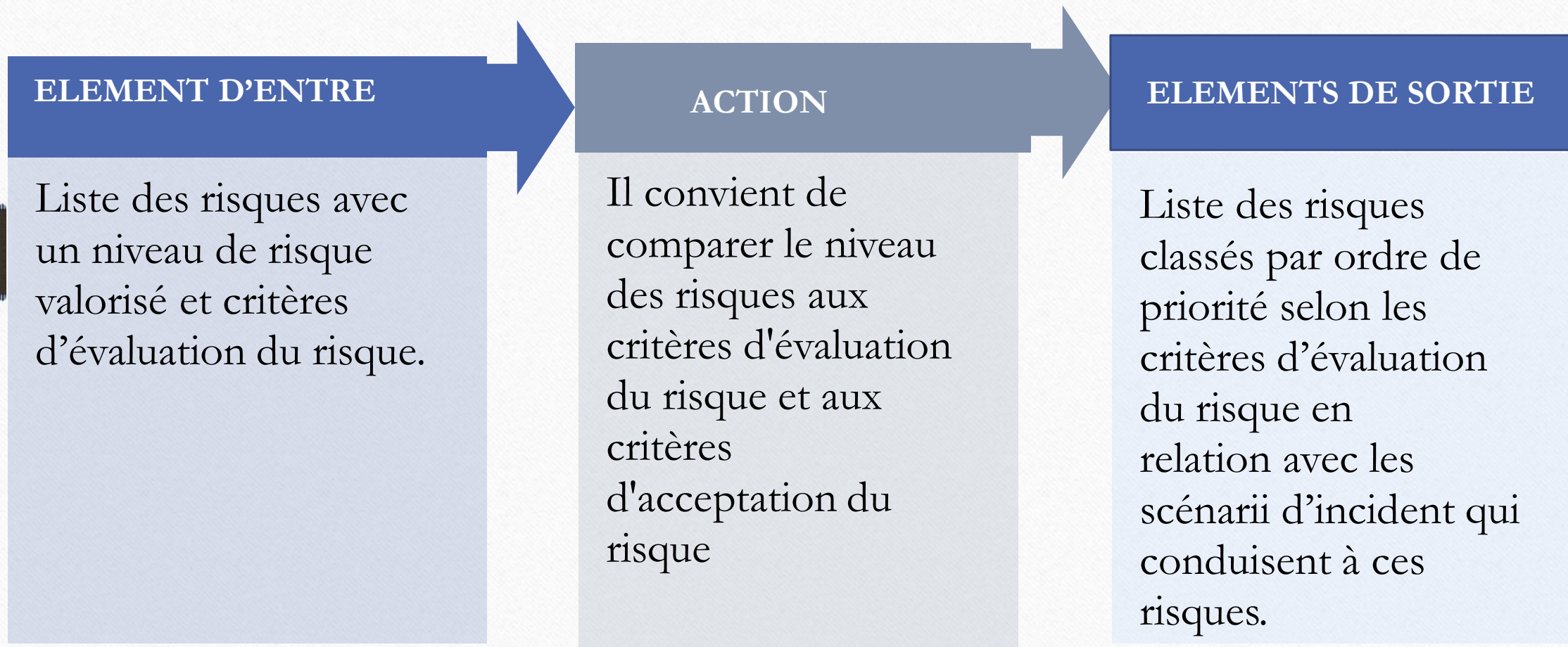


III-ÉVALUATION DES RISQUES

Cette section aidera le participant à acquérir des connaissances sur le processus d'évaluation des risques (ISO/IEC 27005 Article 8.3 Evaluation du risque).



III-ÉVALUATION DES RISQUES (Suite)

- ☐ La dernière étape de l'identification des risques est l'identification des impacts qui pourraient être causés par un scénario d'incident;
- ☐ Un scénario d'incident est la description d'une menace exploitant une vulnérabilité ou un ensemble de vulnérabilités en termes de sécurité de l'information, et ayant un impact;
- ☐ Les conséquences des scénarios d'incident doivent être déterminées en tenant compte des critères d'impact définis lors de l'activité d'établissement du contexte;
- ☐ Un ou plusieurs actifs ou une partie d'un actif peuvent être affectés;
- ☐ L'impact sur l'actif peut être calculé en valeur financière ou par référence à une échelle qualitative;
- ☐ Les conséquences peuvent être temporaires ou permanentes, comme dans le cas de la destruction d'un actif.

III-ÉVALUATION DES RISQUES (Suite)

Evaluer les niveaux de risque en fonction des critères des risques

- ☐ La nature des décisions relatives à l'évaluation du risque et les critères d'évaluation du risque qui seront utilisés pour prendre ces décisions ont été définis lors de l'établissement du contexte;
- ☐ A cette étape, ces décisions et le contexte doivent être revus en détail au regard des risques identifiés ;
- ☐ Afin d'évaluer les risques, il convient que les organismes comparent les risques estimés aux critères d'évaluation du risque définis lors de l'établissement du contexte.

L'évaluation du risque utilise la compréhension du risque obtenue par l'analyse du risque pour prendre des décisions relatives aux actions futures.

Il convient que ces décisions indiquent :

- s'il convient d'entreprendre une activité;
- les priorités de traitement de risque en tenant compte des niveaux de risque estimés.

Les exigences contractuelles, juridiques et réglementaires devraient être prises en compte au cours de l'étape de l'évaluation des risques.

III-ÉVALUATION DES RISQUES (Suite)

ISO/IEC 27005, Annexe E.2.3 Exemple 2 - Classement des menaces par mesures des risques .

Descripteur de menace (a)	Valeur de la conséquence (actif) (b)	Vraisemblance de la menace (c)	Mesure du risque (d)	Classement des menaces (e)
Menace A	5	2	10	2
Menace B	2	4	8	3
Menace C	3	5	15	1
Menace D	1	3	3	5
Menace E	4	1	4	4
Menace F	2	4	8	3

Tableau E.2

III-ÉVALUATION DES RISQUES (Suite)

Une matrice, ou un tableau identique au Tableau E.2, peut être utilisée pour relier les facteurs des conséquences (valeur des actifs) et la vraisemblance des menaces (en tenant compte des aspects des vulnérabilités).

La première étape consiste à évaluer les conséquences (valeur de l'actif) de chaque actif menacé sur une échelle prédéfinie, allant par exemple de 1 à 5 (colonne «b» du tableau). La seconde étape consiste à évaluer la vraisemblance de chaque menace sur une échelle prédéfinie, allant par exemple de 1 à 5 (colonne «c» du tableau).

La troisième étape consiste à calculer la mesure des risques en multipliant ($b \times c$).

