Version6.0

Numéro de document: ISMSFDD2V6.0

Programme du jour

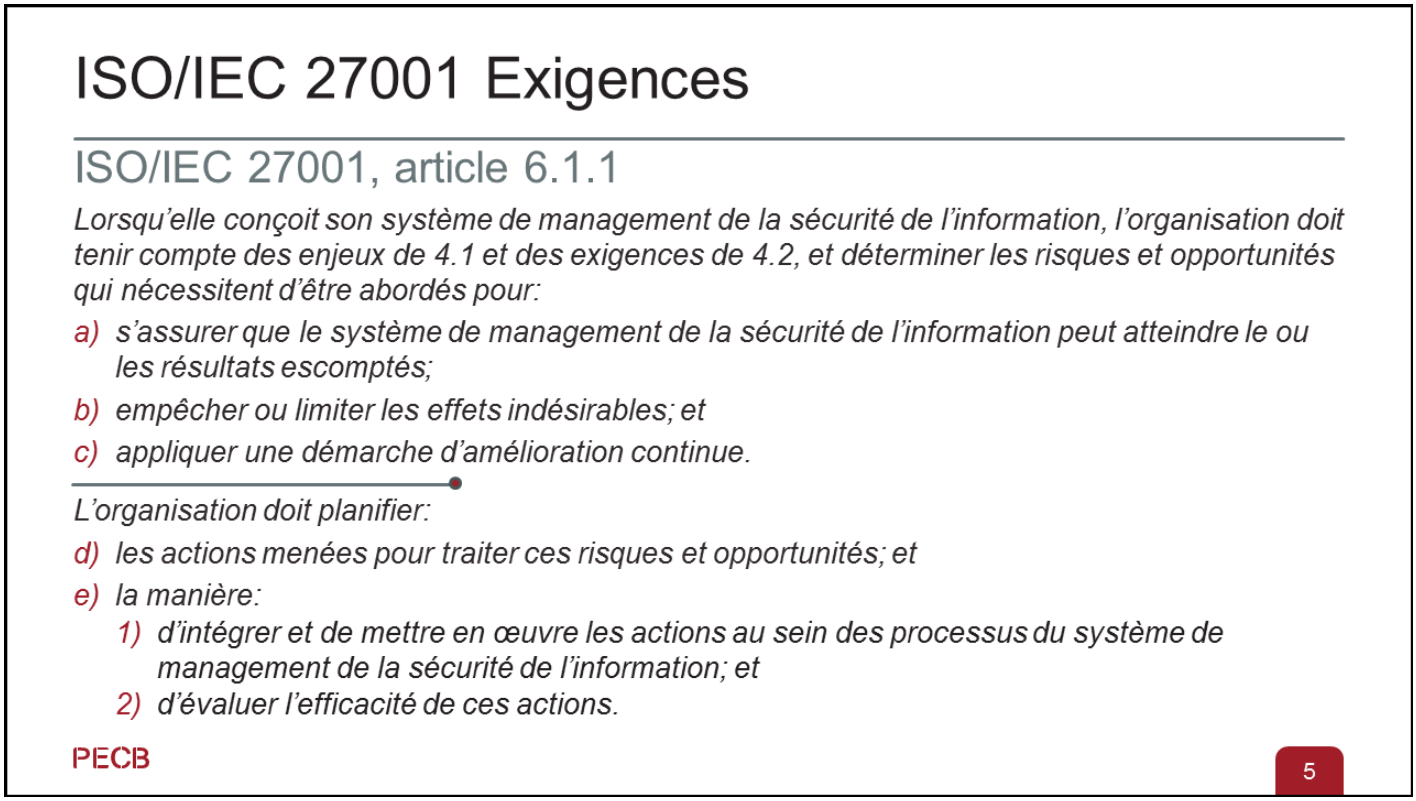
- Section 7 — Planification
- Section 8 — Support
- Section 9 — Fonctionnement
- Section 10 — Évaluation des performances
- Section 11 — Amélioration
- Section 12 — Mesures et objectifs des mesures
- Section 13 — Processus de certification et clôture de la formation

PECB

Objectifs d’apprentissage

1. Acquérir des connaissances sur le processus de gestion des risques
2. Acquérir des connaissances sur la manière de mener des programmes de formation et de sensibilisation
3. Acquérir des connaissances sur la surveillance, le mesurage, l'analyse et l'évaluation de la performance du SMSI
4. Acquérir des connaissances sur les actions correctives et les plans d'action

Cette section fournit des informations qui aideront le participant à acquérir des connaissances sur le processus de gestion des risques, y compris l'identification des risques, l'estimation des risques, l'évaluation des risques et le traitement des risques.



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 définisse 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.*

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;

PECB

6

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.

