

II-CONCEPTS ET DÉFINITIONS LIÉS AU MANAGEMENT DU RISQUE

GÉRER LES RISQUES : POURQUOI ?

Objectifs cités dans la norme ISO/IEC 27005 :

En introduction , au chapitre 1 – Domaine d'application :

- ❑ La présente Norme internationale ... est conçue pour aider à la mise en place de la sécurité de l'information basée sur une approche de gestion de risque;
- ❑ Dans les considérations générales (par 7.1) :

Il est essentiel de déterminer l'objectif de la gestion du risque en sécurité de l'information puisqu'il influence l'ensemble du processus .

L'objectif peut être :

- une réponse aux exigences d'un SMSI;
- la conformité avec la loi et la preuve de la mise en œuvre du devoir de précaution;
- la préparation d'un plan de continuité de l'activité;
- la préparation d'un plan de réponse aux incidents;
- la description des exigences en matière de sécurité de l'information pour un produit, un service ou un mécanisme.

II-CONCEPTS ET DÉFINITIONS LIÉS AU MANAGEMENT DU RISQUE

CONCEPTS DE RISQUE

Le risque est la possibilité de subir une perte. Il est lié à un événement qui pourrait avoir des conséquences négatives ou à une situation où une personne pourrait nuire d'une façon ou d'une autre à une organisation.

Le risque est présent dans toute activité humaine ,il est géré tout le temps consciemment où inconsciemment ,en faisant des choix.

Définition scientifique du risque

Selon le mathématicien ,Daniel Bernoulli (1738) «Le risque est une attente mathématique d'une fonction de probabilité d'événements.»

Autrement ,le risque est la combinaison de la probabilité d'un évènement et de ses conséquences . Le terme «risque» est généralement utilise uniquement lorsqu'il existe au moins la possibilité de conséquences négatives.

Dans certaines situations, le risque provient de la possibilité d'un écart par rapport au résultat ou a l'évènement attendu. La gestion des risques est le processus continu d'identification des risques et la mise en œuvre des plans pour y répondre.

II-CONCEPTS ET DÉFINITIONS LIÉS AU MANAGEMENT DU RISQUE

CONCEPTS DE RISQUE (Suite)

L'ISO/IEC 27000 ,article 3.61 définit le risque comme un effet de l'incertitude sur les objectifs.

Les événements peuvent avoir une vision négative, une vision positive ou les deux.
On peut simplement avoir une vision «neutre»



1.vision positive

Gain potentiel



2.vision neutre

Vraisemblance
d'événement



3.vision négative

Perte potentiel

Note importante tirée du ISO Guide 73:2009 :

L'effet est l'écart, positif ou négatif, par rapport à ce qui est attendu. (l'impact qu'un risque se manifeste).

L'incertitude est l'état, même partiel, de défaut d'information concernant la compréhension ou la connaissance d'un événement, de ses conséquences ou de sa vraisemblance.

Les objectifs peuvent avoir différents aspects et peuvent concerner différents niveaux (niveau stratégique, niveau d'un projet, d'un produit, d'un processus ou d'un organisme tout entier).

II-CONCEPTS ET DÉFINITIONS LIÉS AU MANAGEMENT DU RISQUE

CONCEPTS DE RISQUE (Suite)

Exemples de risque et menaces

Les virus et malwares

Les emails frauduleux

Le piratage

La malversation.

La perte d'informations
confidentielles

L'erreur de manipulation

Le risque physique de perte ou vol.



VIRUS
INFORMATIQUE INDUSTRIEL



L'ESPIONNAGE
INDUSTRIEL



INCENDIE



INONDATION

Un événement considéré comme ayant un impact négatif est un risque qui pourrait entraver la création de valeur ou détruire la valeur existante d'un organisme.

Tout ce qui peut exploiter une vulnérabilité peut être une menace .

II-CONCEPTS ET DÉFINITIONS LIÉS AU MANAGEMENT DU RISQUE

CONCEPTS DE RISQUE (Suite)

Les vulnérabilités: Selon l'ISO 27000 « Faille dans un actif ou dans une mesure de sécurité qui peut être exploitée par une menace ».

Une menace est une cause potentielle d'incident indésirable , qui peut nuire à un système ou à l'organisation (selon l'ISO 27000 ,clause 2.83).

Un actif est quelque chose qui a une valeur pour l'organisme, notamment : des informations, des logiciels, des périphériques physiques, des services, des personnes et de leurs qualifications, de leurs compétences et de leur expérience, les actifs incorporels, etc.

Un **impact** est un changement négatif pénalisant le niveau des objectifs métier atteints.

II-CONCEPTS ET DÉFINITIONS LIÉS AU MANAGEMENT DU RISQUE

CONCEPTS DE RISQUE (Suite)

Menaces humaines: Source de la menace ,motivation et actions de menace

Source de la menace	Motivation	Actions de menace
Pirate informatique, cracker	Défi Ego Rébellion	Piratage informatique Ingénierie sociale Intrusion dans un système Accès non autorisé
Criminel informatique	Destruction d'information Divulgateion illégale d'informations Gain monétaire Modification non autorisée de données	Criminalité informatique Acte frauduleux Corruption d'informations Usurpation Intrusion dans un système

Source:PECB

II-CONCEPTS ET DÉFINITIONS LIÉS AU MANAGEMENT DU RISQUE

CONCEPTS DE RISQUE (Suite)

Menaces humaines: Source de la menace ,motivation et actions de menace

Source de la menace	Motivation	Actions de menace
Espionnage industriel (sociétés, gouvernements étrangers)	Avantage concurrentiel Espionnage économique	Exploitation économique Vol d'informations Intrusion dans la vie privée Ingénierie sociale Intrusion dans un système
Initiés (employés mal formés, malveillants, malhonnêtes)	Curiosité Ego Intelligence Gain monétaire Vengeance Erreurs non intentionnelles	Agression d'un employé Chantage Abus d'ordinateur Fraude et vol Corruption d'informations Saisie de données falsifiées

Source:PECB

II-CONCEPTS ET DÉFINITIONS LIÉS AU MANAGEMENT DU RISQUE

OPPORTUNITÉ DU RISQUE

Si les événements peuvent avoir **une vision négative**, **une vision positive** ou une **vision «neutre»**, les scénarios de risque peuvent représenter des opportunités pour les organismes.

L'opportunité est la circonstance qui survient dans l'environnement de l'organisation, et qui permet une amélioration de sa performance.

La gestion des risques offre l'opportunité de répondre efficacement aux risques et opportunités associés aux incertitudes auxquelles l'organisme est confronté, améliorant ainsi la capacité à créer de la valeur pour l'organisme.

II-CONCEPTS ET DÉFINITIONS LIÉS AU MANAGEMENT DU RISQUE

OPPORTUNITÉ DU RISQUE (Suite)

Stratégie de gestion des risques

Source:PECB

Approche intégrant les différentes facettes

	Stratégie de gestion des risques	Exemples d'application des risques liés à la sécurité de l'information
Positif (Opportunité)	Maximiser le retour sur investissement en prenant en compte la prime de risque	Prendre le risque d'investir dans des projets à fort potentiel de rendement en maîtrisant les risques
Neutre (Incertitude)	Calculer les probabilités de divers scénarios de risque et prédire les tendances	Mettre en place enquête technologique, suivi et revue des risques
Négatif (Menace)	Éviter, transférer, réduire ou maintenir les risques identifiés	Éviter les technologies non sécurisées, mettre en place des contrôles, s'assurer contre les incidents

La gestion efficace des risques permet de prévoir les risques et d'équilibrer le niveau de risque acceptable contre les opportunités connexes.

III-CONCEPTS LIÉS À LA SÉCURITÉ DE L'INFORMATION

SECURITE DE L'INFORMATION

Système d'information : Ensemble des moyens matériels, logiciels et organisationnels qui permettent de recevoir, de conserver et de traiter l'information (données significatives).

La sécurité de l'information détermine quels informations doivent être protégées ,la raison pour laquelle elles doivent l'être ,comment les protéger et de quoi elles doivent être protégées;

En protégeant l'organisation contre les menaces et les vulnérabilités ,la sécurité de l'information réduit les risques et l'impact de ses actifs.

La sécurité de l'information vise généralement cinq principaux objectifs :

- **L'intégrité :** garantir que les données sont bien celles que l'on croit être ;
- **La disponibilité :** maintenir le bon fonctionnement du système d'information;
- **La confidentialité :** rendre l'information inintelligible à d'autres personnes que les seuls acteurs d'une transaction;
- **La non répudiation :** garantir qu'une transaction ne peut être niée;
- **L'authentification :** assurer que seules les personnes autorisées aient accès aux ressources.

III-CONCEPTS LIÉS À LA SÉCURITÉ DE L'INFORMATION

RISQUES LIÉS AUX ACTIFS D'INFORMATION

Le risque lié à la sécurité de l'information est associé à la possibilité que les menaces exploitent les vulnérabilités d'un actif et nuisent donc à un organisme.

Le risque est souvent exprimé en termes de combinaison des conséquences d'un événement et de sa « vraisemblance ».

Dans un contexte de SMSI, les risques liés à la sécurité de l'information peuvent être exprimés comme aspects négatifs associés à la menace.



La vraisemblance varie selon l'exposition aux menaces, le niveau de vulnérabilité et les mesures de sécurité.

La première cible de la sécurité de l'information n'est pas d'accroître les opportunités ou les résultats positifs, mais de limiter les possibilités de perte.

III-CONCEPTS LIÉS À LA SÉCURITÉ DE L'INFORMATION

MESURE DE SECURITE

Les mesures de sécurité de l'information comprennent tous processus, politiques, procédures, lignes directrices, pratiques ou structures organisationnelles, qui peuvent être de nature administrative, technique, de gestion ou juridique, et qui modifient les risques pour la sécurité de l'information.



Mesure technique

pare-feu, systèmes d'alarme, caméras de surveillance, systèmes de détection d'intrusion (IDS)

Mesure administrative :

la structure organisationnelle
séparation des tâches, la rotation des postes, les descriptions de poste, les processus d'approbation

Mesure de direction

la gestion du personnel, y compris la formation et l'encadrement des employés, les revues de direction et les audits

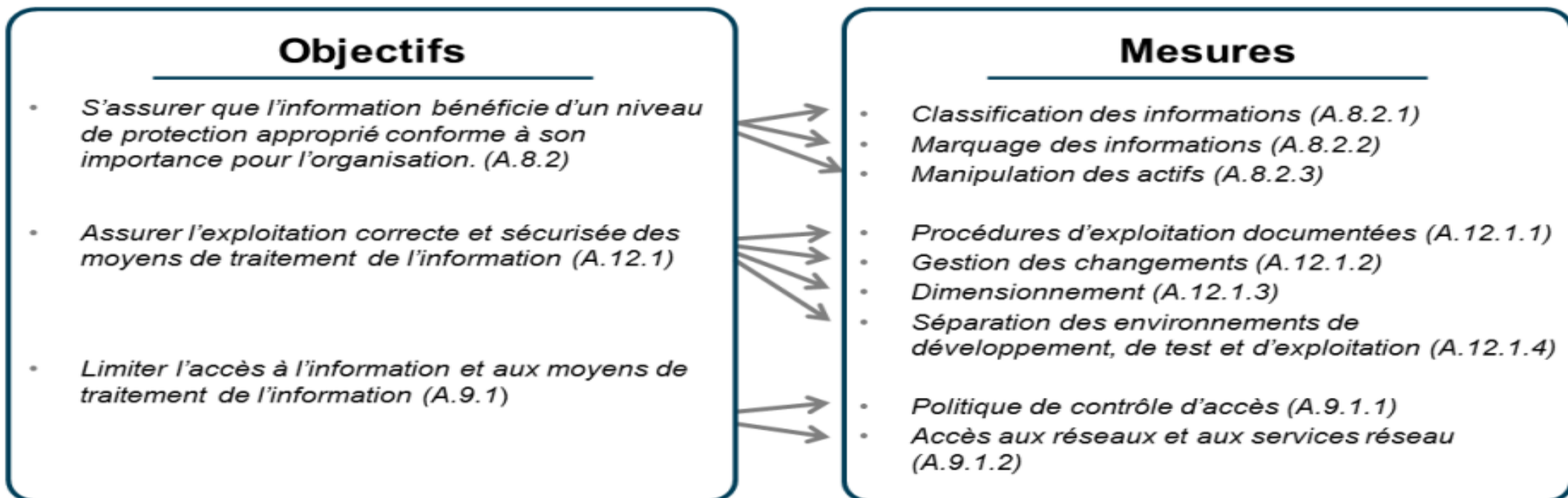
Mesure légale

Les mesures liées à l'application d'une loi, d'exigences réglementaires ou d'obligations contractuelles.

OBJECTIF D'UNE MESURE DE SECURITE

L'objectif d'une mesure de sécurité est de déclarer en décrivant ce qui est attendu de la mise en œuvre des mesures de sécurité (*ISO 27000, clause 2.17*).

ISO/IEC 27001, Annexe A



Source:PECB

IV-PROGRAMME DU MANAGEMENT DU RISQUE

PRINCIPE DE MANAGEMENT DU RISQUE

Le management du risque: activités coordonnées visant à diriger et piloter un organisme vis-à-vis du risque.

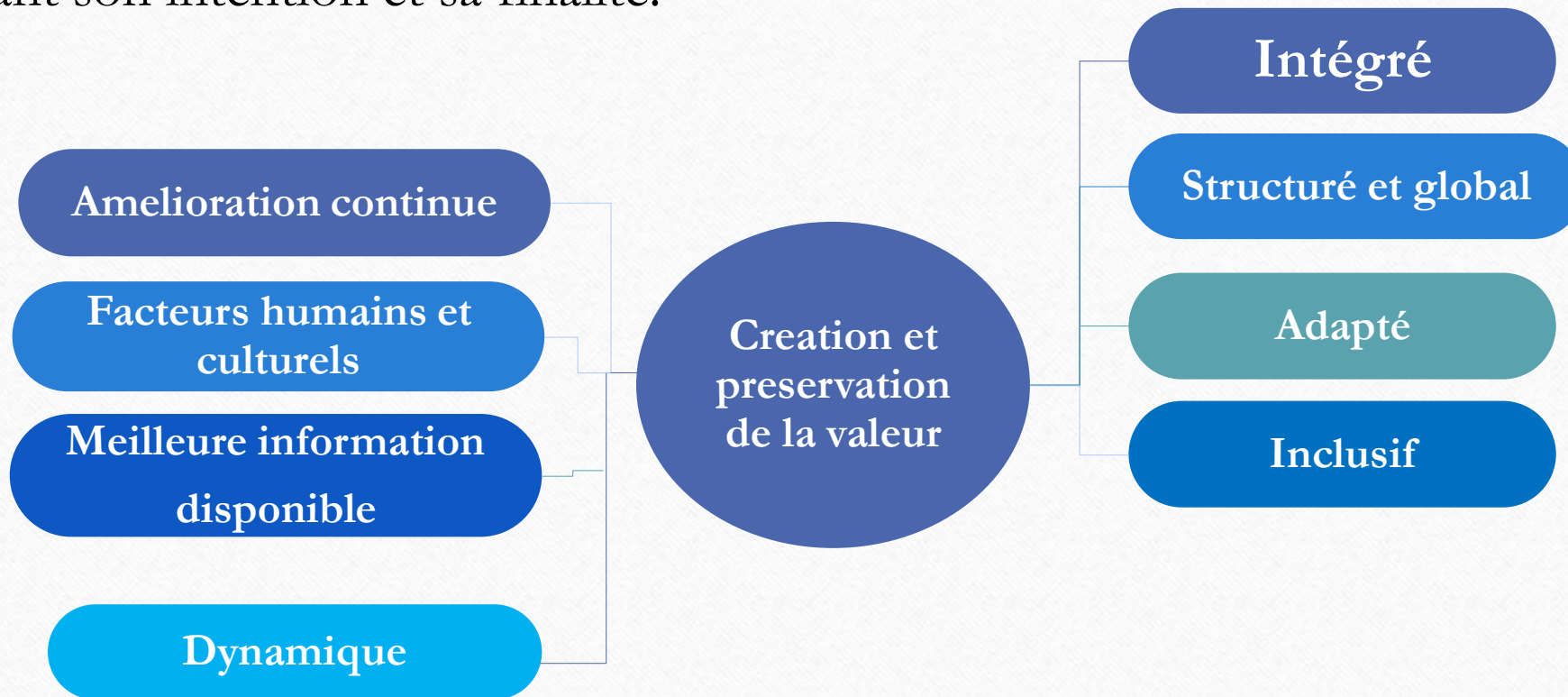
Le management du risque inclut généralement l'appréciation du risque, le traitement du risque, l'acceptation du risque et la communication relative au risque.

Le système de management du risque est l'ensemble d'éléments du système de management qui peuvent inclure la planification stratégique, la prise de décision et d'autres processus vis-à-vis du risque.

IV-PROGRAMME DU MANAGEMENT DU RISQUE

PRINCIPE DE MANAGEMENT DU RISQUE

Les principes de management fournissent les grands axes relatifs aux caractéristiques d'un management du risque efficace et efficient ,en communiquant sa valeur et en expliquant son intention et sa finalité.



IV-PROGRAMME DU MANAGEMENT DU RISQUE

AVANTAGE DU MANAGEMENT DU RISQUE

Le management du risque permet à une organisation de s'assurer qu'elle connaît et comprend les risques auxquels elle est confrontée.



