



© PECB, 2020. Tous droits réservés.

Version6.0

Numéro de document: ISMSLID2V6.0

Les documents fournis aux participants sont strictement réservés à des fins de formation. Aucune partie de ces documents ne peut être publiée, distribuée, affichée sur Internet ou sur un intranet, extraite ou reproduite sous quelque forme ou par quelque moyen que ce soit, électronique ou mécanique, y compris par photocopie, sans l'autorisation écrite préalable de PECB.

Programme du jour 2

Section
8

Leadership et approbation
du projet

Section
11

Processus de gestion des risques

Section
9

Périmètre du SMSI

Section
12

Structure organisationnelle de la
sécurité de l'information

Section
10

Politique de sécurité de
l'information

Section
13

Déclaration d'applicabilité et
décision de la direction de mettre
en œuvre le SMSI

PECB

2

Section 8

Leadership et approbation du projet

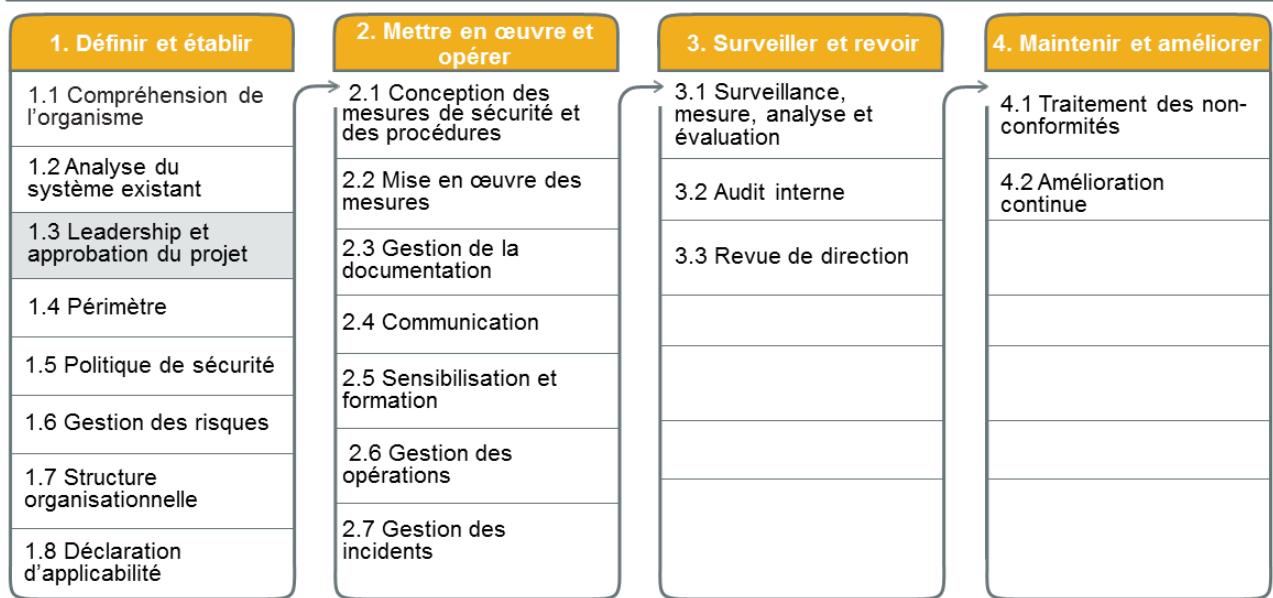
- Étude de faisabilité
- Équipe de projet SMSI
- Exigences en termes de ressources
- Plan du projet SMSI
- Approbation de la direction

PECB

3

Cette section aidera le participant à acquérir des connaissances sur le processus d'officialisation et d'approbation du SMSI, qui comprend l'équipe et le plan de projet SMSI, les ressources nécessaires et l'approbation de la direction.

1.3 Leadership et approbation du projet



PECB

4

ISO/IEC 27001 Exigences

ISO/IEC 27001, article 4.4

L'organisation doit établir, mettre en œuvre, tenir à jour et améliorer continuellement un système de management de la sécurité de l'information, conformément aux exigences de la présente Norme internationale.



PECB

5

Un organisme souhaitant se conformer à ISO/IEC27001 doit au moins:

1. Obtenir l'engagement et l'autorisation de la direction pour mettre en œuvre le SMSI
2. Obtenir les ressources nécessaires pour mettre en œuvre et maintenir le SMSI

1.3 Leadership et approbation du projet

Liste des activités

1.3.1

Réaliser une étude de faisabilité

1.3.2

Établir l'équipe de projet SMSI

1.3.3

Déterminer les exigences du SMSI
en termes de ressources

1.3.4

Concevoir le plan de projet SMSI

1.3.5

Obtenir l'approbation du plan du
projet SMSI par la direction

1.3.1 Réaliser une étude de faisabilité

Une étude de faisabilité (**Business case**) :



PECB

7

Qu'est-ce qu'une étude de faisabilité?

Une étude de faisabilité est un outil qui aide à la planification et à la prise de décisions, incluant celles concernant les opportunités, les choix et le bon moment pour commencer une séquence d'actions. Elle peut habituellement répondre à la question suivante: quelles sont les conséquences financières si nous choisissons X ou Y?

Une étude de faisabilité bien montée doit démontrer quels bénéfices peuvent être attendus d'une décision sur une période donnée. Plus important, elle inclut aussi les méthodes et la logique qui mènent à la quantification des bénéfices. Ce dernier point est crucial, parce que toute étude de faisabilité exige, dans un environnement complexe, des suppositions, des jugements arbitraires et le développement de nouvelles données. En d'autres termes, l'étude est développée selon l'information, au-delà du périmètre des budgets existants et des plans financiers. Ainsi, deux individus travaillant de manière autonome sur le même scénario, en utilisant des calculs financiers exacts, peuvent développer leur étude de faisabilité tout à fait différemment. Pour évaluer la performance, les lecteurs devraient connaître les méthodes qui ont conduit à ces résultats.

Le cœur du projet SMSI repose sur un calendrier qui pourrait s'étaler sur plusieurs mois. Il fournit un cadre qui guide l'équipe de gestion sur la manière de développer des tactiques efficaces. L'étude de faisabilité décrit aussi l'impact global de la mise en œuvre en termes faciles à comprendre pour les profanes des domaines en question. Elle vise les facteurs de succès critiques et les contingences. Elle indique au lecteur la méthodologie pour obtenir les résultats attendus. Elle devrait aussi identifier les risques significatifs potentiels et les signaux de changement dans les résultats.

Page de notes

PECB

8

L'étude de faisabilité répond aux questions des gestionnaires et des utilisateurs :

- Quel est le but du projet ? À quels besoins de l'utilisateur répondra-t-il ?
- Quelles sont les solutions qui ont été étudiées ?
- Pourquoi la solution sélectionnée a-t-elle été choisie ? Quels sont les risques, les contraintes ??
- Combien cela coûte-t-il ? Comment savoir si le projet sera un succès ? Comment expliquer aux employés, aux clients, aux partenaires, etc.? Qui est responsable de ce projet ? Mon travail sera-t-il affecté par ce projet ??

Pour répondre à ces questions, une étude de faisabilité doit contenir au moins cinq parties: les buts ou objectifs du projet et leur incorporation dans la stratégie de l'organisme, les différentes options considérées, la solution choisie, comment le projet sera implémenté et les exigences en termes de ressources pour le projet.

Les trois principales finalités de l'étude de faisabilité dans le management du projet sont les suivantes :

1. Autoriser le projet – en utilisant des cadres de gestion comparables ; les projets peuvent être évalués et autorisés plus exactement sur la base du ROI qu'ils peuvent générer
2. Servir comme premier argument de vente du projet
3. Servir comme point de référence pour tout le cycle de vie du projet

Contenu de l'étude de faisabilité

PMBOK



PECB

9

1. **Environnement** : Liste des faits (inventaire) qui justifient l'existence du projet, les environnements économiques, commerciaux, compétitifs, les opportunités
2. **But et objectifs** : Vision du projet, objectifs généraux et stratégiques/objectifs spécifiques et tactiques, objectifs opérationnels (techniques, économiques et temporels)
3. **Sommaire du projet** : Nom/référence du projet, origine, environnement, état actuel. Ce sommaire énonce les contenus du projet en peu de mots : qu'est-il proposé de faire?
4. **Bénéfices prévus** : Gains souhaités, résultats anticipés, bénéfices financiers (selon le résultat), valeur des bénéfices quantifiés, scénarios financiers, coûts/RSI, risques/coûts du fait de ne rien réaliser, risques du projet (pour le projet même, pour les profits et pour l'activité)
5. **Périmètre préliminaire** : Cadre d'action, périmètre et limites, prérequis
6. **Facteurs de succès critiques** : Ressources matérielles et humaines, contexte
7. **Plan de projet préliminaire**: plan de l'approche du projet, définitions des phases, rapports et livrables
8. **Échéances et jalons** : Activités et modifications d'activités du projet, distribution technique, plan et planification de projet
9. **Rôles et responsabilités**: Fonctions, rôles et ressources pour couvrir la charge de travail
10. **Ressources nécessaires** : Ressources de l'équipe, fonds
11. **Budget** : Contrôles du projet, plans financiers, etc.
12. **Contraintes** : Problèmes anticipés et solutions, hypothèses, options identifiées et estimées, magnitude, échelle et évaluation de la complexité À ces 12 éléments du plan de développement du projet, les deux éléments ci-dessous peuvent être ajoutés et doivent être considérés comme faisant partie d'une sorte de «plan de facilitation» du projet
13. **Communication** : Opérationnelle (choix du média, média, public, etc.) ou promotionnelle (interne et externe)
14. **Suivi du projet** : Indicateurs, tableaux de bord, rapports, revues du projet, traçabilité

1.3.2 Établir l'équipe de projet SMSI

En général, l'équipe de projet SMSI se compose des membres suivants :



PECB

10

Habituellement, l'équipe de projet SMSI consiste en ce qui suit :

1. **Champion de projet** : Personne, habituellement proche du niveau décisionnel de l'organisme, qui s'assure, en utilisant l'influence que procure son mandat dans l'organisme, que le projet reçoit les ressources adéquates et par conséquent que le projet peut être établi. Il agit donc à l'interne comme une sorte de mécène pour le projet.
2. **Chef de projet** : Personne qui établit un projet et le gère tout au long de sa vie opérationnelle. C'est un rôle central dont dépend en grande partie le succès du projet. Généralement, il oriente ou dirige une équipe pour la durée du projet ou pour les différents projets dont il est responsable ; à ce titre, les principaux facteurs de succès sont liés au chef de projet. Il est responsable de :
 - Structurer le projet de manière à réaliser l'unification des équipes qui travaillent vers un objectif commun à court terme
 - Encourager la communication avec les chefs d'équipe afin de s'assurer qu'ils fournissent un soutien systématique pendant toute la période
 - Travailler avec le mécène (ou champion) pour clarifier et formaliser les objectifs
 - Organiser des ateliers d'utilisateurs ou impliquer les utilisateurs dès les premières étapes du projet afin d'identifier leurs besoins
3. **Équipe de gestion de projet** : Toutes les personnes qui ont la responsabilité d'aider à la prise de décisions stratégiques, à l'élaboration des politiques et à l'établissement des objectifs, sous la supervision du responsable du projet.
4. **Équipe de projet** : Toutes les personnes agissant sous la responsabilité du chef de projet et chargées de l'assister dans la gestion des opérations du projet.
5. **Parties intéressées** : Individus ou groupes d'individus qui sont affectés par les prises de décision durant le projet ou qui ont un intérêt dans ses résultats. Cette approche suppose que l'organisme en arrive à un certain équilibre entre les intérêts de ces différentes parties, comme on s'attend à ce que les différentes parties soient conformes à certains intérêts de l'organisme.

Page de notes

PECB

11

Pour améliorer la performance de l'équipe responsable du projet SMSI, la formation , les outils, les techniques et les procédures nécessaires doivent être fournis au personnel. Dans le cas d'un projet SMSI mis en œuvre sur plusieurs sites, il est nécessaire d'étudier les implications de la gestion interculturelle.

Note importante : Il n'est pas nécessaire que tous les membres du projet soient des experts en sécurité de l'information et ce n'est probablement pas souhaitable. La priorité devrait être l'établissement d'une équipe pluridisciplinaire.

Équipe du projet SMSI

Chef du projet SMSI – compétences exigées

Le chef du projet SMSI devrait posséder des connaissances et des compétences dans les secteurs suivants :

Connaissances et compétences dans la gestion de projet

Connaissance de l'organisme et de son environnement

Connaissance de base en management de la sécurité de l'information

Compétences interpersonnelles (communication efficace, négociation, résolution de problèmes, leadership, etc.)

Note :

Le chef du projet SMSI est souvent le responsable de la sécurité de l'information de l'organisme, soutenu par un chef de projet

PECB



12

Un chef du projet SMSI devrait être nommé le plus tôt possible. Il a les responsabilités et l'autorité pour diriger le projet et s'assurer que le système de management de la sécurité de l'information est établi, mis en œuvre et maintenu. L'autorité devrait être confiée au chef de projet SMSI dans le cadre des responsabilités qui lui sont attribuées.

Le choix du chef de projet exige du savoir-faire – l'analyse des écarts peut révéler des besoins techniques ou peut suggérer qu'une meilleure compréhension des affaires est nécessaire. Le périmètre du SMSI peut aussi dicter qui devrait gérer le projet et à quel niveau de l'organisme (en clair, un projet dans un service de dix personnes ne demande pas les mêmes compétences qu'un projet pour une entreprise dans son ensemble). Bien qu'il soit courant que le chef de projet soit le directeur de la sécurité de l'information, de la technologie ou de la gestion des risques d'une grande organisation, un tel rôle peut être indifférent à la mise en œuvre d'un SMSI dans un contexte «localisé». Il n'y a pas de réponse standard, et les aptitudes en gestion de projet ne vont pas nécessairement de pair avec les compétences techniques. Il faut donc faire preuve de discernement.

Comité de pilotage

Durant le projet SMSI

Objectif	Assurer la planification et la surveillance du SMSI
Missions	<ol style="list-style-type: none">1. Planifier la mise en œuvre du SMSI2. Définir le projet SMSI conformément aux objectifs établis par la direction3. Définir les rôles et responsabilités pour le projet SMSI4. Définir les rôles et responsabilités relatives aux opérations et à la maintenance du SMSI (après la mise en œuvre)5. Choisir la méthode d'analyse des risques et les critères d'acceptation des risques6. Gérer les ressources7. Effectuer les revues de direction
Membres	Chef du projet SMSI, responsable de la sécurité, personnes responsables des services clé impliqués dans les domaines d'application suivants : TI, audit, légal, finance, RH, sécurité physique.
Fréquence des réunions	Mensuelle

PECB

13

En général, le comité de pilotage du projet implique le personnel clé de l'entreprise qui a l'expertise requise dans le domaine couvert par le projet afin d'assurer son efficacité.

Dès la mise en œuvre du SMSI, ce comité est particulièrement important puisqu'il servira de relais entre les actions de mise en œuvre et les préoccupations stratégiques de la direction. D'un point de vue tactique, c'est pour cette raison qu'à minima le «champion» et le chef de projet feront partie du comité de pilotage pour inspirer et coordonner.

Note importante: Le comité de pilotage d'un projet SMSI est souvent soutenu par le Comité de sécurité de l'information de l'organisme.

1.3.3 Déterminer les exigences du SMSI en termes de ressources

Les types de ressources évaluées incluront sans s'y limiter :

1. Individus
2. Information et données
3. Installations, équipement et fournitures
4. Systèmes de technologies de l'information et de la communication (TIC)
5. Transport
6. Finances
7. Partenaires et fournisseurs



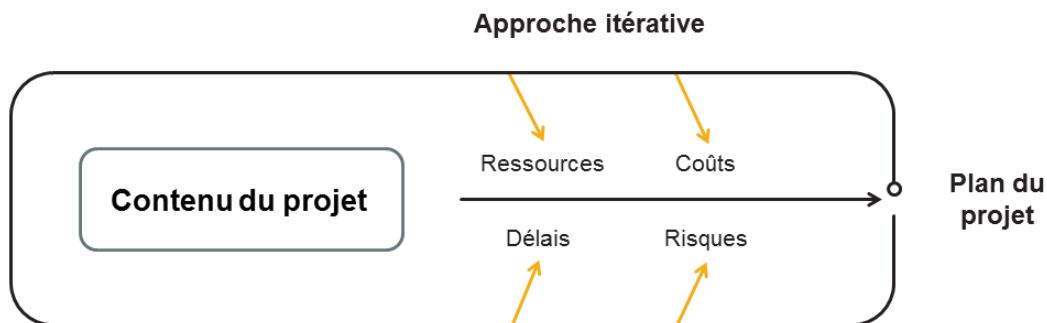
PECB

14

Des efforts réalistes exigent une évaluation approfondie des ressources nécessaires pour reprendre les processus de mission/d'activités aussi vite que possible. Travaillant avec la direction et les experts internes et externes, le chef de projet SMSI devrait assurer que les ressources nécessaires sont correctement identifiées.

1.3.4 Concevoir le plan de projet SMSI

PMBOK



PECB

15

Le plan de projet s'appuie sur les résultats du processus de planification des différentes disciplines pour fournir un document logique et cohérent qui pourra être utilisé pour orienter l'exécution et la direction du projet.

Ce processus exige toujours plusieurs versions. Par exemple, la première étape peut décrire les moyens sans spécifier la durée des activités, tandis que l'étape finale détaillera les ressources spécifiques et les dates.

Le plan de projet est utilisé pour :

- Guider l'exécution du projet
- Conserver un enregistrement écrit de toutes les hypothèses faites durant la planification
- Conserver la trace des critères de sélection entre les différentes options
- Faciliter la communication parmi les parties prenantes
- Planifier les revues du projet principal avec leur périmètre, leur contenu et la date
- Fournir une évaluation comparative pour mesurer le progrès et le contrôle du projet

Contenu du plan de projet SMSI

PMBOK

Un plan de projet inclut typiquement les éléments suivants :

- Charte du projet
- Description de l'approche ou de la stratégie de gestion du projet
- Formulation du contenu du projet avec les livrables et les objectifs
- Structure de répartition de travail du projet (structure « WBS »)
- Coût évalué, date de début prévue et assignation des responsabilités
- Références ; mesures de la performance du coût et du temps
- Jalons majeurs et leur date provisoire
- Personnel clé ou nécessaire
- Risques clés, contraintes, suppositions et réponses proposées
- Problèmes courants et décisions en attente

PECB

16

Dans le cadre de la mise en œuvre d'un SMSI, l'intégration du projet est une étape clé de la réussite. Premier domaine de connaissance étudié par le PMBOK, elle fournit toutes les fonctions permettant une coordination efficace des différents éléments du projet.

À cet égard, le plan de projet consistera en un document sommaire, plus ou moins détaillé, qui peut être réparti dans différents plans de projet, chacun ayant une approche plus granulaire relativement aux sous-projets spécifiques. Ces plans supplémentaires, dans le contexte spécifique de la mise en œuvre du SMSI, identifieront entre autres :

- Charte du projet (PMBOK, Section 5.1.3.1)
- Entrées dans les autres processus (PMBOK, Section 8.1.3.4)
- Charte organisationnelle (PMBOK, Section 9.1.3.3)
- Plan de gestion des risques (PMBOK, Section 11.1.3.1)

Archivage et revue du plan de projet SMSI

PMBOK

- | | |
|--|--|
|  Revue des objectifs du projet et des facteurs de succès |  Revue des livrables à fournir |
|  Revue de la méthode proposée |  Revue des rôles |
|  Mise en évidence des risques et incertitudes inhérents au projet |  Revue des documents du projet |
|  Évaluation des ressources internes nécessaires |  Définition de la fréquence et du contenu des réunions d'avancement |
|  Définition de la séquence des phases et de l'exécution prévue | |

PECB

17

Durant l'étape d'initiation du projet, les rôles et responsabilités de chaque intervenant dans le projet sont clairement définis, étant donné qu'il est de haute importance de définir les fonctions de chaque personne pour assurer une mise en œuvre réussie. Cette étape est relativement courte et généralement limitée à l'entente sur un nombre d'éléments clés qui constituent le plan de projet.

Le plan de projet, défini comme une «feuille de route», sera alors formellement soumis et approuvé par la direction parce qu'il engage l'organisme en termes de ressources matérielles et humaines, mais aussi en termes financiers tel que rapporté précédemment.

La clarification apportée par le formalisme du plan de projet permet à l'équipe de projet de perfectionner et de documenter les exigences fonctionnelles nécessaires à la réalisation des objectifs de l'organisme. En d'autres termes, les éléments listés ci-dessus permettent de préparer les tâches nécessaires suivantes, quoique celles-ci, seules, ne seraient pas suffisantes pour le SMSI initial :

- Définition des processus et fonctions pour mettre en œuvre le projet
- Modélisation/documentation de ces processus
- Définition d'éléments d'entrée et de sortie gérées par le projet
- Identification des impacts organisationnels que le projet pourrait générer
- Identification d'éléments réutilisables de projets précédents pour optimiser le projet actuel

1.3.5 Obtenir l'approbation du plan du projet SMSI par la direction

Principaux avantages de l'engagement de la direction

- Connaissance accrue des lois et règlements
- Répartition optimale des ressources
- Identification des actifs critiques
- Processus de sécurité vérifiés et mesurés

Approbation de la direction



PECB

18

L'engagement et l'implication active de la direction de l'organisme dans le projet est essentiel pour développer et maintenir un SMSI efficace dans le temps. La direction de l'organisme aide à créer une culture de la sécurité de l'information et à éduquer tous les membres de l'organisme dans ce but. La direction doit approuver l'étude de faisabilité et le plan de projet SMSI. Les déclarations de soutien et d'autorisation de la direction doivent être formellement documentées.

Les avantages attendus de l'engagement de la direction à mettre en œuvre le SMSI sont :

1. Meilleure connaissance et prise en compte des lois, règlements, obligations contractuelles et normes applicables en matière de sécurité de l'information dont le but est d'éviter les responsabilités (civiles ou pénales) et les sanctions possibles pour non-conformité
2. Allocation optimale des ressources dévolues à la sécurité de l'information
3. Identification et protection adéquate des actifs critiques de l'organisme
4. Processus et mesures de sécurité contrôlés et mesurés
5. Accès à une information fiable concernant le niveau d'exposition au risque de l'organisme afin que celui-ci puisse prendre les décisions appropriées

Rôle de la direction

Rôle de la direction générale durant le projet SMSI

Objectif	Aligner le SMSI sur les objectifs et la stratégie de l'entreprise
Missions	<ol style="list-style-type: none">1. Établir les objectifs et la stratégie du SMSI2. Valider les rôles et responsabilités des parties prenantes clé du projet3. Valider les politiques de sécurité du SMSI4. Approuver les critères d'acceptation des risques5. Approuver le plan de traitement des risques et permettre la mise en œuvre du SMSI6. Fournir les ressources adéquates pour la mise en œuvre du SMSI
Membres	Direction générale (PDG, CIO, VP Finance, etc.)
Fréquence des réunions	Un certain nombre de réunions aux jalons importants du projet : rapport de l'analyse de risque, plan de traitement des risques, Déclaration d'applicabilité, revue de direction, etc.

PECB

19

ISO/IEC 27001, article 5.1 Leadership et engagement

La direction doit faire preuve de leadership et affirmer son engagement en faveur du système de management de la sécurité de l'information en:

- a. s'assurant qu'une politique et des objectifs sont établis en matière de sécurité de l'information et qu'ils sont compatibles avec l'orientation stratégique de l'organisation;
- b. s'assurant que les exigences liées au système de management de la sécurité de l'information sont intégrées aux processus métiers de l'organisation;
- c. s'assurant que les ressources nécessaires pour le système de management de la sécurité de l'information sont disponibles;
- d. communiquant sur l'importance de disposer d'un management de la sécurité de l'information efficace et de se conformer aux exigences du système de management de la sécurité de l'information;
- e. s'assurant que le système de management de la sécurité de l'information produit le ou les résultats escomptés;
- f. orientant et soutenant les personnes pour qu'elles contribuent à l'efficacité du système de management de la sécurité de l'information;
- g. promouvant l'amélioration continue; et
- h. aidant les autres managers concernés à faire également preuve de leadership dès lors que cela s'applique à leurs domaines de responsabilités.

Questions ?

PECB

20

Section 9

Périmètre du SMSI

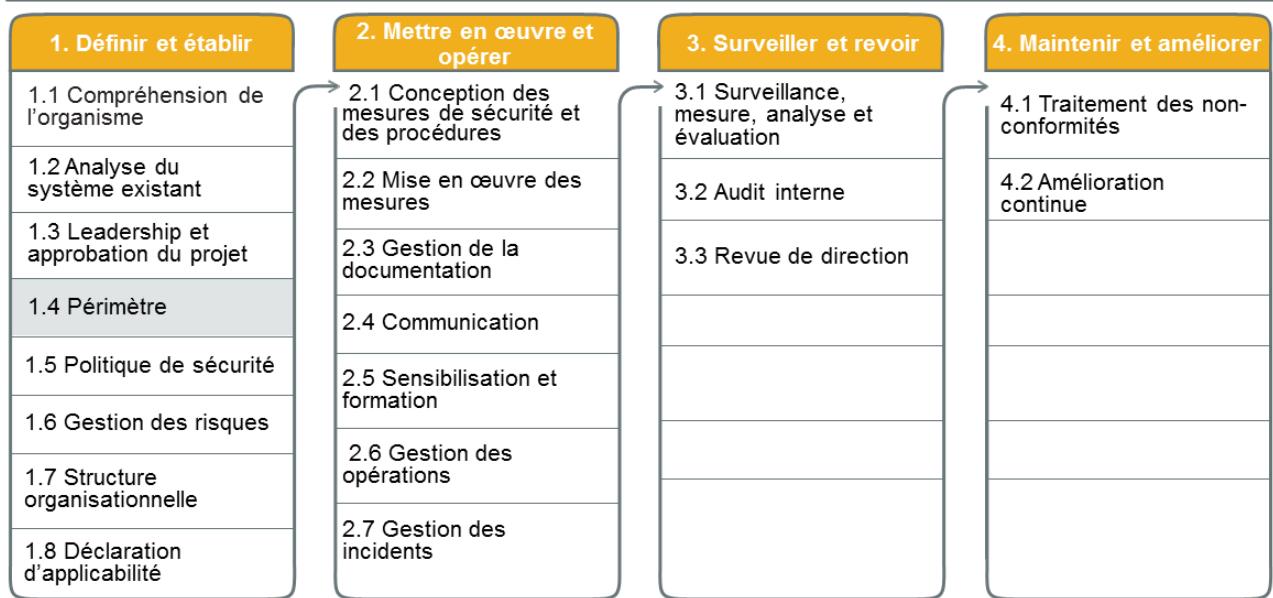
- Limites du SMSI
- Limites organisationnelles
- Limites de la sécurité de l'information
- Limites physiques
- Périmètre du SMSI

PECB

21

Cette section aidera le participant à acquérir des connaissances sur le SMSI, l'organisation, la sécurité de l'information et les limites physiques.

1.4 Définition du périmètre du SMSI



PECB

22

ISO/IEC 27001 Exigences

ISO/IEC 27001, article 4.3

- Pour établir le domaine d'application du système de management de la sécurité de l'information, l'organisation doit en déterminer les limites et l'applicabilité.
- Lorsqu'elle établit ce domaine d'application, l'organisation doit prendre en compte:
 - a) les enjeux externes et internes auxquels il est fait référence en 4.1;
 - b) les exigences auxquelles il est fait référence en 4.2; et
 - c) les interfaces et les dépendances existant entre les activités réalisées par l'organisation et celles réalisées par d'autres organisations.
- Le domaine d'application doit être disponible sous forme d'information documentée.

PECB

23

Un organisme souhaitant se conformer à ISO/IEC27001 doit au moins:

1. Documenter le périmètre du SMSI
2. Définir les limites du système de management
3. Justifier et documenter les exclusions

Note: Durant l'étude de l'Annexe A et de la Déclaration d'applicabilité, nous verrons les mesures de sécurité pouvant être exclues parce que toutes les mesures de sécurité ne peuvent pas être exclues.

ISO/IEC 27003, article 4.3 Détermination du périmètre du système de management de la sécurité

Le périmètre d'un SMSI peut être très différent d'une mise en œuvre à une autre. Par exemple, le périmètre peut inclure:

- un ou plusieurs processus spécifiques;
- une ou plusieurs fonctions spécifiques;
- un ou plusieurs services spécifiques;
- une ou plusieurs sections ou emplacements spécifiques;
- une entité juridique entière; et
- une entité administrative entière et un ou plusieurs de ses fournisseurs.

Page de notes

PECB

24

Lignes directrices

Pour établir le périmètre d'un SMSI, une approche multi-étape peut être suivie :

- f) déterminer le périmètre préliminaire: il convient que cette activité soit menée par un groupe restreint, mais représentatif de représentants de la direction;
- g) déterminer le périmètre affiné: les unités fonctionnelles à l'intérieur et à l'extérieur du périmètre préliminaire devraient être revues, éventuellement suivies d'une inclusion ou d'une exclusion de certaines de ces unités fonctionnelles afin de réduire le nombre d'interfaces le long des limites. Lors de l'affinage du périmètre préliminaire, toutes les fonctions de soutien doivent être considérées comme nécessaires afin de soutenir les activités commerciales incluses dans le périmètre;
- h) déterminer le périmètre final: le périmètre affiné doit être évalué par toute la direction impliquée dans le périmètre affiné. Si nécessaire, il doit être ajusté et décrit précisément; et
- i) approuver le périmètre: l'information documentée décrivant le périmètre devrait être formellement approuvée par la haute direction.