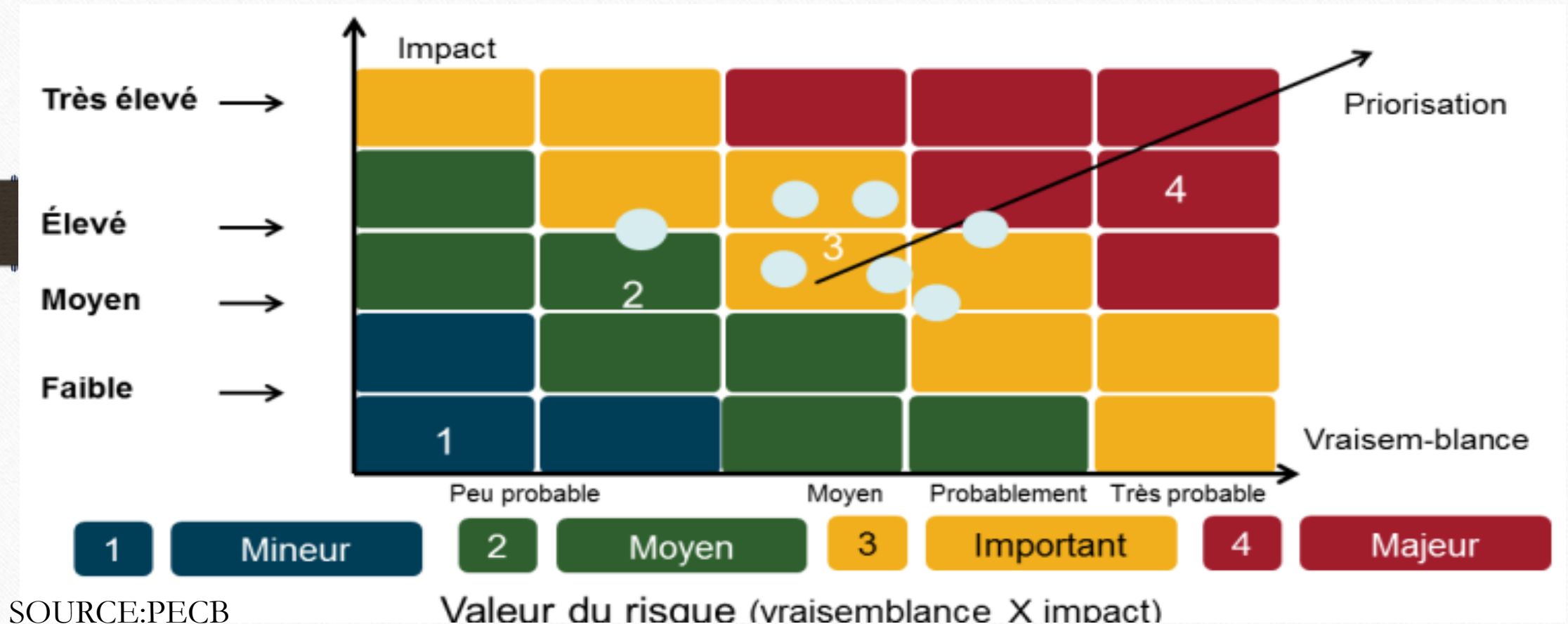
Les menaces peuvent finalement être classées selon l'ordre de leur mesure des risques associée.

Noter que dans cet exemple, 1 est considéré comme la conséquence et la vraisemblance la plus faible.

III-ÉVALUATION DES RISQUES (Suite)

PRIORISATION DES RISQUES

La priorisation des risques est un processus couramment utilisé pour déterminer les risques qui sont importants et qui ont un impact sur l'organisme.



III-ÉVALUATION DES RISQUES (Suite)

La priorisation des risques soutient également le processus de prise de décision en examinant les réponses possibles à divers risques. Une fois les scénarios d'incidents potentiels établis, les critères de classification des risques en termes de priorité devraient être définis.

La valeur zéro de risque n'existe pas. Néanmoins, il est possible de définir un seuil sous lequel l'organisme accepte de ne pas s'engager dans toute activité qui réduit le niveau de risque.

A l'autre extrémité de l'échelle, il y a un seuil au-delà duquel le risque est inacceptable et, en tant que tel, tout doit être fait pour éliminer la source de risque ou réduire le risque de manière fiable.

Le graphique présenté sur la diapositive, sans apporter de solutions, clarifie les choix qui doivent être faits. Une fois les choix effectués, ce processus permet une communication efficace et améliore la cohérence interne des actions de l'organisme par rapport à ses choix fondamentaux.

Les zones définies peuvent être cartographiées dans n'importe quelle matrice de risques pour classer chaque incident générique potentiel et définir le type d'actions requises dans chaque cas.

III-ÉVALUATION DES RISQUES (Suite)

Exemple d'une appréciation des risques

Actif	Menace	Vulnérabilité	Impact			Vraisemblance	Risque
			C	I	D		
Ordinateur Portable							
Serveur de fichier							
Contrat des clients							
Données des patients							

III-ÉVALUATION DES RISQUES (Suite)

1. Identifier une menace pour chaque actifs du tableau ;
2. Identifier une vulnérabilités pour chaque menace;
3. Evaluer l'impact de la confidentialité ,l'intégrité et la disponibilité (sur une échelle de 1à 5)
- 4.Evaluer la vraisemblance (probabilité d'occurrence, sur une échelle de 1à 5);
- 5-Calculez le risque du taux d'impact $(C+I+A/3)$ à la vraisemblance (sur une échelle de 1à 10).

III-ÉVALUATION DES RISQUES (Suite)

Actif	Menace	Vulnérabilité	Impact			Vraisemblance	Risque
			C	I	D		
Ordinateur Portable	Vol	Portabilité	3	1	2	3	5
Serveur de fichier	Virus	Antivirus faible	1	5	3	3	6
Contrat des clients	Vol	Pas de coffre-fort	5	2	2	2	5
Données des patients	Divulgence	Accès non contrôlé	4	1	1	4	6

Si nous avons déterminé que notre seuil d'acceptation des risques était de 5 ,alors deux des risques énumérés sont inacceptables.

IV-APPRÉCIATION DES RISQUES À L'AIDE D'UNE MÉTHODE QUANTITATIVE

Cette section aidera les auditeurs à acquérir des connaissances sur le concept de ROSI, le calcul de l'estimation de perte annuelle (EPA), et le calcul de la valeur d'une mesure de sécurité.

CONCEPT DE ROSI

01

Le concept de ROSI(Retour sur investissement pour la sécurité) est dérivé du concept du ROI (Return On Investment) et a plusieurs definitions et methodes de calcul.

02

La méthode de calcul ROSI décrite dans cette section a été initialement publiée en 1979 par le Federal Bureau of Standards;

03

L'estimation de perte annuelle (EPA) est souvent utilisée pour calculer le ROSI et c'est la perte monétaire annuelle prevue d'un risqué spécifique.