Source:PECB

EXERCICE 2

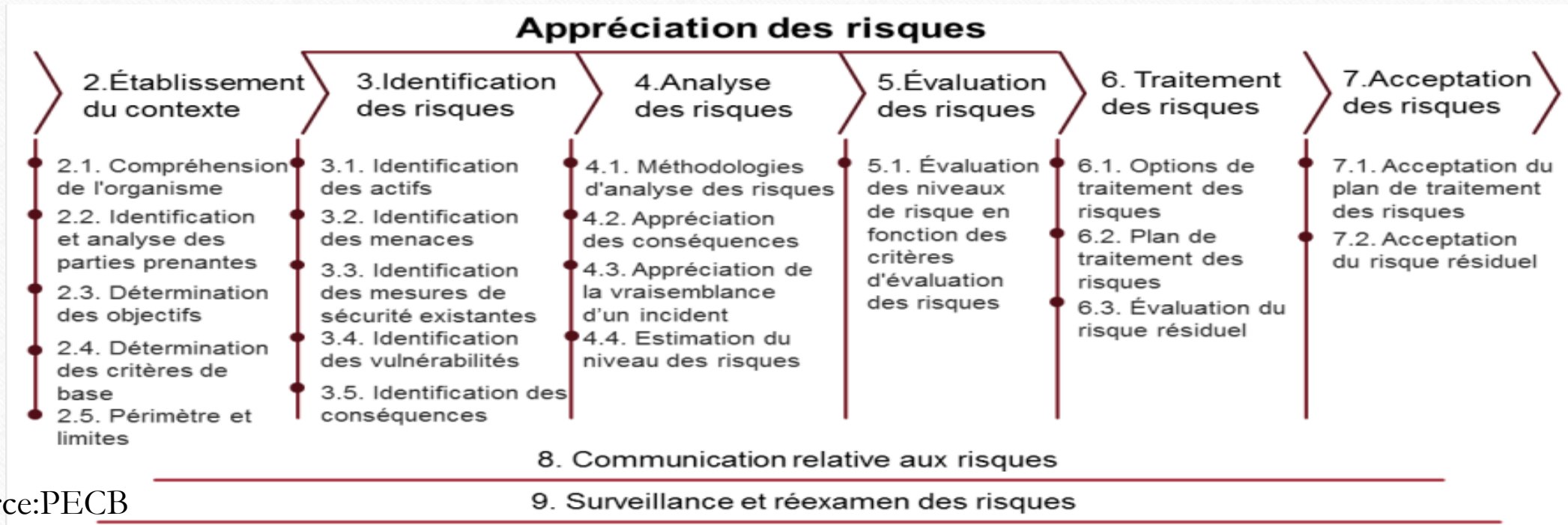
Exercice 2 : Gestion des risques

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

IV-PROGRAMME DU MANAGEMENT DU RISQUE

PROGRAMME DE GESTION DES RISQUES

La gestion des risques est l'ensemble des processus permettant de gérer le risque sur une base continue afin de le surveiller et de le maintenir à un niveau acceptable pour l'organisme. L'appréciation des risques est définie comme le processus permettant d'identifier, d'estimer et d'évaluer le risque d'un organisme.

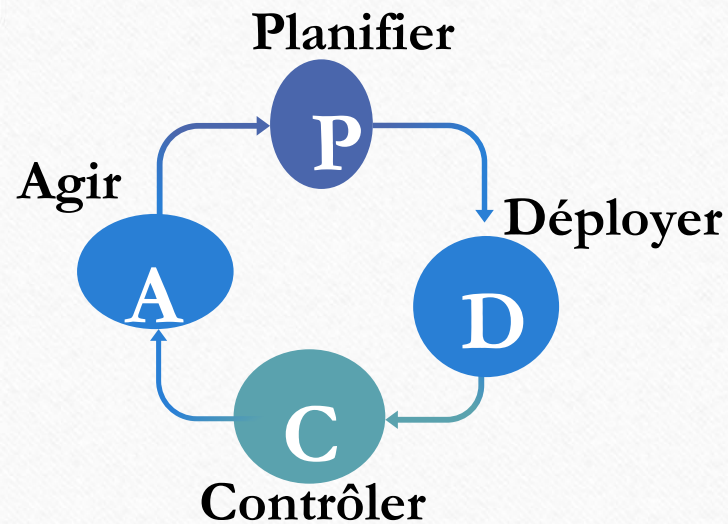


Source:PECB

IV-PROGRAMME DU MANAGEMENT DU RISQUE

PROGRAMME DE GESTION DES RISQUES (Approche processus)

La 27005 adopte le modèle de processus "Plan-Do-Check-Act" (PDCA) ou la roue de Deming qui est appliquée à la structure de tous les processus dans un SMSI.

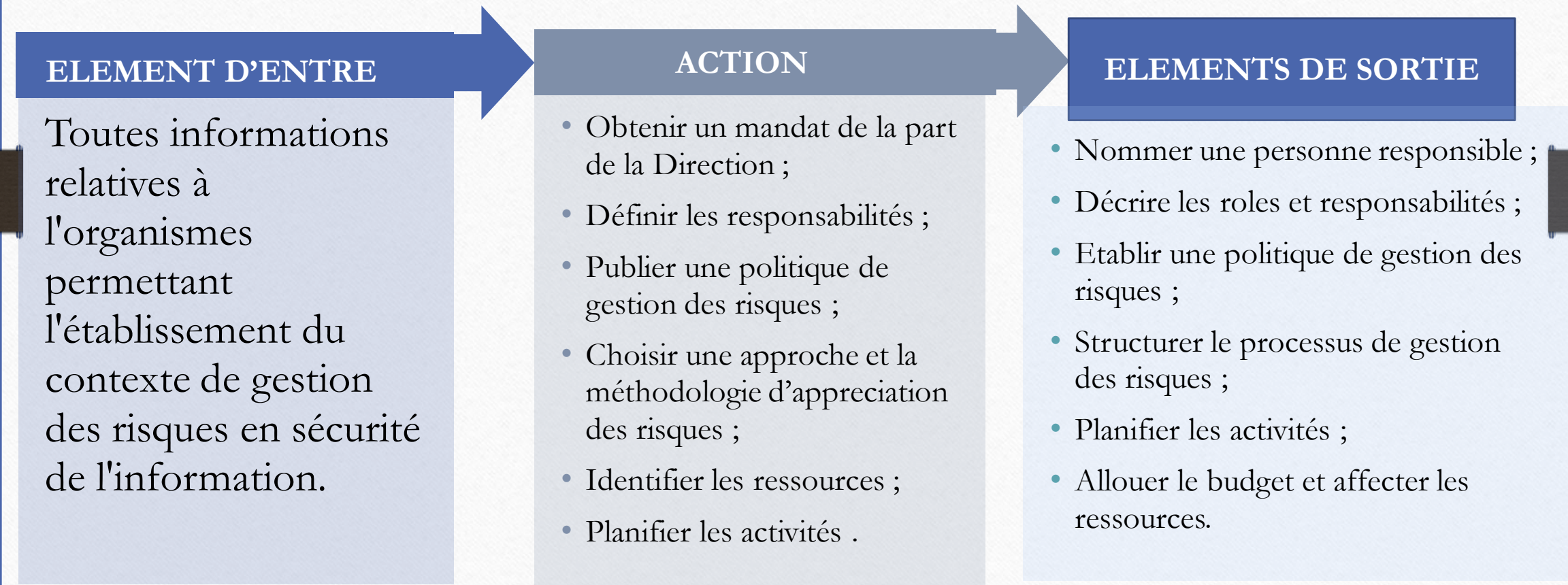


Processus MSI	Processus de gestion du risque en sécurité de l'information
Planifier (établir le système de management)	Établir la politique, les objectifs, les procédures et les processus liés à la gestion des risques et à l'amélioration de la sécurité de l'information
Déployer (mettre en œuvre et exploiter le système de management)	Mettre en œuvre et appliquer la politique, les contrôles, les processus et les procédures du système de management
Contrôler (surveiller et réexaminer le système de management)	Évaluer et, si applicable, mesurer les performances du processus par rapport à la politique, aux objectifs et à l'expérience pratique, et communiquer les résultats à la direction pour examen
Agir (maintenir et améliorer le système de management)	Prendre des actions correctives et préventives, sur la base des résultats de l'audit interne et de la revue de direction, pour améliorer continuellement le système

IV-PROGRAMME DU MANAGEMENT DU RISQUE

PLANIFICATION D'UN PROGRAMME DE GESTION DES RISQUES

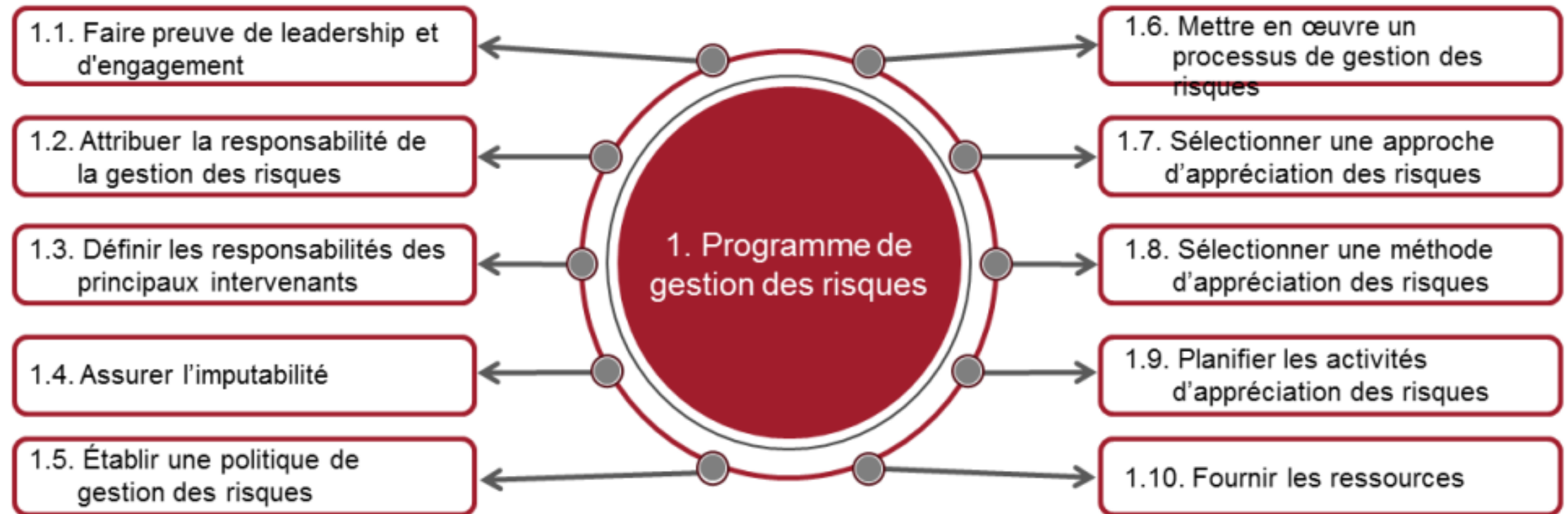
La planification et les responsabilités en matière de gestion des risques en sécurité de l'information au sein de l'organisme devraient être mises en œuvre et maintenues.



IV-PROGRAMME DU MANAGEMENT DU RISQUE

LISTE DES ACTIVITES

La 27005 adopte le modèle de processus "Plan-Do-Check-Act" (PDCA) ou la roue de Deming qui est appliquée à la structure de tous les processus dans un SMSI.



Source:PECB

IV-PROGRAMME DU MANAGEMENT DU RISQUE

COMPRENDRE L'ORGANISME ET SON CONTEXTE

La conception du cadre organisationnel de management du risque comprend l'analyse et la compréhension du contexte externe et interne de l'organisme.

Comprendre l'organisme est indispensable avant de commencer un projet d'évaluation des risques.

L'identification de la structure interne de l'organisme aidera à comprendre le rôle et l'importance de chaque division dans le processus de réalisation des objectifs de l'organisme.

ISO/IEC 27005, article 7.1 Établissement du contexte

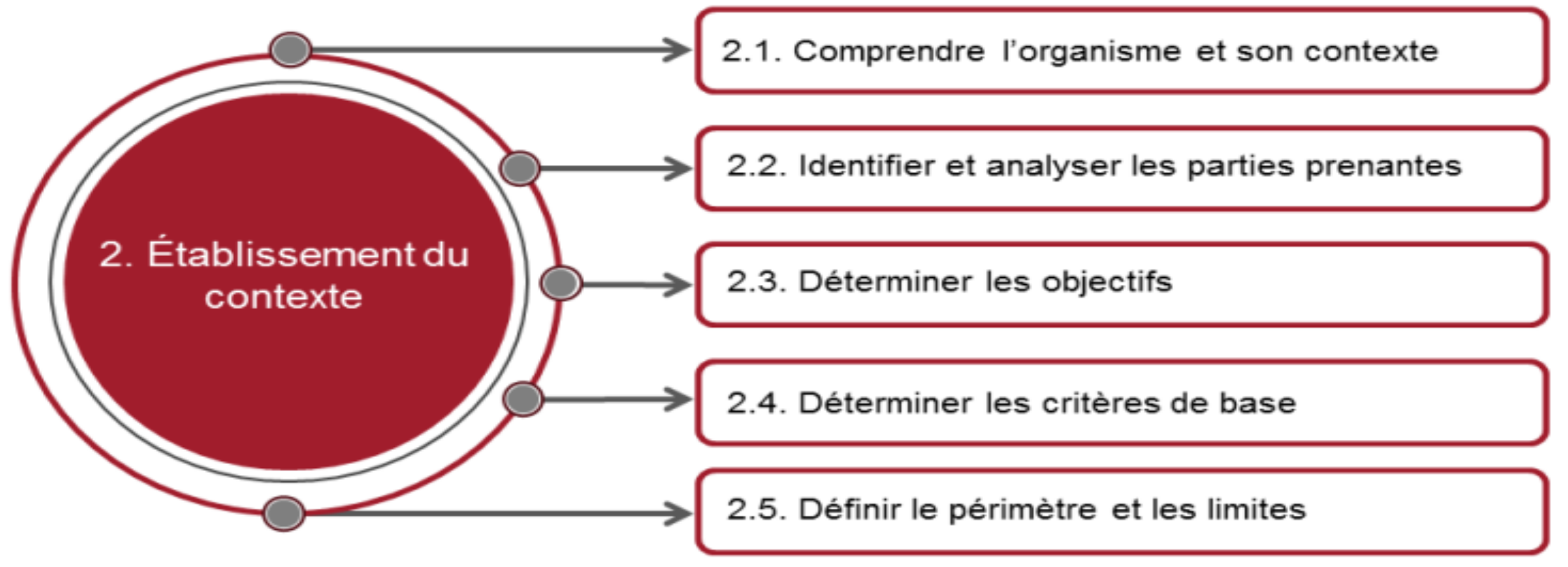
Élément d'entrée : Toutes les informations relatives à l'organisme permettant l'établissement du contexte de la gestion des risques en sécurité de l'information.

Action: Il convient d'établir le contexte externe et interne de la gestion des risques en sécurité de l'information, de définir le domaine d'application et ses limites .

IV-PROGRAMME DU MANAGEMENT DU RISQUE

ÉTABLISSEMENT DU CONTEXTE

LISTE DES ACTIVITES



Source:PECB

IV-PROGRAMME DU MANAGEMENT DU RISQUE

ÉTABLISSEMENT DU CONTEXTE EXTERNE ET INTERNE DE L'ORGANISME.

Plusieurs modèles ont été développés pour analyser et comprendre le contexte stratégique d'un organisme.

Puisque la 27005 n'offre pas de méthode pratique pour analyser le contexte d'un organisme, l'organisme est libre de choisir les outils qu'il juge les plus utiles.

Plusieurs méthodologies existent pour comprendre comment un organisme fonctionne, il est important d'identifier les caractéristiques des facteurs environnementaux externes et internes qui vont influencer la gestion des risques: mission, activités principales, parties prenantes, etc.

Ci-dessous certains des modèles les plus utilisés :

- **Analyse SWOT** (Forces-Faiblesses-Opportunités-Menaces) ;
- **Analyse PEST** (politique, économique, social, technologique) ;
- **L'analyse des cinq forces de Porter** .

IV-PROGRAMME DU MANAGEMENT DU RISQUE

ÉTABLISSEMENT DU CONTEXTE EXTERNE ET INTERNE DE L'ORGANISME.

LE CONTEXTE EXTERNE COMPREND

L'environnement culturel ,social ,politique ,légal ,réglementaire ,financier ,technologique ,naturel et concurrentiel ,au niveau international ,national régional ou local.

Les facteurs et tendances ayant un impact déterminant sur les objectifs de l'organisme ;

Les relations avec les parties prenantes externes ,les perceptions et valeurs relatives à celles-ci.

LE CONTEXTE INTERNE COMPREND

La gouvernance ,la structure organisationnelle ,les rôles et les responsabilités ;

Les politiques, objectifs et stratégies ;

Les capacités ,en termes de ressources et de connaissances ;

Le système d'information ,flux d'information et processus de prise de décision;

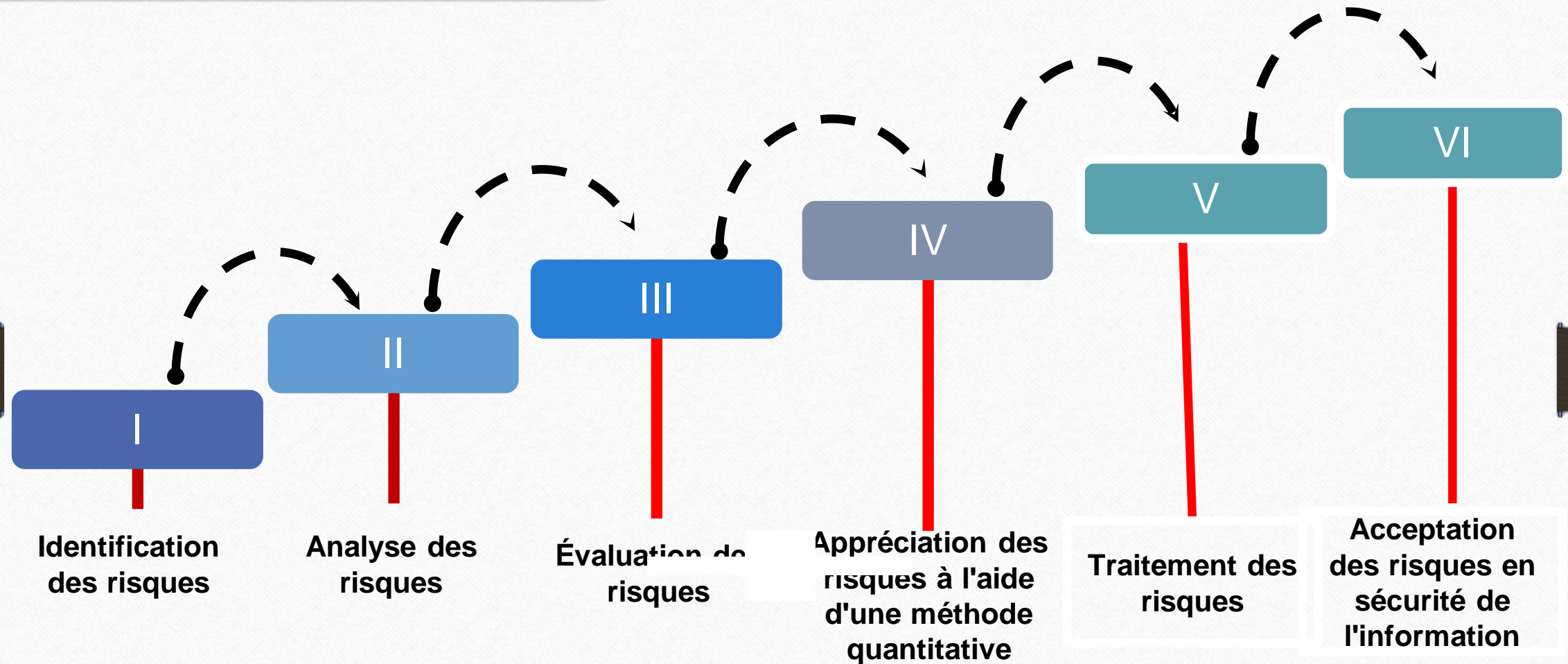
Les relations avec les parties prenantes internes ;

La culture de l'organisme ;

Etc....