Périmètre

Importance

Une définition claire du périmètre, centrée sur les activités clés de l'organisme, est un facteur important de succès de la mise en œuvre du SMSI. Il sera ainsi plus facile de :

- Obtenir le soutien de la direction
- Mobiliser les parties prenantes au projet
- Justifier une plus-value aux parties intéressées

Note importante : L'étendue du périmètre est le premier facteur influençant la quantité d'efforts requis par le projet

PECB

25

Une définition claire du périmètre est un facteur important de succès lors de la mise en œuvre du SMSI. En définissant un périmètre qui s'inscrit dans le prolongement de la mission de l'organisme, il est plus facile d'obtenir l'appui de la direction et la mobilisation des parties prenantes au projet.

Il convient d'éviter les secteurs qui n'apportent aucune valeur aux parties intéressées ou ne correspondent pas à leurs attentes. Par exemple, une banque qui fait certifier son centre de formation selon ISO/IEC 27001 risque de ne pas créer de valeur pour ses clients ni d'augmenter leur perception de la sécurité. Si tel est le cas, cela peut même être considéré comme une duperie.

L'étendue du périmètre sera le premier facteur influençant la quantité d'efforts requis par le projet. Évidemment, pour un organisme de 20 000 employés qui compte 30 divisions réparties dans six pays, il sera plus facile, plus rapide et moins coûteux de ne faire certifier qu'une division ou un processus-clé plutôt que l'ensemble de l'organisme.

S'il existe déjà un système de management au sein de l'organisme tel que celui de la qualité, le périmètre peut, au choix, couvrir le même secteur, chevaucher en partie le système initial ou en être totalement indépendant.

1.4 Périmètre

Liste des activités

1.4.1

Définir les limites organisationnelles du périmètre

1.4.2

Définir les limites de sécurité de l'information

1.4.3

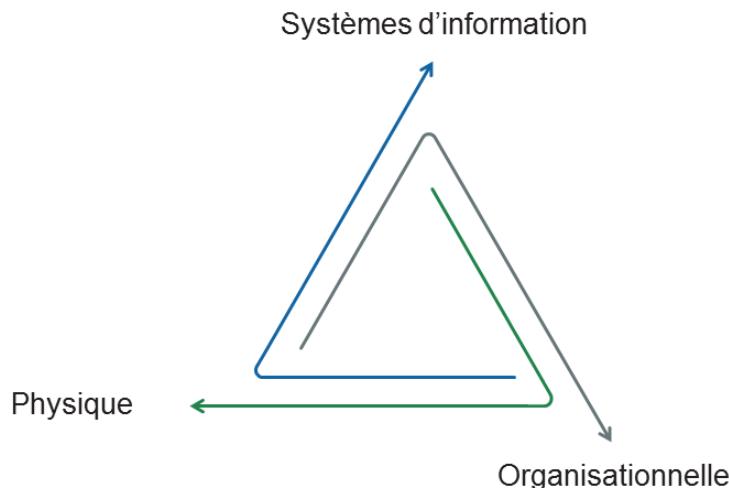
Définir les limites physiques

1.4.4

Définir le périmètre du SMSI

Limites du SMSI

Trois dimensions à prendre en considération :



PECB

27

1. Limites organisationnelles

Deux approches de la définition de « limite » sont généralement appliquées. L'approche réaliste adoptera la définition de limite employée par les utilisateurs eux-mêmes. En revanche, selon une approche commune, le responsable du programme choisira une limite qui atteint ses objectifs analytiques. Les limites géographiques (bureau de l'entreprise, etc.) et temporelles (temps, programmes de bureau) sont des méthodes pratiques pour définir les limites organisationnelles d'un organisme.

2. Les limites des systèmes d'information L'identification des ressources informationnelles d'un système d'information définit la limite de sécurité pour ce système. Les organismes disposent en fait d'une assez grande flexibilité pour déterminer ce qui constitue un système d'information (par exemple, une application principale ou un système de soutien général). Si un ensemble de ressources en information est identifié comme système d'information, ces ressources devraient généralement être sous la même autorité de gestion directe. Il est également possible qu'un système d'information complexe puisse contenir des sous-systèmes multiples disposant chacun de leurs propres limites.

Note: Les ressources informationnelles consistent en l'information qu'elles contiennent ainsi que les ressources associées comme le personnel, l'équipement, le budget et les technologies de l'information dédiées et utilisées en soutien de la ressource.

3. Limites physiques Les limites physiques d'un système peuvent être aussi simples qu'une prise au mur, un port sur un commutateur ou le périmètre d'un coupe-feu. Par exemple, au sein d'un système métropolitain, les limites physiques pourraient être délimitées par le bâtiment particulier d'une ville dans laquelle ce système est exclusivement employé. Sur une base plus systémique, un système peut également être défini par un ensemble particulier de serveurs reliés à des postes de travail dans différents emplacements géographiques et où tous partagent une même base de données. Ainsi, les limites physiques tendent à être plus concrètes que les limites logiques parce que celles-ci sont tangibles.

1.4.1 Définir les limites organisationnelles du périmètre



Un processus clé



Un département



L'ensemble de l'organisation



L'organisation et ses parties prenantes

PECB

28

Il faut tenir compte de ce qui suit :

1. Des unités organisationnelles : département, service, projet, filiale, etc.
2. Des structures organisationnelles et des responsabilités des gestionnaires
3. Des processus métiers : Gestion des ventes, processus d'approvisionnement, embauches, etc.

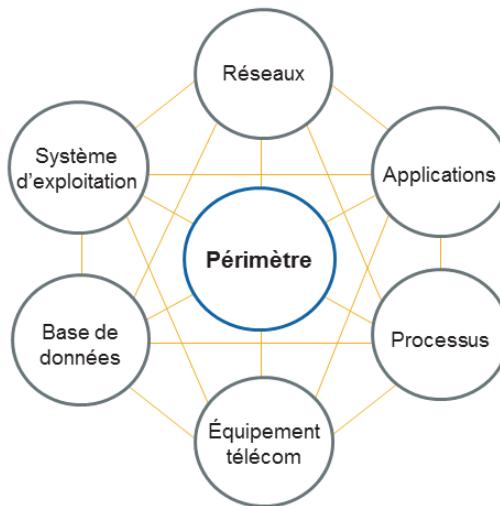
Une méthode efficace pour définir les limites organisationnelles est d'analyser les responsabilités et les zones d'influence des principaux décideurs de l'organisme. Par exemple, un organisme désire mettre en œuvre un SMSI dans son Service des finances; ainsi, en analysant les principaux processus et services qui relèvent du directeur des finances, on peut proposer des limites au niveau organisationnel. Ainsi, si les avantages sociaux des employés sont gérés par le Service des RH (plutôt que par le Service des finances), ceux-ci pourraient être documentés comme étant exclus du périmètre.

Les livrables pour cette activité sont :

1. Description des limites organisationnelles avec justification documentée des exceptions
2. Description des structures organisationnelles incluses dans le SMSI
3. Identification des processus métier et des actifs informationnels (avec leurs propriétaires)
4. Identification de «la direction et des processus de prise de décision»

Note : Si un organisme est très décentralisé en termes de prise de décision, il peut être souhaitable de créer un SMSI différent pour chaque division et de les faire ensuite certifier chacun de façon indépendante. Au contraire, un organisme très centralisé aura plutôt tendance à vouloir ne disposer que d'un SMSI dirigé et contrôlé à partir du siège social.

1.4.2 Définir les limites de sécurité de l'information



- Tous les composants du système doivent être pris en compte ; l'accent ne doit pas être mis uniquement sur les composants matériels.

Note : En théorie, le manque d'infrastructure technique n'empêche pas la certification d'un SMSI.

PECB

29

Pour ce qui est des limites des systèmes d'information, l'ensemble des éléments des systèmes devrait être pris en considération, et non se limiter aux éléments matériels tels que les serveurs et l'équipement de télécommunication. Il faut également considérer les contraintes technologiques et les obligations contractuelles de l'organisme.

Les limites des systèmes d'information se définissent notamment en termes de :

1. Réseaux : réseaux internes, réseaux sans fil, etc.
2. Systèmes d'exploitation : Windows, Linux, etc.
3. Applications : CRM, logiciel de gestion des payes, ERP, utilitaires, base de données
4. Données : fichiers clients, données médicales, recherche et développement, etc.
5. Processus : considérer les processus qui transportent, entreposent ou traitent l'information.
6. Équipements de télécommunication : routeurs, coupe-feu, etc.

Les systèmes d'information supportant les processus métiers devraient être inclus dans les limites organisationnelles du périmètre. Par exemple, il serait inapproprié d'exclure les bases de données clients et le CRM (*Customer Relationship Management*) du périmètre si celui-ci inclut la gestion des comptes clients et le service à la clientèle. L'ensemble des activités d'un processus et les échanges d'information inclus dans le périmètre, y compris les entrées et les résultats, devraient être pris en considération. Par exemple, un organisme prévoit de faire certifier son service d'émission de chèque. À l'interne, un logiciel sert à la saisie des données et à transférer l'information à une tierce partie qui émet les chèques. L'organisme doit s'assurer de la sécurité de l'information, non seulement lors de la saisie en entrée, mais également lors de son transfert et de son traitement externalisé. Cette assurance pourrait prendre la forme, par exemple, d'un accord contractuel.

Note: En théorie, un SMSI sans infrastructure technologique pourrait être certifié ISO/IEC 27001 puisque cette norme concerne la sécurité de l'information et non des systèmes informatiques. On pourrait citer l'exemple d'un centre de conservation d'archives qui ne possède peu ou pas d'infrastructure technologique.

1.4.3 Définir les limites physiques

- L'ensemble des lieux physiques, autant internes qu'externes, inclus dans le SMSI devraient être pris en considération.
- Les sites comprennent tous les emplacements dans le périmètre ou une partie du périmètre, ainsi que les moyens physiques requis pour que ils fonctionnent.
- Dans le cas des sites physiques externalisés, les accords de service applicables et les interfaces avec le SMSI doivent être considérés.



PECB

30

La prise en compte des interfaces avec le SMSI et de l'accord de service applicable est d'une grande importance dans le cas des sites physiques externalisés. Par exemple, si un centre de traitement de données est sous-traité, l'organisme doit tenir compte de l'emplacement géographique où se trouve le centre, même si elle n'en est pas le propriétaire.

1.4.4 Définir le périmètre du SMSI

Le périmètre devrait contenir :

1. Caractéristiques clés de l'organisme
2. Processus organisationnels
3. Descriptions des rôles et responsabilités liés au SMSI
4. Liste des actifs informationnels
5. Liste des systèmes d'information
6. Cartes et plans des sites géographiques
7. Détails et justifications des exclusions



PECB

31

Après avoir défini les limites, les différents éléments du périmètre devraient être intégrés et documentés.

Énoncé du périmètre

Exemples

L'énoncé du périmètre est public et est généralement disponible auprès de l'organisme de certification qui a émis le certificat.

Cet énoncé synthèse sera inscrit sur le certificat. Il devrait être :

1. Aussi simple que possible
2. Compréhensible par les parties externes
3. Assez précis pour exprimer ce qui est couvert par la certification

Exemple : Édition et services d'hébergement Web

PECB

32

Quelques exemples:

2e2 IOM Ltd (UK) : La disposition et l'installation du matériel TI, de logiciel et de services de câblage, incluant la consultation, la formation, le soutien, l'entretien et le plan de reprise d'activité après sinistre pour le *Isle of Man Government* conformément à plus récente version de la Déclaration d'applicabilité.

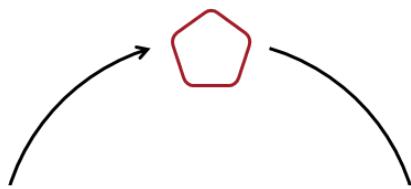
AAD Co Ltd (Japon) : L'impression et la planification, la production et la conception connexes. La planification des sites Web et leur mise en œuvre. Déclaration d'applicabilité, émise le 19juillet 2019, Version 3. Autres sites: Usine de Kawaguchi

Citigroup Technology Infrastructure's (USA) : Ce SMSI s'applique au groupe Sécurité de l'information globale (SIG) de *Citigroup Technology Infrastructure* (CTI). Le SIG est responsable de fournir pour CTI des programmes de sécurité de l'information qui satisfont à toutes les mesures, politiques et pratiques de sécurité de l'information pertinentes qui gouvernent l'activité de Citigroup, en lien avec l'infrastructure technologique et la gestion des risques opérationnels dans l'environnement de l'infrastructure. En conformité avec la version 2.4 datée du 7mars 2020 de la Déclaration d'applicabilité.

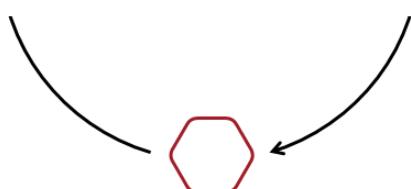
Microsoft, Global Foundation Services Division (USA) : Le management de la sécurité de l'information pour *Microsoft Global Foundation Services Infrastructure* englobant les centres de données énumérés dans ce rapport (Seattle, Quincy, San Antonio, Tokyo, Singapour, etc.) et les équipes spécifiques de la sécurité et de la conformité des services en ligne, des services de centres de données, des services de réseaux mondiaux, des services logiciels de centres de données, du service d'assistance aux centres d'opération, du groupe de soutien des systèmes d'exploitation et de la gestion et du déploiement des actifs, en conformité avec la Déclaration d'applicabilité SMSI de Microsoft GFS en date du 15mars 2020, version 1.3

CIIC HR Management Consulting Co., Ltd. (Chine) : Fourniture d'un service d'enseignement en réseau et des installations et infrastructures connexes pour les services susmentionnés. En conformité avec la plus récente version de la Déclaration d'applicabilité.

Modification du périmètre



Toute modification du périmètre doit faire l'objet d'une évaluation, être approuvée et documentée.



PECB

33

Il est normal que le périmètre change au fil des ans afin que le SMSI continue de permettre à l'organisme de réaliser ses objectifs de sécurité de l'information. Les demandes de modification peuvent avoir les causes suivantes :

- Élargissement du périmètre à d'autres unités de l'organisme
- Modifications dans l'environnement externe (légal, concurrentiel, technologique)
- Prise en compte de nouveaux scénarios de risque
- Etc.

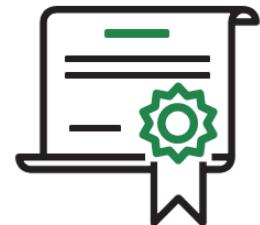
La demande de modification devrait être effectuée selon un processus défini qui passera par le dépôt d'une demande de modification. Toute demande sera justifiée, puis acceptée par le comité de pilotage du SMSI lors d'une revue de direction.

En cas de changement important, une analyse des impacts de la modification du SMSI devrait être menée avant son acceptation finale. En effet, une modification peut entraîner le besoin d'une nouvelle appréciation des risques et la mise en place de nouvelles mesures de sécurité qui n'auraient pas été prévues dans le SMSI initial.

En outre, il faut faire preuve de prudence lors de toute modification du périmètre, étant donné qu'elle peut invalider toute certification qui dépend des termes de la déclaration du périmètre. Il faut donc faire preuve de prudence d'abord lors de la rédaction de la déclaration du périmètre.

Extension du périmètre

- Plusieurs sociétés auditées préfèrent définir un périmètre réduit pour une première certification et effectuer une demande d'extension au cours des années suivantes.
- L'audit d'extension peut être effectué au cours d'un audit de surveillance.
- Si l'extension de certification n'est pas accordée, l'organisme ne perd pas son certificat actuel.



PECB

34

ISO/IEC 17021-1, article 9.6.4.1 Extension du périmètre

En réponse à une demande d'extension du périmètre d'une certification déjà accordée, l'organisme de certification doit entreprendre une revue de la candidature et déterminer toute activité d'audit nécessaire pour décider de la possibilité ou non d'accorder l'extension. Cette démarche peut être effectuée au même moment que l'audit de surveillance.

Exercice 5

PECB

35

Exercice 5 : Définition du périmètre

À partir des informations fournies dans l'étude de cas, indiquez le périmètre du SMSI de l'organisme et déterminez ses limites. La direction souhaite choisir un périmètre qui sera perçu comme ayant une valeur ajoutée pour ses clients et en même temps le délimiter autant que possible pour la certification initiale du SMSI.

Durée de l'exercice : 20 minutes

Commentaires : 15 minutes

Questions ?

PECB

36

Section 10

Politique de sécurité de l'information

- Types de politiques
- Modèles de politiques
- Politique de sécurité de l'information
- Politiques de sécurité spécifiques
- Approbation de la direction
- Publication et diffusion
- Sessions de formation et de sensibilisation
- Contrôle, évaluation et revue

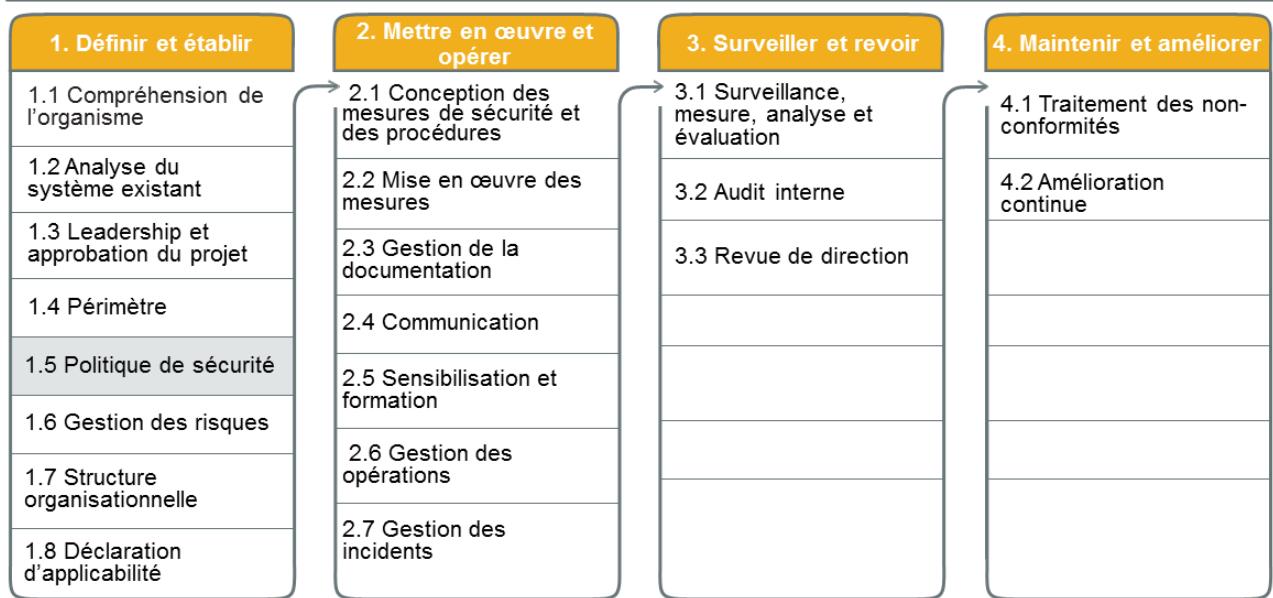
PECB

37



Cette section aidera le participant à acquérir des connaissances sur les politiques de sécurité de l'information, qui comprennent les types de politiques, la création de modèles de politiques, l'approbation de la direction, la publication et la diffusion, la formation, la communication et la sensibilisation, le contrôle, l'évaluation et la revue.

1.5 Politique de sécurité de l'information



PECB

38

ISO/IEC 27001 Exigences

ISO/IEC 27001, article 5.1 et 5.2

5.2 Politique

La direction doit établir une politique de sécurité de l'information qui:

- a) est adaptée à la mission de l'organisation;
- b) inclut des objectifs de sécurité de l'information (voir 6.2) ou fournit un cadre pour l'établissement de ces objectifs;
- c) inclut l'engagement de satisfaire aux exigences applicables en matière de sécurité de l'information; et
- d) inclut l'engagement d'œuvrer pour l'amélioration continue du système de management de la sécurité de l'information.

La politique de sécurité de l'information doit :

- e) être disponible sous forme d'information documentée;
- f) être communiquée au sein de l'organisation; et
- g) être mise à la disposition des parties intéressées, le cas échéant.

5.1 Leadership et engagement

La direction doit faire preuve de leadership et affirmer son engagement en faveur du système de management de la sécurité de l'information en:

- d) communiquant sur l'importance de disposer d'un management de la sécurité de l'information efficace et de se conformer aux exigences du système de management de la sécurité de l'information;

PECB

39

Un organisme qui désire être conforme à ISO/IEC 27001 doit au moins :

1. Publier une politique de sécurité de l'information incluant les quatre points (article 5.2, a-d) requis pour exprimer les intentions de la direction dans le management du SMSI
2. Publier une politique de sécurité de l'information exprimant l'orientation et définissant les dispositions générales relatives à la sécurité de l'information
3. Communiquer les politiques aux parties intéressées concernées

ISO/IEC 27003, article 5.2 Politique

Il convient que la politique de sécurité de l'information reflète la situation commerciale, la culture, les enjeux et les préoccupations de l'organisme en matière de sécurité de l'information. Il convient que l'étendue de la politique de la sécurité de l'information soit conforme au but et à la culture de l'organisme et recherche un équilibre entre la facilité de lecture et l'exhaustivité. Il est important que les utilisateurs de la politique puissent s'identifier à l'orientation stratégique de la politique.

Il convient que la direction décide à quelles parties intéressées la politique devrait être communiquée. La politique de sécurité de l'information peut être écrite de telle sorte qu'il soit possible de la communiquer aux parties intéressées externes concernées en dehors de l'organisme. Des exemples de ces parties intéressées externes sont les clients, les fournisseurs, les contractuels, les sous-traitants et les contrôleurs. Si la politique de sécurité de l'information est mise à la disposition des parties intéressées externes, il convient qu'elle n'inclue pas d'informations confidentielles.

Il convient que la politique de sécurité de l'information soit disponible sous forme d'informations documentées. Les exigences de la norme ISO/IEC 27001 n'impliquent aucun formulaire spécifique pour cette information documentée et, par conséquent, il dépend de l'organisme de décider de la forme la plus appropriée. Si l'organisme dispose d'un modèle standard pour les politiques, il convient que la politique de sécurité de l'information suive ce modèle.

Politique

ISO/IEC 27000, article 3.53

intentions et orientation d'un organisme telles que formalisées par sa direction



PECB

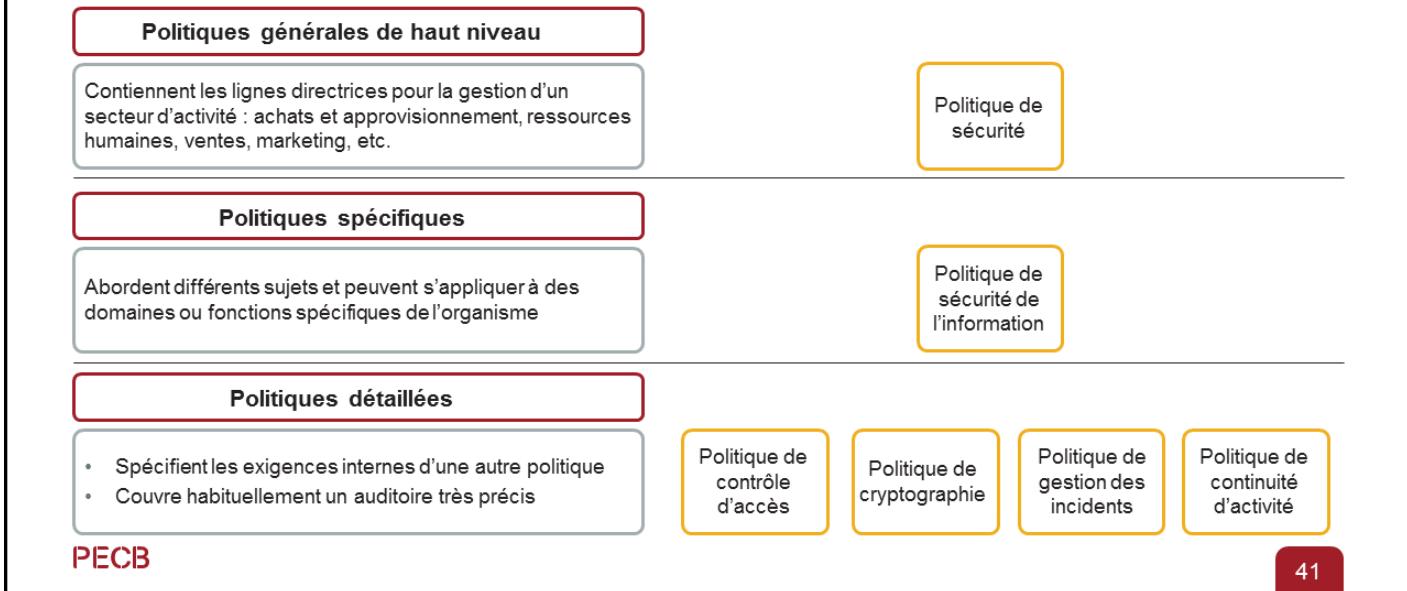
40

Note de terminologie :

Il est important d'éviter de confondre une politique avec une directive, procédure, ligne directrice et autres documents de ce type. La principale caractéristique d'une politique est de fournir une orientation sur un sujet particulier. Des explications détaillées seront fournies dans plusieurs sections du jour 3 de la formation sur la rédaction d'autres types de documents.

Types de politiques

ISO/IEC 27003, Annexe A



La politique de l'organisme est communément identifiée comme une expression formaliste des normes de comportements applicables au sein d'un organisme. Elle définit (sans toutefois les décrire systématiquement) des manières d'agir conformément à ce qui est attendu dans divers domaines où il peut s'avérer nécessaire de mieux définir le cadre organisationnel de travail.

On distingue généralement trois niveaux de politiques au sein d'un organisme :

1.Les politiques générales de haut niveau définissent un cadre général dans lequel la sécurité de l'information sera assurée et les objectifs généraux visant à assurer la continuité de l'activité et à limiter ou prévenir les dommages potentiels aux actifs de l'organisation à un niveau acceptable et, à ce titre, à limiter les conséquences potentielles des incidents de sécurité.

2.Les politiques spécifiques définissent un sous-ensemble de règles et de pratiques encore assez générales, mais qui sont relatives à un domaine précis. Elles sont subordonnées aux politiques générales de haut niveau, le plus souvent.

Note: Ces deux types de politiques sont habituellement soumises à un processus de revue plutôt formaliste et relativement contraignant en raison de leur nature sensible par rapport à la stratégie fonctionnelle de l'organisme qu'elles sont censées soutenir.

3.Les politiques détaillées viennent en appui à la politique de sécurité de l'information (politique spécifique). Elles permettent de préciser les exigences en matière de sécurité interne. Elles déterminent la procédure en vue d'assurer la sécurité de l'information dans des domaines d'application spécifiques. À titre d'exemples, on peut citer les politiques suivantes : politique de sécurité des droits d'accès aux informations et aux infrastructures technologiques, politique sur l'utilisation d'Internet, politique sur l'archivage et la destruction de documents, etc.

Note : Certaines de ces politiques détaillées sont indépendantes, tandis que d'autres sont dépendantes d'une autre politique. Par exemple, un organisme peut avoir une politique de sécurité qui est complétée par des politiques de sécurité physique et de sécurité de l'information. À son tour, la politique de sécurité de l'information peut être la référence pour la publication de politiques spécifiques telles que la politique sur le contrôle d'accès.

1.5 Politique de sécurité de l'information

Liste des activités

1.5.1

Créer des modèles de politiques

1.5.6

Mener des séances de formation et de sensibilisation

1.5.2

Rédiger la politique de sécurité de l'information

1.5.7

Contrôler, évaluer et revoir les politiques

1.5.3

Rédiger des politiques de sécurité spécifiques

1.5.4

Obtenir l'approbation de la direction

1.5.5

Publier et diffuser les politiques

PECB

42

1.5.1 Créer des modèles de politiques

ISO/IEC 27003, Annexe A

- | | |
|--|--|
| <p>1 Administratif</p> <p>2 Résumé de la politique</p> <p>3 Introduction</p> <p>4 Périmètre</p> <p>5 Objectifs</p> | <p>6 Principes</p> <p>7 Responsabilités</p> <p>8 Principaux résultats</p> <p>9 Politiques connexes</p> <p>10 Exigences de la politique</p> |
|--|--|



PECB

43

Avant de rédiger les politiques de l'organisme, il est important de définir une structure type en construisant des modèles. Ceci permet de ne pas oublier un élément important dans la formulation d'une politique, car le document abordera tous les éléments clés d'une telle politique pour couvrir une variété d'environnements où les niveaux de risque sont différents.

Page de notes

PECB

44

ISO/IEC 27003, Annexe A propose de structurer les politiques comme suit :

1. **Administratif** : Titre de la police, version, dates de publication/validité, historique des modifications, propriétaire et approbateur, classification, public visé, etc.
2. **Résumé de la politique** : Une ou deux phrases sommaires (peut être combiné à l'introduction)
3. **Introduction** : Brève explication du sujet de la politique.
4. **Périmètre** : Décrit les parties ou les activités d'un organisme qui sont touchées par la politique. S'il y a lieu, l'article du périmètre énumère les autres politiques qui sont soutenues par la présente politique.
5. **Objectifs** : Décrit les objectifs de la politique.
6. **Principes** : Décrit les règles visant les actions et les décisions nécessaires pour atteindre les objectifs. Dans certains cas, il peut être utile d'identifier les processus clés associés à la politique et ensuite les règles pour exploiter ces processus.
7. **Responsabilités** : Décrit qui est responsable des mesures à prendre pour satisfaire aux exigences de la politique. Dans certains cas, peut comprendre une description des dispositions organisationnelles ainsi que les responsabilités et les autorités des personnes ayant des rôles désignés.
8. **Principaux résultats** : Décrit les résultats de l'organisme si les objectifs sont atteints. Dans certains cas, peut être combiné aux objectifs.
9. **Politiques connexes** : Décrit d'autres politiques pertinentes à l'atteinte des objectifs, habituellement en fournissant des détails supplémentaires sur des sujets précis.
10. **Exigences de la politique** : Décrit en détail les exigences de la politique.