IV-APPRÉCIATION DES RISQUES À L'AIDE D'UNE MÉTHODE QUANTITATIVE (Suite)

Le calcul du ROSI combine le coût de la mise en œuvre des mesures de sécurité des risques et l'appréciation quantitative des risques. De plus, il compare l'économie de perte attendue avec l'estimation de perte annuelle (EPA) [Annual Loss Expectancy (ALE)].

Le calcul du ROSI dépend de trois variables : l'atténuation des risques estimée, le coût de la solution et l'estimation de perte annuelle (EPA). Si la deuxième variable, le coût de la solution, est plus facile à prévoir, les deux autres variables sont des estimations, ce qui rend ROSI plus précis.

Définition des termes qui permettent de calculer le ROSI

VA Valeur de l'actif

FE Facteur d'exposition

EPU=VA x FE Estimation e perte unique

TAO Taux annuel d'occurrence

$$\text{EPA} = \text{EPU} \times \text{TAO}$$

Estimation e perte annuelle
(Montant maximum à consacrer à la protection des actifs)

IV-APPRÉCIATION DES RISQUES À L'AIDE D'UNE MÉTHODE QUANTITATIVE (Suite)

Facteur d'exposition (FE):Ce facteur, exprimé en pourcentage, représente une mesure de l'ampleur de la perte ou de l'impact sur la valeur de l'actif.

Estimation de perte unique (EPU):Cette valeur détermine la perte monétaire pour une seule occurrence de risque. Le calcul de l'estimation de perte unique: la valeur de l'actif x facteur d'exposition ($EPU = VA \times FE$).

Taux annuel d'occurrences (TAO):Ce terme caractérise, sur une base annuelle, la fréquence qu'un risque se présente. Ce taux annuel d'occurrence est de 0 (jamais) et 1 (toujours).

Estimation de perte annuelle (EPA):L'estimation de perte annuelle est la combinaison de la perte anticipée et du taux d'occurrence annuelle anticipé. Elle détermine le montant maximum à dépenser pour protéger un actif contre une menace particulière.

Le calcul est le suivant $EPA = EPU \times TAO$

IV-APPRÉCIATION DES RISQUES À L'AIDE D'UNE MÉTHODE QUANTITATIVE (Suite)

EXEMPLE

Par exemple, si on estime qu'en moyenne, une attaque informatique affecte les trois quarts d'un réseau, le facteur d'exposition (**FE**) de cette menace sera de 75 % (3/4).

Par exemple, si la valeur (VA) de l'équipement informatique est de 100 000 FCFA et puisque le facteur d'exposition est de 75%, l'estimation de perte unique (EPU) serait alors de $VA \times FE = 100000 \times 75\% = 75000$.

Par exemple, si la probabilité d'une cyberattaque sur un ordinateur spécifique au cours de l'année est une fois par mille ans, le taux annuel d'occurrences (TAO) est de 0,001. Si la probabilité était une fois tous les 5 ans, le taux annuel d'occurrence serait de 0,2.

Par exemple, si l'estimation de perte unique (EPU) est de 75 000 et le taux annuel d'occurrence est de 0,2 alors l'estimation de perte annuelle $EPA = EPU \times TAO$ est de 15 000 .

IV-APPRÉCIATION DES RISQUES À L'AIDE D'UNE MÉTHODE QUANTITATIVE (Suite)

CALCUL DE L'ESTIMATION DE PERTE ANNUELLE (EPA)

On estime qu'une surtension peut endommager 25% d'une installation électrique (FE). La valeur d'installation est estimée à 50 Millions (VA) et la probabilité d'une telle surtension est d'une fois tous les 10 ans (TAO).

$$EPU = VA \times FE = 50M \times 0,25 = 12,5 \text{ Millions}$$

$$EPA = EPU \times TAO = 12,5M \times 0,1 = 1,25 \text{ Millions}$$

Ainsi les 1,25 Millions est le montant maximal à consacré annuellement à la protection des actifs contre le risque de surtension.

IV-APPRÉCIATION DES RISQUES À L'AIDE D'UNE MÉTHODE QUANTITATIVE (Suite)

ANALYSE QUANTITATIVE D'UNE ESTIMATION DE PERTE ANNUELLE

ACTIFS	RISQUE	VA	FE	$EPU=VA \times FE$	TAO	$EPA=EPU \times TAO$
Données sensibles	Virus	500 K CFA	10%	50K	20%	10K
Serveur Web	Déni de service	3 M CFA	25%	750 K	10%	75K
Centre de données	Incendie	5M CFA	50%	2,5M	4%	100K
Numéros de carte de crédit	Vol	1 M F CFA	75%	750K	2%	15K

Ce tableau présente les résultats de l'analyse des risques et doit permettre à l'organisme de prendre des décisions claires sur les risques qui doivent être considérés en premier lieu, la probabilité qu'ils se produisent ainsi que les pertes potentielles provenant d'eux. L'organisme peut également fournir les montants qui sont alloués annuellement à titre de contre-mesures pour chacun de ces risques.

III-ÉVALUATION DES RISQUES (Suite)

Calcul de la valeur d'une mesure de sécurité

Valeur = (EPA avant - EPA après – cout annuel de maintenance de la mesure)

Prenons l'exemple sur le cas de la surtension $EPA = EPU \times TAO = 12,5M \times 0,1 = 1,25$ Millions

Coût de la mise en œuvre de la mesure est de 500 K et EPA après est de 250 K

La valeur de la mesure de sécurité = 1,25 M - 500K - 250K = 500K

L'analyse des risques fournit une comparaison des coûts et des avantages puisque le coût annuel des mesures de sécurité pour se protéger contre une menace est comparé à l'estimation de perte annualisée.

En général, une mesure de sécurité ne devrait pas être mise en œuvre si son coût annuel est plus élevé que l'estimation de perte annuelle.

Le coût d'une mesure de sécurité ne signifie pas seulement inclure le coût de la mise en œuvre. Les coûts suivants doivent également être pris en compte pour le calcul du coût total de la mesure: le produit, l'emplacement, la conception, la modification, l'entretien, l'essai, les mises à jour, l'exploitation, le soutien, la productivité, etc.

IV-APPRÉCIATION DES RISQUES À L'AIDE D'UNE MÉTHODE QUANTITATIVE (Suite)

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 \$, le 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 la mesure (c'est-à-dire les clés USB 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 %.

V-TRAITEMENT DES RISQUES

Cette section aidera le participant à acquérir des connaissances sur le processus de traitement du risque, qui comprend les options de traitement des risques, le plan de traitement, et l'évaluation du risque résiduel.

ISO/IEC 27005 ARTICLE 9: Traitement du risque en sécurité de l'information .

ELEMENT D'ENTRE

Liste des risques classés par ordre de priorité en cohérence avec les critères d'évaluation du risque et en relation avec les scénarii d'incident qui conduisent à ces risques.

ACTION

Il convient de choisir des mesures de sécurité pour réduire, maintenir, éviter ou transférer les risques, et de définir un plan de traitement du risque.