Jour 3 à 6 : Identification, appréciation, évaluation, traitement, acceptation, communication et surveillance du risque selon l'ISO/IEC 27005

PLAN



OBJECTIFS PÉDAGOGIQUES

COMPÉTENCES VISÉES :

A la fin de ce module vous serez capable d'acquérir des connaissances pour:



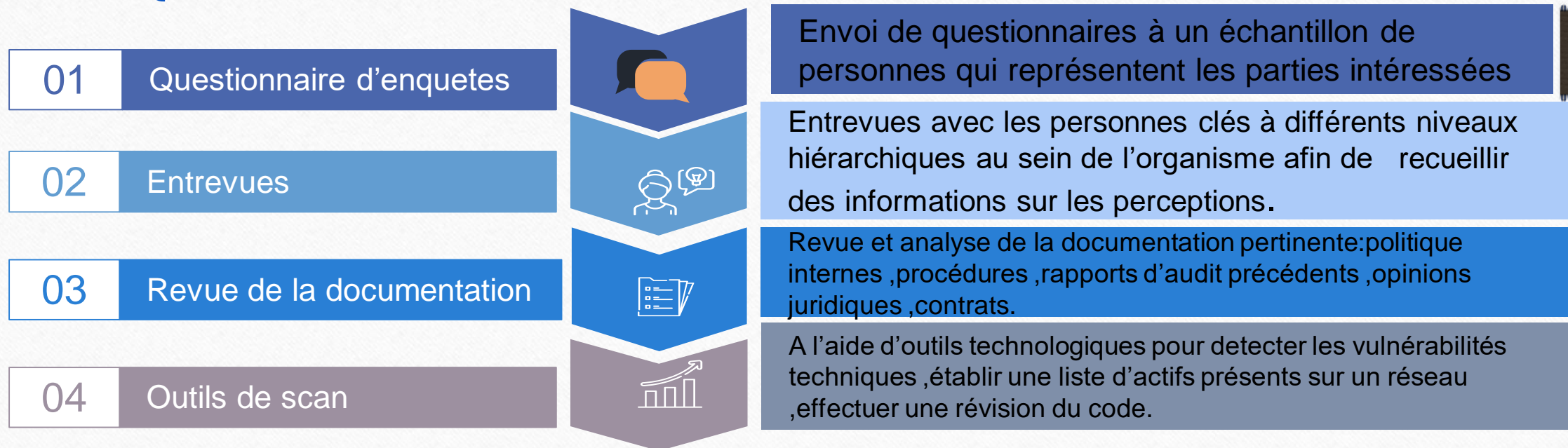
I-IDENTIFICATION DES RISQUES

L'objectifs de l'identification du risque est de déterminer les événements pouvant se produire et causant une perte potentielle. Dans la phase d'identification du risque, tous les risques éventuels devraient être indiqués sous forme de scénarios.

Il convient d'identifier les risques dont la source est ou non sous le contrôle de l'organisme .

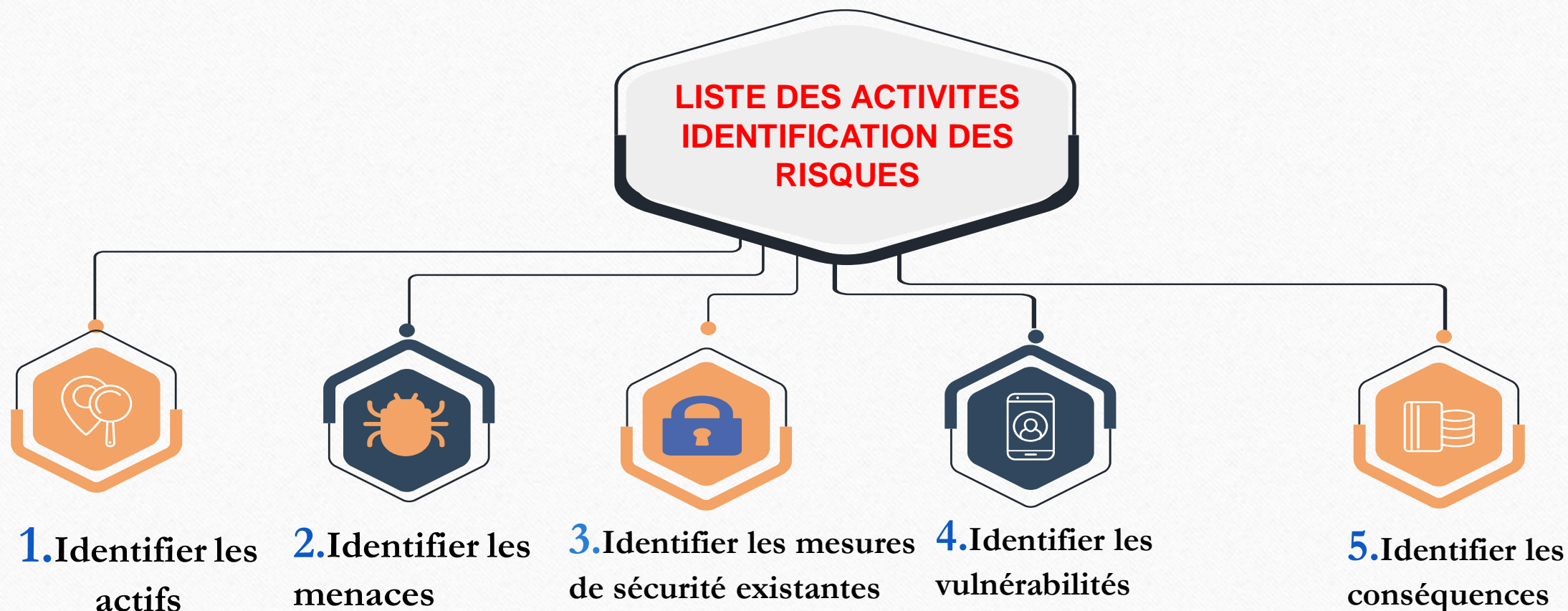
L'équipe de gestion des risques devrait s'appuyer sur une connaissance détaillée du risque à partir de la collecte d'informations obtenues à partir de plusieurs parties intéressées.

TECHNIQUES DE COLLECTE DE L'INFORMATION



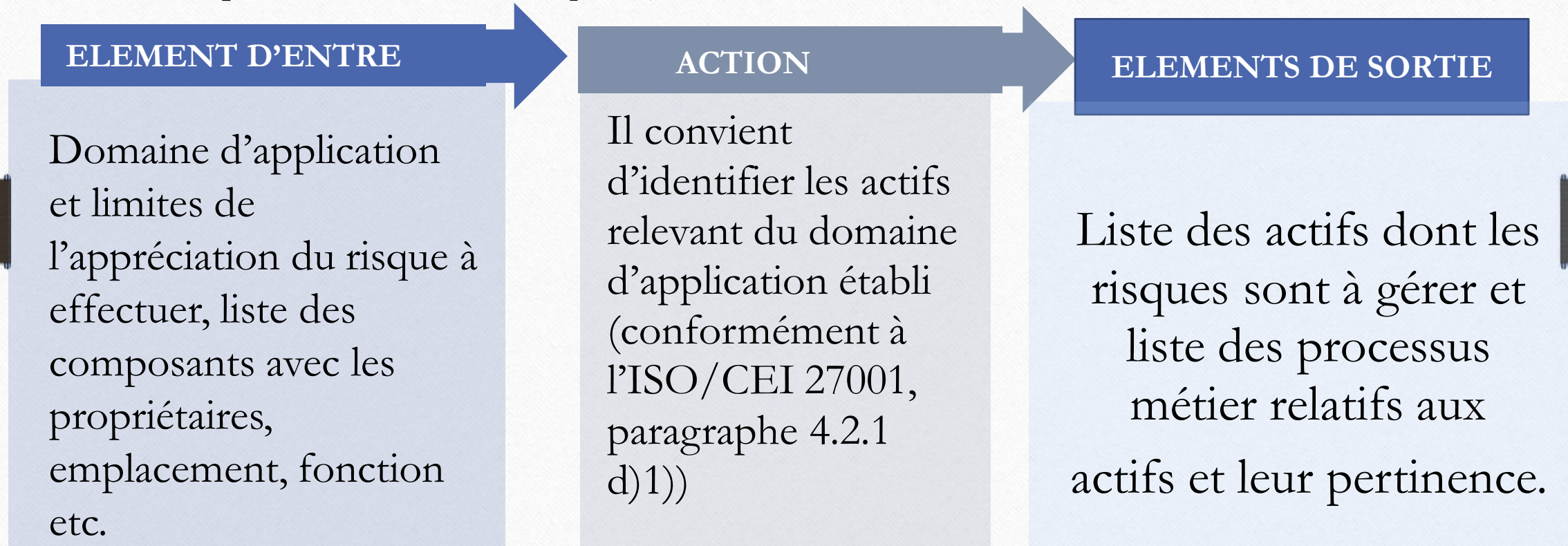
I-IDENTIFICATION DES RISQUES

La collecte d'informations obtenues à partir de plusieurs parties intéressées ,peuvent également aider à déterminer dans quelle mesure les pratiques de l'organisme sont cohérentes et bien comprises et peuvent elles-mêmes être une source pour établir la liste des activités d'identification des risques.



I-1. Identifier les actifs

Un actifs désigne tout élément ayant de la valeur pour l'organisme et nécessitant une protection (biens essentiels). Il convient d'identifier les actifs à un niveau de détail adapté qui fournisse suffisamment d'informations pour l'évaluation des risques. (**ISO/IEC 27005, article 8.2.1.2 Identification des actifs**)

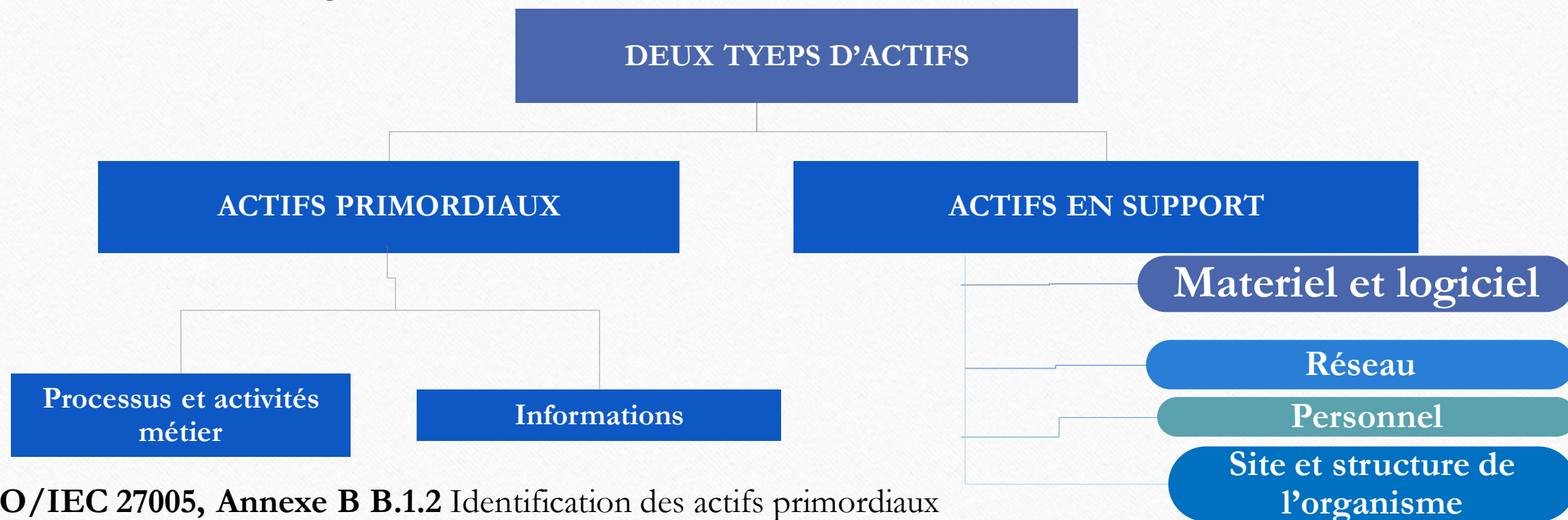


L'identification des actifs devrait être limité à ceux qui ont **la plus grande valeur à l'organisme**.

I-1. Identifier les actifs (suite)

ISO/IEC 27005 divise les actifs en deux grandes catégories :

1. Les **actifs primordiaux** désignent les actifs qui contribuent au processus d'analyse du risque. Ces actifs comprennent les processus opérationnels et l'information.
2. Les **actifs en support** comprennent le matériel, les logiciels, les réseaux informatiques, le personnel, les sites et les structures organisationnelles.



ISO/IEC 27005, Annexe B B.1.2 Identification des actifs primordiaux

I-1. Identifier les actifs (suite)

ISO 9000, article 3.4.1 Processus

Ensemble d'activités corrélées ou en interaction qui utilise des éléments d'entrée pour produire un résultat escompté.

Les processus métier devrait soutenir l'organisme dans la réalisation de sa mission , ils sont divisés en sous-processus, activités et tâches Exemple :

1. Processus : Comptabilité
2. Sous-processus : Gérer les comptes clients, les états de paie, etc.
3. Activité : Créer des factures, écrire le rapport mensuel, etc.
4. Tâches : Vérifier l'adresse courante du client, ajouter des informations dans le système de comptabilité, etc.

Les actifs en support sont généralement plus faciles à identifier parce qu'il s'agit des actifs les plus tangibles, telles que des installations, du mobilier et des fournitures de bureau, le matériel informatique et les logiciels.

I-1. Identifier les actifs (suite)

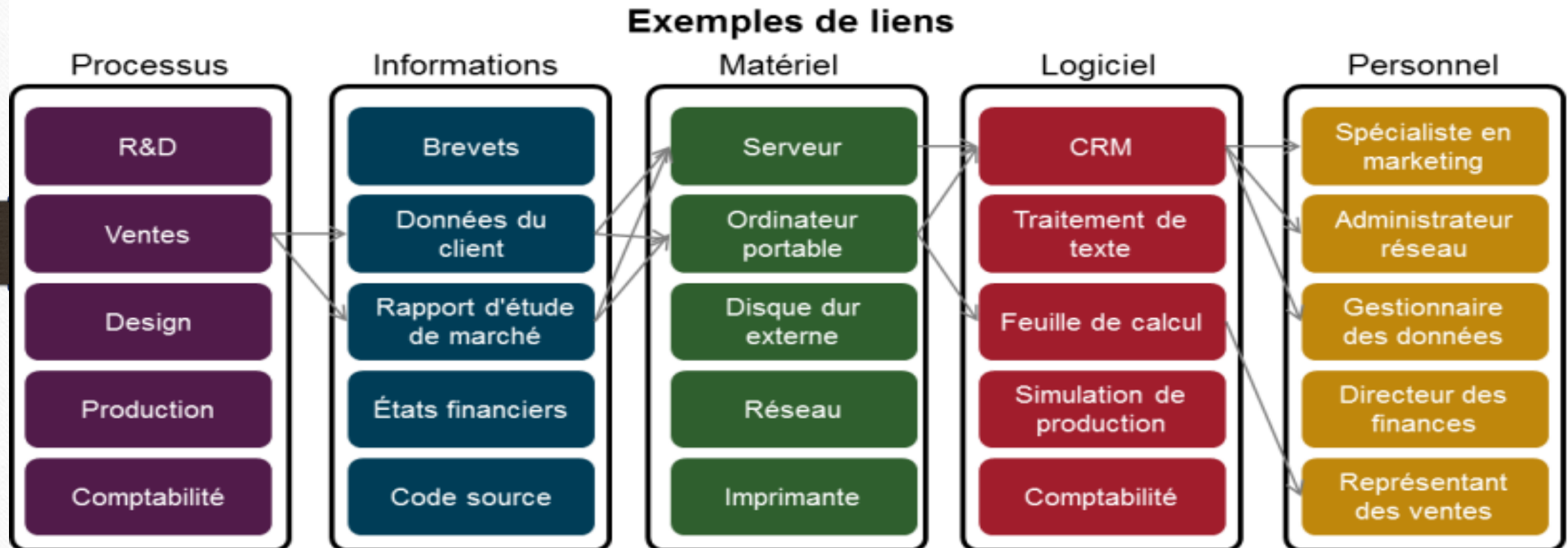
Identification des actifs en support

Catégorie	Définition	Exemple
Matériel	Le type relatif au matériel se compose de tous les éléments physiques prenant en charge des processus	Serveur , ordinateur portable ,imprimante ,Disque dur
Logiciels	Tous les programmes contribuant au fonctionnement d'un ensemble de traitement de données.	Système d'exploitation, logiciels de traitement de texte, ERP
Réseau	Tous les dispositifs de télécommunication utilisés pour interconnecter plusieurs ordinateurs ou éléments distants d'un système d'information.	Routeur, switch , câble réseau , adaptateur Ethernet
Personnel	Tous les personnes impliqués dans le système d'information.	Propriétaire des actifs ,utilisateurs ,développeur , clients
Site	Lieux physiques requis pour que l'activité fonctionne.	Bureaux , zone sécurisée ,salle serveurs ,résidence du personnel ,système de climatisation.
Structure de l'organisme	Cadre organisationnel, assigné pour exécuter les activités.	Siège social, département ,équipes projet ,prestataires ,fournisseurs.

