000€.
plus entretien) de 1000€ réduisant la perte annuelle de 6000€ à 4000€.
plus entretien) de 1000€ réduisant la perte annuelle de 6000€ à 4000€.
plus entretien) de 1000€ réduisant la perte annuelle de 6000€ à 4000€.
plus entretien) de 1000€ réduisant la perte annuelle de 6000€ à 4000€.
plus entretien) de 1000€ réduisant la perte annuelle de 6000€ à 4000€.
plus entretien) de 1000€ réduisant la perte annuelle de 6000€ à 4000€.
plus entretien) de 1000€ réduisant la perte annuelle de 6000€ à 4000€.
plus entretien) de 1000€ réduisant la perte annuelle de 6000€ à 4000€.
plus entretien) de 1000€ réduisant la perte annuelle de 6000€ à 4000€.





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 ?
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%.



#### Exercice 9 : Options de traitement du risque

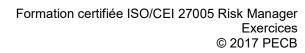
Suite à l'analyse de risque, vous avez identifié que 0,5% des transactions électroniques (chiffre d'affaires de 10 millions) effectuées par cartes de crédit sur le site Web de Voyage Extrême sont de nature frauduleuse et que 70% de ces transactions proviennent de 6 pays.

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.

Option 1:

Option 2:



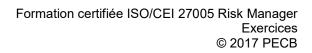


Option 3:
Option 4 :
Exercice 10: Communication des risques
À partir des scénarios de l'exercice 6, veuillez indiquer à quelles parties prenantes internes et
externes vous communiqueriez les risques que vous avez identifiés. Indiquez également
comment vous effectuez cette communication.
1. Parties prenantes internes



Formation certifiée ISO/CEI 27005 Risk Manager Exercices © 2017 PECB

2. Parties prenantes ex	rternes		
		 	• • • • • • • • • • • • • • • • • • • •





— www.pecb.com ——