ELEMENTS DE SORTIE

Plan de traitement du risque et risques résiduels soumis à la décision d'acceptation des dirigeants de l'organisme.

V-TRAITEMENT DES RISQUES (Suite)

ISO /IEC 27000 ,*article 3.72 Traitement du risque* est le processus destiné à modifier un risque

Note 1 à l'article:

Le traitement du risque peut inclure:

- un refus du risque en décidant de ne pas démarrer ni poursuivre l'activité porteuse du risque;
- la prise ou l'augmentation d'un risque afin de saisir une opportunité;
- l'élimination de la source de risque;
- une modification de la vraisemblance;
- une modification des conséquences;
- un partage du risque avec une ou plusieurs autres parties (incluant des contrats et un financement du risque);
- un maintien du risque fondé sur un choix argumenté.

Note 2 à l'article:

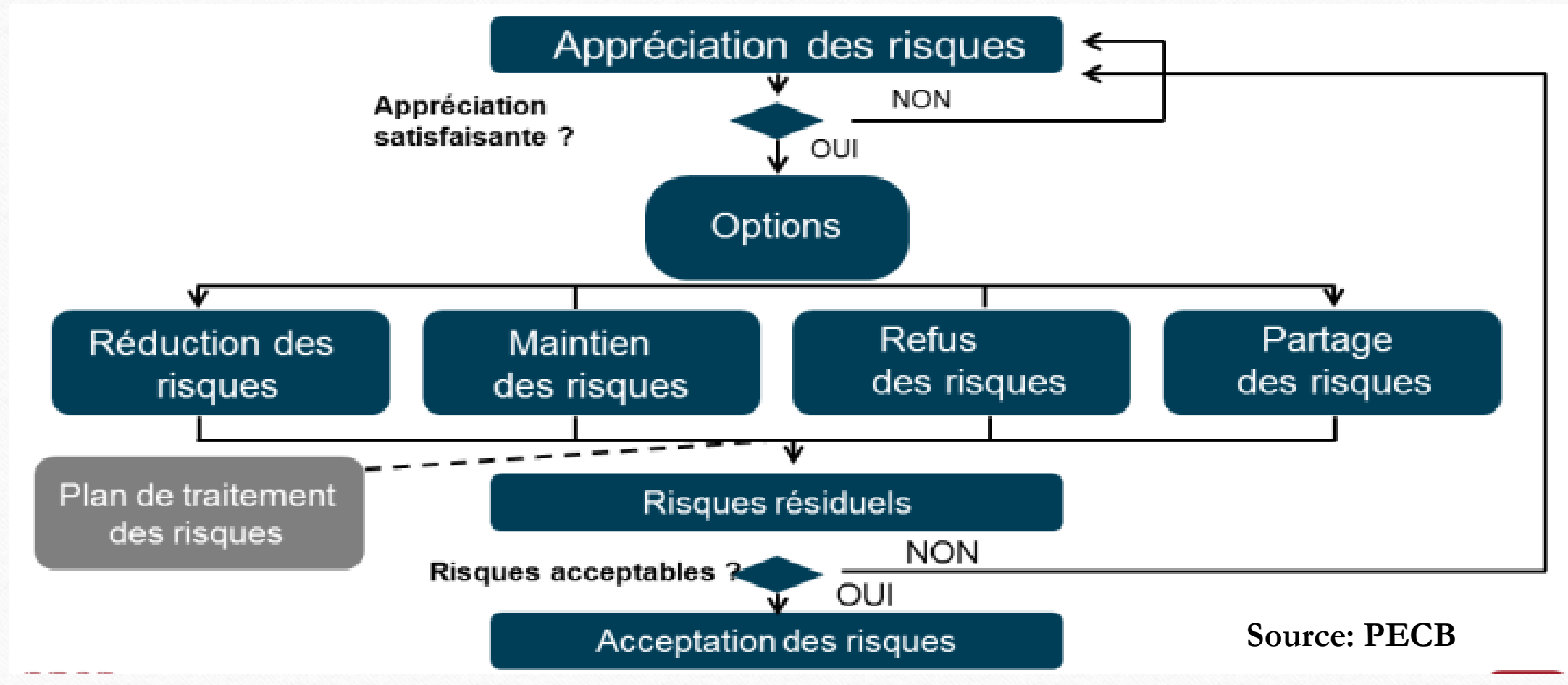
Les traitements du risque portant sur les conséquences négatives sont parfois appelés «atténuation du risque», «élimination du risque», «prévention du risque» et «réduction du risque».

Note 3 à l'article:

Le traitement du risque peut créer de nouveaux risques ou modifier des risques existants.

V-TRAITEMENT DES RISQUES (Suite)

ATIVITE DU TRAITEMENT DU RISQUE



Source: PECB

V-TRAITEMENT DES RISQUES (Suite)

ISO/IEC 27005, article 9.1 Description générale du traitement des risques

Il convient de choisir les options de traitement des risques sur la base des résultats de l'appréciation des risques, du coût prévu de mise en œuvre ainsi que des bénéfices attendus de ces options.

Lorsqu'il est possible d'obtenir d'importantes réductions en réalisant relativement peu de dépenses, il convient de mettre en œuvre ces options.

D'autres options d'améliorations peuvent être peu rentables; il est donc nécessaire de bien les analyser afin de savoir si elles se justifient.

En général, il convient de rendre les conséquences négatives des risques aussi faibles que possible et indépendantes de tout critère absolu. Il convient que les dirigeants tiennent compte des risques rares mais aux impacts importants.

Dans ces cas, il peut être nécessaire de mettre en œuvre des mesures de sécurité qui sont difficilement justifiables sur le plan économique (par exemple, des mesures de sécurité liées à la continuité de l'activité identifiées pour couvrir des risques spécifiques élevés).

Les quatre options relatives au traitement des risques ne s'excluent pas mutuellement.

L'organisme peut parfois retirer des bénéfices substantiels d'une combinaison d'options tels que la réduction de la vraisemblance des risques et de leurs conséquences et le partage ou la conservation de tout risque résiduel.

V-1-Définir les options de traitement des risques

La méthode d'évaluation des risques doit permettre de gérer les risques selon les quatre options suivantes:

01

Réduction du risque

Introduction
,suppression ou
modification de
mesure de sécurité
afin que le risque
résiduel puisse être
réapprécié et jugé
acceptable .



02

Maintien du risque

Décision
d'accepter le
niveau de risque



03

Refus des risques

Annulation ou
modification d'une
activité ou d'un
ensemble d'activité
liées au risque



04

Partage des risques

Décision de partager
les risques avec les
parties
externes:assurance
ou externalisation



V-1-Définir les options de traitement des risques (Suite)

01

Réduction du risque.

Il convient de réduire le niveau de risque par la sélection des mesures de sécurité afin que le risque résiduel puisse être réapprécié et jugé acceptable.