ISO/IEC 27005, Annexe B.1.2 fournit des sous-catégories et des exemples pour chaque catégorie d'actifs présentée dans le tableau ci-dessus.

I-1. Identifier les actifs (suite)

Afin d'obtenir une appréciation fiable de la valeur d'un actif et d'évaluer les risques auxquels il peut être soumis, la relation entre les principaux actifs doit être analysée.



Source:PECB

I-1. Identifier les actifs (suite)

Un propriétaire doit être identifier pour chaque actif , le propriétaire n'a pas nécessairement de droits de propriété sur l'actif ,mais il est responsable de la production du développement ,de l'entretien de l'exploitation et de la sécurité de l'actif.

Le propriétaire est souvent la personne la mieux placée pour déterminer la valeur de l'actif pour l'organisme et pour conserver la connaissance de son statut et de sa localisation.

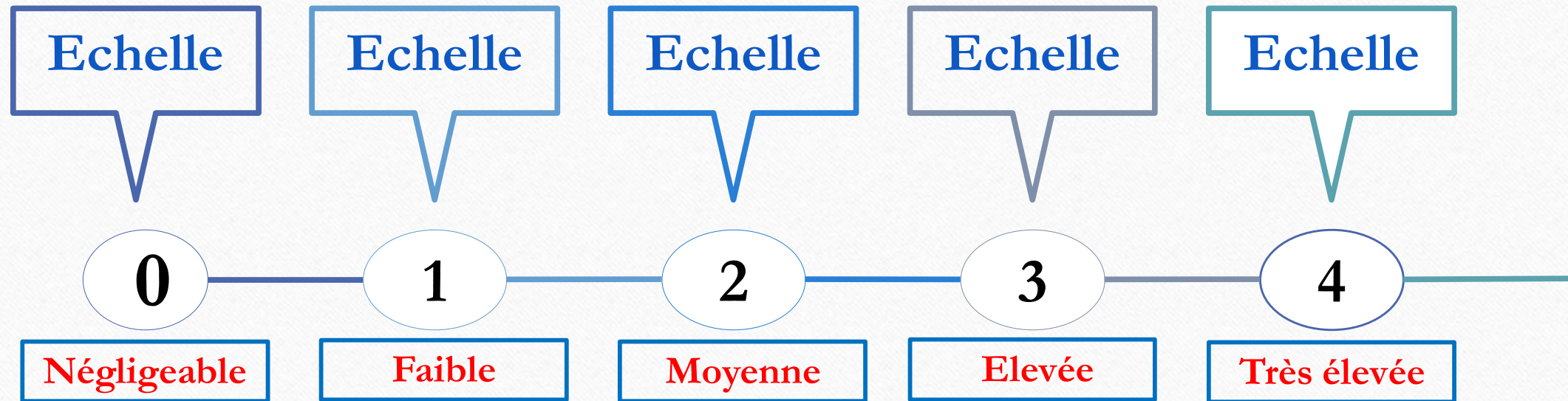
Par exemple, le directeur des ventes est identifié comme le propriétaire et le gestionnaire de bases de données client (le principal actif). En revanche, le serveur hébergeant la base de données (l'actif) peut être sous la responsabilité du responsable des DBA.

ISO/IEC 27005, Annexe B.2 Échelle ,un organisme doit définir ses propres paramètres à l'échelle des valeurs des actifs.

Une fois les critères à considérer établis, il est bon que l'organisme convienne d'une échelle à utiliser. La première étape consiste à déterminer le nombre de niveaux à utiliser. Il n'existe aucune règle relative au nombre de niveaux le plus adapté.

I-1. Identifier les actifs (suite)

Exemple d'échelle de valeur d'actifs



Il incombe entièrement à l'organisme de décider ce qui est considéré comme une conséquence «faible» ou «élevée». Une conséquence désastreuse pour un petit organisme peut paraître faible, voire même négligeable pour un très grande organisme.

I-1. Identifier les actifs (suite)

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.

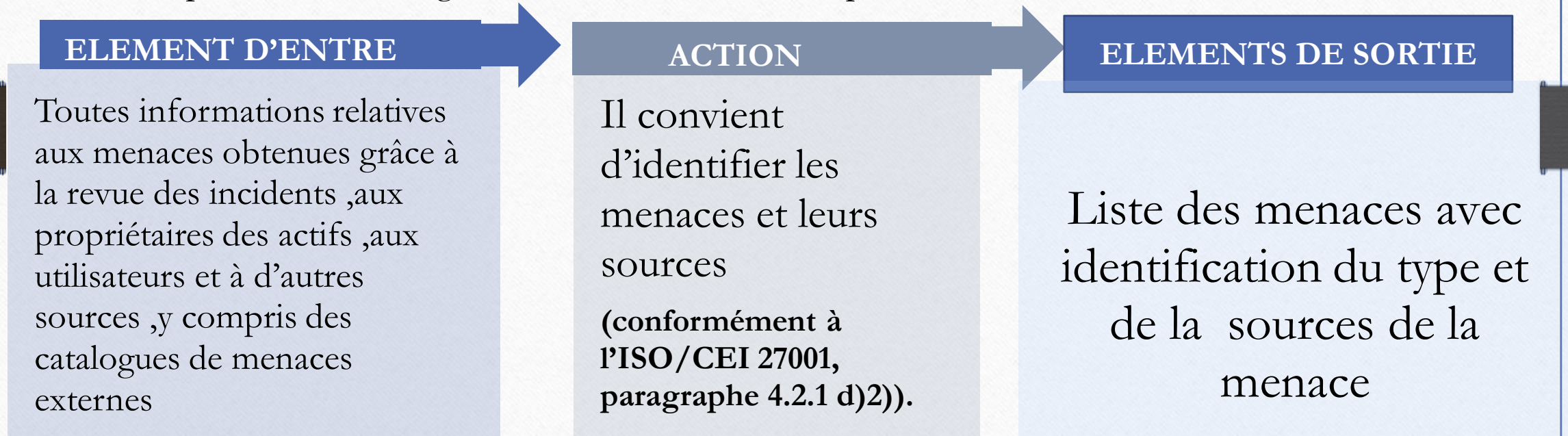
Durée de l'exercice : 20 minutes

I-2. Identifier les menaces

La menace est la cause potentielle d'incident indésirable ,ce qui peut nuire à un système ou à un organisme (ISO/IEC 27000).

Une menace est susceptible d'endommager les actifs tels que des informations ,des processus et des systèmes et par conséquent ,des organismes ISO/IEC 27005) .

Les menaces peuvent être d'origine naturelle ou humaine et peuvent être accidentelles ou délibérées.



De plus amples informations relatives aux types de menace sont disponibles dans l'Annexe C de la ISO/IEC 27005.

I-2. Identifier les menaces

L'Annexe C de la norme ISO/IEC 27005 donne des exemples de menaces typiques qui peuvent être utilisées au cours du processus d'appréciation des risques .

Il convient d'utiliser la liste des menaces de l'Annexe C avec prudence ,l'utiliser comme un guide ou une liste de contrôle pour aider à organiser et à structurer la collecte et la compilation des données pertinentes sur les menaces plutôt que comme une liste de contrôle à suivre aveuglément.

Dans le tableau ci-dessous ,une liste de type de menace ,cette liste n'est pas complète et ne peut prétendre à l'exhaustivité, car de nouvelles menaces apparaissent régulièrement en raison, entre autres, de l'évolution des technologies et des capacités des agents de menace.

Type de menace	Damage physique	Catastrophes naturelles	Perte de services essentiels	Perturbation due à Rayonnements	Compromission d'informations	Défaillances techniques	Actions non autorisées	Compromission des fonctions
EXEMPLE	Incendie	Phénomène climatique	Panne du système de climatisation	Rayonnements électromagnétiques	Vol de supports ou de documents	Panne de matériel	Utilisation non autorisée du matériel	Abus des droits
	Dégât des eaux	Inondation	Perte de la source d'alimentation en électricité	Rayonnements thermiques	Données provenant de sources douteuses	Dysfonctionnement du logiciel	Reproduction frauduleuse de logiciel	Violation de la disponibilité du personnel

I-2. Identifier les menaces

Les menaces peuvent être délibérées (D), accidentelles (A) ou environnementales (E) (naturelles), et peuvent résulter, à titre d'exemples, de dommages ou de la perte de services essentiels. **D** est utilisé pour les actions délibérées destinées aux actifs informationnels, **A** est utilisé pour toutes les actions humaines qui peuvent endommager les actifs informationnels de manière accidentelle et **E** est utilisé pour tous les incidents qui ne reposent pas sur des actions humaines. Les groupes de menaces ne sont pas classés par ordre de priorité.

L'identification de la source permet d'analyser plus en détail les caractéristiques d'une menace et comment sélectionner le traitement approprié pour s'en protéger.

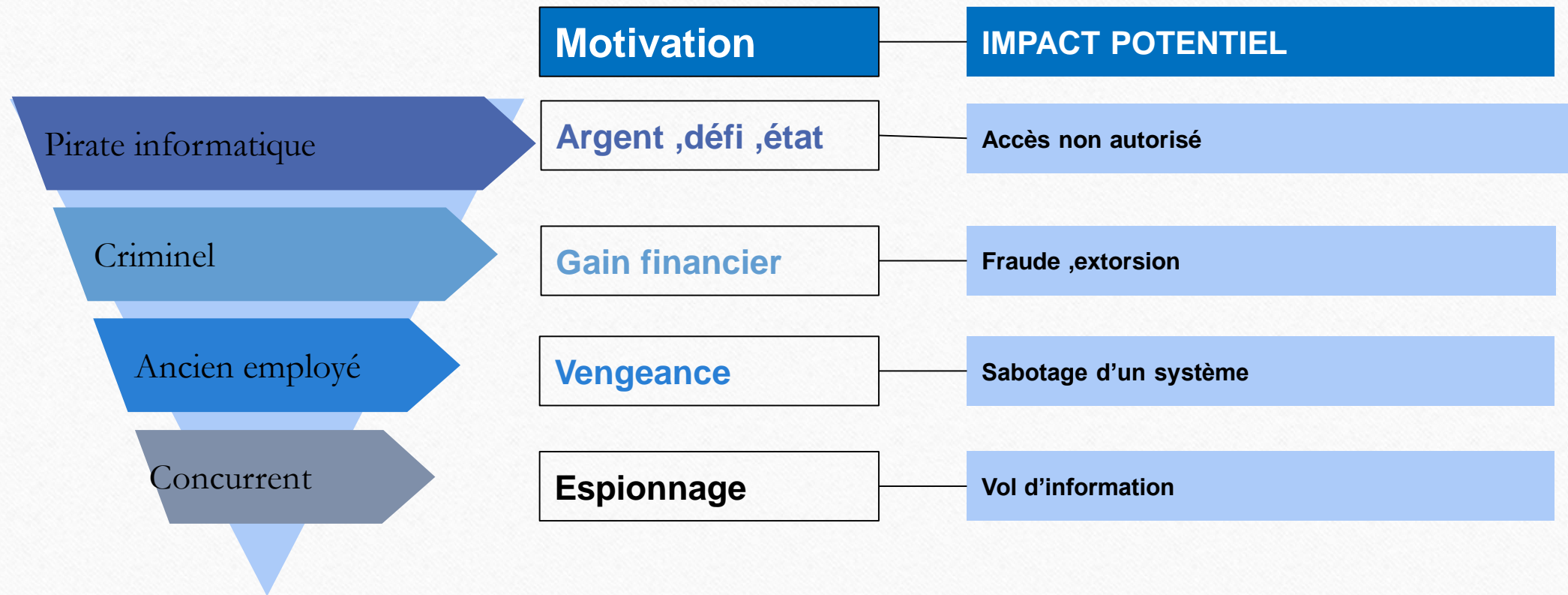
Exemple de source de menaces

TYPE	MENACE	ORIGINE
Dommage physique	Incendie	A,D,E
Compromission des fonctions	Abus des droits	A,D
Compromission d'informations	Vol de matériel	D

TYPE	MENACE	ORIGINE
Catastrophes naturelles	Tremblement de terre	E
Actions non autorisées	Reproduction frauduleuse de logiciel	D
Défaillances techniques	Dysfonctionnement du matériel	A

I-2. Identifier les menaces

Au cours des dernières années, la motivation des gens à mettre en place des menaces à la sécurité de l'information a connu une évolution majeure, passant du simple vandalisme au gain, notamment par la fraude et le marketing ultra-agressif comme publicité sauvage «en ligne» (comme le spam).



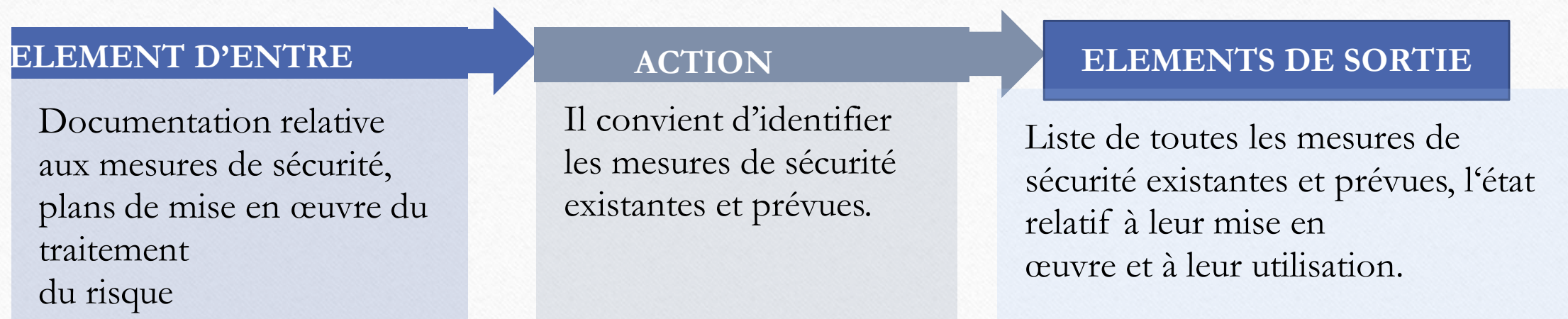
I-3. Identifier les mesures de sécurité existantes

ISO/IEC 27005, article 8.2.1.4 Identification des mesures de sécurité existantes.

Il convient de procéder à une identification des mesures de sécurité existantes pour éviter des travaux ou des coûts inutiles dus, par exemple, à une redondance des mesures de sécurité.

Une mesure de sécurité existante ou prévue peut être identifiée comme étant inefficace, insuffisante ou injustifiée.

Si elle s'avère injustifiée ou insuffisante, il convient de contrôler la mesure de sécurité afin de déterminer s'il convient de la retirer, de la remplacer par une autre mesure de sécurité plus adaptée, ou s'il convient de la laisser en place, par exemple pour des raisons de coûts.