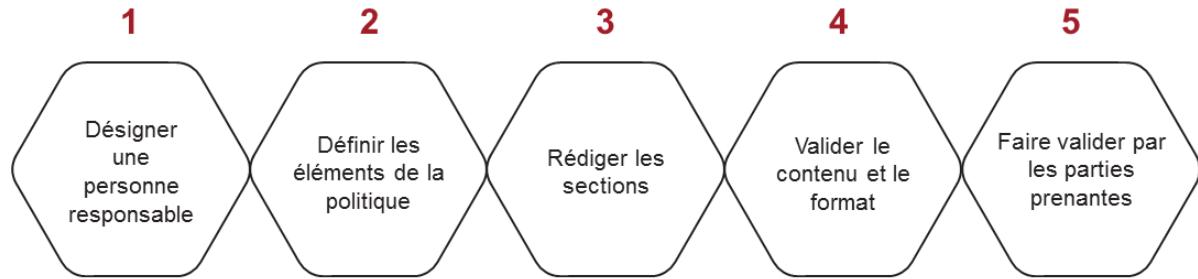
D'autres rubriques peuvent être ajoutées au modèle de politique d'un organisme. Communément, on y retrouve :

11.Définitions : Contient une liste des thèmes utilisés.

12.Sanctions : Décrit la liste des sanctions possibles si un utilisateur enfreint la politique ou inclut une mention générale du type : «Tout utilisateur qui contrevient à la présente politique est passible de sanctions disciplinaires pouvant aller jusqu'au congédiement, incluant des poursuites judiciaires. »

Processus de rédaction d'une politique

Processus général



Il est important d'obtenir l'adhésion à une politique et sa compréhension d'avant sa publication

PECB

45

Après la création du modèle type d'une politique, il faut définir le processus de rédaction des politiques. Voici les étapes typiques du processus de rédaction d'une politique :

1. **Désigner une personne responsable** : Un responsable devrait être désigné et mandaté par la direction pour développer, revoir et évaluer la politique à publier. Habituellement, le responsable de la sécurité de l'information (CISO) est responsable de la gestion et du suivi de la politique de sécurité de l'information ainsi que de politiques détaillées reliées directement à la sécurité. D'autre part, plusieurs des politiques qui peuvent être incluses dans le SMSI sont habituellement la responsabilité d'autres responsables, comme la politique d'achat de matériel TI ou la politique de sécurité physique.
2. **Définir les éléments de la politique** : L'équipe chargée de la politique dresse une liste de tous les sujets qui doivent être traités dans la politique. Au minimum, la politique de sécurité de l'information doit couvrir les exigences du SMSI selon ISO/IEC 27001, article 5.2.
3. **Rédiger les sections** : L'équipe chargée de la rédaction définit les différentes sections. Il faut s'assurer que les énoncés emploient un langage simple, mais précis afin que la politique soit comprise par toutes les parties concernées par sa publication. En outre, il faut éviter d'inclure des spécifications opérationnelles ou des références à des produits particuliers dans la politique. La politique devrait répondre au «Pourquoi» et surtout au «Quoi», et non au «Comment». Le «Comment» sera détaillé dans les procédures.
4. **Valider le contenu et le format** : Le responsable de la politique doit valider le contenu afin de s'assurer que la politique est conforme aux exigences de la norme ISO/IEC 27001 et aux autres politiques de l'organisme. Par exemple, il serait contradictoire de publier une politique autorisant la surveillance et la lecture de toutes les communications des employés si une politique de l'organisme sur le respect de la vie privée l'interdit ou encore si c'est en violation des lois du pays. En ce qui concerne le format, il faut valider que la politique respecte la procédure de gestion documentaire (article 7.5.3) quant à son cycle de vie.

Page de notes

PECB

46

5. Faire valider par les parties prenantes : Afin de s'assurer de l'adhésion et de la compréhension de la politique, il est courant de consulter les employés, les gestionnaires et autres parties prenantes sur la politique afin de récolter leurs commentaires. L'expérience démontre que l'étape de validation d'une politique peut être assez longue selon la taille de l'organisme, la structure organisationnelle et la diversité des parties prenantes impliquées. L'inclusion de ces éléments a un impact direct sur le temps de validation qui peut représenter une proportion d'une à six fois le temps nécessaire à l'élaboration de la politique elle-même.

1.5.2 Rédiger la politique de sécurité de l'information

Modèle (extrait)

Résumé de la politique de sécurité de l'information	La politique de management de la sécurité de l'information vise à assurer un niveau de sécurité adéquat en termes de confidentialité, de disponibilité et d'intégrité des actifs informationnels de [ABC] contre toutes les menaces auxquelles elle pourrait faire face. Le système de management de la sécurité de l'information établit, met en œuvre, exploite, surveille, effectue des revues, maintient et améliore les processus et les mesures liés à la sécurité de l'information selon une approche basée sur les risques.
Introduction	[ABC] devrait veiller au respect de l'intégrité, de la confidentialité et de la disponibilité de l'information produite dans le cadre du SMSI. [ABC] doit veiller à la protection de ses actifs informationnels contre les menaces internes ou externes, accidentelles ou délibérées.
Périmètre du SMSI	La présente politique soutient les politiques de sécurité et de sécurité de l'information. Elle s'applique à toutes les activités de [ABC] comprises dans le périmètre du système de management de la sécurité de l'information.
Objectifs du SMSI	Assurer la continuité des activités métier essentielles ; garantir que toutes les informations traitées, stockées, échangées ou diffusées par l'organisme sont d'une intégrité absolue ; garantir que toutes les informations pertinentes pour l'organisme seront surveillées et stockées selon des procédures permettant de maintenir une confidentialité appropriée ; offrir un choix de mesures de sécurité appropriées et proportionnées pour protéger les actifs et donner confiance aux parties intéressées ; assurer une gestion efficace et efficiente de la sécurité de l'information.
Principes de la politique de sécurité de l'information	[ABC] doit établir, mettre en œuvre, exploiter, surveiller, réviser, maintenir et améliorer un SMSI en se fondant sur une approche documentée des activités à risque et sur le respect de toutes les exigences de la norme ISO/IEC 27001. [ABC] devrait prendre en compte toutes les exigences légales, réglementaires et contractuelles dans le management du SMSI afin d'éviter de violer ses obligations légales, réglementaires ou contractuelles et ses exigences en matière de sécurité. Les exigences légales et réglementaires seront satisfaites en priorité, même si elles sont incompatibles avec la politique décrite dans ce document. [ABC] doit définir et mettre en œuvre un programme de gestion des risques documenté conformément aux exigences de la norme ISO/IEC 27001. Les critères d'évaluation et d'acceptation des risques doivent être établis, formalisés et approuvés par la direction. La présente politique a été approuvée par la direction et fait l'objet d'une revue annuelle.

PECB

47

La politique de sécurité de l'information est habituellement définie en fonction du périmètre du système de management lui-même. Elle est principalement et intrinsèquement liée aux processus d'affaires [x] que le SMSI est censé couvrir.

Cette politique comprend principalement :

- Un cadre qui permet de définir des objectifs et d'établir une orientation et des lignes directrices pour le management de la sécurité de l'information
- Une prise en compte des obligations légales et réglementaires qui s'imposent à l'organisme ainsi que les autres engagements
- Un alignement de la gestion des risques de la sécurité de l'information sur les objectifs stratégiques de l'organisme
- Une liste des critères permettant d'évaluer les risques de sécurité de l'information
- L'approbation formelle par la direction des mesures mentionnées ci-dessus

Bien que le modèle de politique de sécurité de l'information proposé soit applicable à la plupart des organismes, il convient de l'adapter aux conditions spécifiques de chaque organisme.

Rédiger la politique de sécurité de l'information (suite)

Modèle (extrait)

Responsabilités	La direction a la responsabilité de s'assurer que les objectifs et les plans du SMSI sont établis et revus annuellement lors de la revue de direction, que les rôles et responsabilités en matière de sécurité de l'information sont définis, qu'un programme de sensibilisation à la sécurité est mis en œuvre, qu'un audit interne est mené au moins une fois par an et que les ressources nécessaires pour maintenir et améliorer le SMSI sont fournies. Le responsable de la sécurité de l'information est habilité à intervenir sur tous les aspects de la sécurité de l'information chez [ABC]. Il décide, en général, de l'ensemble des conditions nécessaires au bon fonctionnement du SMSI au moyen de directives administratives, préalablement soumises à la direction. Chaque cadre supérieur a la responsabilité de veiller à ce que les personnes qui travaillent sous son contrôle protègent l'information conformément aux politiques de [ABC]. Les utilisateurs de [ABC] (direction, employés, contractuels et tiers utilisateurs) devraient être conscients des risques pour la sécurité de l'information, de leurs responsabilités et de la nécessité de respecter les politiques pour assurer une protection adéquate de l'information.
Résultats attendus	Des mesures de sécurité de l'information appropriées et proportionnées seront mises en œuvre pour protéger les actifs et donner confiance aux parties intéressées. Les décisions en matière de sécurité de l'information seront prises sur la base d'une évaluation des risques encourus par [ABC]. Les exigences légales, réglementaires et contractuelles de [ABC] en matière de sécurité de l'information seront respectées.
Politiques connexes	Politique de sécurité, politique de gestion des ressources humaines, politique de formation et de développement des compétences du personnel

PECB

48

1.5.3 Rédiger des politiques de sécurité spécifiques

Exemple de politique sur l'utilisation du courrier électronique

Résumé de la politique	Le système de courrier électronique est une ressource appartenant à l'organisme et est à la disposition des utilisateurs à des fins professionnelles. Les e-mails occasionnels et non abusifs à usage personnel sont tolérés dans la mesure où ils sont envoyés pendant le temps libre de l'utilisateur et seulement s'ils ne nuisent pas à l'exécution de son travail.
Introduction	Tous les e-mails sortants de l'entreprise peuvent être identifiés comme faisant partie de son image publique, donc une gestion des e-mails est nécessaire pour éviter le risque que les utilisateurs finissent par ternir cette image. Cette politique vise à réglementer l'utilisation des e-mails pour tous les utilisateurs dans le cadre de leur travail.
Périmètre	Cette politique couvre l'utilisation appropriée de tout e-mail envoyé à partir du compte de l'entreprise. Elle s'applique à tous les employés, membres de la direction et employés contractuels qui utilisent un compte e-mail corporatif fourni par l'entreprise.
Objectifs en matière de sécurité de l'information	Empêcher que l'image publique de l'entreprise ne soit entachée par un usage abusif ou par des adresses électroniques d'entreprise inadéquates mises à la disposition des parties prenantes, afin de prévenir les risques de courrier indésirable (spam) résultant d'un usage abusif du courrier électronique à la fois en interne que par des tiers liés à l'entreprise ou même des organismes extérieurs.

PECB

49

Rédiger des politiques de sécurité spécifiques (suite)

Principes de sécurité de l'information	<ul style="list-style-type: none">Utilisation interdite : Le compte e-mail de l'entreprise ne sera pas utilisé à des fins offensantes, insultantes ou racistes. Tout utilisateur qui trouve ce type d'utilisation entre les mains d'un de ses collègues devrait en informer immédiatement le responsable direct.Personnel : L'utilisation raisonnable des ressources de l'entreprise à des fins personnelles est acceptable, mais les e-mails non professionnels seront enregistrés et classés dans des répertoires différents de ceux utilisés à des fins professionnelles. Il est également interdit de transmettre des chaînes d'e-mails ou des blagues. Cette interdiction s'applique également au relais des e-mails reçus de collègues.Surveillance : Les utilisateurs savent qu'ils n'ont aucune intimité au sujet des e-mails de travail stockés ou envoyés par leurs systèmes. L'entreprise surveillera les messages circulant sur son infrastructure sans notification préalable, sans être obligée de rendre cette surveillance continue, voire obligatoire.Sanctions : Tout utilisateur qui enfreint cette politique de l'utilisation des e-mails peut faire l'objet de mesures disciplinaires, y compris le licenciement ou la résiliation finale de son contrat dans le cas du personnel contractuel.
Responsabilités	Il est de la responsabilité du personnel du management des systèmes d'information, en collaboration avec les Ressources humaines, d'assurer la conformité à la présente politique et de prendre les mesures nécessaires pour l'appliquer. Chaque utilisateur doit connaître la présente politique et doit la respecter. L'utilisation d'e-mails par un utilisateur constitue en soi une acceptation tacite de la politique.
Principaux résultats	Réduire les problèmes liés au spam Utiliser le courrier électronique pour l'emploi par les utilisateurs Préserver l'image de l'entreprise
Politiques connexes	Politique de sécurité de l'information ; les relations publiques et l'utilisation des marques de commerce ; Politique de protection de la vie privée

PECB

50

1.5.4 Obtenir l'approbation de la direction

La politique de sécurité de l'information doit :

- Démontrer l'engagement de la direction
- Être approuvée par la direction

La politique doit être signée par un responsable (souvent le PDG), mais le processus d'approbation peut revenir à un comité :

- Conseil d'administration
- Comité de gestion
- Comité de gouvernance de la sécurité



51

PECB

ISO/IEC 27002, article 5.1.1 Politiques de sécurité de l'information

Préconisations de mise en œuvre

Il convient que les organisations définissent, à leur plus haut niveau, une « politique de sécurité de l'information », qui soit approuvée par la direction et qui décrive l'approche adoptée pour gérer les objectifs de sécurité de l'information.

1.5.5 Publier et diffuser les politiques

Principaux modes de communication



Intranet



Réunion



Distribution de copies papier



Session d'orientation des nouveaux employés

PECB

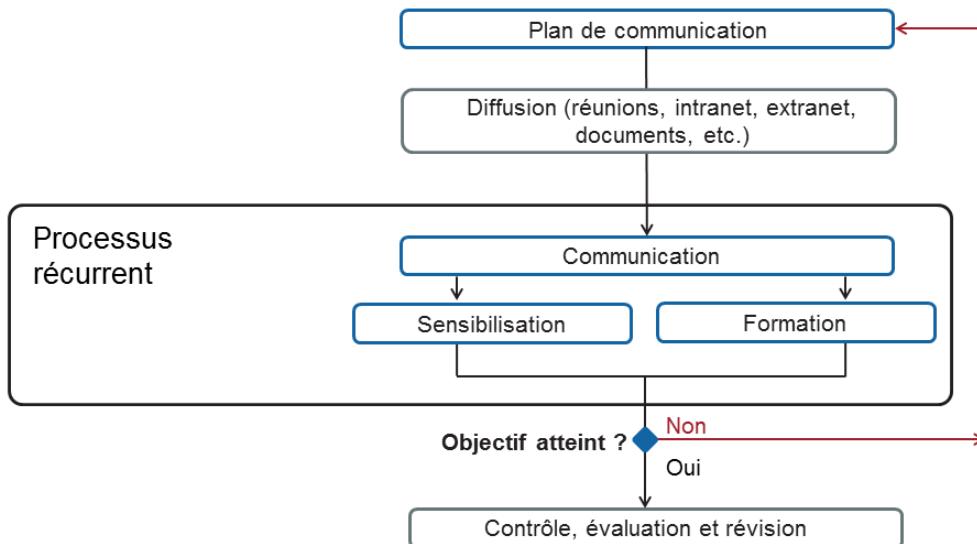
52

Lors de la publication initiale de la politique de sécurité de l'information de l'organisme, il est de bonne pratique (mais non obligatoire) de faire signer la politique par tous les employés de l'organisme, y compris l'équipe de direction. Le formulaire original de signature devrait être conservé dans le dossier de chaque employé au Service des ressources humaines ou par toute autre instance qui en est responsable.

Pour les nouveaux employés, les sensibiliser aux politiques de l'organisation et obtenir leur accord est généralement une étape incluse dans le processus d'accueil et d'intégration d'un nouvel employé.

Si l'on ne procède pas à la signature de la politique, il faut s'assurer d'être en mesure de démontrer que les membres de l'organisme ont compris et appliquent la politique de sécurité de l'information. Par exemple, on peut leur demander de participer à une session de formation.

1.5.6 Mener des séances de formation et de sensibilisation



PECB

53

ISO/IEC 27002, article 5.1.1 Politiques de sécurité de l'information

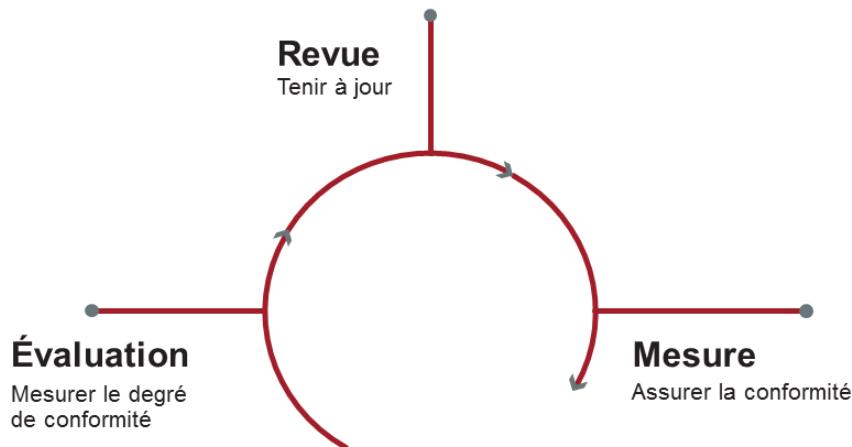
Il convient que ces politiques soient communiquées aux salariés et aux tiers concernés sous une forme pertinente, accessible et compréhensible par leurs destinataires, par exemple dans le contexte d'un « programme d'apprentissage, de formation et de sensibilisation à la sécurité de l'information ».

Pour y parvenir, l'organisme devrait préparer un plan de communication avant la publication de la politique. Ce plan de communication assure la propagation de la politique à l'ensemble du personnel de l'organisme. Une méthode ordonnée de diffusion de la politique de sécurité doit être suivie afin d'atteindre efficacement tous les employés et de s'assurer que chacun a compris et accepte ses responsabilités face à cette politique.

Il est préférable d'entamer la communication de la politique par la publication d'une lettre officielle de la direction. Cette lettre devrait démontrer le soutien et l'engagement de la direction en ce qui concerne la sécurité de l'information dans tout l'organisme.

La politique de sécurité de l'information devrait également être incluse en tant qu'élément à couvrir par les employés dans le programme de sensibilisation à la sécurité de l'information. À ce sujet, voir également la section sur la communication, l'éducation et la formation.

1.5.7 Contrôler, évaluer et revoir les politiques



PECB

54

Le contrôle, l'évaluation et la révision de la politique de sécurité de l'information permettent d'ajuster la politique et d'entrer dans un processus d'amélioration continue. En révisant régulièrement la politique, l'organisme s'assure qu'il reste conforme aux exigences de l'activité et aux contraintes légales.

Mesure: La direction de l'organisme doit s'assurer de la conformité de la politique SI au quotidien dans l'organisme. On doit également prévoir un processus disciplinaire formel pour le personnel ayant enfreint les règles de sécurité. Le processus disciplinaire formel garantit un traitement correct et juste des employés suspectés d'avoir enfreint les règles de sécurité. Il devrait fournir une réponse graduée prenant en considération des facteurs tels que la nature et la gravité de la violation, ainsi que son impact sur l'activité de l'organisme (ISO/IEC 27002, article 7.2.3).

Évaluation : L'organisme doit mettre en place des mécanismes d'évaluation de l'efficacité et de l'application de sa politique SI. Voir aussi la section sur la surveillance et la mesure pour plus de précisions.

Revue: Afin d'assurer son adéquation aux besoins de sécurité de l'organisme, le contenu de la politique SI doit être régulièrement révisé. Pour assurer la pertinence, l'adéquation et l'efficacité de la politique de sécurité de l'information, il convient de réexaminer la politique à intervalles fixés préalablement ou en cas de changements majeurs. En effet, l'apparition de nouvelles menaces et vulnérabilités, l'évolution constante de l'environnement technologique et des façons de faire sont des exemples non exhaustifs d'événements susceptibles d'affecter, partiellement ou en totalité, le caractère opérationnel d'une politique de sécurité.



Questions ?

PECB

55

Section 11

Processus de gestion des risques

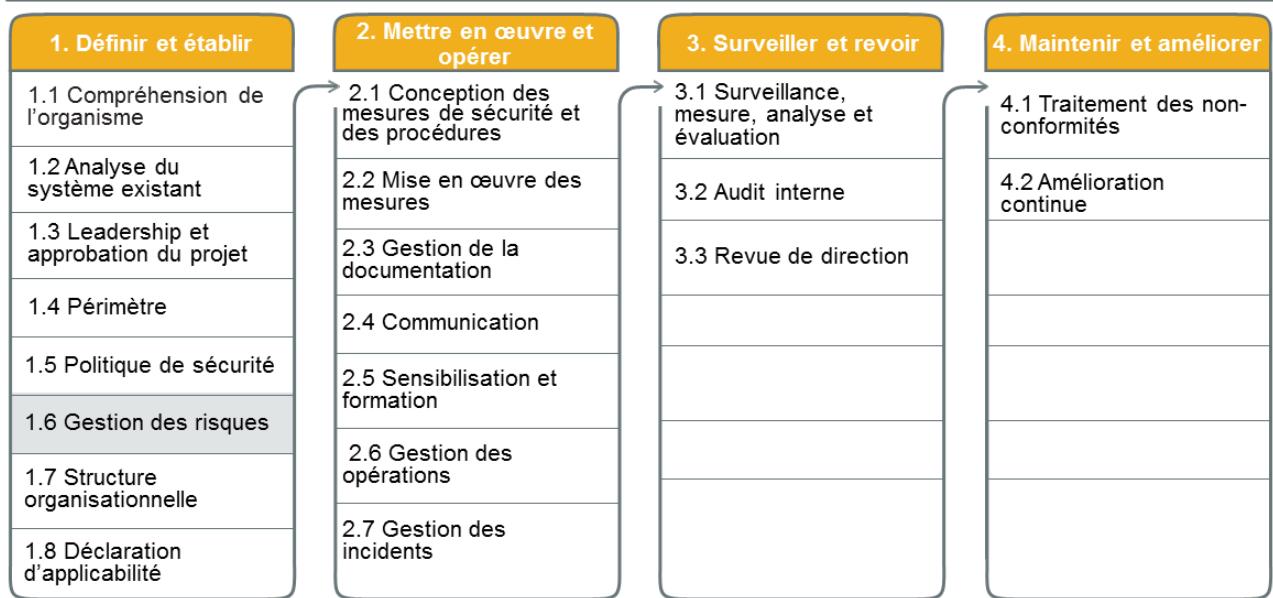
- La norme ISO/IEC 27005
- Approche d'appréciation des risques
- Méthodologie d'appréciation des risques
- Identification des risques
- Estimation des risques
- Évaluation des risques
- Traitement des risques
- Acceptation des risques

PECB

56

Cette section aidera le participant à acquérir des connaissances sur le processus de gestion des risques, qui comprend l'établissement du contexte, l'identification, l'analyse, l'évaluation, le traitement, l'acceptation des risques, ainsi que la communication et la consultation, l'enregistrement et les rapports, la surveillance et la révision.

1.6 Processus de gestion des risques



PECB

57

ISO/IEC 27001 Exigences

ISO/IEC 27001, article 6.1.1

Lorsqu'elle conçoit son système de management de la sécurité de l'information, l'organisation doit tenir compte des enjeux de 4.1 et des exigences de 4.2, et déterminer les risques et opportunités qui nécessitent d'être abordés pour:

- a) *s'assurer que le système de management de la sécurité de l'information peut atteindre le ou les résultats escomptés;*
- b) *empêcher ou limiter les effets indésirables; et*
- c) *appliquer une démarche d'amélioration continue.*

L'organisation doit planifier:

- d) *les actions menées pour traiter ces risques et opportunités; et*
- e) *la manière:*
 - 1) *d'intégrer et de mettre en œuvre les actions au sein des processus du système de management de la sécurité de l'information; et*
 - 2) *d'évaluer l'efficacité de ces actions.*

PECB

58

Un organisme souhaitant se conformer à ISO/IEC27001 doit au moins:

1. Sélectionner et définir une méthodologie d'appréciation des risques
2. Démontrer que la méthodologie choisie fournira des résultats comparables et reproductibles
3. Définir les critères d'acceptation des risques et déterminer les niveaux de risques acceptables

ISO/IEC 27003, article 6.1.1 Généralités

La subdivision des exigences relatives à la prise en compte des risques peut s'expliquer comme suit:

- *elle encourage la compatibilité avec d'autres normes de systèmes de management pour les organismes qui ont des systèmes de management intégrés pour différents aspects tels que la qualité, l'environnement et la sécurité de l'information;*
- *elle exige que l'organisme défuisse et applique des processus complets et détaillés pour l'appréciation et le traitement des risques en matière de sécurité de l'information; et*
- *elle souligne que la gestion des risques liés à la sécurité de l'information est l'élément central d'un SMSI.*

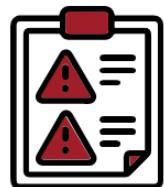
NOTE: Le terme «risque» est défini ainsi : «effet de l'incertitude sur les objectifs» (ISO/IEC 27000:2018, 3.61).

ISO/IEC 27001 Exigences

ISO/IEC 27001, article 6.1.2

L'organisme doit définir et appliquer un processus d'appréciation des risques de sécurité de l'information qui :

- a) établit et tient à jour les critères de risque de sécurité de l'information incluant;
- b) s'assure que la répétition de ces appréciations des risques produit des résultats cohérents, valides et comparables;
- c) identifie les risques de sécurité de l'information;
- d) analyse les risques de sécurité de l'information;
- e) évalue les risques de sécurité de l'information;



59

PECB

ISO/IEC 27001, article 6.1.2 Appréciation des risques de sécurité de l'information (suite)

L'organisme doit définir et appliquer un processus d'appréciation des risques de sécurité de l'information qui :

- a. établit et tient à jour les critères de risque de sécurité de l'information incluant:
 1. les critères d'acceptation des risques;
 2. les critères de réalisation des appréciations des risques de sécurité de l'information;
- b. s'assure que la répétition de ces appréciations des risques produit des résultats cohérents, valides et comparables;
- c. identifie les risques de sécurité de l'information:
 1. applique le processus d'appréciation des risques de sécurité de l'information pour identifier les risques liés à la perte de confidentialité, d'intégrité et de disponibilité des informations entrant dans le domaine d'application du système de management de la sécurité de l'information; et
 2. identifie les propriétaires des risques;
- d. analyse les risques de sécurité de l'information:
 1. apprécie les conséquences potentielles dans le cas où les risques identifiés en 6.1.2 c) 1) se concrétisaient;
 2. procède à une évaluation réaliste de la vraisemblance d'apparition des risques identifiés en 6.1.2 c) 1); et
 3. détermine les niveaux des risques;
- e. évalue les risques de sécurité de l'information:
 1. compare les résultats d'analyse des risques avec les critères de risque déterminés en 6.1.2 a); et
 2. priorise les risques analysés pour le traitement des risques.

L'organisation doit conserver des informations documentées sur le processus d'appréciation des risques de sécurité de l'information.

Page de notes

PECB

60

ISO/IEC 27003, article 6.1.2 Appréciation des risques en sécurité de l'information

Lignes directrices sur l'établissement de critères de risque (6.1.2 a))

Il convient que les critères de risque de sécurité de l'information soient établis en tenant compte du contexte de l'organisme et des exigences des parties intéressées et soient définis conformément aux préférences et aux perceptions des risques de la direction, d'une part, et permettent un processus de gestion des risques réalisable et approprié, d'autre part.

Après avoir établi des critères pour évaluer les conséquences et la vraisemblance des risques en sécurité de l'information, l'organisme devrait également établir une méthode pour les combiner afin de déterminer un niveau de risque. Après avoir établi des critères pour évaluer les conséquences et la vraisemblance des risques en sécurité de l'information, l'organisme devrait également établir une méthode pour les combiner afin de déterminer un niveau de risque.

Après avoir établi des critères pour évaluer les conséquences et la vraisemblance des risques en sécurité de l'information, l'organisme devrait également établir une méthode pour les combiner afin de déterminer un niveau de risque.

Lignes directrices sur la production de résultats d'appréciation cohérents, valides et comparables (6.1.2 b))

Il convient que le processus d'appréciation des risques soit basé sur des méthodes et des outils conçus avec suffisamment de détails afin de conduire à des résultats cohérents, valables et comparables.

Quelle que soit la méthode choisie, le processus d'appréciation des risques en sécurité de l'information devrait assurer que :

- tous les risques, au niveau de détail nécessaire, sont pris en compte;
- ses résultats sont cohérents et reproductibles (c'est-à-dire que l'identification des risques, leur analyse et leur évaluation peuvent être comprises par un tiers et que les résultats sont les mêmes lorsque différentes personnes évaluent les risques dans le même contexte); et
- les résultats des appréciations des risques répétées sont comparables (c'est-à-dire qu'il est possible de comprendre si les niveaux de risque augmentent ou diminuent).