Correction

Élimination

Prévention

Atténuation des impacts

Dissuasion

Détection

Récupération

Surveillance

Sensibilisation

Source: PECB

V-1-Définir les options de traitement des risques (Suite)

L'Annexe A de la norme ISO/IEC 27001 fournit un ensemble d'objectifs de mesures communément acceptés et des mesures de meilleures pratiques à utiliser comme guide de mise en œuvre lors du choix et de la mise en œuvre des mesures visant la sécurité de l'information. Il fournit des orientations sur la mise en œuvre des mesures de sécurité de l'information.

Les articles 5 à 18 de la norme ISO/IEC 27002 fournissent des conseils et des orientations spécifiques sur la mise en œuvre des meilleures pratiques à l'appui des mesures spécifiées dans les articles A.5 à A.18 d'ISO/IEC 27001.

V-1-Définir les options de traitement des risques (Suite)

ISO/IEC 27001 ,Annexe A

Source: PECB

A 5	Politiques de sécurité de l'information	02 Mesures
A 6	Organisation de la sécurité de l'information	07 Mesures
A 7	Sécurité des ressources humaines	06 Mesures
A 8	Gestion d'actifs	10 Mesures
A 9	Contrôle d'accès	14 Mesures
A 10	Cryptographie	02 Mesures
A 11	Sécurité physique et environnementale	15 Mesures
A 12	Sécurité liée à l'exploitation	14 Mesures
A 13	Sécurité des communications	07 Mesures
A 14	Acquisition, développement et maintenance des systèmes d'information	13 Mesures
A 15	Relations avec les fournisseurs	05 Mesures
A 16	Gestion des incidents liés à la sécurité de l'information	07 Mesures
A 17	Aspects de la sécurité de l'information dans la gestion de la continuité de l'activité	04 Mesures
A 18	Conformité	08 Mesures

V-1-Définir les options de traitement des risques (Suite)

02

Maintien du risque.

Si le niveau de risque répond aux critères d'acceptation du risque, il n'est pas nécessaire de mettre en œuvre d'autres mesures de sécurité, le risque peut alors être conservé.



Le maintien du risque actuel doit toutefois être documenté

V-1-Définir les options de traitement des risques (Suite)

03

Refus du risque.

Lorsque les risques identifiés sont jugés trop élevés ou lorsque les coûts de mise en œuvre d'autres options de traitement du risque dépassent les bénéfices attendus, il est possible de prendre la décision d'éviter complètement le risque:

- en abandonnant une ou plusieurs activités prévues ou existantes;
- ou en modifiant les conditions dans lesquelles l'activité est effectuée.



Exemple :

L'organisme évite le risque en:

- cessant de faire des affaires dans certains marchés jugés trop risqués;
- Supprimant l'actif d'une zone à risque ;
- Décidant de ne pas partager l'information sensibles.

V-1-Définir les options de traitement des risques (Suite)

04

Partage des risques

Il convient de partager le risque avec une autre partie capable de gérer de manière plus efficace le risque spécifique en fonction de son évaluation.



C'est la meilleure option quand:

- Il est difficile pour un organisme de réduire le risque à un niveau acceptable;
- L'organisme n'a pas l'expertise pour gérer le risque ;
- Il est plus économique de transférer le risque à un tiers.

Les deux principales méthodes de partage des risques:

Assurance: Toute forme de couverture des risques ou de garantie financière contractée par un organisme en échange du paiement d'une prime.

Externalisation: Toute forme de transfert d'une activité commerciale à un partenaire externe.

V-1-Définir les options de traitement des risques (Suite)

Le déni du risque est une attitude commune, surtout si l'organisme n'a pas subi d'incidents majeurs au cours des dernières années ,**il n'est jamais une option pour le traitement du risque.**

Un gestionnaire de risques qui observe les risques partout et qui en exagère les impacts potentiels risque de perdre toute crédibilité dans son organisme.

“Je n’imagine aucune circonstance qui pourrait causer le naufrage du navire.Je ne veux pas imaginer une catastrophe qui pourrait affecter ce navire...”

Le capitaine du Titanic ,1912

Source: Institute for Governance of Information Systems ISACA ,2014



V-2-Préparer le plan de traitement du risque

Au moment de déterminer la priorité des actions à prendre pour mettre en œuvre l'option de traitement du risque

choisi, l'organisme devrait prendre en compte, entre autres, les éléments suivants:

- La nécessité de communiquer les résultats à la direction ;
- Les processus qui portent le plus haut niveau de risque

Les plans de traitement du risque ont pour but de préciser la manière dont les options de traitement choisies seront mises en œuvre de sorte que les dispositions soient comprises par les personnes concernées et que les progrès par rapport au plan puissent faire l'objet d'un suivi.

A cet effet:

- Il convient que le plan de traitement identifie clairement l'ordre de mise en œuvre du traitement du risque.
- Il convient que les plans de traitement soient intégrés aux plans et processus de management de l'organisme ;
- Il convient que les informations fournies dans le plan de traitement comportent: la justification du choix des options de traitement, y compris les avantages attendus
- les ressources nécessaires, en tenant compte des impondérables.

V-2-Préparer le plan de traitement du risque(Suite)

EXEMPLE

Scénario de risque	Niveau de risque	Priorité	Option de traitement	Mesure	Ressources requises	Responsable	Echéances	Commentaires
Les utilisateurs non autorisés peuvent se connecter à SharePoint via l'extranet et rechercher des fichiers sensibles de l'organisme avec l'identifiant demandé.	6	Élevée	Eviter	Rendre SharePoint inaccessible	10 heures pour reconfigurer et tester le système	Administrateur système et sécurité	14-03/2022 AU 16/03/2022	Effectuer des examens périodiques de la sécurité du système pour s'assurer que la sécurité de SharePoint est adéquate

V-3-Evaluer le risque résiduel

Le risque résiduel peut être défini comme le risque qui demeure après la mise en œuvre des mesures visant à réduire le risque inhérent, et peut être résumé comme suit:

Risque résiduel = risque inhérent - risque traité

Après la mise en œuvre d'un plan de traitement du risque, il y a toujours des risques résiduels.

La valeur de la réduction des risques après le traitement des risques doit être évaluée, calculée et documentée. Les risques résiduels peuvent être difficiles à évaluer, mais une estimation devrait au moins être faite pour s'assurer que la valeur des risques résiduels est conforme aux critères d'acceptation des risques de l'organisme.

L'organisme doit également mettre en place des mécanismes de surveillance des risques résiduels.

Si le risque résiduel est considéré comme inacceptable après la mise en œuvre des mesures, il faut prendre la décision de traiter complètement le risque.

Une autre solution pourrait être de trouver d'autres options de traitement des risques telles que le risque de partage (assurance ou sous-traitance), ce qui permettrait de réduire le risque à un niveau acceptable.