I-3. Identifier les mesures de sécurité existantes (Suite)

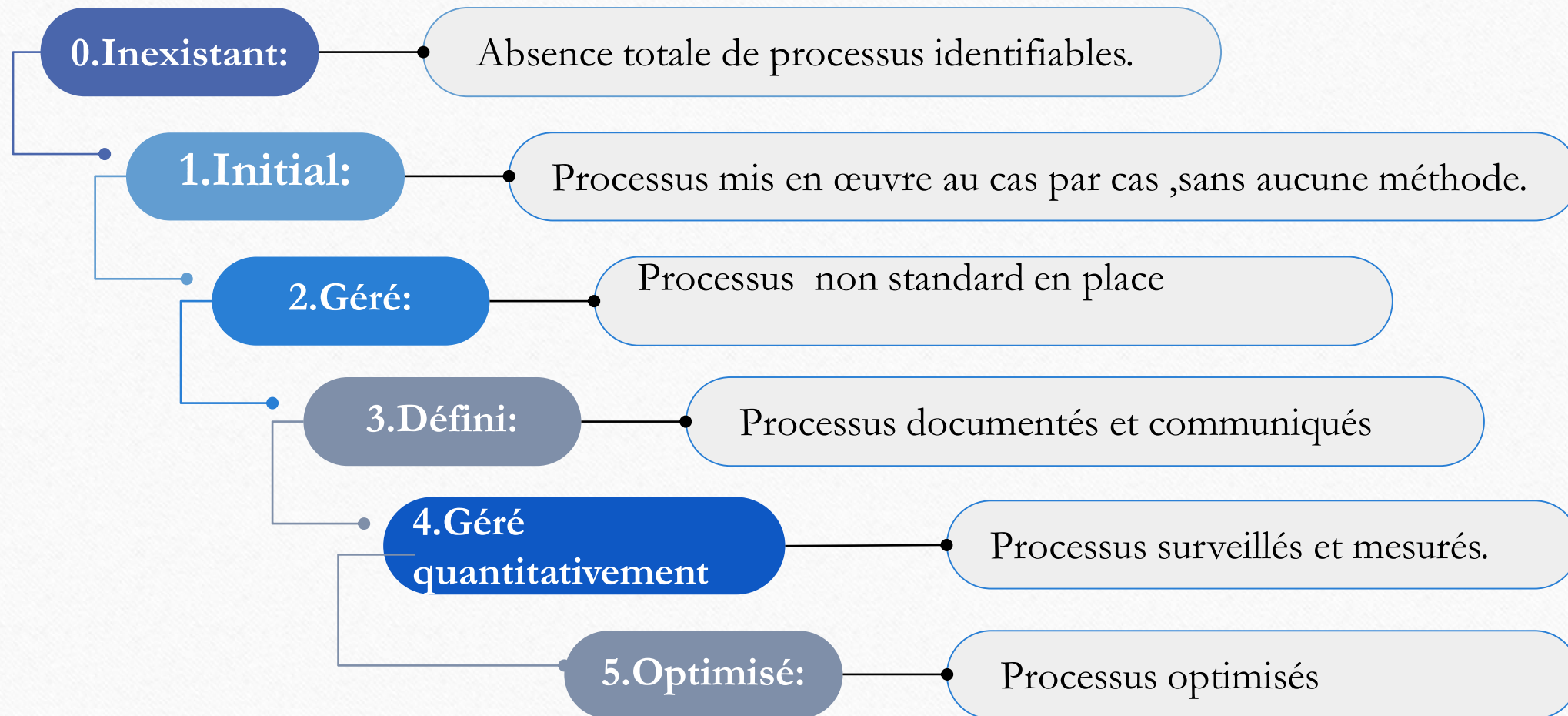
ISO/IEC 27005 8.2.1.4 Identification des mesures de sécurité existantes

Les activités suivantes peuvent s'avérer utiles pour l'identification des mesures de sécurité existantes ou prévues :

- ☐ le réexamen des documents contenant des informations relatives aux mesures de sécurité (par exemple, les plans de mise en œuvre du traitement du risque). Si les processus de gestion de sécurité de l'information sont bien documentés, il convient que toutes les mesures de sécurité existantes ou prévues, ainsi que le statut de leur mise en œuvre, soient mis à disposition;
- ☐ la vérification avec les personnes responsables de la sécurité de l'information (par exemple un responsable de la sécurité de l'information et un responsable de la sécurité du système d'information, un responsable de la sécurité physique ou un responsable des opérations) et avec les utilisateurs afin de vérifier quelles mesures de sécurité sont réellement mises en œuvre pour le processus d'information ou le système d'information considérés;
- ☐ la revue sur site des mesures de sécurité physiques, en comparant les mesures mises en œuvre à la liste des mesures à déployer et en vérifiant les mesures mises en œuvre pour savoir si elles fonctionnent correctement et efficacement;
- ☐ l'examen des résultats des audits internes.

I-3. Identifier les mesures de sécurité existantes(Suite)

Les mesures de sécurité existantes peuvent être évaluées sur les niveaux de maturité.



I-3. Identifier les mesures de sécurité existantes (Suite)

Pour l'identification des mesures de sécurité existantes et prévues, on peut utiliser la liste des mesures de sécurité figurant dans la norme ISO/IEC 27002 (ou Annexe A de la norme ISO/IEC 27001). Cela permet d'avoir un aperçu de la situation actuelle en ce qui concerne les bonnes pratiques de sécurité.

Maitrise des risques de sécurité de l'information	Exigence	Description de la situation actuelle	Maturité actuelle	Maturité cible	Analyse des écarts	Responsable
7.2.1 Approche de gestion des risques	Il convient de choisir ou d'élaborer une approche de gestion des risques adaptée qui inclue des critères d'évaluation d'impact et les critères d'acceptation des risques	Une approche de gestion des risques existe et a été approuvée par la Direction ,mais le document n'a jamais été publié à tous les employés. Seul les participants impliqués dans la gestion des risques sont appelés à l'approuver. Le document n'est pas non plus facile à trouver sur l'intranet de l'organisme.	3	4	La publication n'est pas fournie de manière efficiente au sein de l'organisme	Coulibaly , Konan

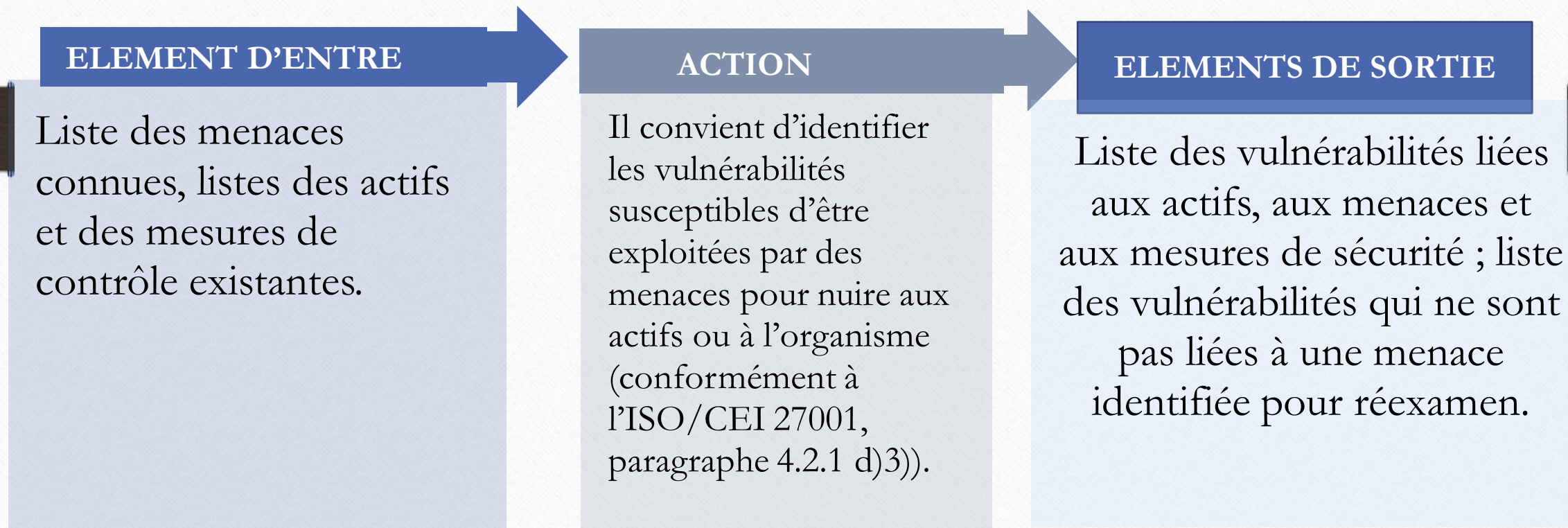
I-3. Identifier les mesures de sécurité existantes (Suite)

Maitrise des risques de sécurité de l'information	Exigence	Description de la situation actuelle	Maturité actuelle	Maturité cible	Analyse des écarts	Responsable
7.3 Domaine d'application et limites	Le champ d'application et les limites de la gestion des risques en matière de sécurité de l'information sont définis de manière à garantir que tous les actifs pertinents sont pris en compte dans l'appréciation des risques.	L'organisme n'a pas relié son information aux objectifs opérationnels stratégiques ,aux politiques stratégiques et aux processus opérationnels de l'organisme. Aucun calendrier n'est prévu pour l'examen.	1	5	L'examen des actifs informationnels de l'organisme et de leur exposition aux risques n'est pas à l'ordre du jour de l'examen annuel de la Direction de l'organisme.	Coulibaly , Konan

I-4. Identifier les vulnérabilités

Cette étape permet de déterminer les vulnérabilités spécifiques aux actifs compris dans le périmètre (domaine d'application). L'étude de vulnérabilité se fait généralement avec les mêmes participants qui ont été impliqués dans l'étude des origines des menaces.

L'évaluation de la vulnérabilité peut être compliquée par une idée fausse que les faiblesses ou lacunes sont toujours associées à des caractéristiques négatives.



I-4. Identifier les vulnérabilités (Suite)

ISO /IEC 27005 8.2.1.5 Identification des vulnérabilités

- ☐ La présence d'une vulnérabilité n'entraîne pas de dommage en elle-même, puisque la présence d'une menace est nécessaire pour l'exploiter;
- ☐ Une vulnérabilité à laquelle ne correspond aucune menace peut ne pas exiger la mise en œuvre d'une mesure de sécurité, mais il convient qu'elle soit identifiée et surveillée en cas de changements ;
- ☐ Il convient de noter qu'une mesure de sécurité mal mise en œuvre, ou présentant un dysfonctionnement, ou encore utilisée de manière incorrecte peut constituer une vulnérabilité;
- ☐ Une mesure de sécurité peut s'avérer efficace, ou non, selon l'environnement dans lequel elle est mise en œuvre.
- ☐ Inversement, une menace à laquelle ne correspond aucune vulnérabilité peut ne pas entraîner de risque.
- ☐ Les vulnérabilités peuvent être liées à des propriétés de l'actif susceptibles d'être utilisées d'une manière, ou à des fins différentes de celles prévues lorsque l'actif a été acheté ou élaboré. Les vulnérabilités dues à différentes sources nécessitent d'être prises en compte, par exemple celles qui sont intrinsèques ou extrinsèques à l'actif.

I-4. Identifier les vulnérabilités (Suite)

ISO /IEC 27000 ,article 3.77

Vulnérabilités: Faille dans un actif ou dans une mesure de sécurité qui peut être exploitée par une ou plusieurs menaces.

01

Une vulnérabilité à laquelle ne correspond aucune menace peut ne pas exiger la mise en oeuvre d'une mesure de sécurité ,mais il convient qu'elle soit identifiée et surveillée en cas de changement.

02

Il convient de noter q'une mesure de sécurité mal mise en oeuvre ,ou présentant un dysfonctionnement ,ou encore utilisée de manière incorrecte peut constituer une vulnérabilité.

ISO /IEC 27005 ,Annexe D

L'Annexe D de la norme ISO/IEC 27005 fournit une typologie de classement des points vulnérables .

Cependant, cette liste de vulnérabilités n'est pas exhaustive et doit être utilisée avec prudence, car de nouvelles vulnérabilités apparaissent régulièrement en raison, entre autres, de l'évolution et des changements technologiques. Le tableau suivant fournit des exemples de vulnérabilités dans divers domaines de sécurité, y compris des exemples de menaces susceptibles d'exploiter ces vulnérabilités.

I-4. Identifier les vulnérabilités (Suite)

Type de vulnérabilité	Exemple de vulnérabilité	Exemples de menaces
Matériel	Maintenance insuffisante/mauvaise installation des supports de stockage	Violation de la maintenabilité du système d'information
Logiciel	Attribution erronée des droits d'accès	Abus de droits
	Interface utilisateur compliquée	Erreur d'utilisation
Réseau	Architecture réseau non sécurisée	Espionnage à distance
	Absence d'identification et d'authentification de l'expéditeur et du destinataire	Usurpation de droits
Personnel	Formation insuffisante à la sécurité	Erreur d'utilisation
	Absence de personnel	Violation de la disponibilité du personnel
Site	Réseau électrique instable	Perte de la source d'alimentation en électricité
	Emplacement situé dans une zone sujette aux inondations	Inondation
Organisme	Absence de procédure formelle relative à l'enregistrement et au retrait des utilisateurs	Abus de droits

I-4. Identifier les vulnérabilités (Suite)

ISO /IEC 27005 ,Annexe D, A.5 Méthodes d'appréciation des vulnérabilités techniques

Il est possible d'utiliser des méthodes proactives comme des tests du système d'information afin d'identifier les vulnérabilités par rapport à la criticité du système de technologie de l'information, des communications (TIC) et des ressources disponibles .

Les tests d'intrusion peuvent être utilisés pour compléter la revue des mesures de sécurité et garantir que les différents aspects du système TIC sont sécurisés.

Les méthodes de tests comprennent :

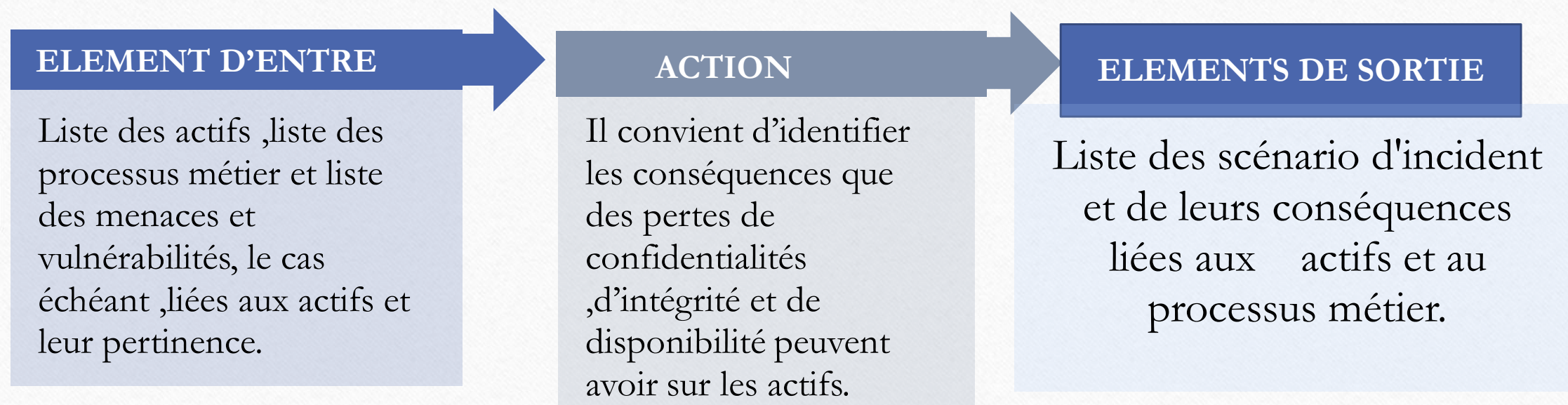


La présence d'une vulnérabilité ne cause pas de dommages en soi ; il doit y avoir une menace réelle de l'exploiter et la possibilité de causer des dommages à un actif.

I-5. Identifier les conséquences

La dernière étape de l'identification des risques est l'identification des conséquences des scénarios d'événements à risque.

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.



Les conséquences peuvent être calculées sur la base des titres financiers ou des échelles qualitatives. Ces effets peuvent être temporaires ou permanents, comme dans le cas de la destruction d'un actif.

I-5. Identifier les conséquences (Suite)

ISO /IEC 27000 ,Article 3.12 CONSÉQUENCE: effet d'un événement affectant les objectifs.

Note 1 à l'article:

Un événement peut engendrer une série de conséquences.

Note 2 à l'article:

Une conséquence peut être certaine ou incertaine; dans le contexte de la sécurité de l'information, elle est généralement négative.

Note 3 à l'article:

Les conséquences peuvent être exprimées de façon qualitative ou quantitative.

Note 4 à l'article:

Des conséquences initiales peuvent déclencher des réactions en chaîne.

Les conséquences de l'occurrence d'un risque peuvent être évaluées différemment en fonction de l'implication des parties intéressées dans l'évaluation des risques. Les impacts importants sur l'organisme devraient être documentés en conséquence.

I-5. Identifier les conséquences (Suite)

DISPONIBILITÉ

- Dégradation des performances
- Interruption de service
- Inaccessibilité du service
- Interruption des opérations

INTÉGRITÉ

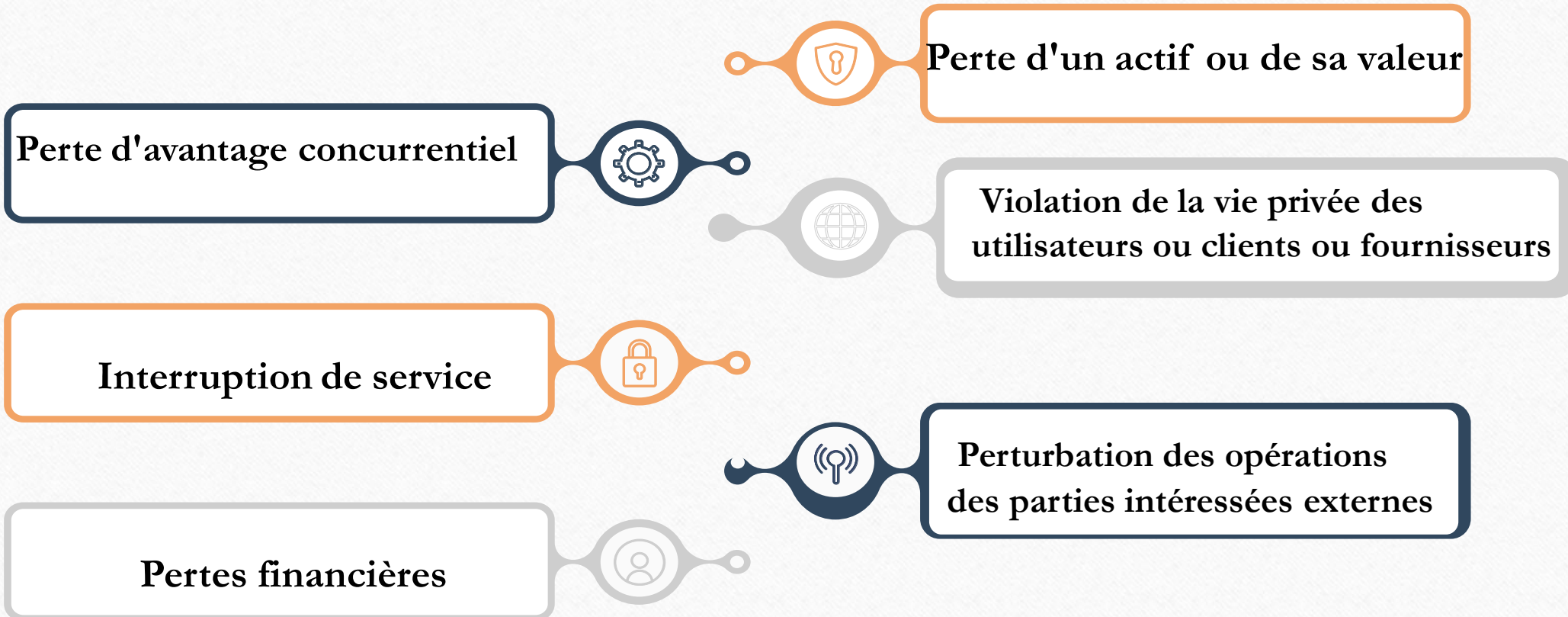
- Changement accidentel
- Modification délibérée
- Résultats incorrects
- Résultats incomplets
- Perte de données

CONFIDENTIALITÉ

- Violation de la vie privée des utilisateurs ou clients
- Violation de la vie privée du personnel de l'organisme
- Divulgence d'information confidentielles

I-5. Identifier les conséquences (Suite)

Ci-dessous une liste de quelques conséquences potentielles qui peuvent avoir une incidence sur la disponibilité, l'intégrité ou la confidentialité (ou plus souvent un mélange des trois à la fois)



I-5. Identifier les conséquences (Suite)

Exemple de menaces ,vulnérabilités et conséquences

Menace	Vulnérabilité	Conséquence
Vol de matériel	Entrepôt non surveillé	Pertes monétaires
Corrosion	Sensibilité à l'humidité	Panne de matériel
Erreur d'entrée de données	Interface utilisateur compliquée	Base de données corrompue
Écoute électronique	Ligne de communication non protégée	Interception des communications
Pirate informatique	Transfert de mots de passe en clair	Vol d'informations
Corruption de données	Pas de processus de gestion des documents	Documentation du SMSI périmée

SOURCE:PECB

I-5. Identifier les conséquences (Suite)

ISO /IEC 27000 ,Article 3.21 ÉVÉNEMENT: occurrence ou changement d'un ensemble particulier de circonstances

Note 1 à l'article:

Un événement peut être unique ou se reproduire. Il peut avoir plusieurs causes.