Lignes directrices sur l'identification des risques en sécurité de l'information (6.1.2 c))

Licensed to Boni Leon KOUADIO (noura.dilan@gmail.com)

©Copyrighted material PECB®. Single user license only, copying and networking prohibited. Downloaded: 2020-07-25

L'identification des risques est le processus qui consiste à trouver, reconnaître et décrire les risques. Il s'agit d'identifier les sources de risque, les événements, leurs causes et leurs conséquences potentielles. Le but de l'identification des risques est d'établir une liste complète des risques à partir des événements susceptibles de créer, d'améliorer, de prévenir, de dégrader, d'accélérer ou de retarder la réalisation des objectifs de sécurité de l'information.

Lignes directrices sur l'analyse des risques en sécurité de l'information (6.1.2 d))

L'analyse des risques a pour objectif de déterminer le niveau de risque.

ISO 31000 est référencée dans ISO/IEC 27001 en tant que modèle général. ISO/IEC 27001 exige que, pour chaque risque identifié, l'analyse des risques soit fondée sur l'appréciation des conséquences résultant des risques et sur l'évaluation de la vraisemblance que ces conséquences se produisent pour déterminer un niveau de risque.

Les techniques d'analyse des risques basées sur les conséquences et la vraisemblance peuvent être :

1. *qualitatives, en utilisant une échelle d'attributs qualificatifs (par exemple, élevé, moyen, faible);*
2. *quantitatives, en utilisant une échelle avec des valeurs numériques (p. ex., coût, fréquence ou vraisemblance d'occurrence); ou*
3. *semi-quantitatives, en utilisant des échelles qualitatives avec valeurs assignées.*

Page de notes

PECB

61

Lignes directrices sur l'évaluation des risques en sécurité de l'information (6.1.2 e))

L'évaluation des risques analysés consiste à utiliser les processus décisionnels de l'organisme pour comparer le niveau de risque apprécié pour chaque risque avec les critères d'acceptation prédéterminés afin de déterminer les options de traitement des risques.

ISO/IEC 27001 Exigences

ISO/IEC 27001, article 6.1.3

L'organisation doit définir et appliquer un processus de traitement des risques de sécurité de l'information pour:

- a) choisir les options de traitement des risques appropriées, en tenant compte des résultats de l'appréciation des risques;*
- b) déterminer toutes les mesures nécessaires à la mise en œuvre de(s) (l')option(s) de traitement des risques de sécurité de l'information choisie(s);*
- c) comparer les mesures déterminées ci-dessus en 6.1.3 b) avec celles de l'Annexe A et vérifier qu'aucune mesure nécessaire n'a été omise;*
- d) produire une déclaration d'applicabilité contenant les mesures nécessaires (voir 6.1.3 b) et c)) et la justification de leur insertion, le fait qu'elles soient mises en œuvre ou non, et la justification de l'exclusion de mesures de l'Annexe A;*
- e) élaborer un plan de traitement des risques de sécurité de l'information; et*
- f) obtenir des propriétaires des risques l'approbation du plan de traitement des risques et l'acceptation des risques résiduels de sécurité de l'information.*

PECB

62

ISO/IEC 27003, article 6.1.3 Traitement des risques en sécurité de l'information

Lignes directrices sur les options de traitement des risques en sécurité de l'information (6.1.3 a))

Les options de traitement des risques sont:

- a. éviter les risques en décidant de ne pas commencer ou poursuivre l'activité à l'origine des risques ou en supprimant la source des risques (par exemple, en fermant un portail de commerce électronique);*
- b. prendre des risques supplémentaires ou accroître les risques afin de saisir une opportunité d'affaires (par exemple, ouvrir un portail de commerce électronique);*
- c. modifier les risques en modifiant la vraisemblance (par exemple, réduire les vulnérabilités) ou les conséquences (par exemple, diversifier les actifs), ou les deux;*
- d. partager les risques avec d'autres parties par l'assurance, la sous-traitance ou le financement des risques; et*
- e. conserver les risques en fonction des critères d'acceptation des risques ou par décision éclairée (par exemple, maintenir le portail de commerce électronique existant tel qu'il est).*

Lignes directrices sur la détermination des mesures de sécurité nécessaires (6.1.3 b))

Il convient qu'une attention particulière soit accordée à la détermination des mesures de sécurité de l'information nécessaires. Il convient que toute mesure soit déterminée en fonction des risques de sécurité de l'information précédemment appréciés. Si un organisme a une mauvaise appréciation des risques de sécurité de l'information, elle a une mauvaise base pour son choix de contrôles de la sécurité de l'information.

Lignes directrices sur la comparaison avec les mesures d'ISO/IEC 27001:2013, Annexe A (6.1.3 c))

ISO/IEC 27001:2013, Annexe A comprend une liste complète des objectifs et des mesures. Les utilisateurs du présent document sont priés de se reporter à la représentation générique des mesures dans l'Annexe A d'ISO/IEC 27001:2013 pour s'assurer qu'aucune mesure nécessaire n'est négligée. En comparaison avec ISO/IEC 27001:2013, l'Annexe A peut également identifier des mesures autres que celles déterminées en 6.1.3 b) qui peuvent être plus efficaces pour modifier les risques en sécurité de l'information.

Page de notes

PECB

63

Lignes directrices sur la production d'une déclaration d'applicabilité (SoA) (6.1.3 d))

Le SoA contient:

- toutes les mesures nécessaires (tel que déterminé aux Articles 6.1.3 et 6.1.3 b) c)) et, pour chaque mesure:
 - la justification de l'inclusion de la mesure ; et
 - que la mesure soit mise en œuvre ou non (par exemple, entièrement mis en œuvre, en cours, pas encore commencé) ; et
 - la justification de l'exclusion de l'une des mesures d'ISO/IEC 27001:2013, Annexe A.

Lignes directrices sur la formulation d'un plan de traitement des risques en sécurité de l'information (6.1.3 e))

ISO/IEC 27001:2013 ne spécifie pas de structure ou de contenu pour le plan de traitement des risques en sécurité de l'information. Cependant, il convient que le plan soit formulé à partir des éléments sortants de 6.1.3 a) à c). Ainsi, le plan devrait documenter pour chaque risque traité :

- options de traitement choisies;
- mesures nécessaires; et
- état de mise en œuvre.

D'autres contenus utiles peuvent inclure :

- propriétaire de risque; et
- risques résiduels prévus après la mise en œuvre des actions.

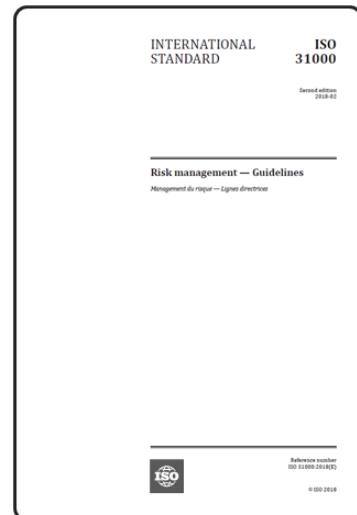
Lignes directrices sur l'obtention de l'approbation des propriétaires de risques (6.1.3 f))

Lorsque le plan de traitement des risques en sécurité de l'information est formulé, il convient que l'organisme obtienne l'autorisation des propriétaires de risques. Il convient que cette autorisation soit fondée sur des critères d'acceptation des risques définis ou une concession justifiée s'il y a une déviation.

Dans le cadre de ses processus de management, il convient que l'organisme enregistre l'acceptation du risque résiduel par le propriétaire du risque et l'approbation du plan par la direction.

ISO 31000

- ISO 31000 fournit un cadre générique de management du risque.
- Elle peut s'appliquer à tout type de risque, indépendamment de sa nature ou de ses conséquences.
- Elle n'est pas destinée à des fins de certification.



PECB

64

ISO 31000, article 1 Domaine d'application

Le présent document fournit des lignes directrices concernant le management du risque auquel sont confrontés les organismes. L'application de ces lignes directrices peut être adaptée à tout organisme et à son contexte.

Le présent document fournit une approche générique permettant de gérer toute forme de risque et n'est pas spécifique à une industrie ou un secteur.

Le présent document peut être utilisé tout au long de la vie de l'organisme et peut être appliqué à toute activité, y compris la prise de décisions à tous les niveaux.

Étant donné qu'ISO 31000 ne fournit pas de méthode spécifique de management du risque dans le contexte du SMSI, il appartient à chaque organisme d'en identifier et d'en sélectionner une qui correspond à son contexte, ses activités commerciales et ses pratiques de management et opérationnelles.

ISO/IEC 27005

- Adaptation du cadre de référence d'ISO 31000 à la sécurité de l'information
- Aligné sur les exigences d'ISO/IEC 27001
- Répond au « quoi ? » et au « pourquoi ? » la gestion des risques s'applique à la sécurité de l'information
- Chaque organisation doit choisir une méthodologie d'appréciation des risques adaptée à son contexte.



PECB

65

ISO/IEC 27005, article 1 Domaine d'application

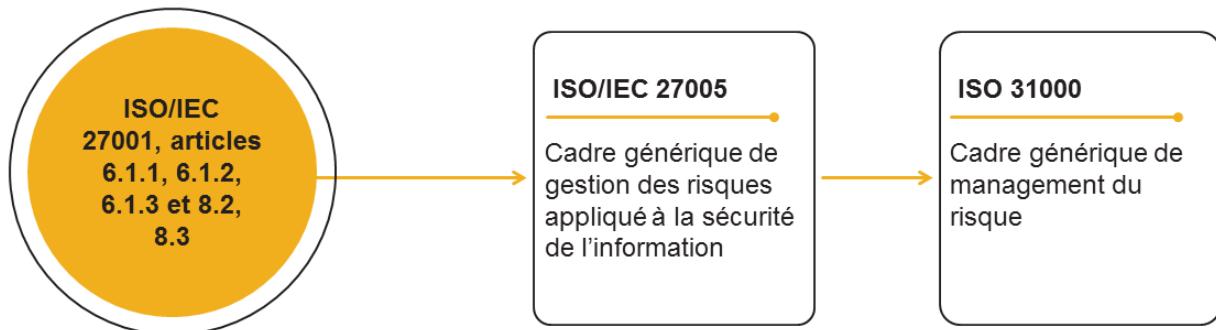
Le présent document contient des lignes directrices relatives à la gestion des risques en sécurité de l'information.

Le présent document appuie les concepts généraux énoncés dans l'ISO/IEC27001; il est conçu pour aider à la mise en place de la sécurité de l'information basée sur une approche de gestion des risques.

Il est important de connaître les concepts, les modèles, les processus et les terminologies décrites dans l'ISO/IEC27001et l'ISO/IEC27002afin de bien comprendre le présent document.

Le présent document est applicable à tous types d'organismes (par exemple les entreprises commerciales, les agences gouvernementales, les organisations à but non lucratif) qui ont l'intention de gérer des risques susceptibles de compromettre la sécurité des informations de l'organisme.

Liens entre les normes ISO/IEC 27001, ISO/IEC 27005 et ISO 31000



Note importante : Il n'est pas obligatoire de se référer à ISO/IEC 27005 et à ISO 31000 pour obtenir une certification ISO/IEC 27001.

PECB

66

Basée sur la structure d'ISO 31000, la norme ISO/IEC 27005 explique en détail comment mener l'appréciation et le traitement des risques, dans le cadre de la sécurité de l'information. Il s'agit de la mise en œuvre du cycle d'amélioration continue PDCA (Planifier, Déployer, Contrôler, Agir) pour la gestion des risques telle qu'il est utilisé dans toutes les normes des systèmes de management. Dans ce cas, ISO/IEC 27005 peut être assez facilement reliée aux articles correspondants de la norme ISO/IEC 27001 sur la gestion des risques (articles 6.1.2 et 6.1.3), ce qui conduit finalement à la certification de l'organisation.

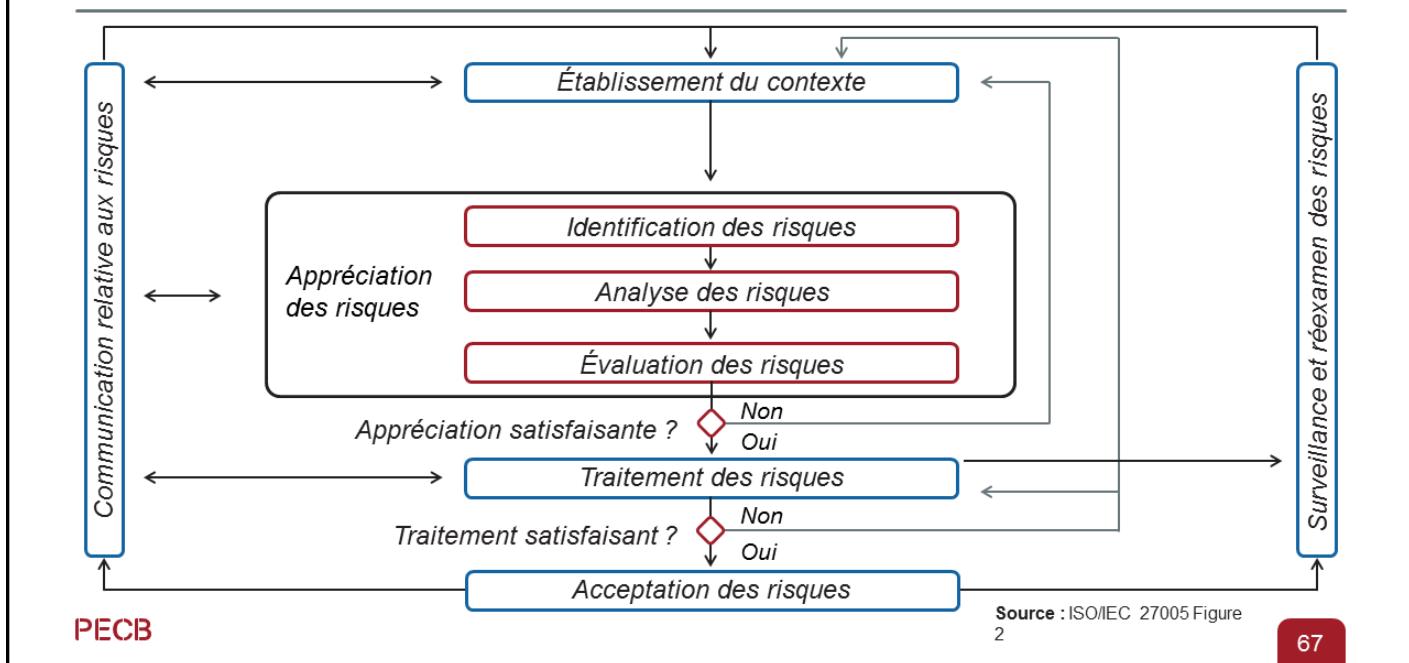
ISO/IEC 27005Introduction

Le présent document contient des lignes directrices relatives à la gestion des risques en sécurité de l'information dans un organisme. Cependant, le présent document ne fournit aucune méthodologie spécifique à la gestion des risques en sécurité de l'information. Il est du ressort de chaque organisme de définir son approche de la gestion des risques, en fonction, par exemple, du périmètre d'un système de management de la sécurité de l'information (SMSI), de ce qui existe dans l'organisme dans le domaine de la gestion des risques, ou encore de son secteur industriel. Plusieurs méthodologies existantes peuvent être utilisées en cohérence avec le cadre décrit dans le présent document pour appliquer les exigences du SMSI. Le présent document est fondé sur la méthode d'identification des risques liés à des actifs, des menaces et des vulnérabilités, qui n'est plus exigée par l'ISO/IEC 27001; il existe d'autres approches qui peuvent être utilisées.

Le présent document ne contient pas de préconisations directes concernant la mise en œuvre des exigences du SMSI spécifiées dans l'ISO/IEC 27001.

Le présent document s'adresse aux responsables et aux personnels concernés par la gestion des risques en sécurité de l'information au sein d'un organisme et, le cas échéant, aux tiers prenant part à ces activités.

Processus de gestion des risques



Comme le montre la figure ci-dessus, le processus de gestion des risques peut être itératif pour les activités d'appréciation ainsi que le traitement des risques. Si les activités d'appréciation des risques ont fourni suffisamment de preuves que les mesures déterminées réduiront les risques à un niveau acceptable, l'étape suivante consiste à mettre en œuvre des options de traitement des risques. Toutefois, si les informations sont insuffisantes pour déterminer le niveau de risque ou que le niveau de risque projeté après traitement est inacceptable, une nouvelle itération de l'appréciation des risques devra être conduite pour des parties ou la totalité du périmètre. Si le traitement des risques n'est pas suffisant et que l'établissement du contexte et l'appréciation des risques sont corrects, une nouvelle itération du traitement des risques sera effectuée, sinon, une nouvelle itération de l'établissement du contexte sera conduite.

L'efficacité du traitement des risques peut dépendre en partie de l'exactitude de l'appréciation des risques. Il est possible que le traitement des risques n'aboutisse pas directement à un niveau acceptable de risque résiduel et, si tel est le cas, une nouvelle itération de l'appréciation des risques devrait être entreprise.

La communication des risques aux parties intéressées de l'organisation et la surveillance des risques constituent des activités continues.

1.6 Gestion des risques

Liste des activités

1.6.1

Établissement du contexte

1.6.6

Acceptation des risques

1.6.2

Identification des risques

1.6.7

Communication relative aux risques

1.6.3

Analyse des risques

1.6.8

Enregistrement et élaboration de rapports

1.6.4

Évaluation des risques

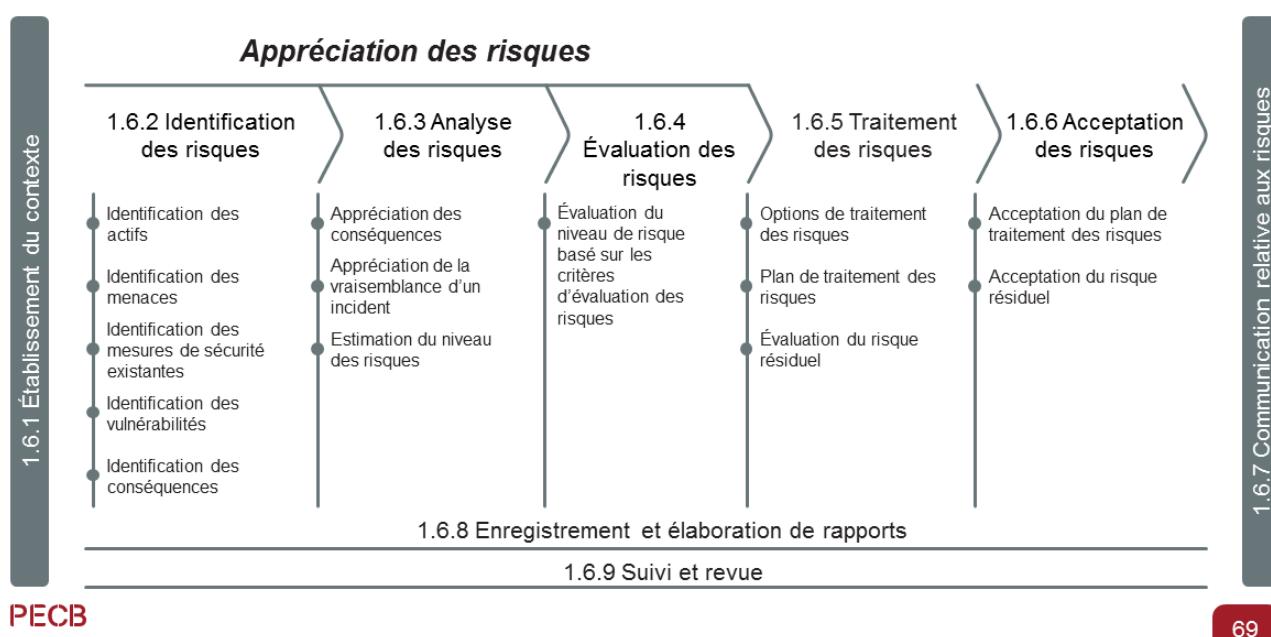
1.6.9

Suivi et revue

1.6.5

Traitement des risques

Processus de gestion des risques de PECB



Note importante:

Il convient de noter que le processus de gestion des risques n'est pas un processus autonome, comme pourrait le suggérer le diagramme de la diapositive. La norme ISO 31000 souligne l'importance d'intégrer le processus de gestion des risques dans les processus, activités ou systèmes de l'organisation.

1.6.1 Établissement du contexte

ISO/TR 31004, article 3.3.3.1

Il convient d'évaluer les modalités existantes du management du risque de l'organisme, en incluant le contexte et la culture.

a

Il est important de tenir compte de toutes les obligations légales, réglementaires ou commerciales, ainsi que des exigences de certification découlant des systèmes de management et des normes auxquels l'organisme a choisi d'adhérer. L'objectif de cette étape est de permettre une adaptation personnalisée et minutieuse de la conception du cadre organisationnel de management du risque et du plan de mise en œuvre, ainsi que de permettre leur alignement sur la structure, la culture et le système général de management de l'organisme.

b

Il est important d'étudier le processus utilisé pour gérer les risques et les aspects du cadre organisationnel de management du risque existant permettant la mise en pratique de ce processus.

c

Il convient de définir des critères de risque appropriés. Les critères de risque doivent être cohérents avec les objectifs de l'organisme et alignés sur son attitude face au risque. Si les objectifs changent, les critères de risque nécessitent d'être ajustés en conséquence. Il est important pour un management du risque efficace que les critères de risque soient élaborés de sorte à correspondre à l'attitude de l'organisme face au risque et à ses objectifs.

PECB

70

ISO/TR 31004, article 3.3.3.2

En s'appuyant sur les évaluations décrites en 3.3.3.1, il convient que l'organisme détermine quels aspects de l'approche existante du management du risque:

- peuvent être préservés à l'avenir (voire être étendus à d'autres types de prise de décision);*
- nécessitent des modifications ou des améliorations;*
- n'ajoutent plus de valeur et qu'il convient d'abandonner.*

Il convient que l'organisme développe, documente et communique ses modalités de gestion du risque. Il convient que l'importance et le contenu des normes, des principes directeurs et des modèles de l'organisme liés au management du risque reflètent le contexte et la culture organisationnels.

Sélection d'une méthodologie d'appréciation des risques

Critères à considérer

- | | |
|--|---|
| <p>1 Compatibilité avec l'ensemble des critères requis par ISO/IEC 27001</p> <p>2 Vocabulaire de la méthodologie</p> <p>3 Existence d'outils logiciels facilitant l'utilisation</p> <p>4 Documentation, formations, soutien, personnel qualifié disponible</p> | <p>5 Utilisation facile et pragmatique de la méthodologie</p> <p>6 Coût d'utilisation</p> <p>7 Existence de moyens de comparaisons (métriques, études de cas, etc.)</p> |
|--|---|

PECB

71

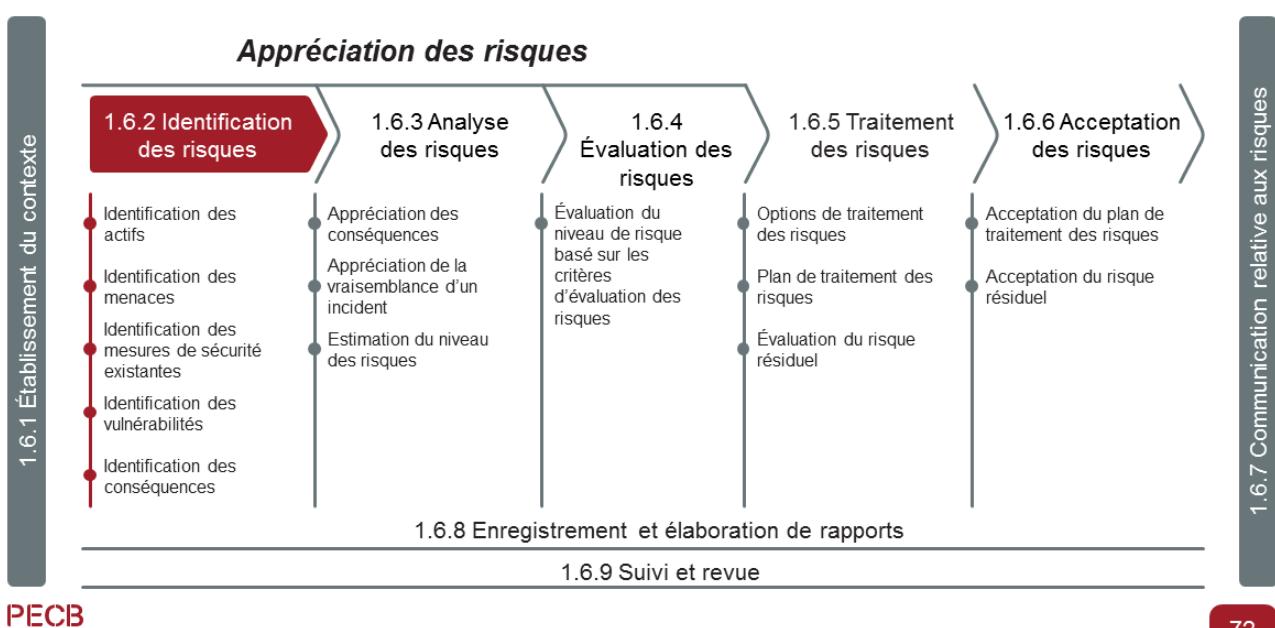
Toute méthodologie de gestion et d'appréciation des risques qui respecte les critères minimaux d'ISO/IEC 27001 est acceptable, même une méthode développée en interne, à condition de pouvoir démontrer qu'elle peut fournir des résultats comparables et reproductibles.

Toute analyse des risques devrait au moins prendre en compte les critères d'évaluation définis par ISO/IEC 27001. Les mesures prises produiront des effets recherchés, elles préviendront et réduiront les effets indésirables et amélioreront également les processus de l'organisation. En outre, l'analyse de risques doit permettre la sélection de critères objectifs pour déterminer un niveau de risque acceptable.

Méthodologie :

- Les impacts potentiels ont-ils été identifiés?
- La probabilité d'occurrence d'une défaillance de sécurité est-elle évaluée?
- Quelqu'un peut-il utiliser les mêmes données et atteindre le même résultat?
- Le processus peut-il être répété et produire des résultats cohérents dans le temps?
- Est-ce que le processus prend en compte l'analyse de l'impact des changements?

1.6.2 Identification des risques



PECB

72

ISO 31000, article 6.4.2 Identification du risque

L'identification du risque a pour but de rechercher, reconnaître et décrire les risques qui peuvent aider ou empêcher un organisme d'atteindre ses objectifs. Il est essentiel que les informations utilisées pour l'identification des risques soient pertinentes, appropriées et à jour.

L'organisme peut utiliser un éventail de techniques pour identifier les incertitudes pouvant avoir une incidence sur un ou plusieurs objectifs. Il convient de prendre en compte les facteurs suivants et leurs relations:

- sources de risque tangibles et intangibles;
- causes et événements;
- menaces et opportunités;
- vulnérabilités et capacités;
- changements intervenus au niveau du contexte externe et interne;
- indicateurs de risques émergents;
- nature et valeur des actifs et des ressources;
- conséquences et leur impact sur les objectifs;
- limitations des connaissances et fiabilité des informations;
- facteurs liés au temps;
- biais, hypothèses et convictions des personnes impliquées.

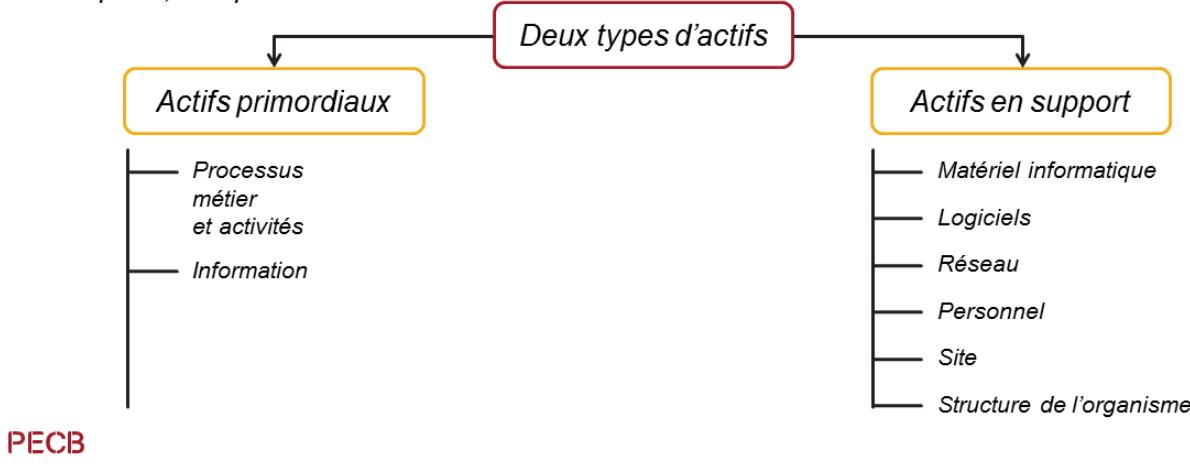
Il convient que l'organisme identifie les risques, que leurs sources soient ou non sous son contrôle. Il convient de tenir compte du fait qu'il peut y avoir plusieurs types de résultat pouvant avoir diverses conséquences tangibles ou intangibles.

Identification des actifs

ISO/IEC 27005, article 8.2.2 et Annexe B.1.1

Définition de l'actif

Un actif désigne tout élément ayant de la valeur pour l'organisme et nécessitant, par conséquent, une protection.



73

ISO/IEC 27005, article 8.2.2 Identification des actifs (suite)

Préconisations de mise en œuvre:

Il convient de réaliser l'identification des actifs à un niveau de détail adapté qui fournit suffisamment d'informations pour l'appréciation des risques. Le niveau de détail utilisé pour l'identification des actifs influence la quantité totale d'informations réunies pendant l'appréciation des risques. Le niveau peut être affiné lors d'itérations ultérieures de l'appréciation des risques.