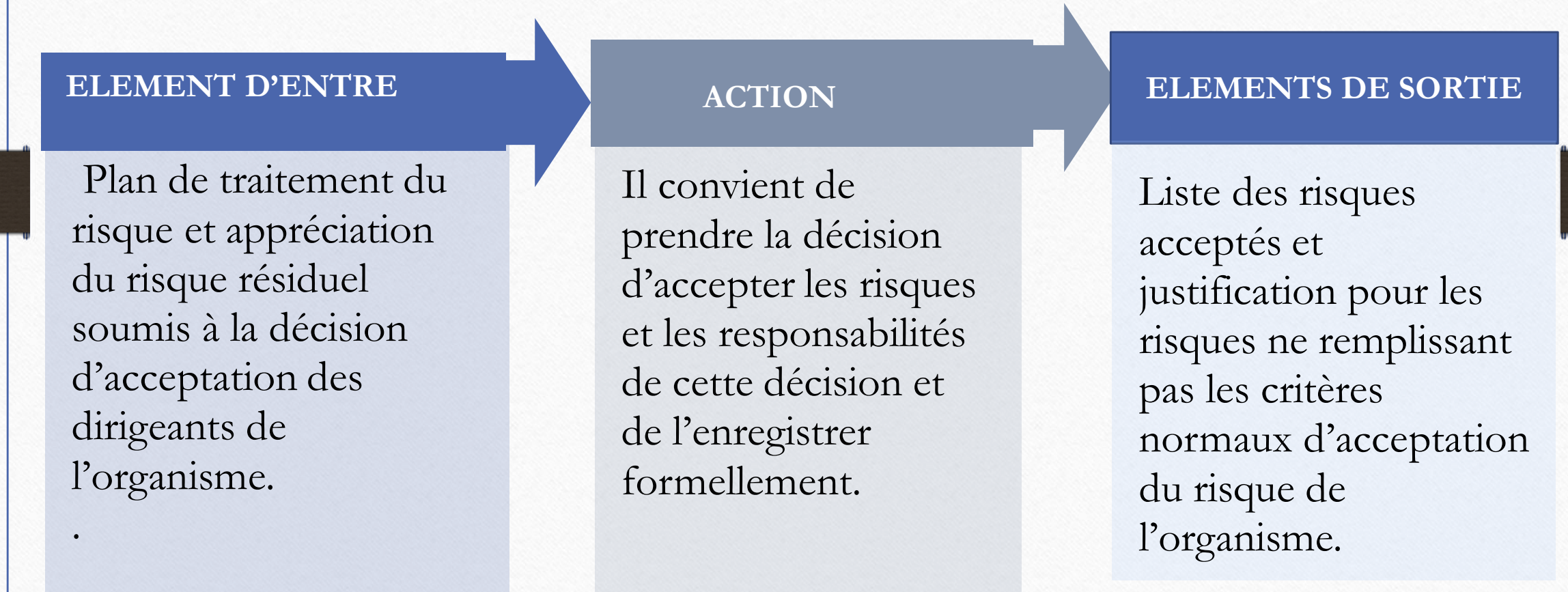
Même s'il est préférable d'éliminer complètement les risques qui dépassent les critères d'acceptation des risques de l'organisme, il n'est pas toujours possible de réduire tous les risques à un niveau acceptable.

En toutes circonstances, les risques résiduels doivent être compris, acceptés et approuvés par la direction.

VI-Acceptation des risques en sécurité de l'information

Cette section aidera le participant à acquérir des connaissances sur le processus d'acceptation des risques, qui comprend l'acceptation du plan de traitement des risques et l'acceptation des risques résiduels.

ISO/IEC 27005 ,Article 10: Acceptation du risque en sécurité de l'information



VI-Acceptation des risques en sécurité de l'information

Certains facteurs peuvent influencer notre opinion quant à l'existence d'un risque acceptable , ce sont:

01 Avantages en prenant le risque: Ce facteur de tolérance au risque vient de la logique du profit, du gain et de la reconnaissance.

02 Contrôle du risque: Lorsque nous avons le contrôle, ou l'impression que nous avons le contrôle sur les risques, les biais de confirmation arrive. Le biais de confirmation est un processus qui nous fait croire que la décision est sécuritaire, malgré les risques réels. Le contrôle nous donne le sentiment de confiance et une sous-estimation du risque.

03 Temps jusqu'à ce que les effets soient connus: Parfois, il faut plus de temps pour ressentir les effets du traitement du risque, donc les personnes ont tendance à accepter le risque plutôt que d'attendre les résultats de ce dernier.

04 Aversion au risque: Tentative de réduire l'incertitude

05 Familiarité avec la tâche (ou complaisance): Cela se produit lorsqu'un employé a terminé avec succès le même travail plusieurs fois et a la compétence de le faire à nouveau, sans penser à d'autres risques. Cet état est également nommé «inconsciemment compétent.»

VI-Acceptation des risques en sécurité de l'information

As Low As Reasonably Practicable (ALARP)

Le principe ALARP est utilisé comme une approche pour déterminer si le risque identifié est acceptable ou non. Il stipule que les risques identifiés doivent être réduits à un niveau qui est «aussi bas que raisonnablement possible»

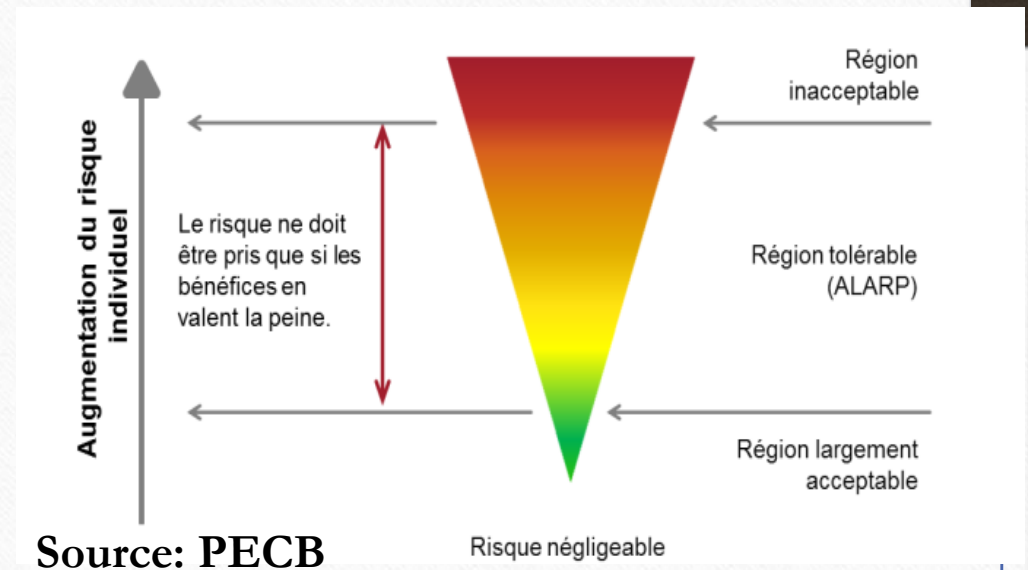
La région à risque tolérable est également appelée région ALARP, puisque le risque tolérable n'est acceptable que si toutes les pratiques raisonnables de réduction des risques ont été mises en œuvre.