Note 2 à l'article:

Un événement peut consister en quelque chose qui ne se produit pas.

Note 3 à l'article:

Un événement peut parfois être qualifié «d'incident» ou «d'accident».

Un événement dans le cadre de la gestion des risques peut également être appelé: scénario d'incident ou scénario de risques.

I-5. Identifier les conséquences (Suite)

Exemple d'un scénario d'incident

Royaume-Uni

Corruption de plusieurs sites Web du Parti conservateur

(Vital Security, 01/03/2010)

L'attaque implique la corruption du site Web du Parti conservateur, encourageant les visiteurs à voter pour le Parti travailliste. Les messages des attaquants comprennent une évaluation de la sécurité du site et des slogans politiques.

Actifs informationnels	Contenu du site Web du Parti conservateur
Actif de support	Serveur hébergeant le site Web du Parti conservateur
Aspect sécurité	Intégrité
Vulnérabilité	Failles de sécurité du serveur Web
Menace	Pirates informatiques
Conséquence	Image du Parti conservateur

SOURCE:PECB

Exercice 6: Identification des menaces, vulnérabilités et impacts

Identifier 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

L'équipe de guides touristiques

Durée de l'exercice : 20 minutes

II-ANALYSE DES RISQUES

Cette section vous aidera à acquérir des connaissances sur le processus d'analyse des risques, qui comprend l'appréciation des conséquences, l'appréciation de la vraisemblance d'un incident et l'estimation du niveau des risques.

L'analyse des risques (identification et appréciation) peut se faire à différents niveaux selon l'importance des actifs dans le domaine d'application et la complexité des scénarios de risques à analyser. Selon les circonstances, une méthodologie d'analyse des risques peut être qualitative, quantitative ou une combinaison des deux.

Ci-dessous la liste des activités d'analyse des risques.



1

Identifier les méthodologies
d'analyse des risques

Apprécier les conséquences



2



3



Apprécier la vraisemblance
d'un incident

Estimer le niveau des risques

4



II-1-Identifier les méthodologies d'analyse des risques

Une méthodologie d'analyse des risques peut être qualitative, quantitative ou une combinaison des deux.

ISO/IEC Article 8.2.2.1 Méthodologies d'estimation du risque.

Analyse qualitative des risques

Analyse qualitative des risques utilise une échelle d'attributs qualificatifs pour décrire l'ampleur des conséquences potentielles (par exemple : faible, moyenne et élevée) ainsi que la probabilité de leur occurrence.

Dans une **approche qualitative**, on développe des scénarios de risque en attribuant un niveau d'importance aux menaces, aux vulnérabilités et à l'impact potentiel d'atteindre un niveau de risque. En fin de compte, on calcule le risque et on recommande des mesures de sécurité appropriées. Il est à noter que les résultats d'une approche qualitative sont pertinents lorsque l'on peut comparer les scénarios de risque entre eux.

Analyse quantitative des risques

L'analyse quantitative utilise une échelle comportant des valeurs numériques (plutôt que les échelles descriptives utilisées lors de l'estimation qualitative), à la fois pour les conséquences et pour la vraisemblance, à l'aide de données obtenues à partir de sources diverses.

L'**analyse quantitative des risques** utilise l'analyse mathématique et financière en attribuant une valeur monétaire à chaque composante de l'appréciation des risques et aux pertes potentielles.

II-1-Identifier les méthodologies d'analyse des risques (suite)

Le degré de détail, la rigueur, la répétabilité et la reproductibilité requis dépendent des circonstances, de la disponibilité de données fiables et des besoins décisionnels de l'organisme. L'approche appropriée peut être sélectionnée en fonction du contexte de l'organisme (interne et externe) et de l'exposition au risque.

Chacune des approches présentées dans la figure ci-dessous a ses avantages et ses inconvénients.

Analyse quantitative des risques

Utilisation des mathématiques

Données objectives (nombre)

Exprimées en unités monétaires

Basée sur la capacité des experts à
estimer le risque en termes
financiers

Analyse qualitative des risques

Utilisation de scénarios de risque

Données subjectives

Sous forme d'échelle descriptive

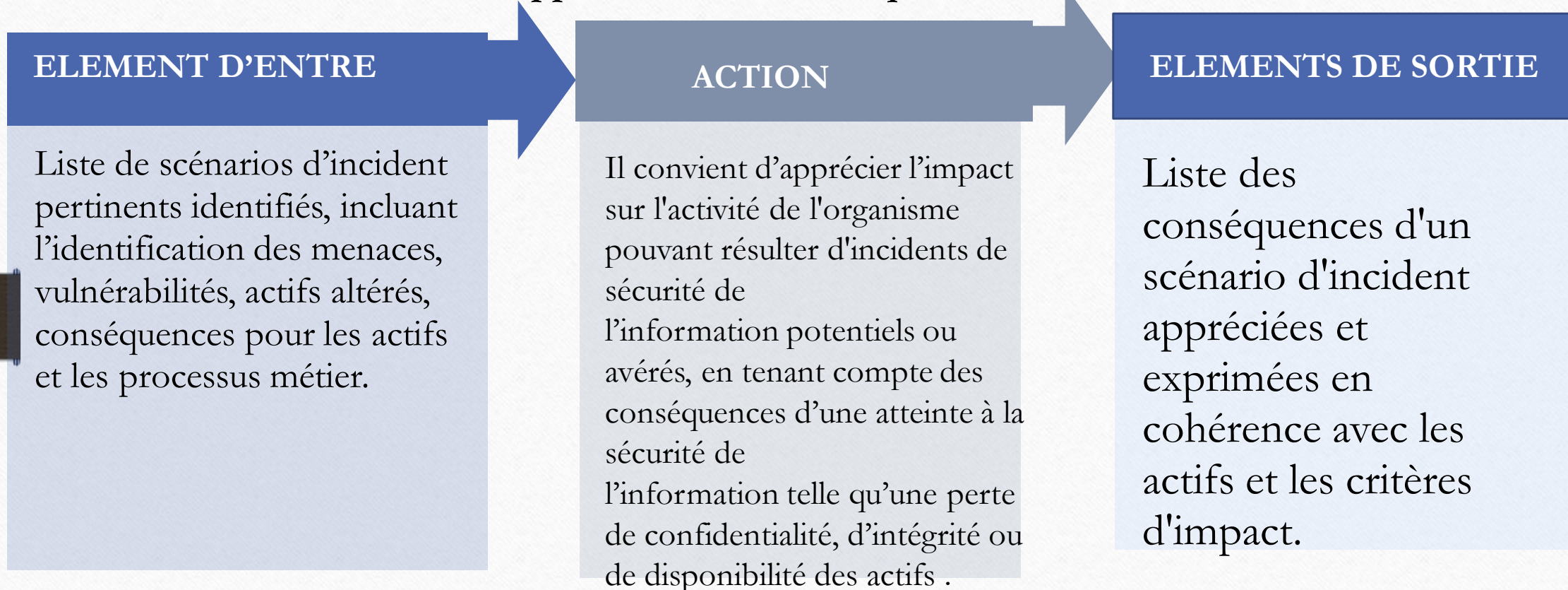
Basée sur les perceptions
du risque
par les parties intéressées

Quantitative	Qualitative
1	Faible
2	Moyenne
3	Élevée

SOURCE:PECB

II-2.Apprécier les conséquences

ISO/IEC 27005 ,Article 8.2.2.2:Appréciation des conséquences



II-2.Apprécier les conséquences (Suite)

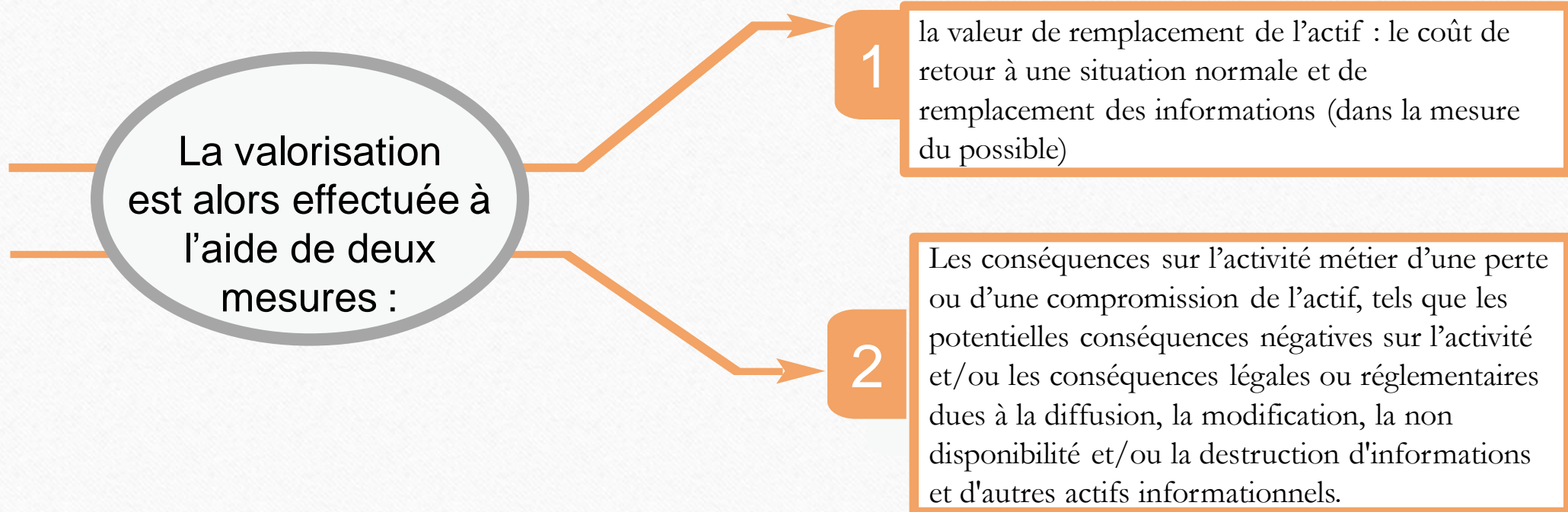
L'estimation de l'impact est effectuée régulièrement dans le cadre de la préparation de plans de continuité d'activité ou de plans de reprise après sinistre, mais elle peut être utilisée à un niveau supérieur dans le contexte de l'estimation des conséquences des scénarios d'incidents élaborés.

- ☐ Les impacts estimés peuvent être exprimés en termes qualitatifs ou quantitatifs .
- ☐ La valeur de l'impact dépend généralement de la valeur et de l'importance des actifs touchés par le scénario d'incident.
- ☐ L'appréciation peut être obtenue par une analyse de l'impact sur les activités de l'entreprise.

II-2.Apprécier les conséquences (Suite)

Le concept d'impact sur l'activité est utilisé pour mesurer les conséquences . La valeur d'un impact sur l'activité métier peut être exprimée de manière qualitative et quantitative, cependant une méthode d'attribution d'une valeur financière peut, en général, fournir davantage d'informations pour la prise de décision et permettre, ainsi, un processus de décision plus efficace.

La valorisation d'un actif commence par la classification des actifs en fonction de leur criticité en termes d'importance des actifs pour l'accomplissement des objectifs métiers de l'organisme.



II-2.Apprécier les conséquences (Suite)

La valorisation des actifs est un facteur clé de l'appréciation des impacts d'un scénario d'incident car l'incident peut affecter plus d'un actif (par exemple des actifs dépendants) ou uniquement une partie d'un actif. Différentes menaces et vulnérabilités ont des impacts différents sur les actifs, comme une perte de confidentialité, d'intégrité ou de disponibilité. L'appréciation des conséquences est donc liée à la valorisation des actifs, basée sur l'analyse des impacts sur l'activité métier.

Les conséquences ou l'impact sur l'activité métier, peuvent être déterminés en modélisant les résultats d'un événement ou d'un ensemble d'événements, ou par extrapolation d'études expérimentales ou de données passées.

Les conséquences peuvent être exprimées en termes de critères d'impact financier, technique ou humain, ou d'autres critères pertinents dans le contexte de l'organisme. Dans certains cas, plus d'une valeur numérique est nécessaire pour spécifier les conséquences à différents moments, sites, groupes ou situations.

Il convient de mesurer les conséquences en termes de délais et de coûts à l'aide de la même approche que celle utilisée pour la vraisemblance des menaces et la vulnérabilité.

Il convient de conserver la cohérence de l'approche quantitative ou qualitative.

II-2.Apprécier les conséquences (Suite)

En général, la valeur déterminée par l'impact sur l'entreprise est sensiblement plus élevée que le simple coût de remplacement de l'actif. Pour obtenir une estimation qui correspond à la réalité, il faut prendre en compte à la fois les conséquences directes et indirectes.

ISO/IEC 27005 ,ANNEXE B.3 Appréciation des impacts

IMPACTS DIRECTS:

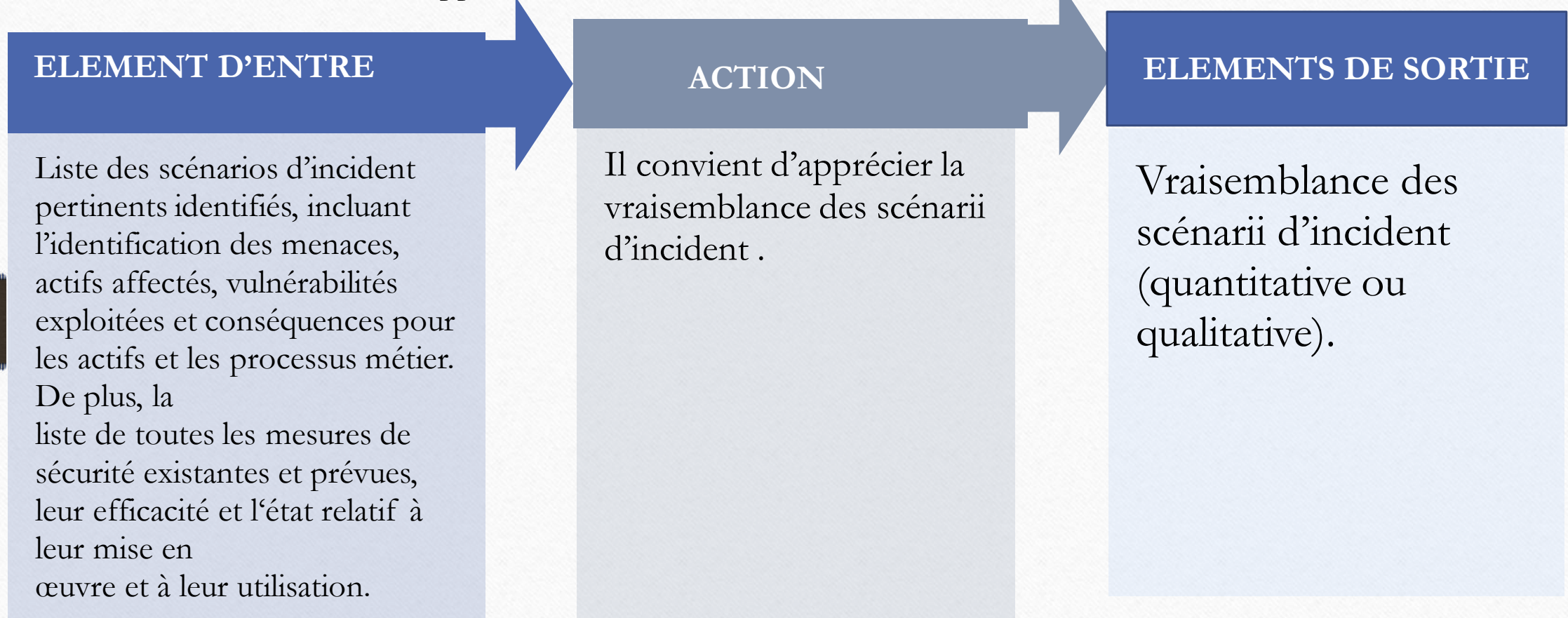
- a) la valeur financière de remplacement d'un actif (ou d'une partie d'un actif) perdu;
- b) le coût d'acquisition, de configuration et d'installation du nouvel actif ou de sauvegarde;
- c) le coût des opérations interrompues en raison de l'incident jusqu'à ce que le service fourni par le ou les actifs soit restauré;
- d) les résultats d'impact d'une violation de la sécurité de l'information.