Il convient d'identifier un propriétaire pour chaque actif afin d'associer à celui-ci une personne responsable et redevable. Le propriétaire de l'actif ne jouit peut-être pas de droits de propriété sur l'actif, mais est responsable de sa production, de son développement, de sa maintenance, de son utilisation et de sa protection selon le cas. Le propriétaire de l'actif est souvent la personne la plus à même de déterminer la valeur qu'il représente pour l'organisme.

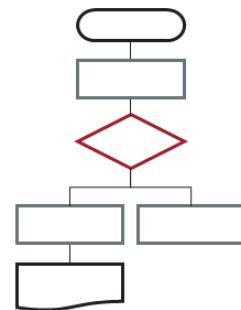
ISO/IEC 27005 divise les actifs en deux grandes catégories :

1. **Actif primordial** : Les actifs primordiaux désignent ceux qui contribuent au processus d'analyse des risques. Ces actifs sont des processus métier et des informations.
2. **Actif en support** : Les actifs en support : comportent le matériel informatique, les logiciels, les réseaux informatiques, le personnel, les sites et les structures organisationnelles.

Identification des processus métier

L'identification des processus métier devrait :

- Soutenir l'organisme dans la réalisation de sa mission
- Être compatible avec les autres processus au sein de l'organisme
- Être liée à une obligation légale ou contractuelle



PECB

74

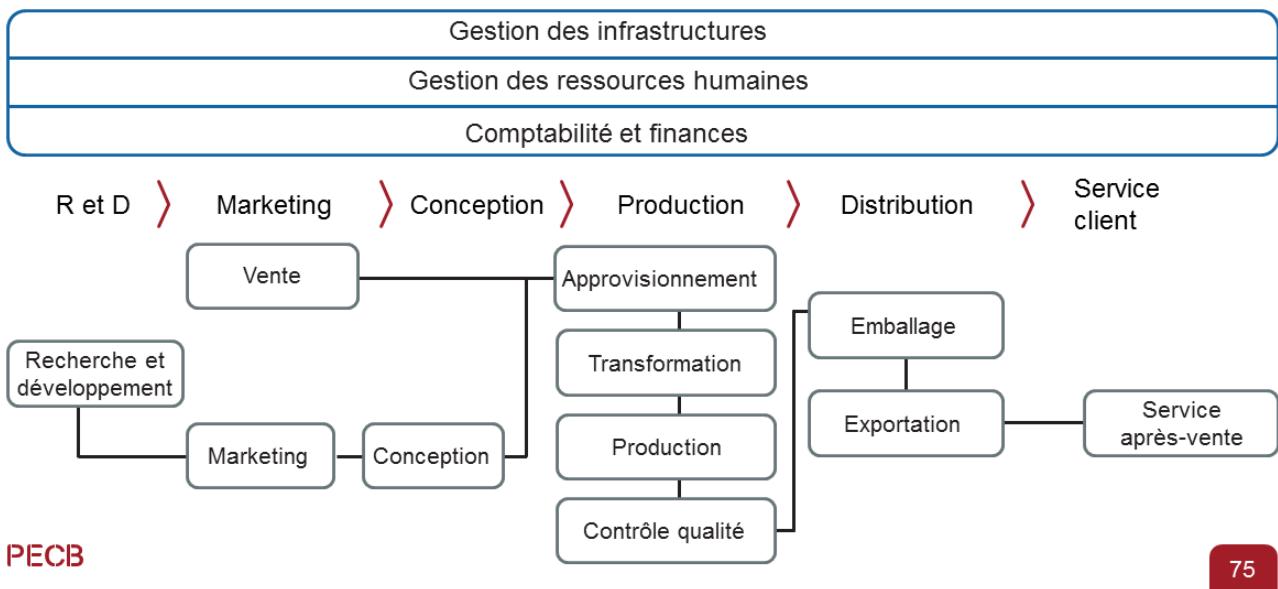
Lors de la cartographie des processus métier, les processus sont divisés en sous-processus, activités et tâches.
Exemple:

1. **Processus:** Comptabilité
2. **Sous-processus :** Gestion des comptes clients, gestion des salaires, etc.
3. **Activités :** Créer les factures, rédiger le rapport mensuel, etc.
4. **Tâches :** Vérifier l'adresse actuelle du client, ajouter des informations au système comptable, etc.

Il est à noter que, lors d'une analyse des risques, un organisme n'est pas dans l'obligation d'entrer dans un niveau de détail si granulaire qu'il inclurait toutes les tâches associées aux processus analysés.

Principaux processus métier

Exemple basé sur la chaîne de valeur de Porter



75

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

Selon Michael Porter, on peut distinguer, parmi les processus impliqués dans la chaîne de valeur :

1. **Processus principaux:** Processus qui contribuent directement à la création de matériel et à la vente de produits tels que la R et D, le marketing, la conception, la production, la distribution et le service clients
2. **Processus de support:** Processus qui soutiennent les activités principales et forment l'infrastructure de l'organisme, comme la gestion de l'infrastructure, la gestion des ressources humaines, la comptabilité et les finances

Identification des actifs informationnels

Actifs informationnels à considérer :

- Actifs vitaux permettant à l'organisme de réaliser sa mission
- Actifs contenant de l'information qui a une valeur économique, administrative ou légale pour l'organisme
- Actifs soumis à des coûts de collecte, d'acquisition ou de stockage

PECB

76

Un organisme possède généralement quantité d'actifs informationnels vitaux. Néanmoins, tous les actifs ne sont pas nécessairement soumis à l'analyse. Cette analyse devrait se limiter aux actifs informationnels qui ont une valeur économique, administrative ou légale pour l'organisme.

Afin de faciliter l'analyse, les actifs informationnels devraient être consolidés en groupes ayant à peu près les mêmes caractéristiques et le même niveau de classification. Par exemple, on peut identifier les données comptables comme un seul actif au lieu de les traiter par sous-ensembles : données salariales, comptes à recevoir, comptes à payer, relevés bancaires, etc.

Voici quelques exemples d'actifs informationnels qui sont fréquemment identifiés comme importants pour l'organisme :

- Dossiers des employés
- Listes de clients
- Plan stratégique de l'organisme
- Configuration de réseau
- Brevets
- Données comptables

Identification des actifs en support

Catégories

Catégorie	Définition	Exemples
Matériel informatique	Tous les éléments physiques qui soutiennent les processus	Serveur, portable, imprimante, disque dur, etc.
Logiciels	Tous les programmes qui contribuent au traitement de données	Système d'exploitation, logiciel de traitement de textes, de comptabilité, etc.
Réseaux	Tous les dispositifs de télécommunications utilisés pour interconnecter plusieurs ordinateurs ou éléments d'un système d'information physiquement distants	Routeur, coupe-feu, câble réseau, commutateur, pont, etc.
Personnel	Toutes les personnes impliquées dans le système d'information	Propriétaire, utilisateur, développeur, dépositaire, client, décideur, etc.
Sites	Endroits physiques où les opérations se déroulent	Bureau, salle de serveur, résidence des employés, zone sécurisée, système d'air conditionné, etc.
Structure de l'organisme	Cadre organisationnel assigné à la réalisation des activités	Siège social, division, département, équipes de projet, sous-traitants, fournisseurs, etc.

PECB

77

Les actifs en support sont généralement les plus faciles à identifier parce qu'ils comprennent les actifs les plus concrets, comme les installations, les meubles et fournitures de bureau, l'équipement TI ainsi que les logiciels.

L'AnnexeB.1.3 de la norme ISO/IEC 27005 fournit des sous-catégories et des exemples pour chacune des catégories d'actifs présentées.

Échelle de valeur d'un actif

Exemple

Échelle	Valeur de l'actif
Négligeable	0
Faible	1
Modéré	2
Haute	3
Très élevée	4

PECB

78

Exemples d'échelles de valeurs des actifs :

- Échelle de considération allant de faible à moyenne, puis élevée.
- Échelle plus granulaire établissant une distinction entre négligeable, faible, moyenne, élevée et très élevée.

Identification des menaces

ISO/IEC 27005, article 8.2.3

Il convient d'identifier les menaces et leurs sources

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

Les menaces peuvent être d'origine naturelle ou humaine et peuvent être accidentnelles ou délibérées. Il convient d'identifier les sources de menace à la fois accidentnelles et délibérées.

Une menace peut survenir de l'intérieur ou de l'extérieur de l'organisme.

Il convient aussi d'identifier les menaces de manière générique et par type (à titre d'exemples: des actions non autorisées, des dommages physiques, des défaillances techniques) puis, lorsque cela est pertinent, des menaces individuelles particulières peuvent être identifiées au sein d'une classe générique.

PECB

79

ISO/IEC 27005, article 8.2.3 Identification des menaces

Certaines menaces peuvent affecter plus d'un actif. Dans ce cas, elles peuvent avoir différentes conséquences selon l'actif affecté.

Les éléments d'entrée de l'identification des menaces et de l'estimation de la vraisemblance (voir 8.3.3) peuvent être obtenus auprès des propriétaires ou des utilisateurs d'actifs, auprès de l'équipe des ressources humaines, auprès des services généraux et des experts en sécurité de l'information, des experts en sécurité physique, du service juridique et d'autres organismes pertinents (y compris des organismes juridiques), des services météorologiques, des compagnies d'assurance et des autorités gouvernementales. Lors du traitement des menaces, il convient que les aspects relatifs à l'environnement et à la culture soient également pris en compte.

Lors de la réalisation d'une appréciation, il convient de tenir compte de l'expérience obtenue en interne à partir d'incidents et d'appréciations de menaces antérieures. Il peut s'avérer utile de consulter d'autres catalogues de menaces (pouvant être spécifiques à un organisme ou à un secteur d'activité) afin de compléter le cas échéant la liste de menaces génériques. Les statistiques et catalogues relatifs aux menaces sont disponibles auprès d'organisations industrielles, d'administrations gouvernementales, d'organismes juridiques, de compagnies d'assurance, etc.

Lors de l'utilisation de catalogues relatifs aux menaces ou de résultats d'appréciations de menaces antérieures, il convient de garder à l'esprit que les menaces sont sans cesse en évolution, notamment lorsque l'environnement de l'activité métier ou les systèmes d'information changent.

Identification des mesures de sécurité existantes

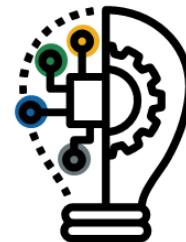
ISO/IEC 27005, article 8.2.4

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

- *la revue des documents contenant des informations relatives aux mesures de sécurité (par exemple, les plans de mise en œuvre du traitement des risques). 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 considéré;*
- *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.*

PECB

80



Pour assurer l'identification des mesures de sécurité existantes et prévues, une comparaison avec l'ensemble des mesures établies à l'Annexe A de la norme ISO/IEC 27001 peut être effectuée. Cela permet d'établir le statut actuel par rapport aux bonnes pratiques de sécurité.

L'identification des mesures de sécurité existantes devrait être faite pour éviter un travail ou des coûts inutiles, par exemple, la duplication de mesures ou la mise en œuvre de mesures inutiles. En outre, tout en identifiant les mesures de sécurité existantes, une analyse de ces mesures devrait être menée pour s'assurer qu'elles fonctionnent correctement. Les revues de direction, les tableaux de bord et les rapports d'audit peuvent également fournir des informations sur l'efficacité des mesures de sécurité existantes.

En plus de considérer les mesures de sécurité déjà en place dans l'organisme, on devrait aussi analyser les mesures de sécurité dont la mise en œuvre est planifiée.

Lors de l'analyse des mesures de sécurité existantes ou planifiées, ces mesures pourraient être jugées inefficaces ou injustifiées. Si les mesures ne sont pas justifiées ou ne permettent pas de traiter un risque, elles devraient être revérifiées afin de déterminer s'il convient qu'elles soient supprimées, remplacées par d'autres mesures plus appropriées, ou s'il est préférable qu'elles restent en place pour des raisons de coûts liés à leur suppression.

Si une mesure de sécurité n'est pas efficace ou ne fonctionne pas comme prévu, elle peut elle-même constituer une vulnérabilité.

Identification des vulnérabilités

ISO/IEC 27005, article 8.2.5

- *Il convient d'identifier les vulnérabilités susceptibles d'être exploitées par des menaces pour nuire aux actifs ou à l'organisme.*
- *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.*



PECB

81

L'appréciation des vulnérabilités peut être compliquée par une perception erronée courante selon laquelle les vulnérabilités des actifs sont associées à des caractéristiques négatives. De nombreuses vulnérabilités ont effectivement des caractéristiques négatives comme un système d'information dont les correctifs (*patches*) ne sont pas à jour.

Par contre, pour d'autres vulnérabilités, les faiblesses peuvent être associées à des caractéristiques positives lesquelles pourraient avoir des effets secondaires indésirables. Par exemple, la mobilité des ordinateurs portables est un avantage souhaitable pour lequel on paie un prix plus élevé, mais cette mobilité augmente la probabilité que l'ordinateur portable soit volé.

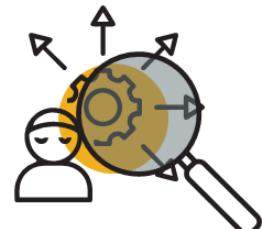
Les vulnérabilités peuvent être intrinsèques ou extrinsèques. Les vulnérabilités intrinsèques sont liées aux caractéristiques inhérentes des actifs. Les vulnérabilités extrinsèques sont liées aux caractéristiques des circonstances spécifiques de l'actif. Par exemple, un serveur qui n'a pas une capacité suffisante pour traiter des données est victime d'une vulnérabilité intrinsèque, et si ce serveur est dans un sous-sol en zone inondable, il est aussi touché par une vulnérabilité extrinsèque.

Identification des conséquences

ISO/IEC 27005, article 8.2.6

Il convient que les organismes identifient les conséquences opérationnelles des scénarios d'incident en termes de (sans s'y limiter):

- temps d'investigation et de réparation;
- temps (de travail) perdu;
- perte d'opportunités;
- santé et sûreté;
- coût financier des compétences spécifiques nécessaires pour réparer les dommages; et
- image et valorisation financière de l'entreprise.



PECB

82

La conséquence des scénarios d'incidents est déterminée sur la base des critères d'impact définis au cours de la phase d'établissement du contexte. Un impact peut découler d'un ou de plusieurs aspects. Les conséquences sur les actifs peuvent être calculées sur la base de sécurités financières ou d'échelles qualitatives. Ces effets peuvent être temporaires ou permanents, comme c'est le cas avec la destruction d'un actif.

La dernière étape de l'identification des risques est l'identification des conséquences des scénarios d'événements à risque. Un scénario d'incident est la description d'une menace exploitant une vulnérabilité ou un ensemble de vulnérabilités liées à la sécurité de l'information et qui engendre une conséquence négative.

Les conséquences de l'occurrence d'un incident peuvent être évaluées différemment selon les parties intéressées impliquées dans l'appréciation des risques. Les impacts significatifs pour l'organisme devraient être documentés en conséquence.

Note terminologique:

ISO/IEC 27001 utilise le terme «impact» et ISO/IEC 27005 «conséquence» et décrit les scénarios d'occurrence d'incident comme des «défaillances de sécurité».



Exercice 6

PECB

83

Exercice6: Identification des menaces, des vulnérabilités et des impacts

Identifiez au moins deux scénarios de menaces et de vulnérabilités associées aux actifs ci-dessous, et indiquez les impacts potentiels. Précisez également si le risque affecterait la confidentialité, l'intégrité et la disponibilité.

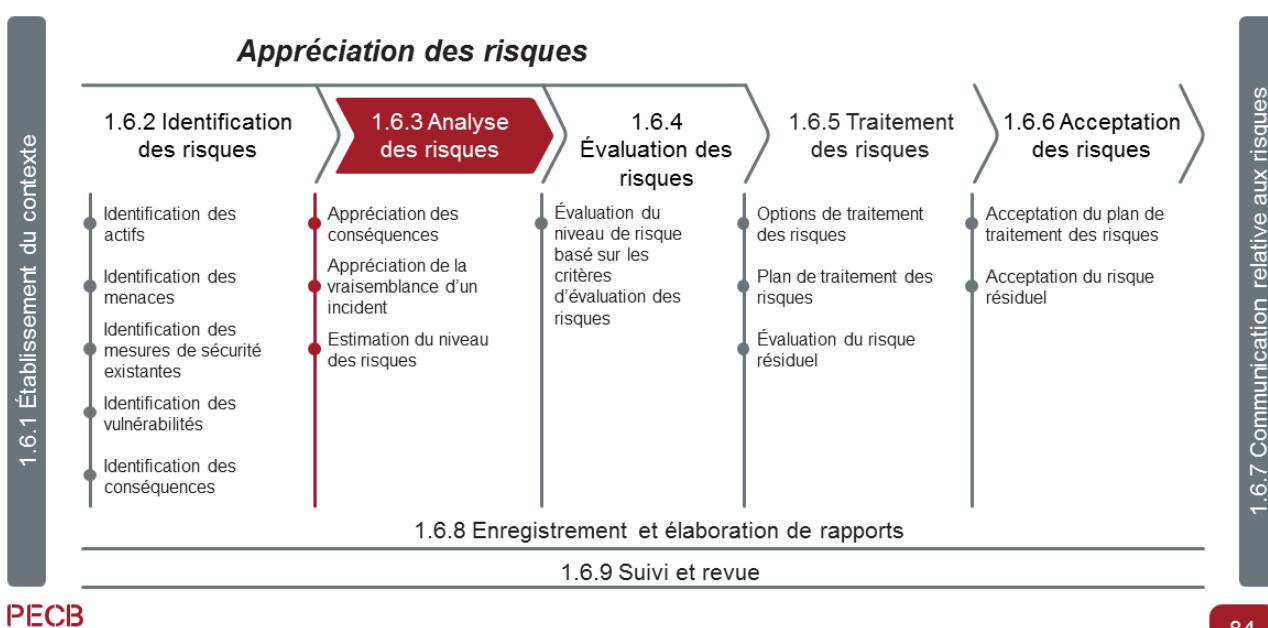
Complétez la matrice des risques et soyez prêt à discuter de vos réponses après l'exercice:

1. Processus de comptabilité
2. Informations personnelles des clients
3. Équipe de guides touristiques

Durée de l'exercice: 20 minutes

Commentaires: 20 minutes

1.6.3 Analyse des risques



ISO 31000, article 6.4.3 Analyse du risque

L'analyse du risque a pour but de comprendre la nature du risque et ses caractéristiques, y compris le niveau de risque, le cas échéant. L'analyse du risque implique la prise en compte détaillée des incertitudes, des sources de risque, des conséquences, de la vraisemblance, des événements, des scénarios, des moyens de maîtrise et de leur efficacité. Un événement peut avoir des causes et conséquences multiples et affecter des objectifs multiples.

L'analyse du risque peut être menée à différents niveaux de détail et de complexité selon la finalité de l'analyse, la disponibilité et la fiabilité des informations et les ressources disponibles. Les techniques d'analyse peuvent être qualitatives, quantitatives, ou une combinaison de celles-ci, selon les circonstances et l'utilisation prévue.

Il convient que l'analyse du risque prenne en compte des facteurs tels que:

- la vraisemblance des événements et des conséquences;
- la nature et l'importance des conséquences;
- la complexité et l'interconnexion;
- les facteurs liés au temps et la volatilité;
- l'efficacité des moyens de maîtrise existants;
- les niveaux de sensibilité et de confiance.

L'analyse du risque peut être influencée par toute divergence d'opinions, biais, perceptions du risque et jugements. Les influences supplémentaires sont la qualité des informations utilisées, les hypothèses et exclusions posées, toute limitation des techniques et la façon dont elles sont mises en œuvre. Il convient que ces influences soient prises en compte, documentées et communiquées aux décideurs.

Les événements extrêmement incertains peuvent être difficiles à quantifier. Cela peut poser problème lors de l'analyse d'événements ayant de graves conséquences. Dans de tels cas, l'utilisation d'une combinaison de techniques permet généralement d'acquérir une connaissance plus approfondie.

Page de notes

PECB

85

L'analyse du risque fournit des données permettant d'évaluer le risque, de prendre la décision de le traiter ou non et de quelle manière, et permet de choisir la stratégie et les méthodes de traitement les plus performantes. Les résultats fournissent des renseignements en vue des décisions quand il faut effectuer des choix et que les options impliquent différents types et niveaux de risque.

Analyse quantitative, semi-quantitative et qualitative des risques

Analyse qualitative

Cette méthode définit les conséquences, la probabilité et le niveau de risque en fonction de catégories ou de niveaux non numériques (par exemple, très faible, faible, moyen, élevé, très élevé), peut combiner les conséquences et la probabilité, et évalue le niveau de risque en fonction de critères qualitatifs.

Analyse semi-quantitative

Cette méthode utilise des échelles numériques d'évaluation des conséquences et des probabilités, et les combine pour produire un niveau de risque à l'aide d'une formule.

Analyse quantitative

Cette méthode estime les valeurs pratiques des conséquences et de leurs probabilités, et produit des valeurs du niveau de risque dans des unités spécifiques définies lors de l'élaboration du contexte.

PECB

86

Analyse qualitative :

Ce type d'appréciation soutient la communication des résultats de risque aux décideurs. Lorsqu'on utilise une approche qualitative de l'analyse des risques, une explication claire de tous les termes employés et de la base de tous les critères devrait être consignée. Pourquoi? Parce qu'à moins que chaque valeur ne soit clairement définie ou caractérisée par des exemples significatifs, différents experts s'appuyant sur leurs expériences individuelles pourraient produire des résultats très différents. Pour remédier à cette situation et augmenter les chances de répétabilité et de reproductibilité, on peut rédiger des notes explicatives pour les valeurs appréciées (par exemple, expliquer que la valeur X est élevée pour des raisons Y, Z) en utilisant des fonctions bien définies pour combiner des valeurs qualitatives.

Analyse semi-quantitative :

Les échelles peuvent être linéaires ou logarithmiques, ou avoir une autre relation ; les formules utilisées peuvent aussi varier. Ce type d'appréciation peut apporter les avantages d'une analyse quantitative et qualitative des risques.

Analyse quantitative :

L'analyse quantitative complète des risques n'est pas toujours possible ou souhaitable en raison d'un manque d'information sur le système ou l'activité analysée, d'un manque de données, de biais, d'hypothèses ou de préjugés des personnes concernées ou simplement parce que les coûts dépassent les avantages d'une analyse quantitative (par exemple, le temps et les efforts des spécialistes, le déploiement et l'utilisation des outils requis.) En outre, la signification des résultats quantitatifs n'est pas toujours claire et peut nécessiter une interprétation et des explications – en particulier pour expliquer les hypothèses et les contraintes liées à l'utilisation des résultats. Dans pareilles circonstances, un classement comparatif semi-quantitatif ou qualitatif des risques par des spécialistes connaissant bien leur domaine respectif peut encore être efficace.

Lorsque la quantification complète a été effectuée, il convient de reconnaître que les niveaux de risque calculés sont des estimations. Il faut veiller à ce qu'on ne leur attribue pas un niveau d'exactitude et de précision incompatible avec l'exactitude des données et des méthodes employées.

Analyse des risques quantitative ou qualitative

Les risques peuvent être appréciés de diverses façons, y compris de manière qualitative, semi-quantitative ou quantitative.

Analyse quantitative des risques

- Utilise des mathématiques
- Données objectives (chiffrées)
- S'exprime en unité monétaire
- Basée sur la capacité des experts à estimer le risque en termes financiers

Analyse qualitative des risques

- Utilise des scénarios de risque
- Données subjectives
- S'exprime sur une échelle descriptive
- Basée sur la perception des risques par les parties intéressées

PECB

87

Chacune des approches présentées ci-dessus a ses avantages et ses inconvénients. 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'organisation. L'approche appropriée peut être choisie en fonction du contexte de l'organisation (environnement interne et externe) et de l'exposition au risque.

Appréciation des conséquences

ISO/IEC 27005, article 8.3.2

- *Un 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 pour l'accomplissement des objectifs métiers de l'organisme.*
- *Cette valorisation peut être déterminée par une analyse d'impact sur l'activité métier. La valeur, déterminée par la conséquence sur l'activité, est souvent nettement supérieure au simple coût de remplacement, en fonction de l'importance que joue l'actif dans l'accomplissement des objectifs métiers de l'organisme.*

PECB

88

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

Facteurs à considérer

ISO/IEC 27005, Annexe B.3

Un impact immédiat (opérationnel) est direct ou indirect.

1) Direct:

- 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; et
- d) les résultats d'impact d'une violation de la sécurité de l'information.

PECB

2) Indirect:

- a) le coût de l'opportunité (les ressources financières nécessaires pour remplacer ou réparer un actif qui aurait été utilisé ailleurs);
- 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; et
- e) la violation des codes éthiques de conduite.

89

L'impact de la perte d'un actif sur les activités est en général nettement plus élevé que le simple coût de remplacement de l'actif. Pour obtenir une estimation correspondant à la réalité, il faut tenir compte à la fois des conséquences directes et indirectes.

Exemple de matrice d'appréciation des risques

ISO/IEC 27005, Tableau E.2

	Très faible vraisemblance	Faible vraisemblance	Vraisemblance moyenne	Vraisemblance élevée	Vraisemblance très élevée
Impact très faible	0	1	2	3	4
Impact faible	1	2	3	4	5
Impact moyen	2	3	4	5	6
Impact élevé	3	4	5	6	7
Impact très élevé	4	5	6	7	8

PECB

90

Des échelles similaires peuvent être développées pour apprécier l'impact sur l'environnement, les actifs, la réputation, etc.

Appréciation de la vraisemblance d'un incident

Niveau	Échelle qualitative	Vraisemblance
0	Très rare	Moins d'une fois par 50 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 année (en moyenne)
4	Probable	Plusieurs fois par année
5	Presque courant	Plusieurs fois par mois
6	Courant	Plusieurs fois par semaine
7	Très courant	Plusieurs fois par jour

PECB

91

Après avoir identifié les scénarios d'incident pertinents et avoir estimé leurs conséquences, il convient d'estimer la probabilité d'occurrence de chaque scénario. Il est nécessaire d'estimer la probabilité réaliste d'un incident de sécurité de l'information et les impacts associés aux mesures de sécurité déjà en place.

Page de notes

PECB

92

IEC 31010:2009, article 5.3.4 Analyse de vraisemblance et estimation de la probabilité

Trois approches générales sont couramment utilisées pour estimer la probabilité. Elles peuvent être utilisées individuellement ou conjointement :

- a. *Utilisation de données historiques pertinentes afin d'identifier des événements ou des situations qui se sont produits dans le passé et ainsi extrapoler la probabilité de leur occurrence dans le futur. Il convient que les données utilisées soient adaptées au type de système, d'installation, d'organisation ou d'activité considéré et aux normes de fonctionnement de l'organisation considérée. Si, du point de vue historique, la fréquence d'occurrence est très faible, il peut s'avérer impossible d'estimer la probabilité. Cela concerne particulièrement les occurrences nulles, lorsque personne ne suppose que l'événement, la situation ou la circonstance va se produire dans le futur.*
- b. *Prévision des probabilités à l'aide de techniques prédictives telles que l'analyse par arbre de panne et l'analyse par arbre d'événements (voir Annexe B). Si les données historiques ne sont pas disponibles ou appropriées, il est nécessaire de déduire les probabilités par une analyse du système, de l'activité, de l'équipement ou de l'organisation ainsi que l'échec ou la réussite qui en découle. Les données numériques liées aux équipements, personnes, organisations et systèmes sur la base d'expériences opérationnelles ou de sources de données publiées sont alors combinées pour produire une estimation de la probabilité de l'événement de tête. Lorsque des techniques prédictives sont utilisées, il est important d'assurer que, lors de l'analyse, il a été dûment tenu compte de l'éventualité de défaillance de mode commun qui implique la défaillance de plusieurs pièces ou composants différents du système. Des techniques de simulation peuvent s'avérer nécessaires pour estimer la probabilité de défaillance des équipements et de la structure du fait du vieillissement et d'autres processus de dégradation, en calculant les effets des incertitudes.*
- c. *L'avis d'un expert peut être utilisé dans un processus systématique et structuré pour estimer la probabilité. Il convient que ces avis experts se fondent sur toutes les informations disponibles applicables, y compris les données historiques, spécifiques au système et à l'organisation, expérimentales, de conception, etc. Il existe un certain nombre de méthodes formelles permettant d'obtenir des avis experts qui fournissent une aide à la formulation de questions appropriées. Les méthodes disponibles comprennent l'approche Delphi, les méthodes de comparaison par paires, de catégorisation et de probabilité absolue.*

Appréciation de la vraisemblance d'un incident

Exemple d'une expression quantitative

- 1 L'année dernière, 730 incidents liés à la réinitialisation du mot de passe ont été signalés par un organisme.
- 2 $730 \text{ incidents} / 365 \text{ jours} = 2 \text{ anomalies/jour}$
- 3 La vraisemblance du scénario d'un incident relié à la réinitialisation du mot de passe dans cet organisme est :

2 incidents par jour

Estimation du niveau des risques

ISO/IEC 27005, article 8.3.4

- *Il convient d'estimer le niveau des risques de tous les scénarios 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. De plus, elle peut prendre en compte les bénéfices en termes de coût, les préoccupations des parties prenantes et d'autres variables en vue de l'évaluation du risque.*
- *Le risque estimé est une combinaison de la vraisemblance d'un scénario d'incident et de ses conséquences.*

PECB

94

Estimation purement numérique

Si l'organisation dispose de données sur les incidents passés ou actuels, en particulier les incidents passés, ces données peuvent être utilisées pour estimer les risques futurs. Néanmoins, il convient d'utiliser également d'autres méthodes pour faire ces estimations.