De plus, toute personne qui exploite un processus comportant des risques dans la région tolérable doit démontrer qu'elle a atteint le risque le plus faible possible.

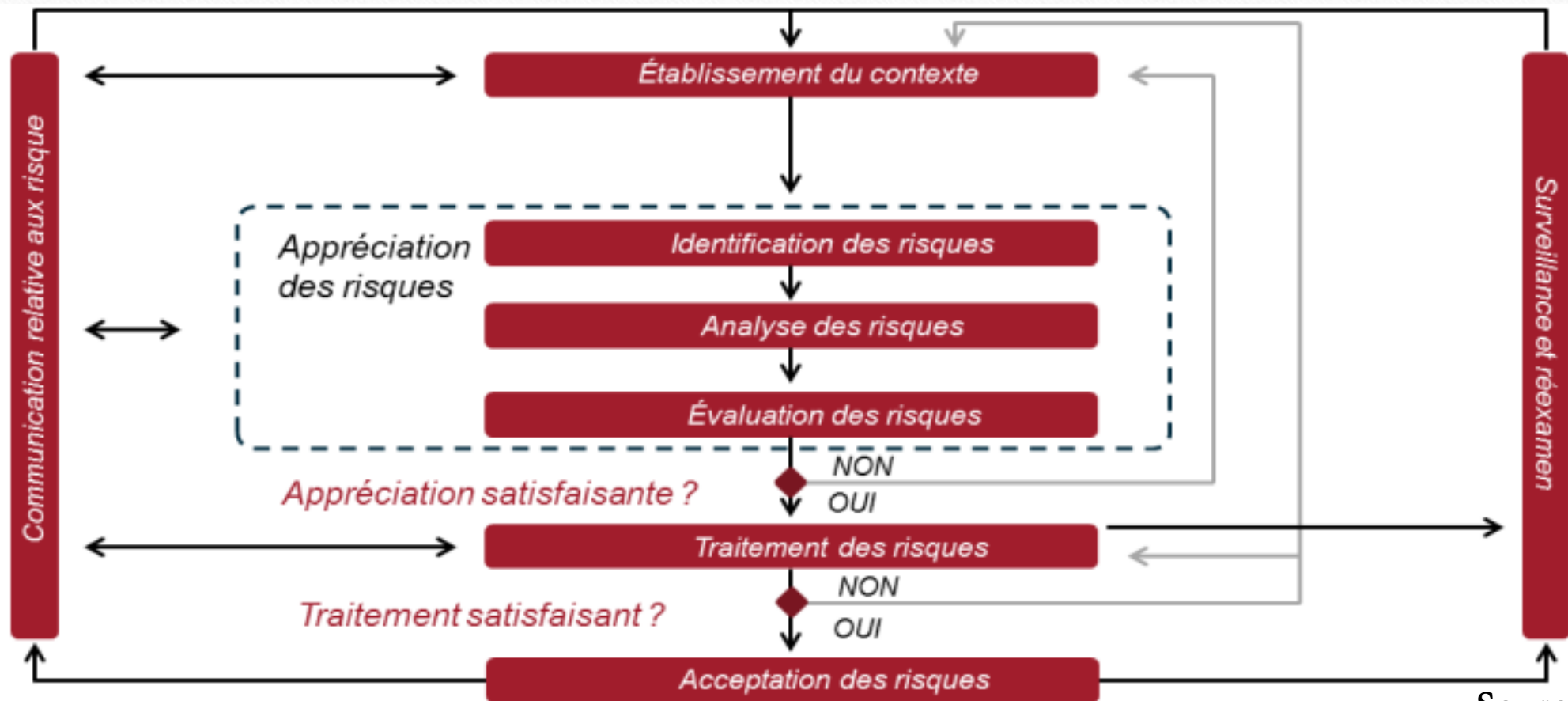
Région inacceptable: Le risque est trop élevé pour être acceptable et des mesures de réduction des risques doivent être mis en place.

Région tolérable (ALARP) : Le risque est inférieur au niveau inacceptable, mais n'est pas acceptable sans envisager d'autres mesures pour réduire le risque.

Région largement acceptable: Le risque est largement acceptable et d'autres mesures ne sont pas considérées comme nécessaires.



VI-Acceptation des risques en sécurité de l'information




Source: PECB


Comme l'illustre la Figure ci-dessus, le processus de gestion des risques en sécurité de l'information peut être itératif pour les activités d'appréciation et/ou de traitement des risques.

VI-1-Acceptation le plan de traitement risques

Acceptation du risque résiduel par les propriétaires du risque



Il est important que les dirigeants en charge réexaminent et approuvent les plans de traitement du risque proposés et les risques résiduels associés, puis enregistrent les conditions associées à l'approbation.