IMPACTS INDIRECTS:

- a) le coût de l'opportunité (les ressources financières nécessaires pour remplacer ou réparer un actif qui
- b) le coût des opérations interrompues;
- c) le mauvais usage potentiel des informations obtenues en raison d'une atteinte à la sécurité;
- d) la violation des obligations statutaires ou réglementaires;
- e) la violation des codes éthiques de conduite.

II-3. Appréciation de la vraisemblance d'un incident

ISO/IEC 27005 , article 8.2.2.3 Appréciation de la vraisemblance d'un incident



Une fois les scénarios d'incident identifiés, il est nécessaire d'apprécier la vraisemblance de la réalisation d'un scénario et de son impact, à l'aide de techniques d'analyse qualitatives et quantitatives. Il convient de tenir compte de la fréquence de survenance des menaces et de la facilité d'exploitation des vulnérabilités.

II-3. Appréciation de la vraisemblance d'un incident (Suite)

ISO /IEC 31000 ,Article 3.7:La vraisemblance est la possibilité que quelque chose se produise

Note 1 à l'article:

Dans la terminologie du management du risque , le mot «vraisemblance» est utilisé pour indiquer la possibilité que quelque chose se produise, que cette possibilité soit définie, mesurée ou déterminée de façon objective ou subjective, qualitative ou quantitative, et qu'elle soit décrite au moyen de termes généraux ou mathématiques (telles une probabilité ou une fréquence sur une période donnée).

Note 2 à l'article:

Le terme anglais «likelihood» (vraisemblance) n'a pas d'équivalent direct dans certaines langues et c'est souvent l'équivalent du terme «probability» (probabilité) qui est utilisé à la place. En anglais, cependant, le terme «probability» (probabilité) est souvent limité à son interprétation mathématique. Par conséquent, dans la terminologie du management du risque, le terme «vraisemblance» est utilisé avec l'intention qu'il fasse l'objet d'une interprétation aussi large que celle dont bénéficie le terme «probability» (probabilité) dans de nombreuses langues autres que l'anglais.

II-3. Appréciation de la vraisemblance d'un incident (Suite)

ISO/IEC 27005 , article 8.2.2.3 Appréciation de la vraisemblance d'un incident

Il convient de tenir compte de la fréquence de survenance des menaces et de la facilité d'exploitation des vulnérabilités, en prenant en considération :

- ☐ l'expérience et les statistiques applicables à la vraisemblance des menaces;
- ☐ pour les menaces de source délibérée : la motivation et les capacités, qui évolueront au cours du temps, les ressources disponibles pour les attaquants potentiels, ainsi que la perception de l'attrait et de vulnérabilité des actifs pour un attaquant potentiel;
- ☐ pour les menaces de source accidentelle : les facteurs géographiques, par exemple la proximité d'usines chimiques ou d'exploitations pétrolières, la possibilité de conditions météorologiques extrêmes et les facteurs susceptibles d'influencer les erreurs humaines et les dysfonctionnements des équipements;
- ☐ les vulnérabilités, à la fois individuellement et agrégées ;
- ☐ les mesures de sécurité existantes et leur efficacité pour réduire les vulnérabilités.

II-3. Appréciation de la vraisemblance d'un incident (Suite)

Classification par niveau des vraisemblances

Niveau	Échelle qualitative	Vraisemblance
0	Très rare	Moins d'une fois par 100 ans
1	Rare	Une fois tous les 10 ans en moyenne
2	Possible	Une fois tous les 3 ans en moyenne
3	Très possible	Une fois par an en moyenne
4	Probable	Plusieurs fois par année
5	Peu fréquent	Plusieurs fois par mois
6	Fréquent	Plusieurs fois par semaine
7	Très fréquent	Plusieurs fois par jour

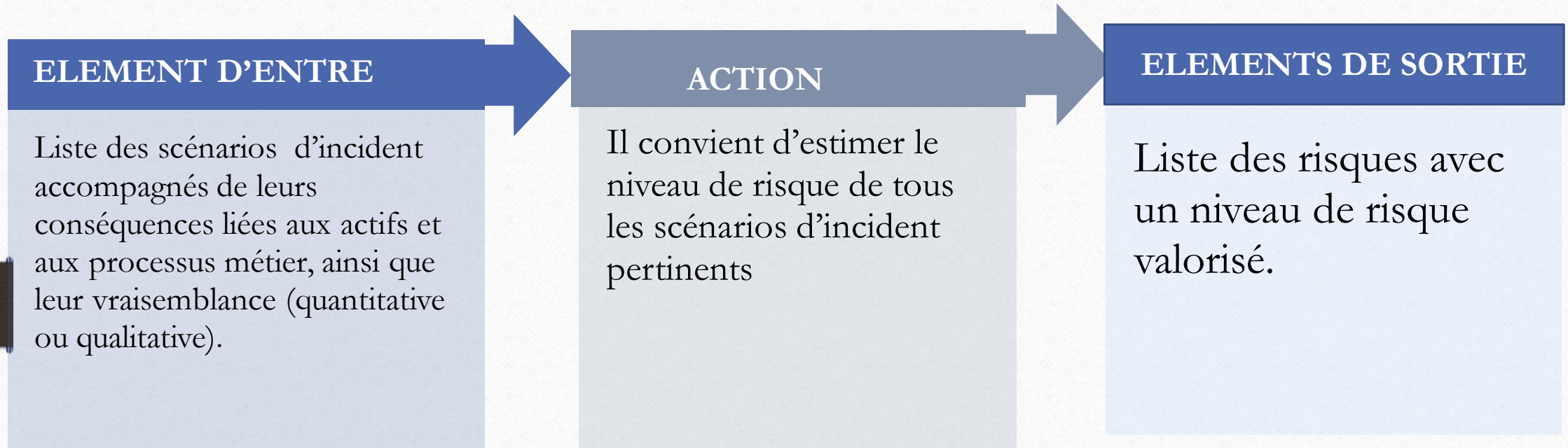
Exemple d'une expression quantitative

1. En 2021, l'organisme a enregistré 730 incidents liés à la réinitialisation du mot de passe.
2. $730 \text{ incidents} / 365 \text{ jours} = 2 \text{ incidents par jour}$
3. La vraisemblance du scénario d'incident lié à la réinitialisation du mot de passe dans cet organisme est de **2 incidents par jour**.
Sa classe est donc au niveau 7 donc très fréquent.

SOURCE:PECB

II-4. Estimer le niveau des risques

ISO/IEC 27005 ,Article 8.2.2.4 Estimation du niveau de risque

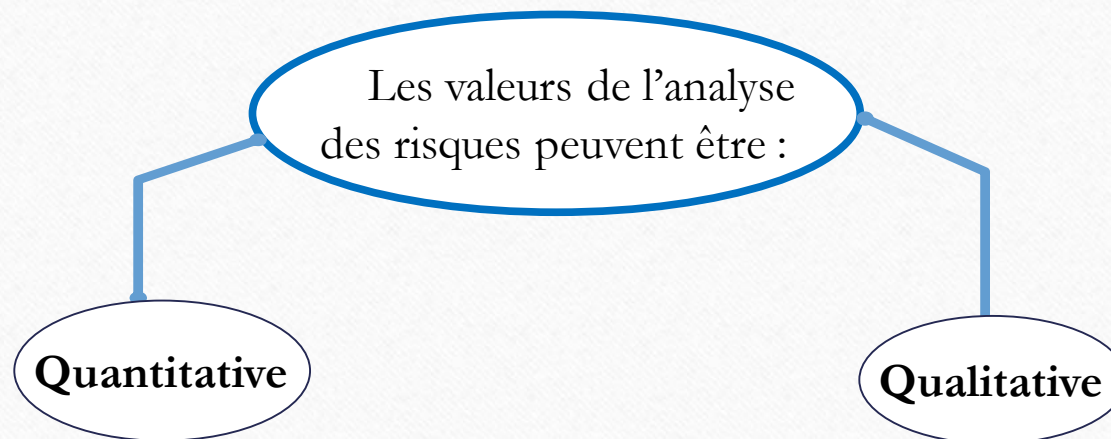


II-4. Estimer le niveau des risques (Suite)

L'appréciation du niveau permet de définir les priorités et la chronologie des actions.

Niveau de risque importance d'un risque exprimée en termes de combinaison des conséquences (3.12) et de leur vraisemblance. (ISO/IEC 27000).

- Il convient d'estimer le niveau de risque de tous les scénarii d'incident pertinents ;
- L'analyse des risques attribue des valeurs à la vraisemblance et aux conséquences d'un risque .Ces valeurs peuvent être quantitatives ou qualitatives ;
- L'analyse des risques est basée sur l'appréciation des conséquences et de la vraisemblance.
- Le risque estimé est une combinaison de la vraisemblance d'un scénario d'incident et de ses conséquences.



Le niveau d'estimation du risque prend en compte

- Avantage du cout ;
- Préoccupations des parties intéressées ;
- Autres variables .

II-4. Estimer le niveau des risques (Suite)

ISO/IEC 27005, Annexe E.2.2 - Exemple 1 Matrice avec valeurs prédéfinies

	Vraisemblance d'un scénario d'incident	Très faible (Très peu probable)	Faible (Peu probable)	Moyenne (Possible)	Élevée (Probable)	Très élevée (Fréquente)
Impact sur l'activité	Très faible	0	1	2	3	4
	Faible	1	2	3	4	5
	Moyen	2	3	4	5	6
	Élevé	3	4	5	6	7
	Très élevé	4	5	6	7	8

Classement des menaces par mesures de risque

II-4. Estimer le niveau des risques (Suite)

Pour chaque actif, on considère les vulnérabilités pertinentes et leurs menaces correspondantes. Si une vulnérabilité n'a pas de menace correspondante ou si une menace n'a pas de vulnérabilité correspondante, il n'existe actuellement aucun risque.

La rangée appropriée de la matrice est désormais identifiée grâce à la valeur de l'actif et la colonne appropriée grâce à la vraisemblance de la menace et la facilité d'exploitation. Par exemple, si la valeur de l'actif est égale à 3, la menace est «élevée» et la vulnérabilité est «faible», la mesure des risques est égale à 5. À supposer que la valeur d'un actif soit égale à 2, par exemple pour une modification, le niveau de menace est «faible», la facilité d'exploitation est «élevée» et la mesure des risques est alors égale à 4.

La taille de la matrice, en termes du nombre de catégories de vraisemblance de menace et de catégories de facilité d'exploitation, et du nombre de catégories de valorisation des actifs, peut être ajustée selon les besoins de l'organisme. Des colonnes et rangées supplémentaires exigent des mesures de risques supplémentaires.

La valeur de cette approche consiste à classer les risques à traiter.

II-4. Estimer le niveau des risques (Suite)

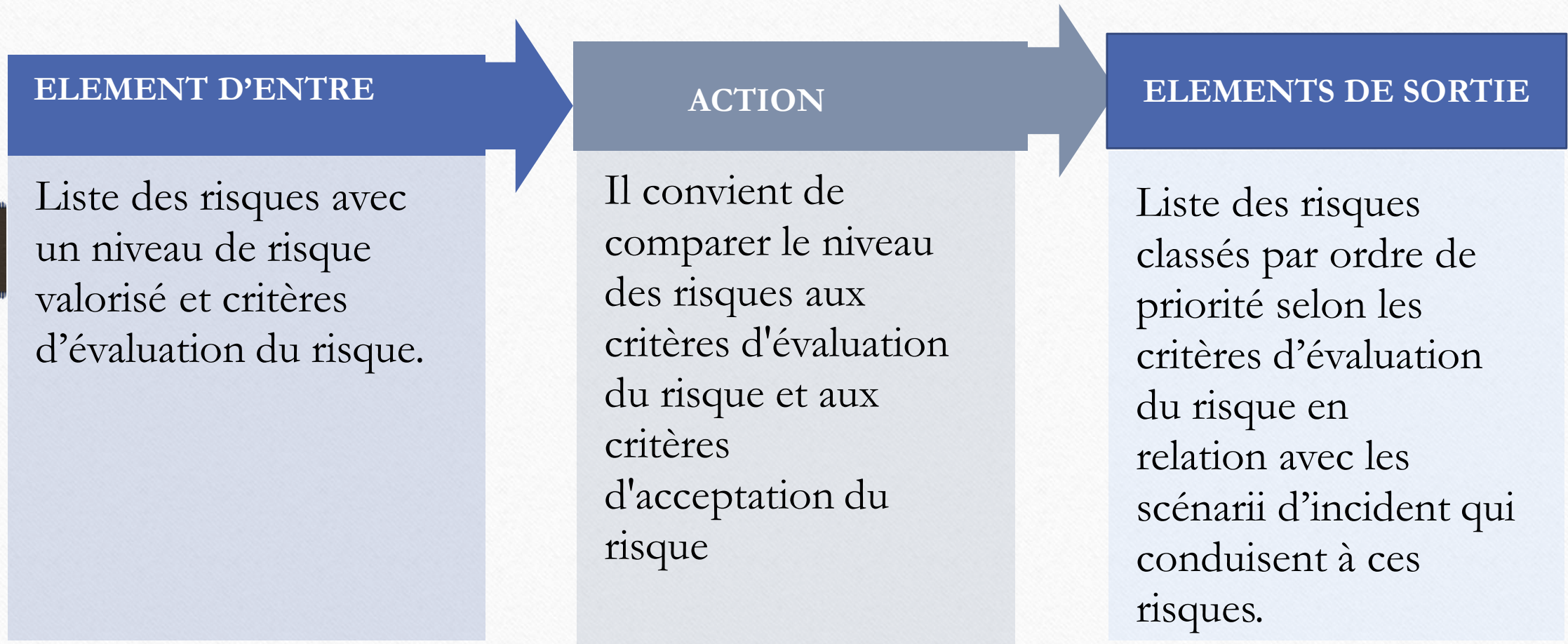
Exercice 7 : Feuille de travail sur le risque lié aux actifs informationnels

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

Durée de l'exercice : 15 minutes

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 ($b \times c$).

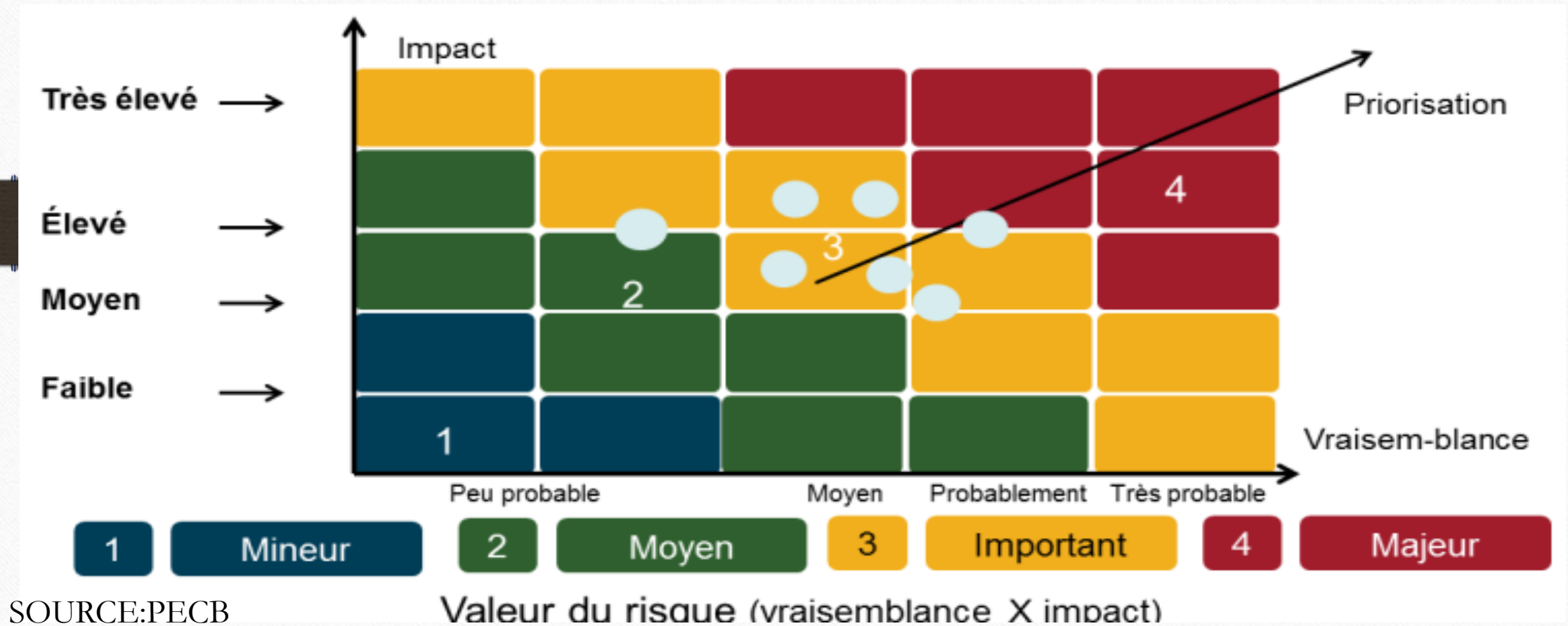
Les menaces peuvent finalement être classées selon l'ordre de leur mesure des risques associée.

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.



SOURCE:PECB

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).