Bien que les données sur les incidents passés puissent être utiles, elles ne le sont pas nécessairement lorsqu'il s'agit d'évaluer les risques qui découlent de nouvelles activités. L'objectif de l'appréciation des risques découlant des nouvelles activités est d'identifier les incidents à niveau de risque élevé qui n'ont pas encore causé d'incidents. Ainsi, nous pouvons prévenir d'éventuels incidents.

Il est possible de calculer les probabilités d'incidents potentiels en utilisant des données externes. Par exemple, les données antérieures sur les accidents de la route peuvent être utilisées pour calculer les risques de transport routier associés aux employés qui voyagent en voiture. Ces statistiques permettent de calculer les probabilités d'incidents plus graves, mais aussi plus rares. Mais un tel calcul n'est pas toujours possible.

Exemple de matrice d'estimation des risques

ISO/IEC 27005, Tableau E.1

Valeur de l'actif	Vraisemblance – Menace								
	Faible			Modéré			Haute		
	Niveau de vulnérabilité								
0	0	1	2	1	2	3	2	3	4
1	1	2	3	2	3	4	3	4	5
2	2	3	4	3	4	5	4	5	6
3	3	4	5	4	5	6	5	6	7
4	4	5	6	5	6	7	6	7	8

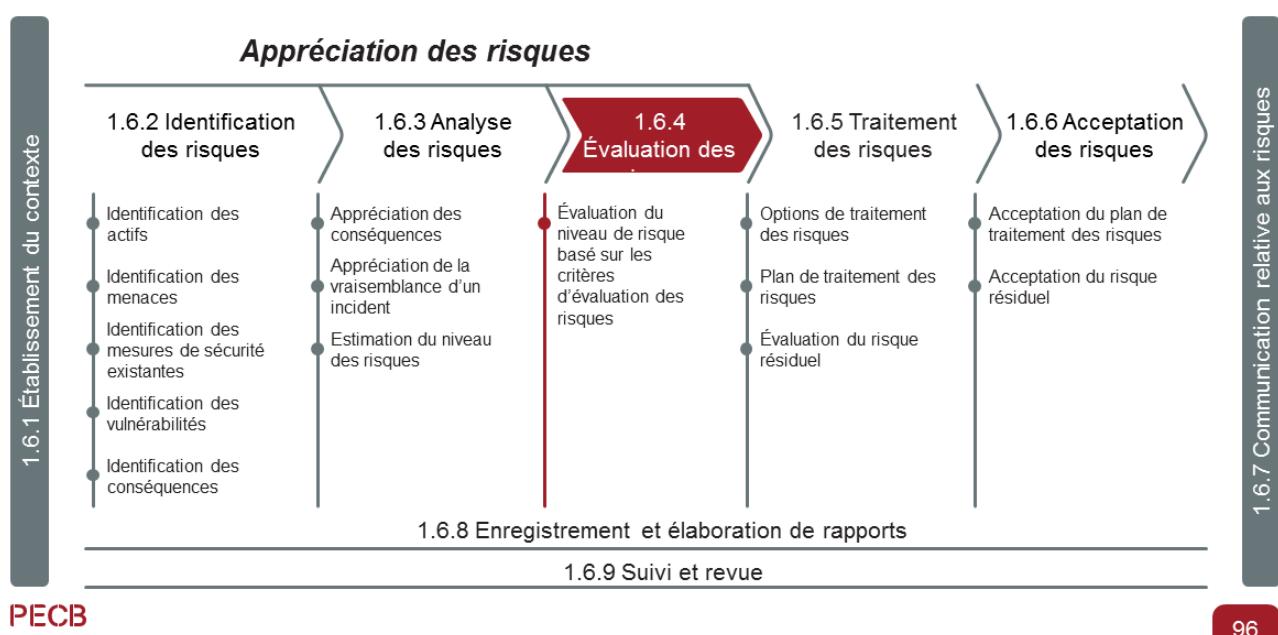
PECB

95

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

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 (mais il convient de prêter une attention particulière au cas où la situation change). 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.

1.6.4 Évaluation des risques



ISO Guide 73, article 3.7.1 Évaluation du risque

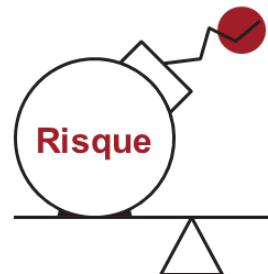
Processus de comparaison des résultats de l'analyse du risque avec les critères du risque afin de déterminer si le risque et/ou son importance sont acceptables ou tolérables

NOTE: L'évaluation du risque aide à la prise de décision relative au traitement du risque

Évaluation du niveau de risque basé sur les critères d'évaluation des risques

ISO 31000, article 6.4.4

- *L'évaluation du risque a pour but de déboucher sur des décisions plus judicieuses.*
- *L'évaluation du risque consiste à comparer les résultats de l'analyse du risque aux critères de risque établis afin de déterminer si une action supplémentaire est exigée.*



PECB

97

ISO/IEC 27005, article 8.4 Évaluation des risques

La nature des décisions relatives à l'évaluation du risque et aux critères d'évaluation du risque utilisés pour prendre ces décisions est définie lors de l'établissement du contexte. À cette étape, il convient que ces décisions et le contexte soient revus en détail au regard des risques identifiés. Afin d'évaluer les risques, il convient que les organismes comparent les risques estimés (à l'aide de méthodes ou d'approches choisies comme abordé dans l'Annexe E) aux critères d'évaluation du risque définis lors de l'établissement du contexte.

Il convient que les critères d'évaluation du risque utilisés pour prendre des décisions soient cohérents avec le contexte interne et externe de gestion des risques en sécurité de l'information et qu'ils tiennent compte des objectifs de l'organisme, du point de vue des parties prenantes etc. Les décisions prises lors de l'activité d'évaluation du risque sont essentiellement basées sur le niveau acceptable de risque. Toutefois, il convient de considérer également les conséquences, la vraisemblance et le degré de confiance dans l'identification et l'analyse des risques. L'agrégation de plusieurs risques faibles ou moyens peut engendrer des risques globaux nettement supérieurs qu'il convient de traiter en conséquence.

Exemple d'évaluation des risques

ISO/IEC 27005, Tableau E.3

Descripteur de menace (a)	Valeur de la conséquence (actif) (b)	Vraisemblance de la menace (c)	Mesure des risques (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

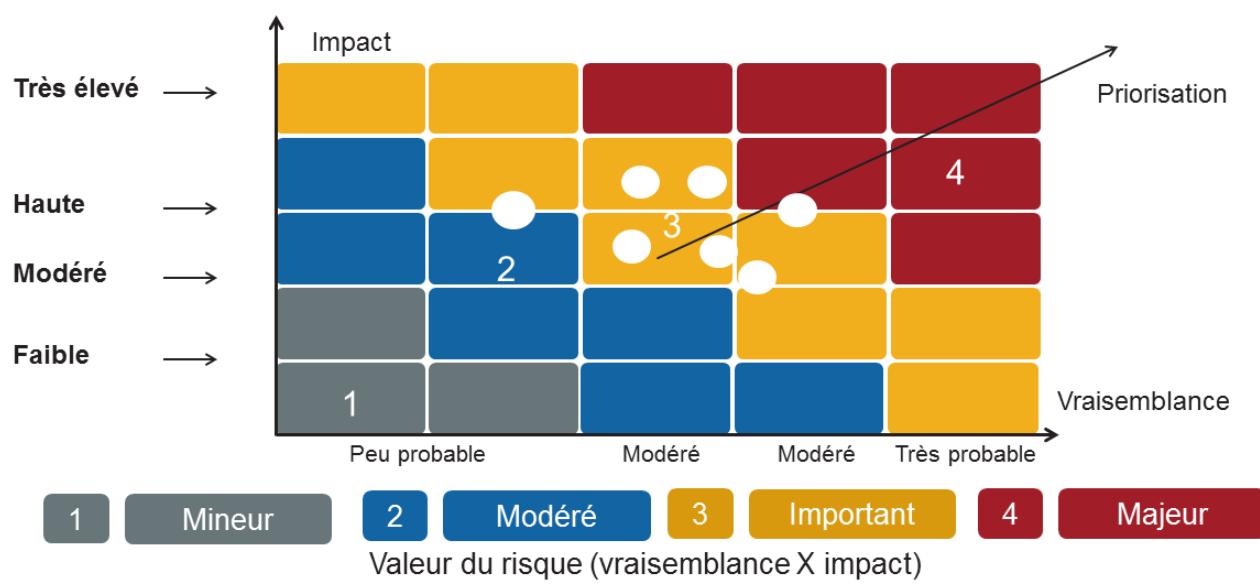
PECB

98

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

Une matrice, ou un tableau identique au Tableau E.3, 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.

Priorisation des risques



PECB

99

La priorisation des risques est un processus couramment utilisé pour identifier les risques qui sont importants et qui ont un impact sur l'organisation. Elle aide également au processus de prise de décisions en tenant compte des réponses possibles à divers risques. Une fois les scénarios d'incidents potentiels élaborés, les critères de classification des risques en fonction de leur priorité doivent être définis.

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

À l'autre bout de l'échelle, il existe un seuil au-delà duquel le risque est intolérable ; il faut alors tout faire pour éliminer sa source ou réduire le risque de façon fiable.

Le graphique de la diapositive, sans fournir de solutions, précise les choix qu'il convient de faire. Ce processus permet, une fois les choix opérés, de les communiquer efficacement et d'améliorer la cohérence interne des actions de l'organisme par rapport à ses choix fondamentaux.

Les zones définies peuvent être éventuellement reportées sur n'importe quelle matrice des risques pour classifier chaque incident générique potentiel et définir le type d'action requis dans chaque cas.

Exemple d'appréciation des risques

Considérations

- L'exemple présenté dans les diapositives suivantes :
 - ▷ Ne provient d'aucune méthode particulière d'appréciation des risques
 - ▷ Sert simplement à illustrer les liens entre la logique et les concepts
 - ▷ Fournit des tableaux récapitulatifs similaires utilisés selon les outils des méthodes courantes
- Les valeurs des échelles de l'exemple ont été volontairement réduites (souvent de 1 à 5) pour faciliter la représentation des données.

Exemple d'appréciation des risques

Identification des actifs

Identifier d'abord certains actifs dans le périmètre.

Actif	Menace	Vulnérabilité	Impact			Vraisemblance	Risque
			C	I	D		
Ordinateur portable							
Serveur de fichiers							
Contrats clients							
Données sur les patients							

PECB

101

Exemple d'appréciation des risques

Identification des menaces

Ensuite, identifier les menaces pour chaque actif (par souci de simplicité, n'identifier qu'une seule menace par actif).

Actif	Menace	Vulnérabilité	Impact			Vraisemblance	Risque
			C	I	D		
Ordinateur portable	Vol						
Serveur de fichiers	Virus						
Contrats clients	Vol						
Données sur les patients	Divulgation						

PECB

102

Exemple d'appréciation des risques

Identification des vulnérabilités

Ensuite, identifier la vulnérabilité pour chaque menace (par souci de simplicité, n'identifier qu'une seule vulnérabilité par menace).

Actif	Menace	Vulnérabilité	Impact			Vraisemblance	Risque
			C	I	D		
Ordinateur portable	Vol	Portabilité					
Serveur de fichiers	Virus	Antivirus faible					
Contrats clients	Vol	Pas de coffre-fort					
Données sur les patients	Divulgation	Accès non contrôlé					

PECB

103

Exemple d'appréciation des risques

Appréciation de l'impact

Évaluer l'impact selon la confidentialité, l'intégrité et la disponibilité (sur une échelle de 1 à 5).

Actif	Menace	Vulnérabilité	Impact			Vraisemblance	Risque
			C	I	D		
Ordinateur portable	Vol	Portabilité	3	1	2		
Serveur de fichiers	Virus	Antivirus faible	1	5	3		
Contrats clients	Vol	Pas de coffre-fort	5	2	2		
Données sur les patients	Divulgation	Accès non contrôlé	4	1	1		

PECB

104

Exemple d'appréciation des risques

Appréciation de la vraisemblance

Évaluer la vraisemblance (probabilité, sur une échelle de 1 à 5).

Actif	Menace	Vulnérabilité	Impact			Vraisemblance	Risque
			C	I	D		
Ordinateur portable	Vol	Portabilité	3	1	2	3	
Serveur de fichiers	Virus	Antivirus faible	1	5	3	3	
Contrats clients	Vol	Pas de coffre-fort	5	2	2	2	
Données sur les patients	Divulgation	Accès non contrôlé	4	1	1	4	

PECB

105

Exemple d'appréciation des risques

Estimation du niveau des risques

Calculer le risque en additionnant la moyenne des impacts ($C+I+D/3$) à la vraisemblance (sur une échelle de 1 à 10).

Actif	Menace	Vulnérabilité	Impact			Vraisemblance	Risque
			C	I	D		
Ordinateur portable	Vol	Portabilité	3	1	2	3	5
Serveur de fichiers	Virus	Antivirus faible	1	5	3	3	6
Contrats clients	Vol	Pas de coffre-fort	5	2	2	2	5
Données sur les patients	Divulgation	Accès non contrôlé	4	1	1	4	6

PECB

106

Exemple d'appréciation des risques

Risques inacceptables

Si le niveau d'acceptabilité est de 5, alors deux des risques listés sont inacceptables.

Actif	Menace	Vulnérabilité	Impact			Vraisemblance	Risque
			C	I	D		
Ordinateur portable	Vol	Portabilité	3	1	2	3	5
Serveur de fichiers	Virus	Antivirus faible	1	5	3	3	6
Contrats clients	Vol	Pas de coffre-fort	5	2	2	2	5
Données sur les patients	Divulgation	Accès non contrôlé	4	1	1	4	6

PECB

107

Exemple d'appréciation des risques

Traitement des risques

Pour traiter les risques, des mesures qui réduisent l'impact ou la vraisemblance devraient être mises en œuvre.

Actif	Menace	Vulnérabilité	Impact			Vraisemblance	Risque
			C	I	D		
Ordinateur portable	Vol	Portabilité	3	1	2	3	5
Serveur de fichiers	Virus	Antivirus faible	1	5	3	3	6
Contrats clients	Vol	Pas de coffre-fort	5	2	2	2	5
Données sur les patients	Divulgation	Accès non contrôlé	4	1	1	4	6

PECB

108

Exemple d'appréciation des risques

Traitement des risques

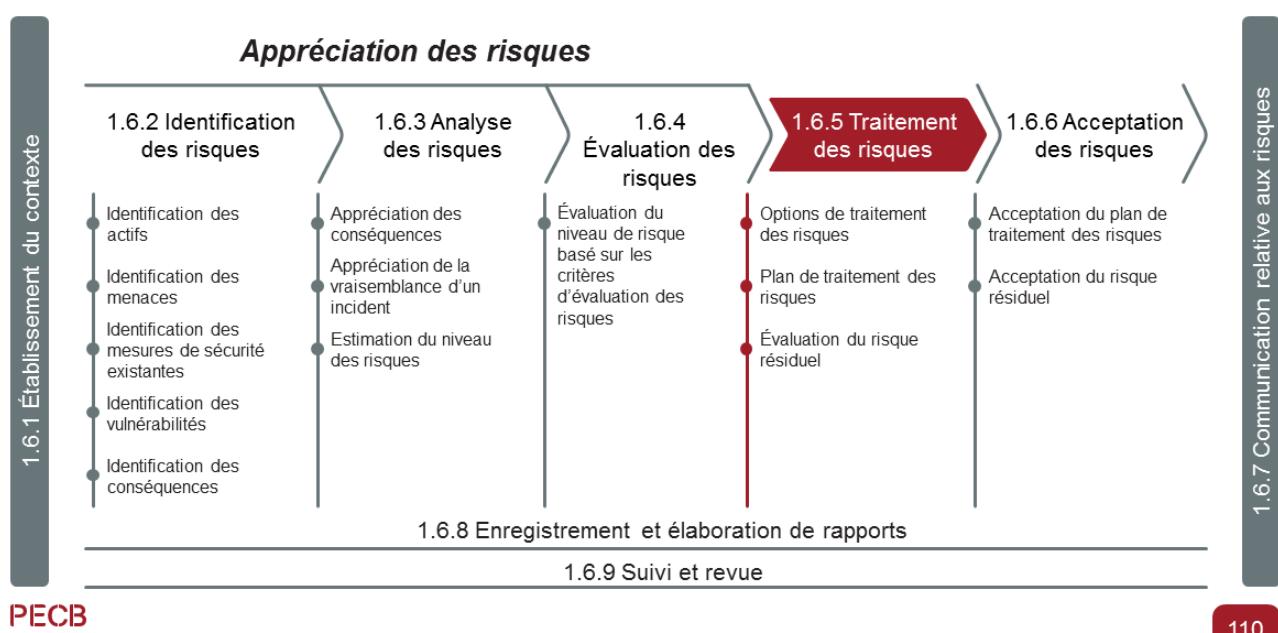
Recalculer le risque une fois que les mesures ont modifié l'impact ou la vraisemblance.

Actif	Menace	Vulnérabilité	Impact			Vraisemblance	Risque
			C	I	D		
Ordinateur portable	Vol	Portabilité	3	1	2	3	5
Serveur de fichiers	Virus	Antivirus faible	1	2	3	3	5
Contrats clients	Vol	Pas de coffre-fort	5	2	2	2	5
Données sur les patients	Divulgation	Accès non contrôlé	1	1	1	3	4

PECB

109

1.6.5 Traitement des risques



ISO Guide 73, article 3.8.1 Traitement du risque

processus destiné à modifier un risque

Note1:Le traitement des risques peut inclure:

- un refus du risque en décidant de ne pas démarrer ou 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], et
- un maintien du risque fondé sur une décision argumentée.

Note2: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 ».

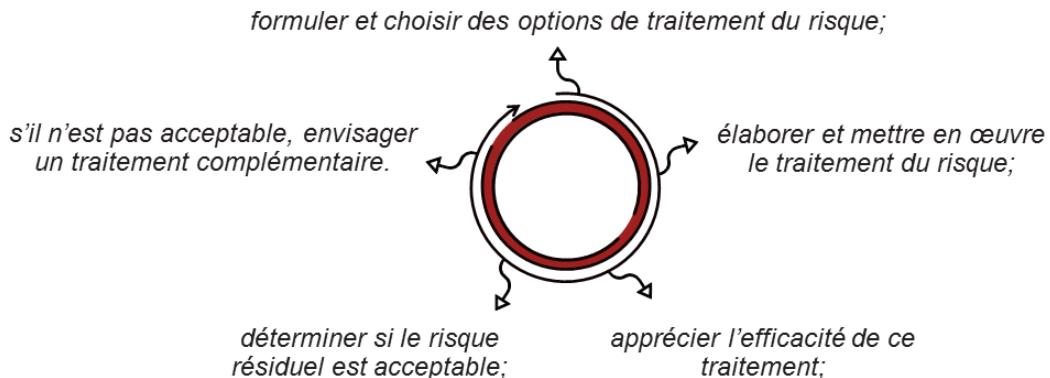
Note3:Le traitement du risque peut créer de nouveaux risques ou modifier des risques existants.

Traitement des risques

ISO 31000, article 6.5.1

Le traitement du risque a pour but de choisir et de mettre en œuvre des options pour aborder le risque.

Le traitement du risque implique un processus itératif:



PECB

111

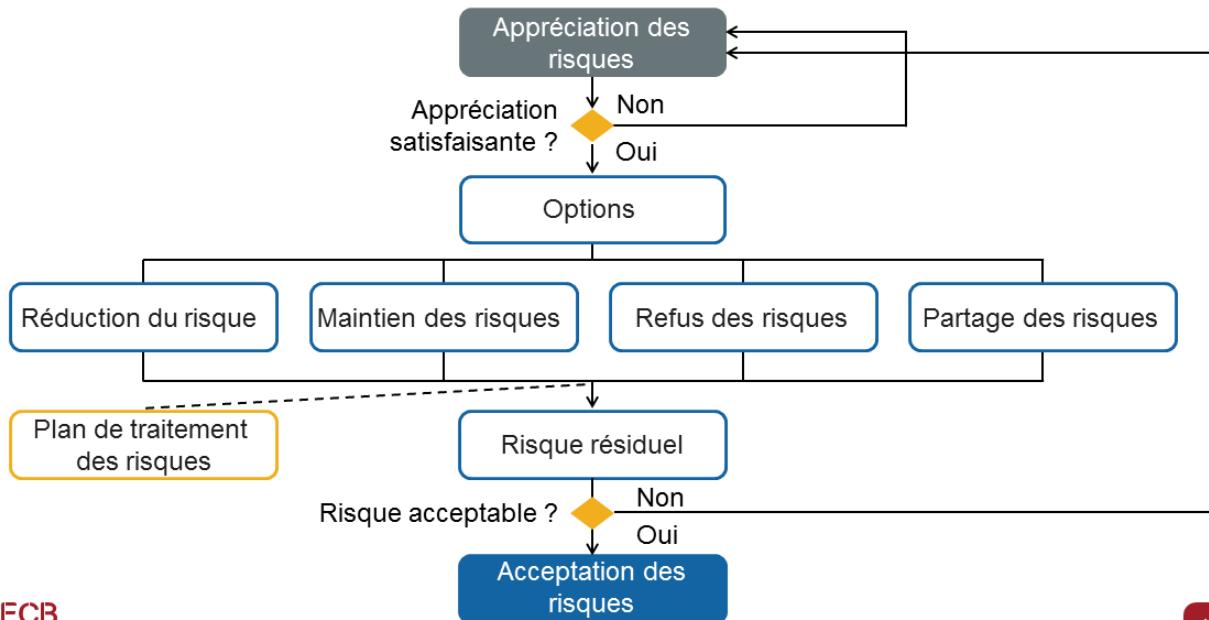
Le processus de traitement des risques comprend les activités suivantes :

1. Déterminer les options pour atténuer les risques
2. Évaluer les options proposées pour atténuer les risques
3. Élaborer et mettre en œuvre des plans d'action pour atténuer les risques

Il est préférable de concentrer d'abord les efforts sur le traitement des risques de haut niveau, puis de procéder graduellement au traitement des risques de bas niveau.

Choisir la meilleure option de traitement des risques signifie que les coûts associés à la mise en œuvre de ces options n'excèdent pas les avantages qu'ils présentent. Les coûts devraient être au moins égaux aux avantages. Toutefois, lorsqu'on effectue une telle analyse coûts-bénéfices, il faut aussi tenir compte du contexte de l'organisation.

Activités de traitement des risques



PECB

112

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

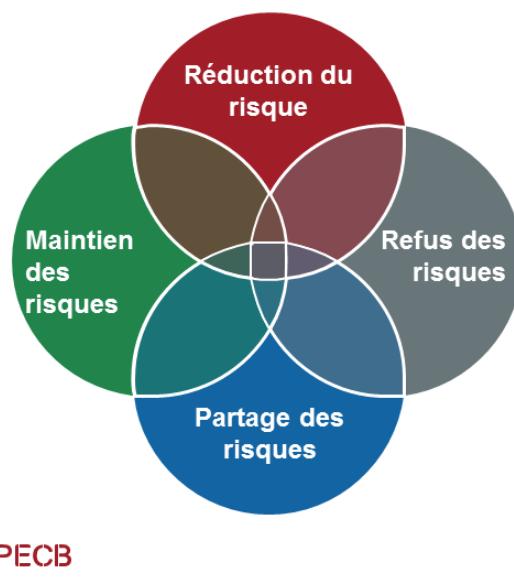
Il convient de choisir les options de traitement des risques sur la base des résultats de l'appréciation des risques, du coût prévu de mise en œuvre ainsi que des bénéfices attendus de ces options.

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).

Options de traitement des risques

ISO/IEC 27005, article 9.2



PECB

Réduction du risque	Refus des risques
Introduction, suppression ou modification des mesures de sécurité afin que le risque résiduel puisse être réapprécié et jugé acceptable.	Annulation ou modification d'une ou plusieurs activités liées au risque
Maintien des risques	Partage des risques
Décision d'accepter le niveau de risque actuel	Décision de partager les risques avec les parties externes : assurance ou externalisation

113

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

ISO/IEC 27005, article 9.2 Réduction du risque

Il convient de choisir des mesures de sécurité adaptées et justifiées afin de répondre aux exigences identifiées par l'appréciation et le traitement des risques. Il convient qu'il tienne également compte du coût et du délai de mise en œuvre des mesures de sécurité ou des aspects techniques, environnementaux et culturels. Il est souvent possible de diminuer le coût total de maintenance d'un système grâce à des mesures de sécurité de l'information correctement choisies.

ISO/IEC 27005, article 9.3 Maintien des risques

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

Il existe certains risques pour lesquels l'organisme peut ne pas être en mesure de déterminer les mesures de risques appropriées ou pour lesquels les coûts associés à ces mesures sont plus élevés que de simplement laisser le risque se matérialiser. Dans ce cas, l'organisme peut décider qu'il vaut mieux vivre avec les conséquences du risque. L'organisme devra documenter cette décision afin que les propriétaires de risques soient informés des risques et en acceptent les conséquences.

ISO/IEC 27005, article 9.4 Refus des risques

Lorsque les risques identifiés sont jugés trop élevés ou lorsque les coûts de mise en œuvre d'autres options de traitement des risques 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. Par exemple, pour les risques découlant d'incidents naturels, il peut être plus rentable de déplacer physiquement les moyens de traitement de l'information à un endroit où le risque n'existe pas ou est maîtrisé.

Page de notes

PECB

114

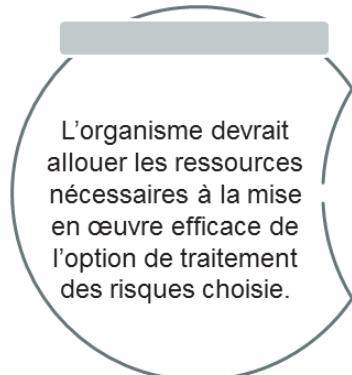
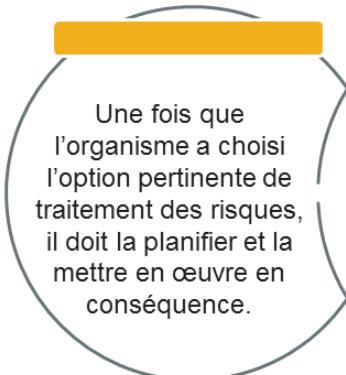
ISO/IEC 27005, article 9.5 Partage des risques

Le partage du risque implique la décision de partager certains risques avec des parties externes. Il peut créer de nouveaux risques ou modifier les risques identifiés existants. Par conséquent, un autre traitement des risques peut s'avérer nécessaire. Le partage peut être effectué à l'aide d'une assurance qui couvre les conséquences ou en sous-traitant à un partenaire dont le rôle consiste à surveiller le système d'information et à entreprendre des actions immédiates destinées à arrêter une attaque avant qu'un niveau de dommages défini ne soit atteint.

ISO 31000, article 6.5.2 Sélection des options de traitement du risque

Lors du choix des options de traitement du risque, il convient que l'organisme tienne compte des valeurs, des perceptions et de l'implication potentielle des parties prenantes et examine les moyens les plus appropriés de communiquer et de les consulter. À efficacité égale, certains traitements du risque peuvent être plus acceptables que d'autres pour certaines parties prenantes.

Plan de traitement des risques



PECB

115

Lorsqu'elle détermine la priorité des actions à prendre pour mettre en œuvre l'option de traitement des risques choisie, il convient que l'organisme prenne en compte, entre autres, les éléments suivants :

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

ISO 31000, article 6.5.3 Élaboration et mise en œuvre des plans de traitement du 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. 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, en concertation avec les parties prenantes appropriées.

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 personnes responsables de l'approbation et de la mise en œuvre du plan;
- les actions proposées;
- les ressources nécessaires, en tenant compte des impondérables;
- les mesures des performances;
- les contraintes;
- les rapports et le suivi requis;
- le moment où les actions sont censées être entreprises et achevées.

Plan de traitement des risques

Exemple

Risque (vulnérabilité/menace)	Les utilisateurs non autorisés peuvent se connecter à SharePoint par l'extranet et rechercher des fichiers de l'organisation avec l'identifiant demandé.
Niveau de risque	6
Priorité	Haute
Option de traitement	Refus
Détails de mesure	Rendre SharePoint inaccessible
Ressources nécessaires	10 heures pour reconfigurer et tester le système
Responsable	David Smith, administrateur SharePoint et John McGee, administrateur de coupe-feu
Dates de début et de fin	01-03-2018/02-03-2020
Maintenance nécessaire/commentaires	Faire des revues de sécurité périodiques du système pour s'assurer qu'une sécurité adéquate est fournie pour SharePoint

PECB

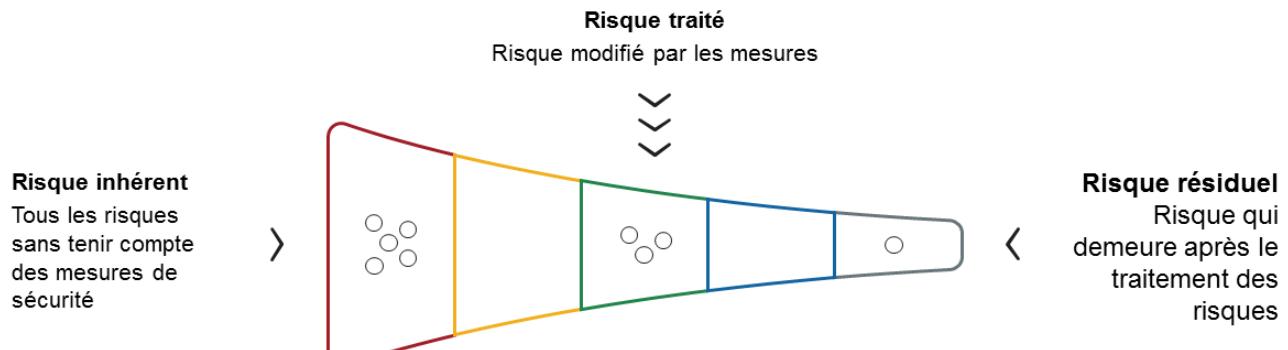
116

Comme présenté dans le tableau ci-dessus, le plan de traitement adoptera probablement une approche plus ou moins élaborée, mais il devrait au moins clarifier les points suivants :

- Actions à prendre
- Ressources à allouer
- Responsabilités
- Priorités à séquencer

Approbation du risque résiduel

ISO/IEC 27001, article 6.1.3 f)



Les propriétaires de risque doivent être informés des risques résiduels et en accepter la responsabilité.