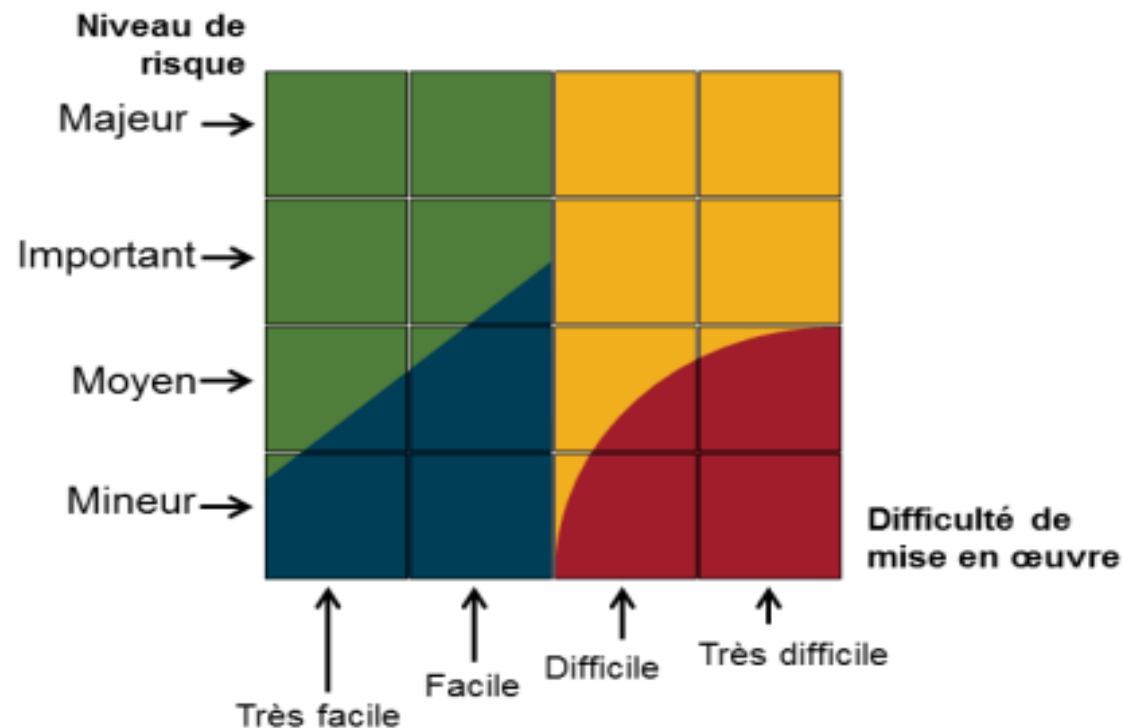


Les critères d'acceptation du risque peuvent être plus complexes et ne pas consister simplement à savoir si un risque résiduel se situe au-dessus ou en-dessous d'un seuil unique.

VI-1-Acceptation le plan de traitement risques (suite)

C'est la décision de la direction de définir les attentes en ce qui concerne le plan de traitement des risques pour chaque niveau de risque.

Exemple de présentation à la Direction



Source: PECB

VI-1-Acceptation le plan de traitement risques

Comme le montre la diapositive précédente , pour les risques «de niveau majeur» qui ont une difficulté de mise en œuvre classée entre très facile et facile, le plan de traitement des risques doit être mis en œuvre immédiatement. En revanche, si la difficulté de mise en œuvre est classée entre difficile et très difficile, c'est la direction qui doit décider de la manière de procéder avec le plan de traitement des risques.

Toutefois, pour les risques de niveau «mineur ou moyen», le plan de traitement des risques pourrait être mis en œuvre immédiatement, la mise en œuvre du plan de traitement des risques pourrait être planifiée ou le risque pourrait simplement être accepté en fonction de la difficulté de la mise en œuvre du plan de traitement des risques.

VI-2-Acceptation le risques résiduel

Dans l'image ci-dessous, le risque résiduel est représenté d'une manière tridimensionnelle, où il est le multiple de la valeur de l'actif, de l'impact de la menace et de la vulnérabilité de l'actif. La probabilité est prise en compte dans l'impact de la menace.

Après l'application des contre-mesures par la mise en place de mesures de sécurité, il est très probable qu'un élément de risque résiduel soit encore présent.

Le risque résiduel peut être calculé à partir de:

La valeur de l'actif

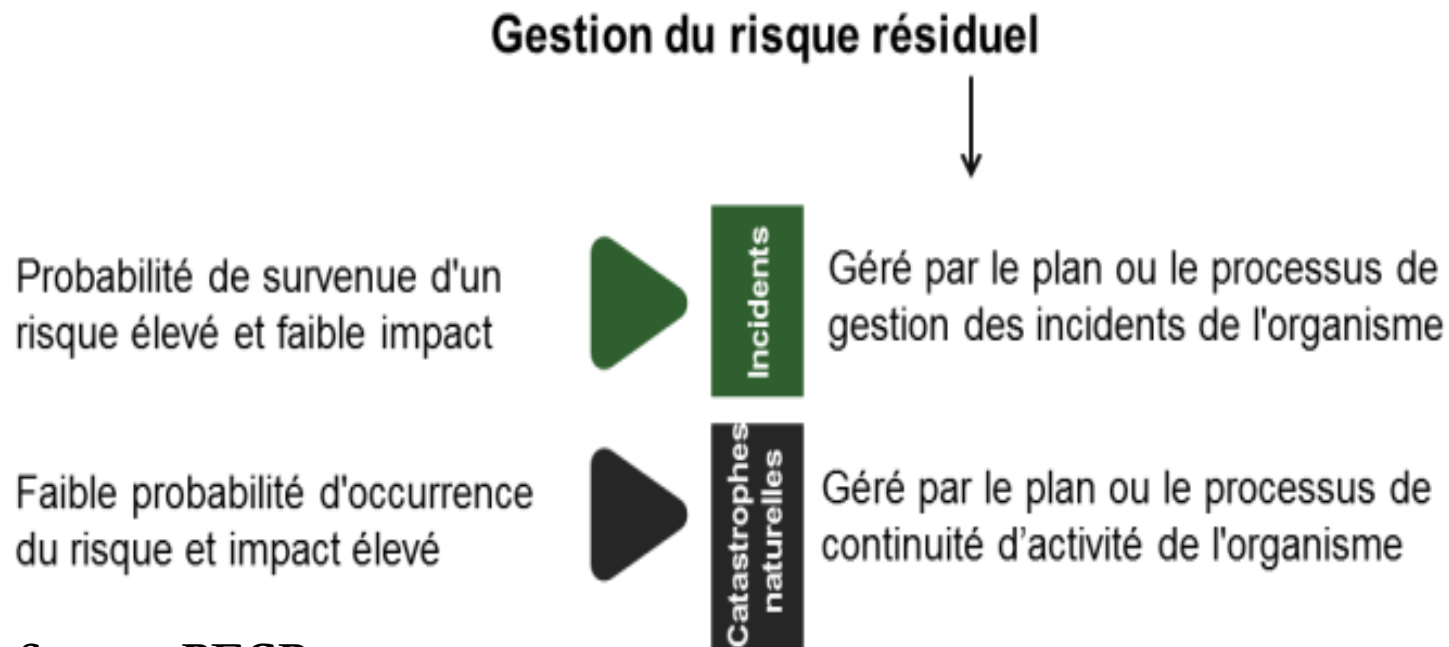
La probabilité d'une menace spécifique

La vulnérabilité de l'actif

L'impact de la menace

VI-2-Acceptation le risques résiduel (suite)

Après l'acceptation du risque, tous les risques résiduels ne disparaissent pas. Les risques dont l'incidence est élevée ou faible sont gérés par le plan ou le processus de gestion des incidents de l'organisme. Les risques à faible occurrence et à impact élevé (catastrophe) sont gérés par le plan ou le processus de continuité d'activité de l'organisme.



Source: PECB

VI-2-Acceptation le risques résiduel (suite)

Exercice 9 : Options de traitement des risques

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.

Durée de l'exercice : 15 minutes

VI-2-Acceptation le risques résiduel (suite)

Exercice 9 : Options de traitement des risques

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.

Durée de l'exercice : 15 minutes

BIBLIOGRAPHIE

- ISO/IEC Guide 73:2002, Risk management – Vocabulary – Guidelines for use in standards
- La norme ISO/CEI 27005:2008
- Cours de formation PECB sur la Norme ISO/IEC 27005 : Risk manager
- Cours de formation PECB sur la norme ISO/CEI 27001
- <https://www.iso.org/fr/isoiec-27001-information-security.html>

**Merci de votre
attention**