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

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

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:

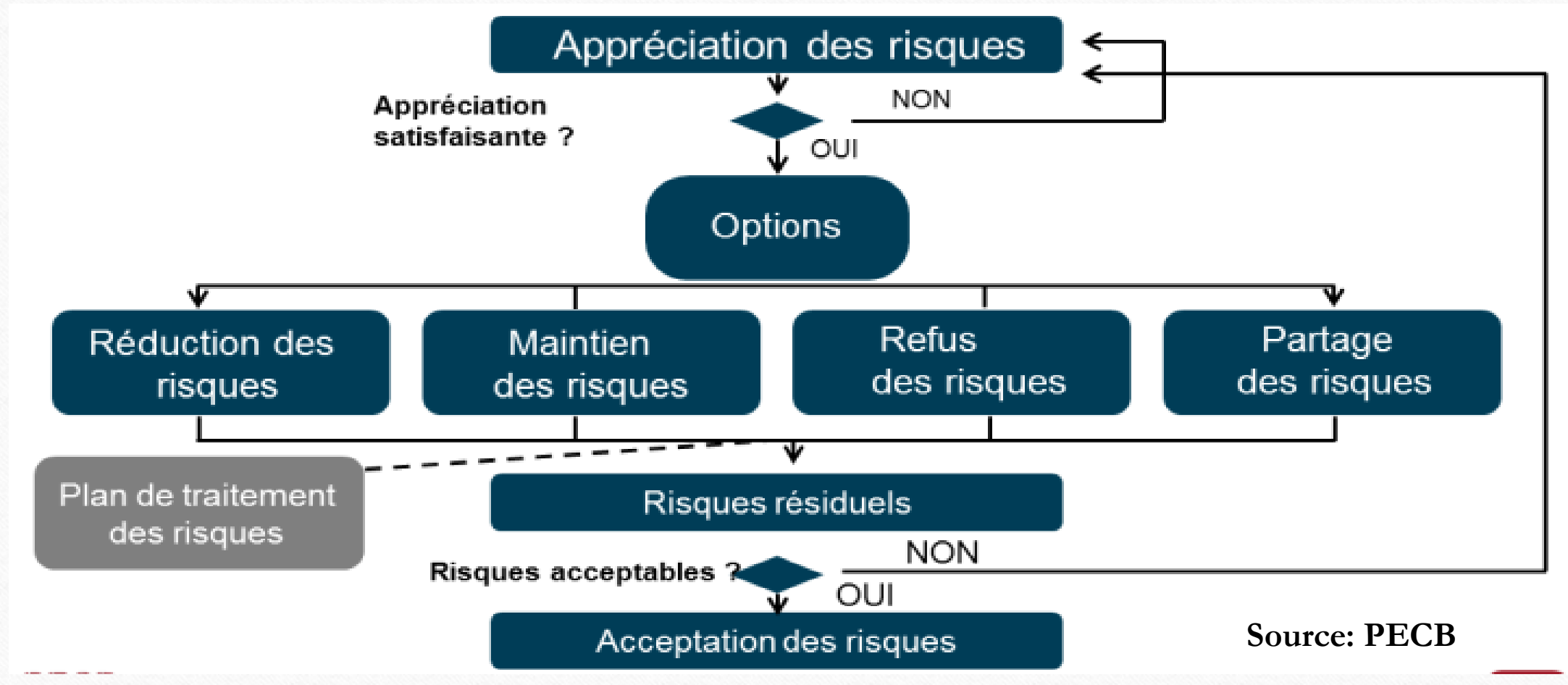
Les traitements du risque portant sur les conséquences négatives sont parfois appelés «atténuation du risque», «élimination du risque», «prévention du risque» et «réduction du risque».

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.

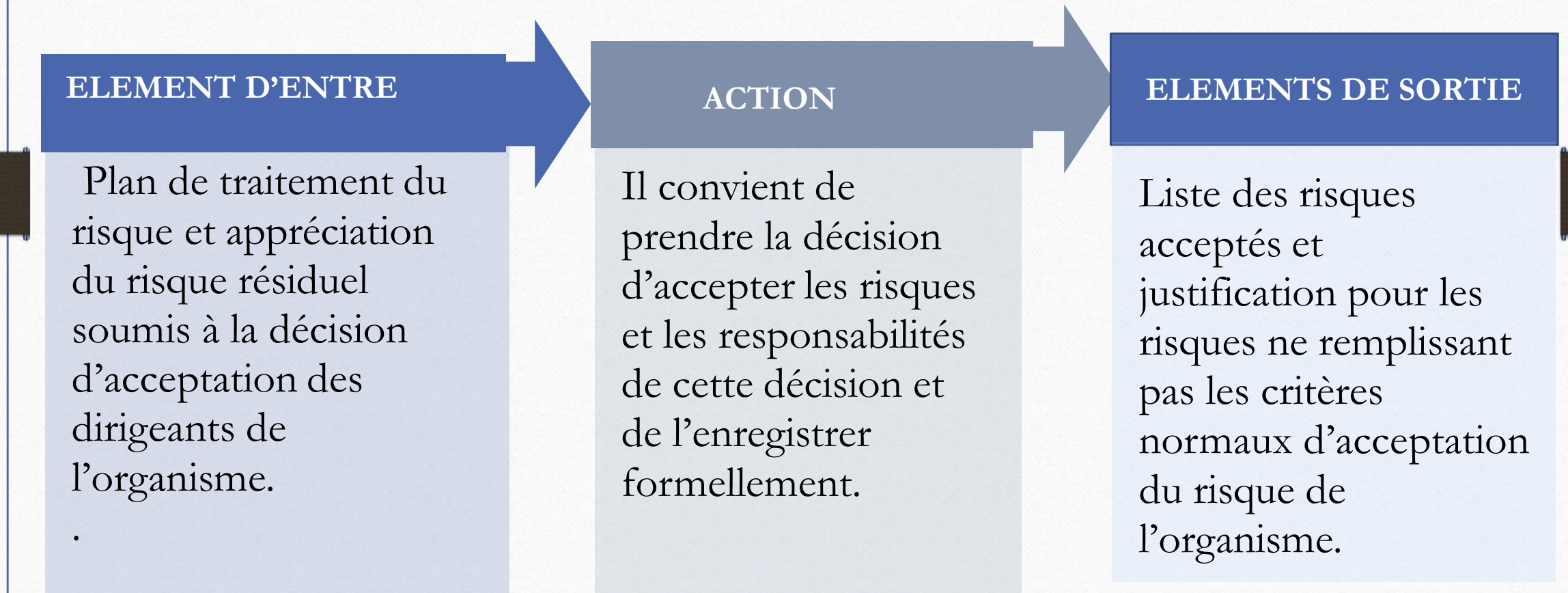
Même s'il est préférable d'éliminer complètement les risques qui dépassent les critères d'acceptation des risques de l'organisme, il n'est pas toujours possible de réduire tous les risques à un niveau acceptable.

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»

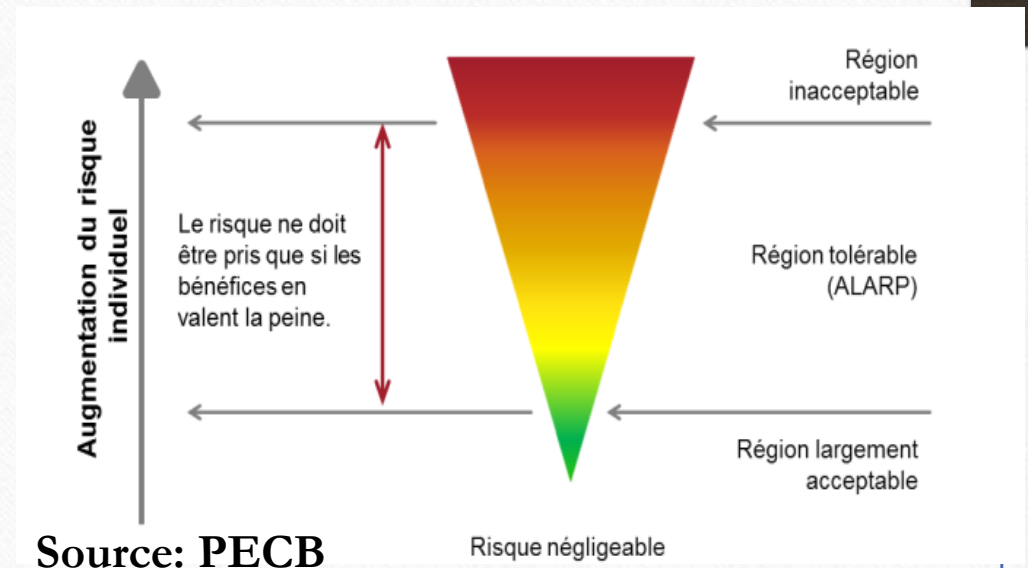
La région à risque tolérable est également appelée région ALARP, puisque le risque tolérable n'est acceptable que si toutes les pratiques raisonnables de réduction des risques ont été mises en œuvre.

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.

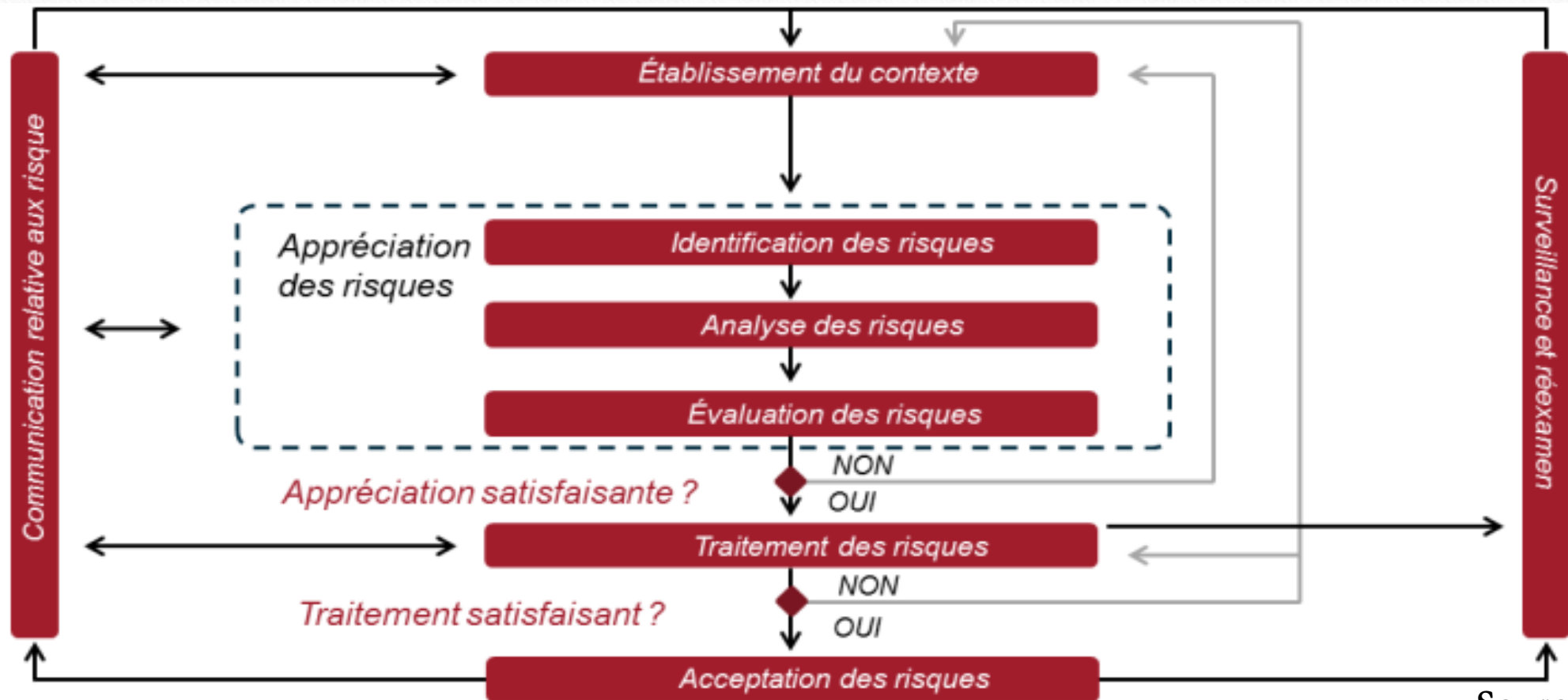
Région tolérable (ALARP) : Le risque est inférieur au niveau inacceptable, mais n'est pas acceptable sans envisager d'autres mesures pour réduire le risque.

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



Source: PECB

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.

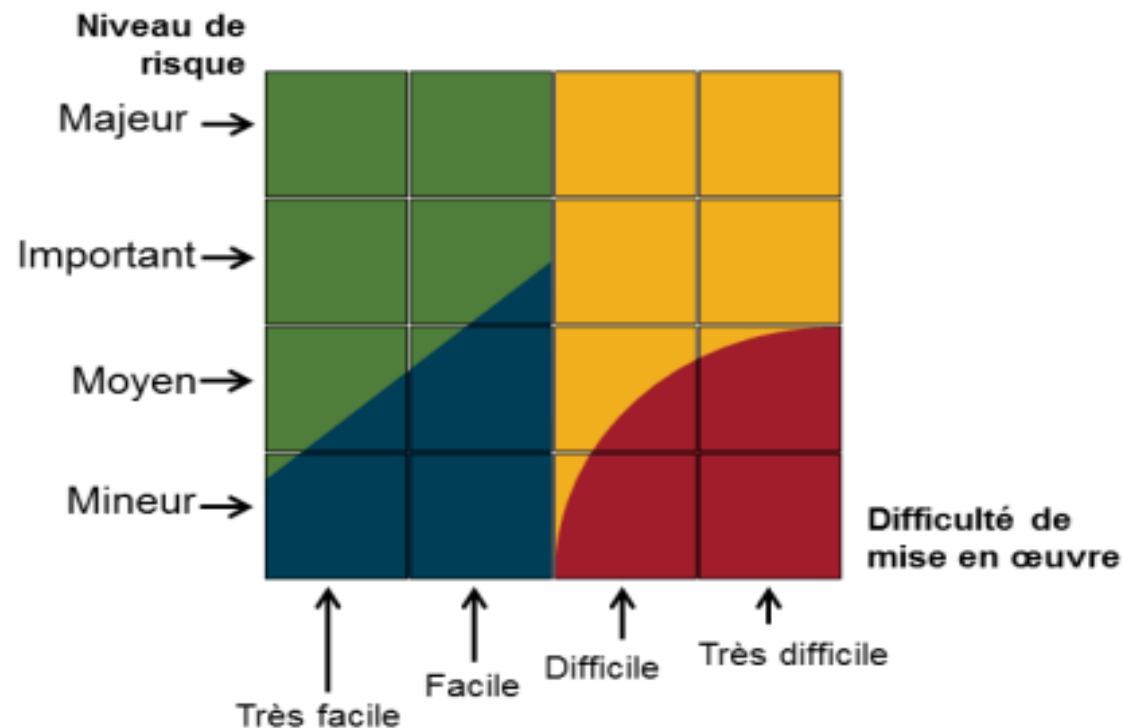


Les critères d'acceptation du risque peuvent être plus complexes et ne pas consister simplement à savoir si un risque résiduel se situe au-dessus ou en-dessous d'un seuil unique.

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



Légende	
D	Risque accepté
M	Décision de la direction
I	Mise en œuvre immédiate
P	Mise en œuvre prévue

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

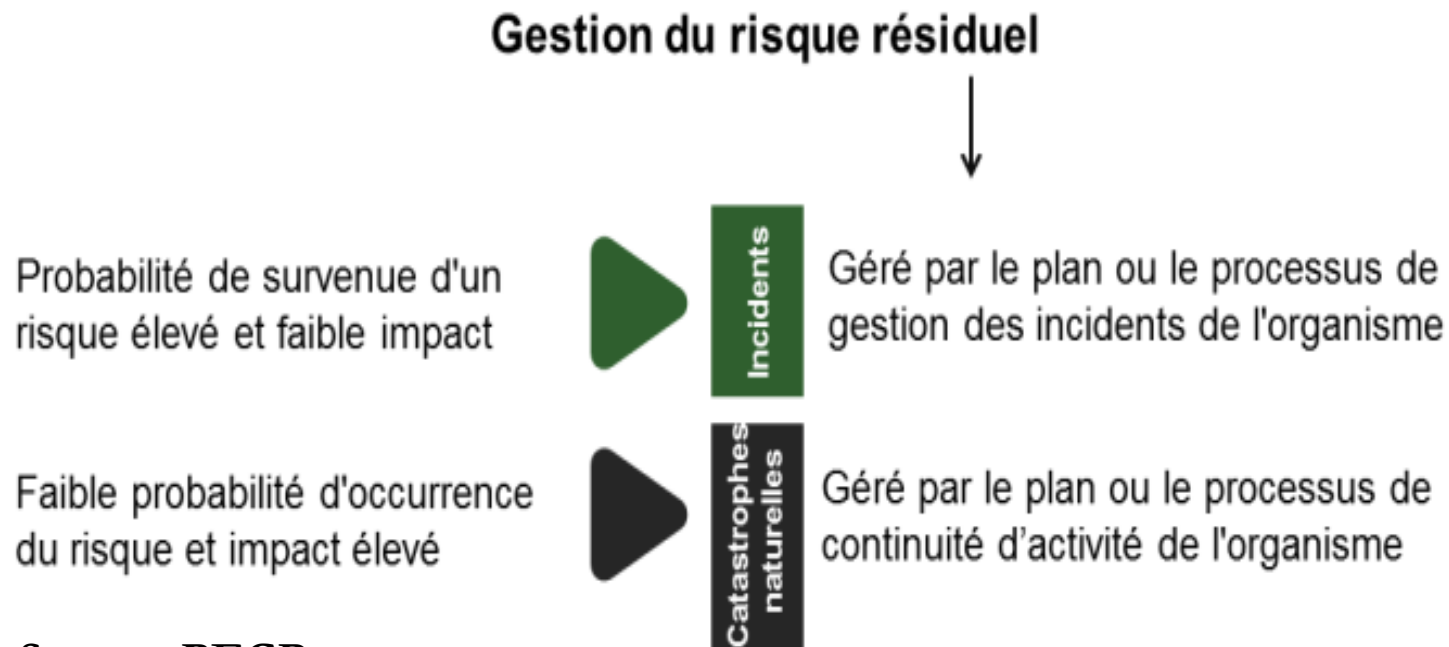
La probabilité d'une menace spécifique

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
- N. Mayer and J-P. Humbert, "La gestion des risques de sécurité des systèmes d'informations", MISC 24, March-April 2006.
- <https://www.iso.org/fr/isoiec-27001-information-security.html>
- <https://www.ssi.gouv.fr/entreprise/management-du-risque/la-methode-ebios-risk-manager/>
- <http://www.itilfrance.com/>
- <http://meharipedia.x10host.com/wp/telechargements/document2/>
- <https://www.riskmanagementstudio.com/download/>

**Merci de votre
attention**