PECB

117

La notion de risque résiduel peut être définie comme étant le risque qui demeure après la mise en œuvre de mesures visant à réduire le risque inhérent et peut être résumée comme suit :

$$\text{Risque résiduel} = \text{risque inhérent} - \text{risque traité}$$

Après la mise en œuvre d'un plan de traitement des risques, il y a toujours des risques résiduels. **La valeur de la réduction des risques suivant le traitement des risques devrait être évaluée, calculée et documentée.** Le risque résiduel peut être difficile à évaluer, mais une évaluation devrait être faite pour assurer que la valeur du risque résiduel respecte les critères d'acceptation du risque 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, une décision doit être prise pour traiter entièrement le risque. Une option est d'identifier d'autres options de traitement des risques comme le partage des risques (assurance ou externalisation) pour réduire le risque à un niveau acceptable. Une autre option pourrait être d'accepter (volontairement) le risque. Même si c'est une bonne pratique de ne tolérer aucun risque pour lequel le critère d'acceptation des risques est défini par 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.

Exercice 7

PECB

118

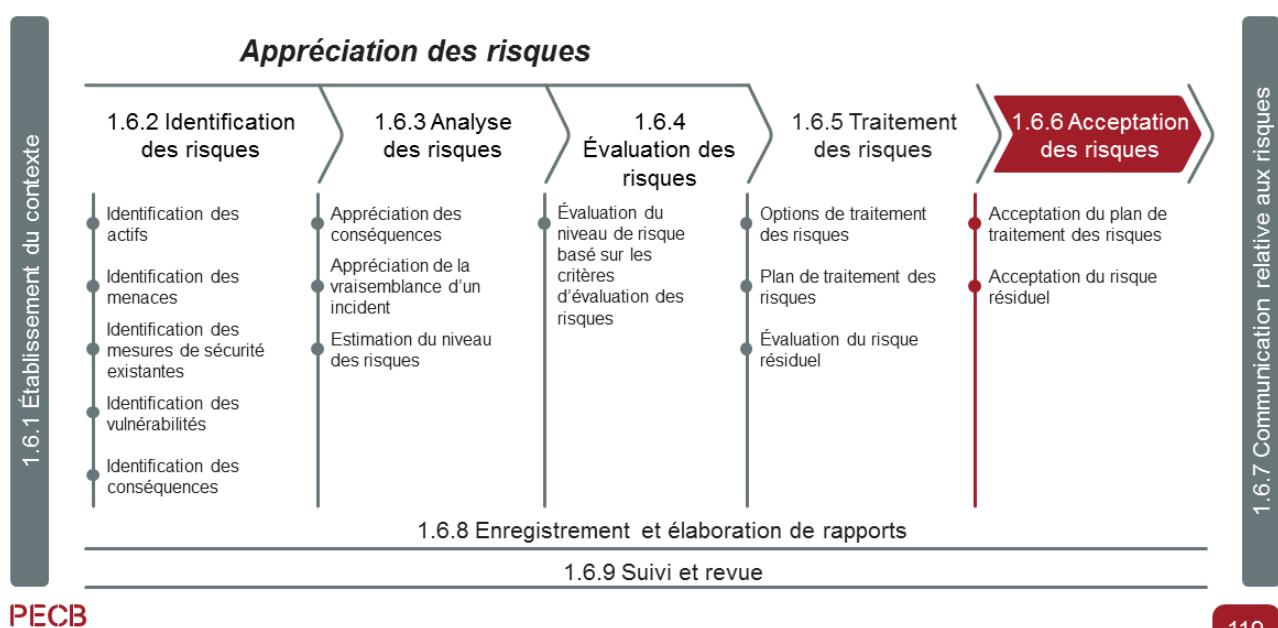
Exercice 7 : Options de traitement des risques

À la suite de l'analyse des risques, vous avez identifié que 0,5 % des transactions électroniques (chiffre d'affaires de 10 millions) effectuées par carte de crédit sur le site Web de l'entreprise sont de nature frauduleuse et que 70 % proviennent de transactions dans six pays. La direction de Scientia Online Library veut prendre une décision sur le traitement des risques. Préparez un résumé leur présentant les quatre options possibles pour traiter ce risque et les actions à entreprendre pour chaque option.

Durée de l'exercice : 20 minutes

Commentaires : 15 minutes

1.6.6 Acceptation des risques

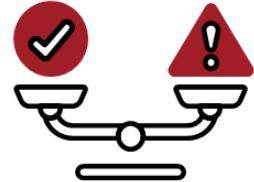


ISO/IEC 27005, article 10 Acceptation des risques en sécurité de l'information

Il convient que les plans de traitement des risques décrivent la manière dont les risques vont être traités afin de remplir les critères d'acceptation des risques. Il est important que les dirigeants en charge réexaminent et approuvent les plans de traitement des risques proposés et les risques résiduels associés, puis enregistrent les conditions associées à l'approbation.

Acceptation des risques

- L'acceptation des risques traite des avantages qu'une organisation espère obtenir si le risque est accepté.
- Ainsi, un niveau de risque élevé ne peut être accepté que si le niveau des avantages est également élevé.
- La culture d'un organisme détermine dans une large mesure les niveaux d'acceptation des risques.



PECB

120

L'acceptation des risques diffère suivant les secteurs d'activité, les organismes et les services d'un organisme.

Exemples d'acceptation des risques:

1. **Investissement** – La plupart des placements comportent un certain niveau de risque.
2. **Assurance** – L'ensemble de l'industrie de l'assurance est basée sur des hypothèses de risques pour des frais définis.
3. **Contrats dérivés** – Les contrats qui tirent leur valeur des taux de change ; le risque est transféré d'un organisme à l'autre.
4. **Projets** – Les projets comportent un risque de dépassement de coûts.
5. **Valeur nette (Business equity)** – Chaque actif détenu par un organisme est à risque. Ce risque est accepté en vertu de l'hypothèse que les rendements potentiels augmentent à mesure que le risque augmente.

ISO Guide 73, article 3.7.1.6 Acceptation du risque

décision argumentée en faveur de la prise d'un risque particulier

Note 1 à l'article: L'acceptation du risque peut avoir lieu sans traitement du risque ou au cours du processus de traitement du risque.

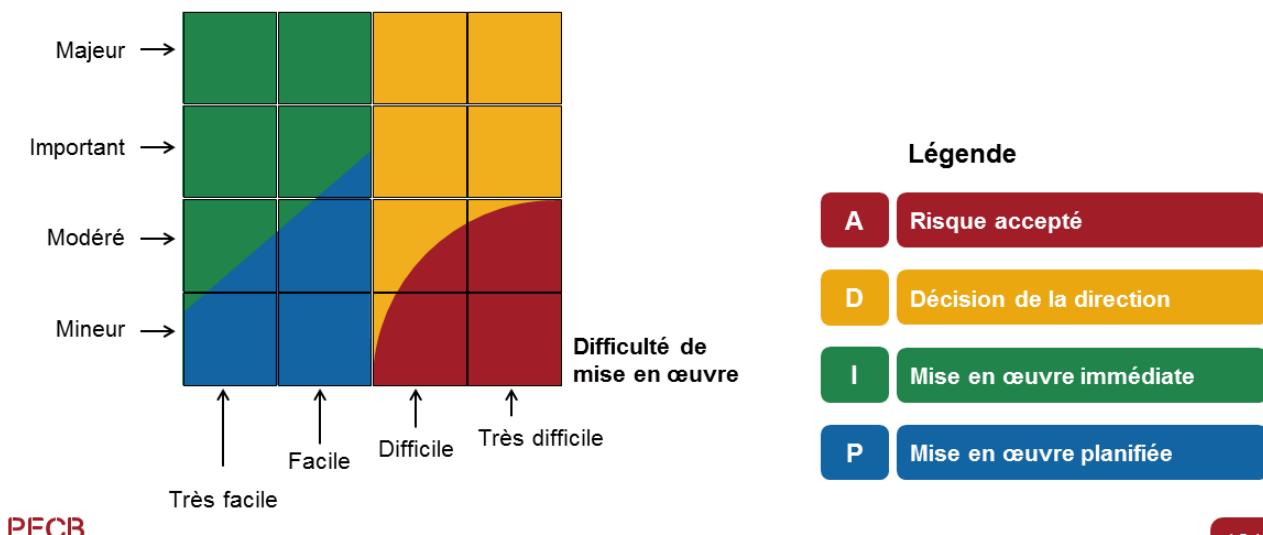
Note 2 à l'article: Les risques acceptés font l'objet d'une surveillance et d'une revue.

Source: Popov, Georgi, Lyon, K. Bruce & Hollcroft, Bruce. *Risk Assessment – A Practical Guide to Assessing Operational Risks*. Wiley:2016.

Acceptation du plan de traitement des risques

Présentation à la direction (exemple)

Niveau de risque



121

C'est à la direction qu'il appartient de définir les attentes concernant le plan de traitement des risques pour chaque niveau de risque.

Comme le montre la diapositive, pour les risques majeurs 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, la direction devrait décider de la manière d'appliquer le plan de traitement des risques.

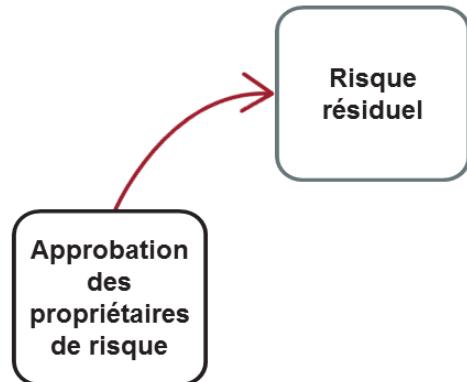
Toutefois, pour les risques mineurs ou modérés, le plan de traitement des risques pourrait être mis en œuvre immédiatement, la mise en œuvre du plan pourrait être planifiée ou le risque pourrait simplement être accepté en fonction de la difficulté de la mise en œuvre du plan.

Acceptation du risque résiduel

ISO/IEC 27005, article 10

Acceptation du risque résiduel par les propriétaires de risque

- Il est important que les dirigeants en charge réexaminent et approuvent les plans de traitement des risques proposés et les risques résiduels associés, puis enregistrent les conditions associées à l'approbation.
- Les critères d'acceptation des risques peuvent être plus complexes et ne pas consister simplement à savoir si un risque résiduel se situe au-dessus ou au-dessous d'un seuil unique.



PECB

122

Acceptation des risques ne répondant pas aux critères d'acceptation des risques

ISO/IEC 27005, article 10

- *Dans certains cas, le niveau des risques résiduels ne remplit pas les critères d'acceptation des risques, car les critères appliqués ne tiennent pas compte des circonstances prédominantes.*
- *Par exemple, il peut être avancé qu'il est nécessaire d'accepter les risques, car les bénéfices liés à ces risques sont très avantageux ou parce que le coût de la réduction du risque est trop élevé.*
- *De telles circonstances indiquent que les critères d'acceptation des risques sont inadaptés et qu'il convient, si possible, de les réviser.*

PECB

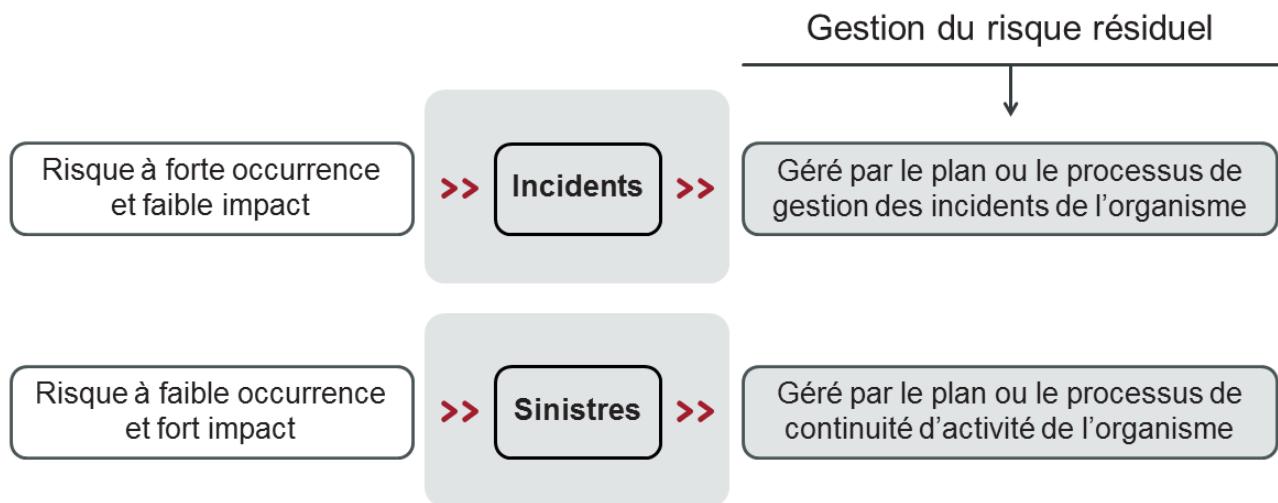
123

ISO/IEC 27005, article 10 Acceptation des risques en sécurité de l'information (suite)

Toutefois, il n'est pas toujours possible de les réviser rapidement. Dans ce cas, les décideurs peuvent accepter des risques qui ne remplissent pas les critères normaux d'acceptation. Si cela s'avère nécessaire, il convient que le décideur commente explicitement les risques et inclut une justification de la décision d'outrepasser les critères normaux d'acceptation.

Gestion du risque résiduel

Dans le processus de sécurité de l'information



PECB

124

Après l'acceptation des risques, tous les risques résiduels ne disparaissent pas. Les risques à forte occurrence et faible impact sont gérés par le processus de gestion des incidents de l'organisme. Les risques à faible occurrence et fort impact (sinistre) sont gérés par le plan ou le processus de continuité d'activité de l'organisme.

1.6.7 Communication relative aux risques

ISO 31000, article 6.2

- *La communication et la consultation ont pour but d'aider les parties prenantes pertinentes à comprendre le risque, les principes de prise de décisions et les raisons pour lesquelles certaines actions sont nécessaires.*
- *La communication vise à accroître la sensibilisation et la compréhension du risque, alors que la consultation implique l'obtention d'un retour et d'informations pour étayer la prise de décisions.*
- *Il convient que la communication et la consultation avec les parties prenantes internes et externes concernées aient lieu à toutes les étapes du processus de management du risque.*

PECB

125

ISO 31000, article 6.2 Communication et consultation (suite)

Une étroite coordination entre les deux facilite des échanges d'informations factuels, opportuns, pertinents, précis et compréhensibles tout en prenant en compte la confidentialité et l'intégrité des informations ainsi que le droit à la vie privée des personnes.

Une bonne communication et une bonne consultation exigent des entretiens et des réunions honnêtes avec toutes les parties intéressées afin que tous leurs besoins soient identifiés et satisfaits.

Pour obtenir des résultats bénéfiques, il est important d'élaborer avant tout une stratégie de communication, puis de la mettre en œuvre.

La deuxième partie importante est la consultation. Le gestionnaire de risque est considéré comme un consultant ou un coach interne. Son rôle consiste à aider les employés moins expérimentés à acquérir l'expertise nécessaire en matière de gestion des risques afin d'atteindre les buts et objectifs d'optimisation des risques.

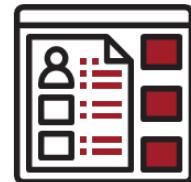
Sources :

1. Project Management Institute. 2017. *A guide to the project management body of knowledge (PMBOK guide)*. Newtown Square, Pa: Project Management Institute.
2. Louisot, Jean-Paul et Ketcham, H. Christopher. *Enterprise Risk Management*. Willey: 2009.

1.6.8 Enregistrement et élaboration de rapports

ISO 31000, article 6.7

- *Il convient que le processus de management du risque et ses résultats soient documentés et fassent l'objet de rapports selon des mécanismes appropriés.*
- *L'enregistrement et l'élaboration de rapports a pour but de:*
 - ▷ *communiquer sur les activités de management du risque et leurs résultats au sein de l'organisme;*
 - ▷ *fournir des informations en vue de la prise de décisions;*
 - ▷ *améliorer les activités de management du risque;*
 - ▷ *faciliter l'interaction avec les parties prenantes, y compris celles ayant la responsabilité des activités de management du risque.*



PECB

126

ISO 31000, article 6.7 Enregistrement et élaboration de rapports (suite)

Il convient que les décisions concernant la création, la conservation et le traitement des informations documentées tiennent compte, sans toutefois s'y limiter, de leur utilisation, du caractère sensible des informations et du contexte externe et interne.

1.6.9 Surveillance et réexamen des risques

ISO 31000, article 6.6

Suivi et revue

- *Le suivi et la revue ont pour but de s'assurer et d'améliorer la qualité et l'efficacité de la conception, de la mise en œuvre et des résultats du processus.*
- *Il convient que le suivi continu et la revue périodique du processus de management du risque et de ses résultats soient planifiés dans le processus de management du risque, en définissant clairement les responsabilités.*

Suivi et revue

PECB

127

ISO 31000, article 6.6 Suivi et revue (suite)

Il convient que le suivi et la revue aient lieu à toutes les étapes du processus. Le suivi et la revue comprennent la planification, le recueil et l'analyse d'informations, l'enregistrement des résultats et le retour d'information.

Il convient d'intégrer les résultats du suivi et de la revue aux activités de management des performances de l'organisme, de suivi des résultats et d'élaboration de rapports.



Questions ?

PECB

128

Section 12

Structure organisationnelle de la sécurité de l'information

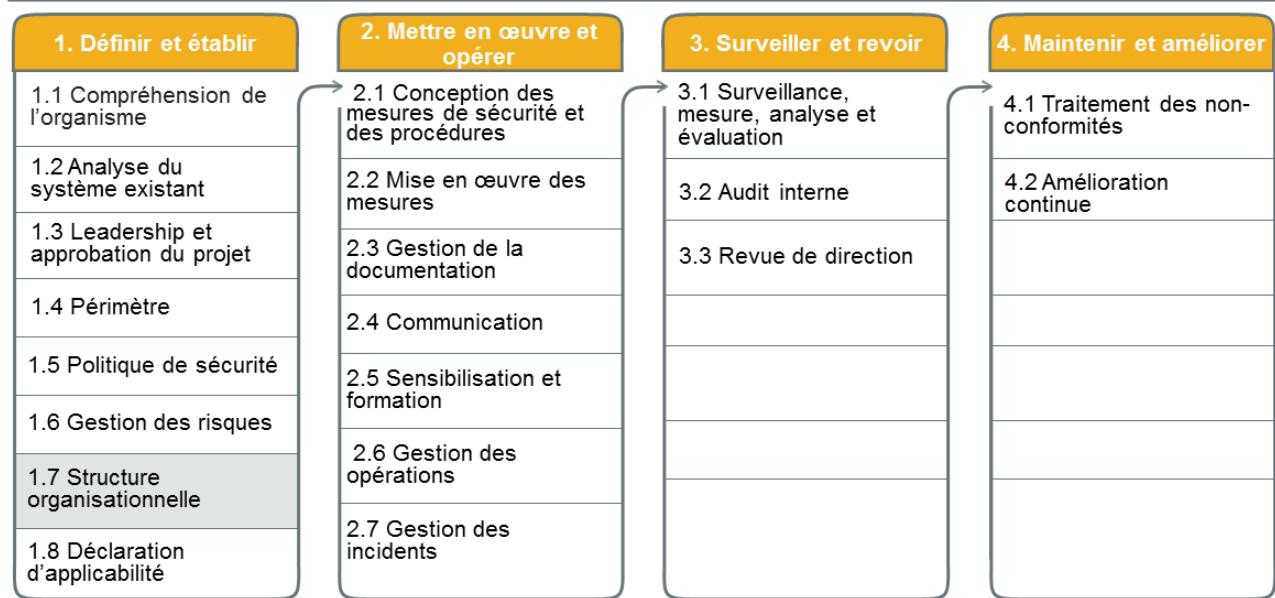
- Structure organisationnelle
- Nommer un coordonnateur de la sécurité de l'information
- Rôles et responsabilités des parties prenantes
- Rôles et responsabilités des comités

PECB

129

Cette section aidera le participant à acquérir des connaissances sur la structure organisationnelle ainsi que les rôles et responsabilités des parties prenantes et comités.

1.7 Définition de la structure organisationnelle de sécurité de l'information



PECB

130

ISO/IEC 27001 Exigences

ISO/IEC 27001, article 5.3

La direction doit s'assurer que les responsabilités et autorités des rôles concernés par la sécurité de l'information sont attribuées et communiquées au sein de l'organisation.

La direction doit désigner qui a la responsabilité et l'autorité de:

- a) *s'assurer que le système de management de la sécurité de l'information est conforme aux exigences de la présente Norme internationale; et*
- b) *rendre compte à la direction des performances du système de management de la sécurité de l'information.*

NOTE



La direction peut également attribuer des responsabilités et autorités pour rendre compte des performances du système de management de la sécurité de l'information au sein de l'organisation.

PECB

131

Un organisme souhaitant se conformer à la norme ISO/IEC 27001 doit au moins définir les rôles et responsabilités des principales parties prenantes en ce qui concerne le SMSI.

Note importante: Il n'est pas nécessaire de mettre en œuvre un ou plusieurs comités de sécurité de l'information dans l'organisme pour se conformer à ISO/IEC 27001, à l'exception du comité de pilotage (le sujet sera traité au jour 4 de la présente formation). Il existe en revanche de bonnes pratiques adaptées à la réalité d'un grand organisme. Dans une entreprise de 10 personnes, la création de comités spécifiques à la sécurité de l'information est inadéquate ou même inutile.

ISO/IEC 27003, article 5.3 Rôles, responsabilités et autorités au sein de l'organisme

Il convient qu'au-delà des rôles spécifiquement liés à la sécurité de l'information, les responsabilités et les autorités pertinentes de sécurité de l'information soient incluses dans d'autres rôles. Par exemple, les responsabilités de sécurité de l'information peuvent être incorporées dans les rôles de:

- g) propriétaires d'informations;
- h) propriétaires de processus;
- i) propriétaires d'actifs (par exemple, les propriétaires d'application ou d'infrastructure);
- j) propriétaires de risques;
- k) fonctions de coordination de la sécurité de l'information ou de responsable (ce rôle particulier est normalement un rôle de support dans le SMSI);
- l) gestionnaires de projet;
- m) gestionnaires hiérarchiques; et
- n) utilisateurs d'informations.

1.7 Définition de la structure organisationnelle de sécurité de l'information

Liste des activités

1.7.1

Définir la structure organisationnelle pour gérer la sécurité de l'information

1.7.2

Nommer un coordonnateur de la sécurité de l'information

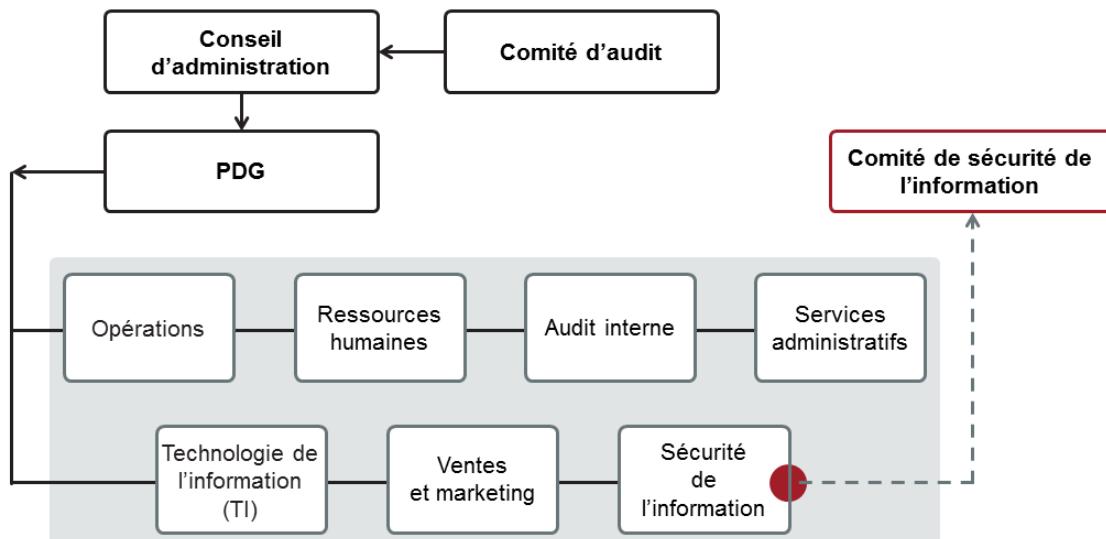
1.7.3

Définir les rôles et responsabilités des parties prenantes

1.7.4

Définir les rôles et responsabilités des principaux comités

1.7.1 Définir la structure organisationnelle pour gérer la sécurité de l'information



PECB

133

Un des éléments les plus importants lors de la définition de la mise en œuvre et de la gouvernance du management de la sécurité de l'information est le positionnement hiérarchique du CISO (*Chief Information Security Officer*) dans l'organisme.

Avant de définir une structure de gouvernance de sécurité de l'information, l'organisme doit considérer plusieurs facteurs : la mission, le périmètre, les besoins de l'activité, la structure organisationnelle et fonctionnelle, les clients servis, le degré de centralisation ou de régionalisation et la culture interne.

L'organisme devrait élaborer une structure de gouvernance pour la sécurité de l'information qui répondra pleinement aux exigences suivantes :

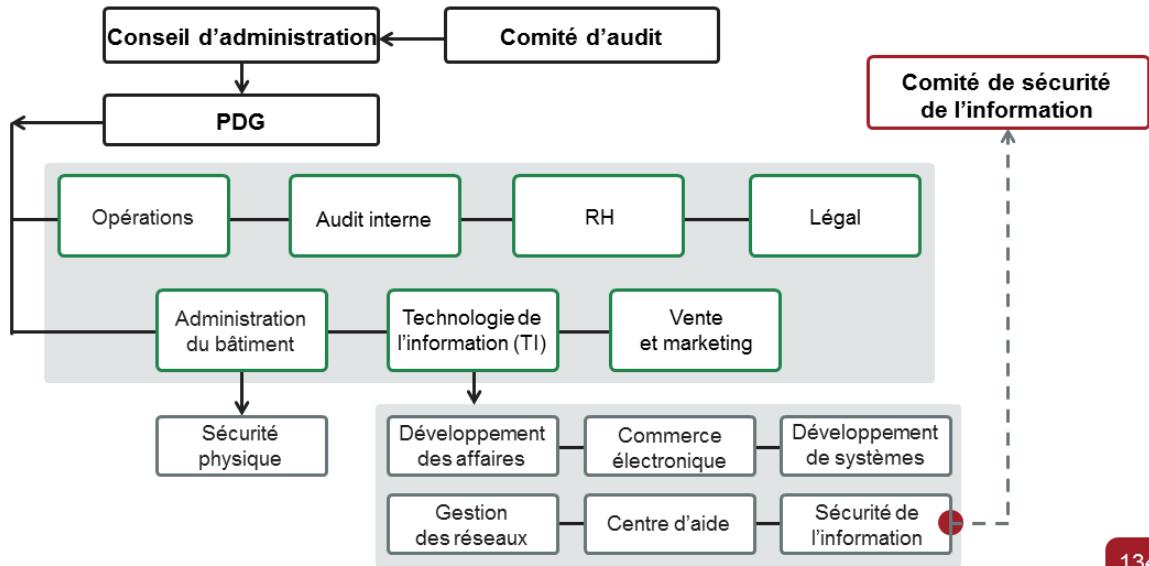
- Absence de conflits réels et potentiels
- Proximité du niveau de décision
- Soutien solide de la part de la direction
- Haute capacité d'influence
- Intégration de toutes les préoccupations de sécurité
- Couverture de l'information sans égard au médium ou aux moyens utilisés pour communiquer

En outre, les activités liées à la sécurité de l'information doivent être coordonnées par un responsable de la sécurité de l'information qui établit les liens de coopération et de collaboration avec les autres branches de l'organisation.

Cette approche fonctionne mieux pour les organismes de taille moyenne à grande, pour lesquels le SMSI considéré couvre l'ensemble de l'organisme dans son périmètre. Une évolution raisonnable et appropriée doit être appliquée lorsque le périmètre de l'organisme couvert par le SMSI est nettement plus restreint.

Structure organisationnelle traditionnelle

Sécurité de l'information et département des TI



Traditionnellement, le responsable de la sécurité de l'information et son équipe sont rattachés au département de technologie de l'information de l'organisme. Plus de 50% des entreprises possèdent ce modèle de gouvernance de la sécurité de l'information. Il présente l'avantage de réunir les différentes expertises techniques de sécurité au sein du même département.

Cependant, il y a plusieurs inconvénients qui font de ce modèle un type de structure à éviter :

1. Indépendance inexiste dans les fonctions de sécurité de l'information liées aux systèmes TI
2. Faible capacité d'influence du fait que le CISO est au même niveau ou à un niveau inférieur à celui des responsables avec qui il doit composer sur les questions de sécurité
3. Distance par rapport aux autorités décisionnelles
4. Conflits d'intérêts potentiels et réels
5. Faible intégration de toutes les préoccupations de sécurité de l'information
6. Préoccupations portant principalement sur la sécurité et la technologie opérationnelles de la sécurité de l'information

Ce type de structure ne permet pas au CISO d'exercer correctement son mandat. Régulièrement, la direction des technologies de l'information serait dans une situation de conflits d'intérêts réels ou potentiels. La présence d'un niveau hiérarchique additionnel entre le CISO et la direction ralentit le processus d'échanges et la prise de décision en ce qui concerne la sécurité de l'information. Il existe aussi un risque d'interférence par le responsable des TI dans les communications et rapports du CISO pour la direction. Il serait approprié, pour la gestion de ce risque d'interférence que le CISO adresse ses rapports directement au comité de management de la sécurité de l'information plutôt qu'au management des ressources de l'information.

Les notes fournies sous la diapositive précédente concernant l'évolution s'appliquent également ici.

1.7.2 Nommer un coordonnateur de la sécurité de l'information

- Les activités de sécurité de l'information doivent être coordonnées par les représentants des différentes parties de l'organisme qui ont un rôle et une fonction pertinente
- Typiquement, la coordination de la sécurité de l'information devrait impliquer la coopération et la collaboration des responsables, utilisateurs, administrateurs, concepteurs d'application, auditeurs, personnel de la sécurité et experts de secteurs comme l'assurance, le droit, les ressources humaines, le management des TI ou des risques.



1.7.3 Définir les rôles et responsabilités des parties prenantes

Rôle	Principales responsabilités
Responsable de la sécurité de l'information	Coordonner les activités liées au management de la sécurité de l'information et des opérations du SMSI
Conseiller juridique	Identifier les exigences de conformité (légales, réglementaires et contractuelles) et l'analyse
Responsable des ressources humaines	Mettre en œuvre et gérer la formation et la sensibilisation à la sécurité de l'information, considérer les mesures de sécurité dans les processus des RH (recrutement, cessation d'emploi, processus disciplinaire)
Gestionnaire des installations	Mettre en œuvre et gérer les contrôles de sécurité physique (contrôle d'accès aux immeubles, protection contre les incendies, entretien électrique, etc.)
Responsable des TI	Mettre en œuvre et gérer les solutions et les mesures techniques dans la gestion des opérations quotidiennes.
Responsable du Service clients	Mettre en œuvre et gérer les services aux utilisateurs et les contrôles liés (contrôle d'accès, gestion des incidents, etc.)
Responsable des relations publiques	Valider l'impact sur la réputation de l'organisme, communiquer avec les parties prenantes externes
Auditeur interne	Valider la conformité au SMSI et aux mesures de sécurité
Responsable de la documentation	Assurer, à toutes les étapes du cycle de vie des documents, qu'ils possèdent toutes les qualités nécessaires à la bonne gestion de la connaissance et de l'héritage de l'information, de la conservation de la preuve et de l'application de la loi

PECB

136

Les rôles et responsabilités des parties prenantes qui ont une fonction et des tâches directement liées au SMSI devraient être clairement définis. La description des tâches de responsabilités peut être documentée de différentes façons : le manuel de sécurité de l'information, les fiches de postes, les contrats d'embauche, la politique de sécurité, etc.

Le responsable d'une tâche peut la déléguer à d'autres, mais pas les responsabilités. Par exemple, le directeur des RH délègue habituellement des activités comme le recrutement et la cessation d'emploi à son personnel. Cependant, il reste ultimement responsable du fonctionnement des processus des RH.

Dans le cas de la gestion d'un actif, un propriétaire peut assigner un «gardien» qui, par délégation, assurera la sécurité de l'information des actifs sous sa responsabilité.

Sa tâche consistera donc à :

1. Autoriser et répondre à l'utilisation des actifs
2. Assurer que les mesures de sécurité appropriées sont en place, mises en œuvre et vérifiées périodiquement
3. Maîtriser l'analyse des risques et s'assurer du management du risque résiduel après l'approbation du propriétaire
4. S'assurer de la sensibilisation des utilisateurs

La taille de l'organisme dictera les rôles et les titres qui combleront les besoins au sein du SMSI

Responsable d'un processus ou d'une mesure de sécurité

Rôles et responsabilités principaux

Quelles sont les missions ?	Comment mettre en œuvre ?	Quand ?
Déterminer les objectifs pour les processus/mesures de sécurité	Discuter avec la direction, le responsable de la sécurité de l'information et le personnel concerné	Une fois par année
Être un relais entre le responsable de la sécurité de l'information et tous ceux impliqués dans les opérations des processus/mesures de sécurité	<ul style="list-style-type: none">– Communiquer et renseigner sur les enjeux du processus du SMSI– Encourager les rapports d'incidents, de défaillances, les suggestions d'amélioration, etc.– Communiquer les décisions du comité de sécurité de l'information et les revues de direction	Continu
Assurer le bon fonctionnement des processus/mesures de sécurité et la disponibilité de toute la documentation pertinente	Vérifier que les processus/mesures de sécurité sont appliqués chaque jour	Continu
Assurer la conformité de la documentation avec la réalité (gestion des dossiers, enregistrements, procédures et autres documents relatifs)	Tenir compte des résultats d'audits, des rapports du comité de sécurité de l'information et des commentaires des parties prenantes	Continu
Assurer la disponibilité de l'information pour surveiller et mesurer le processus	Vérifier que les éléments définis dans le tableau de surveillance des objectifs et de surveillance sont disponibles	Selon la périodicité des indicateurs
Faire le suivi du traitement des non-conformités et des actions correctives et préventives sur le processus	Vérifier que les formulaires de notification du tableau de surveillance sont correctement remplis	Après chaque rapport

PECB

137

Au moment de la rédaction de la Déclaration d'applicabilité, le responsable de chaque mesure de sécurité sélectionnée devrait être identifié.

Ces responsables d'un processus ou d'une mesure de sécurité seront engagés dans les diverses étapes de mise en œuvre du SMSI.

1. Formulation des objectifs de sécurité de l'information
2. Rédaction de la Déclaration d'applicabilité
3. Conception des mesures de sécurité et rédaction de politiques et procédures spécifiques
4. Transfert du projet SMSI aux opérations du SMSI
5. Élaboration des indicateurs
6. Suivi des non-conformités

1.7.4 Définir les rôles et responsabilités des principaux comités



PECB

138

Il est important de noter que la création de ces comités n'est pas considérée comme une nécessité. Ainsi, il est courant de réutiliser les comités existants en élargissant leur périmètre. Une approche multidisciplinaire de la sécurité de l'information devrait être promue. Ainsi, il faut préconiser l'inclusion de membres qui possèdent diverses aptitudes et venant d'unités différentes de l'organisme.

En plus des comités, il est nécessaire d'établir des liens avec les experts en dehors de l'organisme pour développer des contacts, incluant avec des autorités pertinentes afin de suivre les tendances et les enjeux liés à la sécurité de l'information.

La mesure dans laquelle les comités sont productifs dans les organisations de petite taille doit être soigneusement évaluée, afin de ne pas créer un fardeau plutôt que de maintenir un sentiment d'indépendance en matière de surveillance.

Comité exécutif

Objectif	Exigences annuelles
Niveau d'intervention	Niveau stratégique
Missions	<ol style="list-style-type: none">1. Assurer l'inclusion des valeurs de l'organisme et de ses buts d'activité dans le processus du management de la sécurité de l'information2. Établir les objectifs annuels et la stratégie du SMSI3. S'assurer que les revues de direction annuelles ont lieu4. Fournir les ressources adéquates pour le bon fonctionnement du SMSI5. Contrôler : contribution aux processus métier du SMSI, optimisation des coûts6. Approuver les projets majeurs liés à la sécurité de l'information7. Valider et approuver les mises à jour de l'appréciation des risques8. Communiquer avec les parties prenantes
Membres	Direction générale (PDG, VP Information, VP Finance)
Fréquence des réunions	Une à quatre fois l'an

PECB

139

Le comité exécutif est l'organe central pour la direction, le contrôle, la validation, la prise de décision et l'arbitrage dans le management du SMSI. Il est composé de représentants du conseil d'administration de l'organisme.

Ce comité détermine la stratégie de développement du SMSI et assure son évolution. Il décide de l'allocation des ressources nécessaires pour réaliser les buts et joue un rôle de surveillance. Il arbitre tous les conflits et s'assure du respect des valeurs de l'organisme.

C'est le seul comité expressément cité dans une exigence d'ISO/IEC 27001 et il convient qu'il se réunisse au moins une fois par année. Il est très rare qu'un organisme établisse un comité exécutif spécifique pour la sécurité de l'information. Le plus souvent, c'est un point de l'ordre du jour du comité exécutif qui est responsable de la conduite générale des activités de l'organisme.

Comité de sécurité de l'information

Objectif	Assurer le fonctionnement adéquat du SMSI et des mesures de sécurité
Niveau d'intervention	Niveau tactique
Missions	<ol style="list-style-type: none">1. Assurer le bon déroulement des opérations du SMSI2. Promouvoir la cohérence en sécurité de l'information dans l'organisme3. Maintenir l'appréciation des risques de l'organisme4. Être la liaison entre les Opérations et la direction5. Gérer les problèmes de sécurité de l'information et proposer des solutions aux non-conformités6. Contrôler la mise en œuvre des plans d'action et l'implémentation des actions correctives découlant de l'analyse des risques
Membres	CISO, responsable du SMSI, responsable des services clés (TI, audit, légal, finance, RH, sécurité physique)
Fréquence des réunions	Mensuelle

140

Ce comité est composé des représentants de diverses divisions de l'organisme et est habituellement présidé par le CISO. Les représentants de différentes unités sont souvent considérés comme des officiers de liaison pour les problèmes liés à la sécurité de l'information. Le rôle de ce comité est d'assurer la coordination et la coopération sur la sécurité de l'information dans l'organisme.

Spécifiquement, le Comité de sécurité de l'information favorise la cohérence de la sécurité de l'information au sein de l'organisme et surveille l'orientation stratégique et les priorités des actions convenues par la direction. Ce comité est responsable des opérations quotidiennes, mais assure également le bon déroulement des opérations du SMSI et la mise en œuvre des plans d'actions et des actions correctives qui découlent de l'analyse des risques.

Afin d'éviter la prolifération des comités dans l'organisme, le comité de sécurité de l'information peut, dans l'éventualité d'un incident majeur, jouer le rôle de comité de gestion de crise (voir la section sur la gestion des incidents).

Comités opérationnels

Objectif	Exigences annuelles
Niveau d'intervention	Niveau opérationnel
Missions	1. Assurer la mise en œuvre des mesures de sécurité 2. Gérer la documentation du SMSI 3. Améliorer le SMSI, traiter les non-conformités
Membres	Dépend du comité spécifique
Fréquence des réunions	Hebdomadaire

PECB

141

Selon la taille de l'organisme et sa culture interne, certaines responsabilités dans la sécurité de l'information devraient être confiées aux comités opérationnels. La duplication des comités devrait être évitée et les responsabilités devraient être intégrées aux structures déjà en place comme le Comité de gestion des changements, le Comité de gestion des ressources humaines, le Comité d'assurance de la qualité, etc.

Il convient que le CISO participe aux divers comités comme membre ou qu'il soit représenté par un officier de liaison de sécurité de l'information.

Questions ?

PECB

142

Section 13

Déclaration d'applicabilité et décision de la direction de mettre en œuvre le SMSI

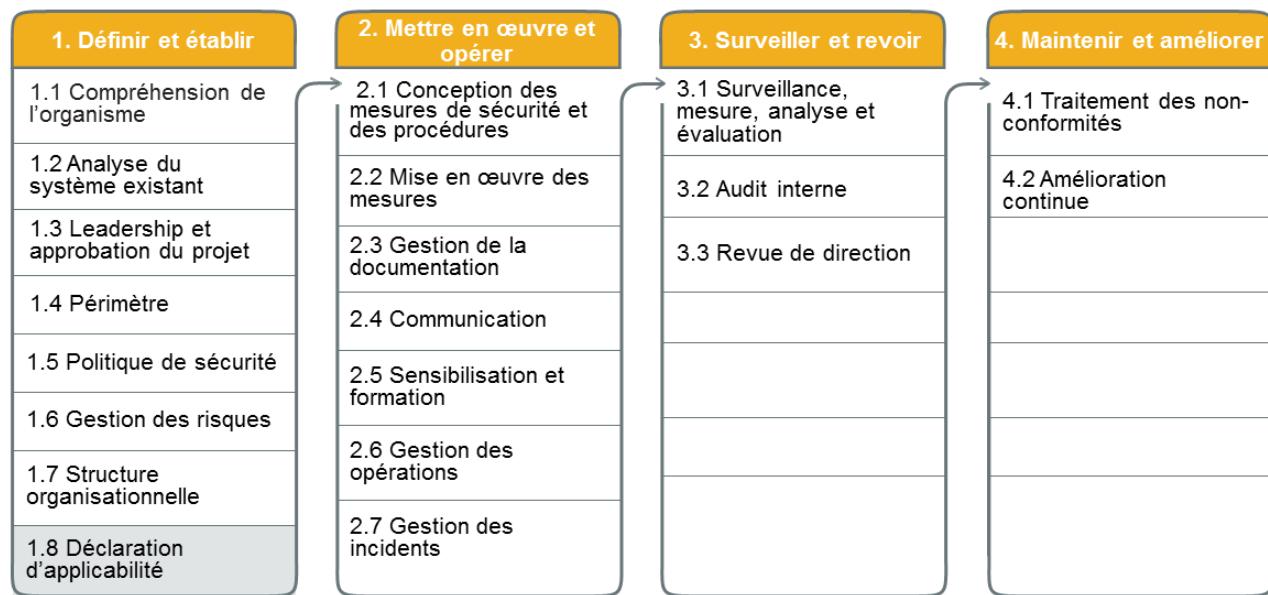
- Revue et sélection des objectifs et mesures de sécurité applicables
- Justification des mesures de sécurité sélectionnées
- Justification des mesures de sécurité exclues
- Rédiger la Déclaration d'applicabilité
- Approbation de la direction

PECB

143

Cette section aidera le participant à identifier les mesures de sécurité à inclure dans le SMSI, à justifier la sélection des mesures choisies et exclues et à obtenir l'approbation officielle de la direction avant la mise en œuvre du SMSI.

1.8 Déclaration d'applicabilité et décision de la direction de mettre en œuvre le SMSI



PECB

144

ISO/IEC 27001 Exigences

ISO/IEC 27001, article 6.1.3 d)

produire une déclaration d'applicabilité contenant :

- *les mesures nécessaires*
- *la justification de leur insertion*
- *le fait qu'elles soient mises en œuvre ou non*
- *la justification de l'exclusion de mesures de l'Annexe A*



Note

ISO/IEC 27001 n'exige PAS que l'organisme choisisse ses mesures uniquement à partir de l'Annexe A.

PECB

145

Un organisme souhaitant se conformer à la norme ISO/IEC 27001 doit au moins :

- Être en mesure de démontrer que son SMSI est aligné sur la mission de l'organisme ainsi que sur ses objectifs et ses stratégies d'affaires
- Connaître et tenir compte des enjeux de la sécurité de l'information liés à son secteur d'activités tels que les risques, les contraintes légales et réglementaires ainsi que les exigences des clients

Note: ISO/IEC 27001 n'exige PAS que l'organisation sélectionne ses mesures UNIQUEMENT à partir de l'Annexe A. L'organisation est libre de sélectionner des mesures de toute source ou de les créer elle-même. Ce qu'il faut, c'est qu'un «contrôle sanitaire» soit effectué en examinant les mesures de l'Annexe A et en s'assurant que chacune d'elles a été considérée. S'il s'avère que les mesures de l'Annexe A ne sont pas utilisées d'une autre manière et n'ont pas été oubliées, elles doivent être ajoutées dans le SoA avec une justification quant à leur non-application.

Définition – Déclaration d'applicabilité

Déclaration documentée décrivant les objectifs et les mesures de sécurité pertinentes et applicables au SMSI d'un organisme.



PECB

146

La Déclaration d'applicabilité est plus qu'une liste de contrôle des mesures de sécurité de l'Annexe A à mettre en œuvre dans le SMSI. C'est un document clé du SMSI qui sert de référence pour l'auditeur externe durant l'audit de certification. C'est un des premiers documents qu'il analysera. C'est aussi un des documents que la direction doit valider et approuver avant le début des opérations du SMSI.

Note de terminologie:

- La notion de «Déclaration d'applicabilité» est spécifique à la norme ISO/IEC 27001. Il n'y a pas d'équivalence dans les autres normes de système de management tel qu'ISO 9001 ou ISO 14001.
- Même dans d'autres langues, plusieurs organismes utilisent le terme anglais, «Statement of Applicability» ou son acronyme, SoA ou SOA.

1.8 Déclaration d'applicabilité

Liste des activités

1.8.1

Revoir et sélectionner les objectifs
et mesures de sécurité applicables

1.8.2

Justifier les mesures sélectionnées

1.8.3

Justifier les mesures exclues

1.8.4

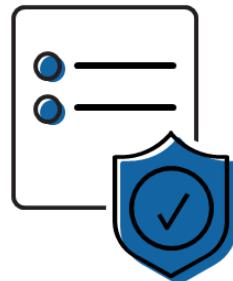
Rédiger la Déclaration d'applicabilité

1.8.5

Obtenir l'approbation de la direction

1.8.1 Revoir et sélectionner les objectifs et mesures de sécurité applicables

- Tous les référentiels de mesures peuvent être utilisés comme sources de mesures de sécurité.
- L'organisme doit passer en revue les 114 mesures de l'Annexe A afin d'identifier celles qui sont applicables et celles qui ne seront pas retenues dans le cadre du SMSI.
- La plupart des organismes déclarent plus de 80 mesures applicables.



PECB

148

Dans un premier temps, l'organisme doit passer en revue les 114mesures de sécurité de l'Annexe A afin de distinguer celles qui sont applicables de celles qui ne seront pas retenues dans le cadre du SMSI. Le choix d'appliquer ou non une mesure de sécurité devrait se justifier essentiellement par l'appréciation des risques. C'est pourquoi la Déclaration d'applicabilité ne devrait pas être rédigée avant le dépôt du rapport d'analyse des risques et de traitement des risques.

Les mesures de sécurité proposées dans l'Annexe A peuvent se révéler suffisantes pour traiter l'ensemble des scénarios de risque que l'organisme a identifiés. On peut faire appel à d'autres référentiels pour mettre en place des mesures de sécurité supplémentaires (exemples : COBIT, PCI, etc.) afin de les intégrer au SMSI. Il convient de noter que les mesures de sécurité supplémentaires doivent également être décrites dans la Déclaration d'applicabilité.

La plupart des organismes déclarent plus de 80mesures de sécurité applicables. Il convient toutefois d'éviter de tomber dans l'excès. Un SMSI n'intégrant que les mesures de sécurité obligatoires risque de ne pas être protégé efficacement. À l'inverse, la décision de déclarer applicables toutes les mesures sans prendre le temps d'évaluer les besoins de l'organisme peut être tout aussi inefficace. Des mesures de sécurité risquent alors d'être mises en œuvre sans répondre à un réel besoin, alourdissant ainsi considérablement la charge que représente la maintenance du système.

De plus, la sélection des mesures de sécurité devrait prendre en compte le rapport coût/bénéfice. Étant donné qu'un SMSI supporte l'organisme dans la réalisation de ses objectifs d'affaires, il est soumis à des impératifs économiques. Les mesures de sécurité mises en œuvre se doivent d'être «rentables» pour l'organisme.

En conclusion, dans la logique de la norme, les mesures de sécurité déclarées dans le SMSI doivent être alignées sur les activités de l'organisme et non l'inverse.

1.8.2 Justifier les mesures sélectionnées

- L'organisme devrait justifier les raisons de sélection de chaque mesure retenue dans le SMSI.
- C'est la réponse au « pourquoi » de chaque mesure.

Exemple :

La sécurité dans les accords conclus avec les fournisseurs (A.15.1.2) : Les exigences applicables liées à la sécurité de l'information doivent être établies et convenues avec chaque fournisseur pouvant accéder, traiter, stocker, communiquer ou fournir des composants de l'infrastructure informatique destinés à l'information de l'organisation.

Justification de sélection : Assurer la sécurité de l'information et des moyens d'accès, de traitement, de stockage, de communication ou de fourniture des composants de l'infrastructure TI pour l'information appartenant à l'organisme et qui est gérée par des fournisseurs.

PECB

149

L'organisme justifiera les raisons de sélection de chaque mesure de sécurité incluse dans le SMSI. Cette activité peut sembler futile à première vue, voire inutile. Pourquoi faut-il justifier les mesures de sécurité sélectionnées et non uniquement celles qui sont exclues? L'objectif de cette exigence de la norme ISO/IEC 27001 est d'obliger l'organisme à documenter les objectifs associés à chaque mesure. C'est la réponse au «pourquoi» de chaque mesure.

Voici quelques exemples de justifications liées à des mesures sélectionnées :

ISO/IEC 27001, Annexe A.12.1.2 Gestion des changements

Les changements apportés à l'organisation, aux processus métier, aux systèmes et moyens de traitement de l'information ayant une incidence sur la sécurité de l'information doivent être contrôlés.

Justification de sélection : Assurer la confidentialité, l'intégrité et la disponibilité de l'information et des moyens de traitement de l'information appartenant à l'organisme lorsqu'il y a des changements aux systèmes et aux méthodes de traitement de l'information.

ISO/IEC 27001, Annexe A.17.1.2 Mise en œuvre de la continuité de la sécurité de l'information

L'organisation doit établir, documenter, mettre en œuvre et tenir à jour des processus, des procédures et des mesures permettant de fournir le niveau requis de continuité de sécurité de l'information au cours d'une situation défavorable.

Justification de sélection : Assurer la disponibilité de l'information en temps voulu lorsqu'une interruption ou une panne affecte les processus métier critiques.

1.8.3 Justifier les mesures exclues

- L'organisme devrait justifier les raisons d'exclusion de chaque mesure de l'Annexe A exclue du SMSI.
- Les raisons d'exclusions les plus souvent invoquées sont les suivantes :
 - ▷ Violation d'une obligation légale, statutaire ou contractuelle (exemple : Sélection des candidats, A.7.1.1)
 - ▷ Aucune activité liée à cette mesure de sécurité n'est en fonction dans l'organisme (exemple : Télétravail A.6.2.2)

PECB

150

L'organisme justifiera les raisons d'exclusion de chaque mesure de sécurité de l'Annexe A d'ISO/IEC 27001. Il y a plusieurs raisons valables pour lesquelles un organisme peut invoquer l'exclusion des mesures de sécurité. Voici quelques exemples de raisons qui peuvent conduire à l'exclusion des mesures de sécurité :

ISO/IEC27001, Annexe A.7.1.1 Sélection des candidats

Des vérifications doivent être effectuées sur tous les candidats à l'embauche conformément aux lois, aux règlements et à l'éthique et être proportionnées aux exigences métier, à la classification des informations accessibles et aux risques identifiés.

Justification d'exclusion : Conformément à la convention collective conclue avec les employés, aucun contrôle de sécurité ne sera effectué.

ISO/IEC27001, Annexe A.6.2.2 Télétravail

Une politique et des mesures de sécurité complémentaires doivent être mises en œuvre pour protéger les informations consultées, traitées ou stockées sur des sites de télétravail.

Justification d'exclusion : Le télétravail est interdit dans l'organisme.

Notes importantes:

- Dans la plupart des cas, un organisme peut déclarer une mesure applicable et expliquer ce qu'elle couvre et ses limites. Dans l'exemple de la mesure A.7.1.1, cette mesure ne nécessite pas l'utilisation de tous les moyens nécessaires pour mener une enquête approfondie auprès de toute personne par une enquête de solvabilité, une validation des casiers judiciaires, une vérification des qualifications, etc. Un organisme pourrait simplement justifier qu'il demandera que l'inspection soit menée sur les certificats d'origine et qu'il validera deux références pour chaque candidat.
- Dans la plupart des cas, un organisme peut déclarer qu'une mesure de sécurité s'applique même si l'organisme ne pratique pas l'activité. Voici un exemple : un organisme a déclaré que la mesure sur le télétravail (A.6.2.2) n'est pas applicable, car le télétravail est interdit. Cependant, la mesure pourrait être appliquée et l'organisme pourrait alors documenter dans sa politique de sécurité de l'information que le télétravail est interdit.

1.8.4 Rédiger la Déclaration d'applicabilité

Exemple

Mesure	Applicable	Description	Justification	Documentation	Responsable
A.5.1.1 Politiques de sécurité de l'information	Oui	<p>La politique de sécurité de l'information, approuvée par la direction, est en vigueur depuis le 21 décembre 2017.</p> <p>Une copie a été transmise à tous les employés et parties prenantes concernées. La version officielle est disponible sur l'intranet</p>	Apporter à la sécurité de l'information une orientation et un soutien de la part de la direction, conformément aux exigences métier et aux lois et réglementations en vigueur	Politique de sécurité-3213PO	Responsable de la sécurité de l'information

PECB

151

ISO/IEC 27001 n'indique pas la forme que doit prendre la Déclaration d'applicabilité. Elle exige toutefois une liste précise des mesures de sécurité (choisies ou non), les raisons de ces choix et les mesures prises pour mettre en œuvre les mesures choisies. Les mesures supplémentaires mises en place doivent aussi apparaître dans la Déclaration d'applicabilité.

Il est de bonne pratique d'inclure dans la Déclaration d'applicabilité le titre ou la fonction du responsable de la mesure de sécurité ainsi que la liste des documents ou des enregistrements s'y rattachant. Le modèle proposé par PECB comporte les sections suivantes :

- 1. Mesure de sécurité :** Indique la mesure de sécurité avec sa référence à l'Annexe A d'ISO/IEC 27001.
- 2. Applicable :** Indique si la mesure de sécurité est applicable ou non.
- 3. Description sommaire :** Décrit en quelques phrases la mesure déclarée et sa mise en œuvre dans l'organisme. Une manière simple de le faire est d'utiliser la méthode des 6W (Who, What, When, Where, How, Why – Qui, Quoi, Quand, Où, Comment, Pourquoi). Il est à noter que le «pourquoi» est adressé dans la colonne «justification».
 - Par exemple:** Une politique de sécurité de l'information (quoi), approuvée par la direction (qui), est en vigueur depuis le 21décembre 2017 (quand). Une copie a été transmise (comment) à tous les employés et les parties prenantes concernées (qui). La version officielle est disponible sur l'intranet (où).
- 4. Justification:** Décrit les raisons de sélection ou d'exclusion de la mesure de sécurité.
- 5. Document :** Indique les documents (politiques et procédures) ou les enregistrements liés à cette mesure de sécurité.
- 6. Responsable :** Le propriétaire de la mesure est la personne responsable des actions liées à cette mesure. Son nom et sa fonction dans l'organisme doivent être inscrits dans le document. Si la mesure de sécurité est non applicable, la personne qui est en mesure de prouver sa non-applicabilité doit être identifiée et contactée afin de faciliter le travail des auditeurs (internes et externes) ; ce faisant, les organisations savent qui doit être contacté lors des révisions ultérieures de la Déclaration d'applicabilité.

Rédiger la Déclaration d'applicabilité

Exemple

Mesure	Applicable	Description	Justification	Documentation	Responsable
A.5.1.2 Revue des politiques de sécurité de l'information	Oui	La politique de sécurité de l'information est revue chaque année lors de la revue de direction et une résolution formelle la reconduit pour une année supplémentaire. En cas de changements majeurs, une révision peut avoir lieu en cours d'année à la demande du CISO ou de la direction.	Assurer que la politique de sécurité est maintenue à jour et qu'elle demeure alignée sur les objectifs de l'organisme	1. Procédure-revue-direction-312PR 2. Politique-sécurité-3213PO 3. Procédures de revue de direction 2017	Responsable de la sécurité de l'information
A.6.2.2 Télétravail	Non	-----	Notre organisme n'a aucune activité liée au télétravail.	Aucun document	Responsable des TI

PECB

152

1.8.5 Obtenir l'approbation de la direction

Preuves potentielles de l'autorisation de la direction

- Résolution du conseil d'administration ou du comité de pilotage
- Lettres officielles
- Enregistrement des revues de directions

Approbation de la direction



PECB

153

Pour obtenir l'autorisation de la direction de mettre en œuvre le SMSI, quelques documents doivent avoir été préparés, dont:

- Rapport d'analyse des risques
- Plan de traitement des risques (incluant l'identification des risques résiduels)
- Déclaration d'applicabilité

Habituellement, ces documents sont présentés lors d'une revue de direction avec le dépôt d'un rapport d'étape du projet SMSI. À l'issue de cette revue de direction, on devrait obtenir de la direction les résolutions suivantes :

- Approbation de la Déclaration d'applicabilité
- Autorisation de mettre en œuvre le SMSI
- Autorisation écrite de la direction quant à la mise en œuvre du SMSI

À la suite de l'autorisation formelle de mise en œuvre du SMSI, il est de bonne pratique de faire une annonce officielle. Cela peut se manifester par l'envoi d'une lettre officielle de la direction au personnel ou par une réunion de lancement.



Questions ?

PECB

154

Page de notes

PECB

155

Page de notes

PECB

156