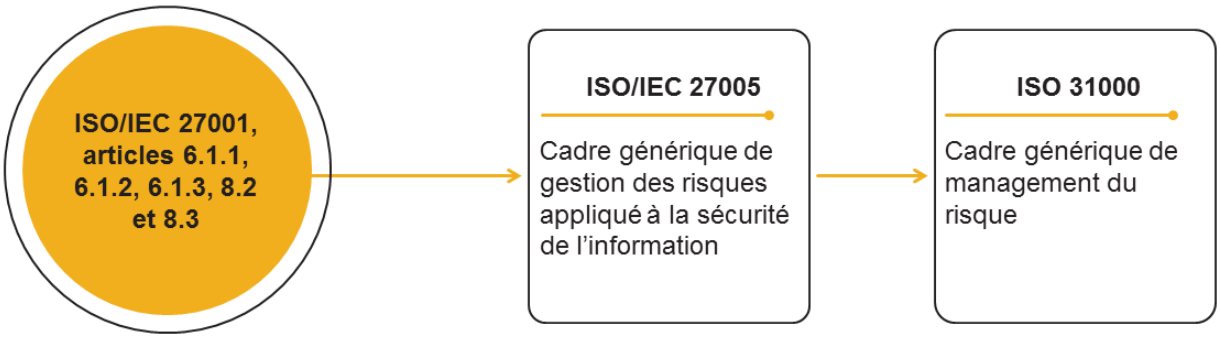
ISO/IEC 27001 Exigences

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 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.*

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

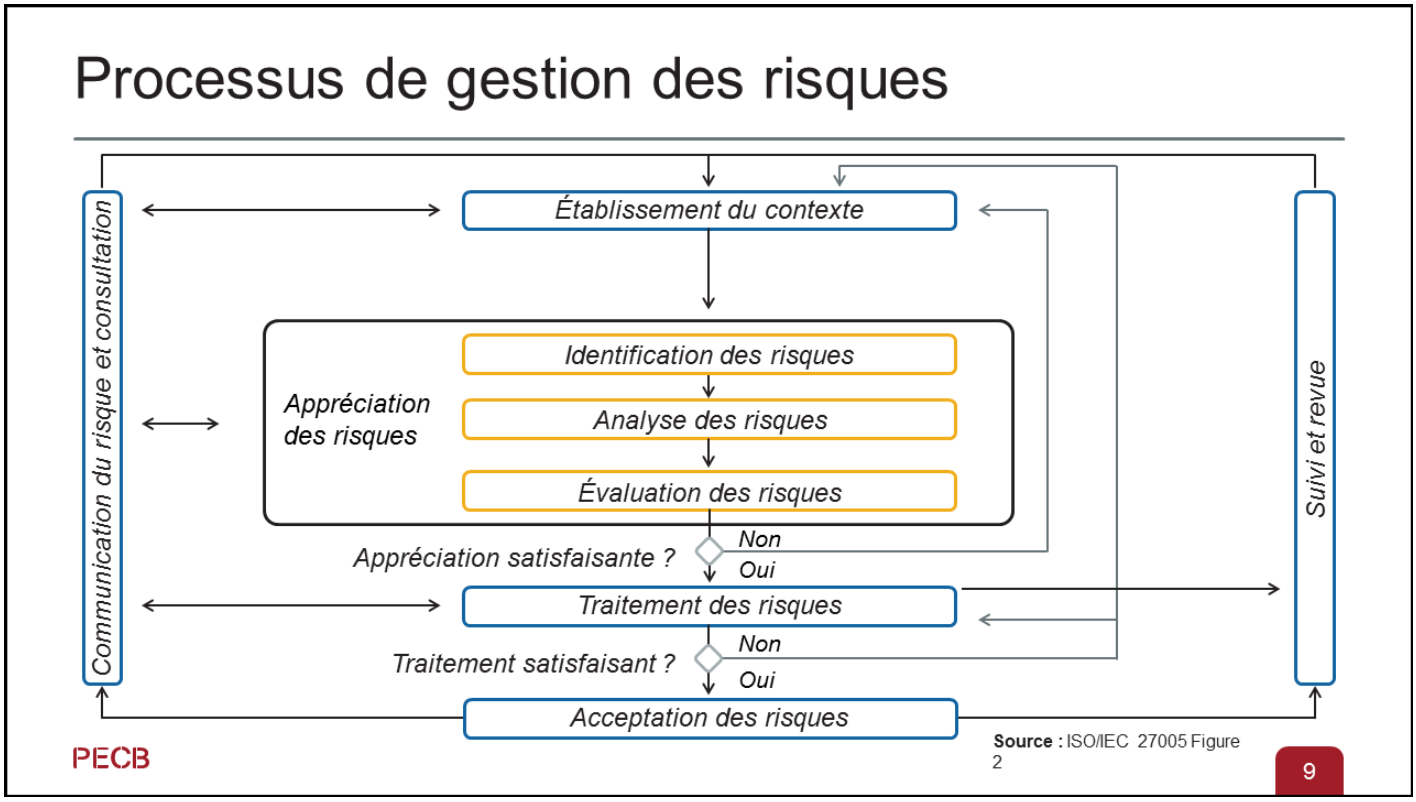


Note importante : L'application du processus de gestion des risques prévu dans ISO/IEC 27005 et ISO 31000 n'est pas obligatoire pour obtenir la certification selon ISO/IEC 27001.

PECB

8

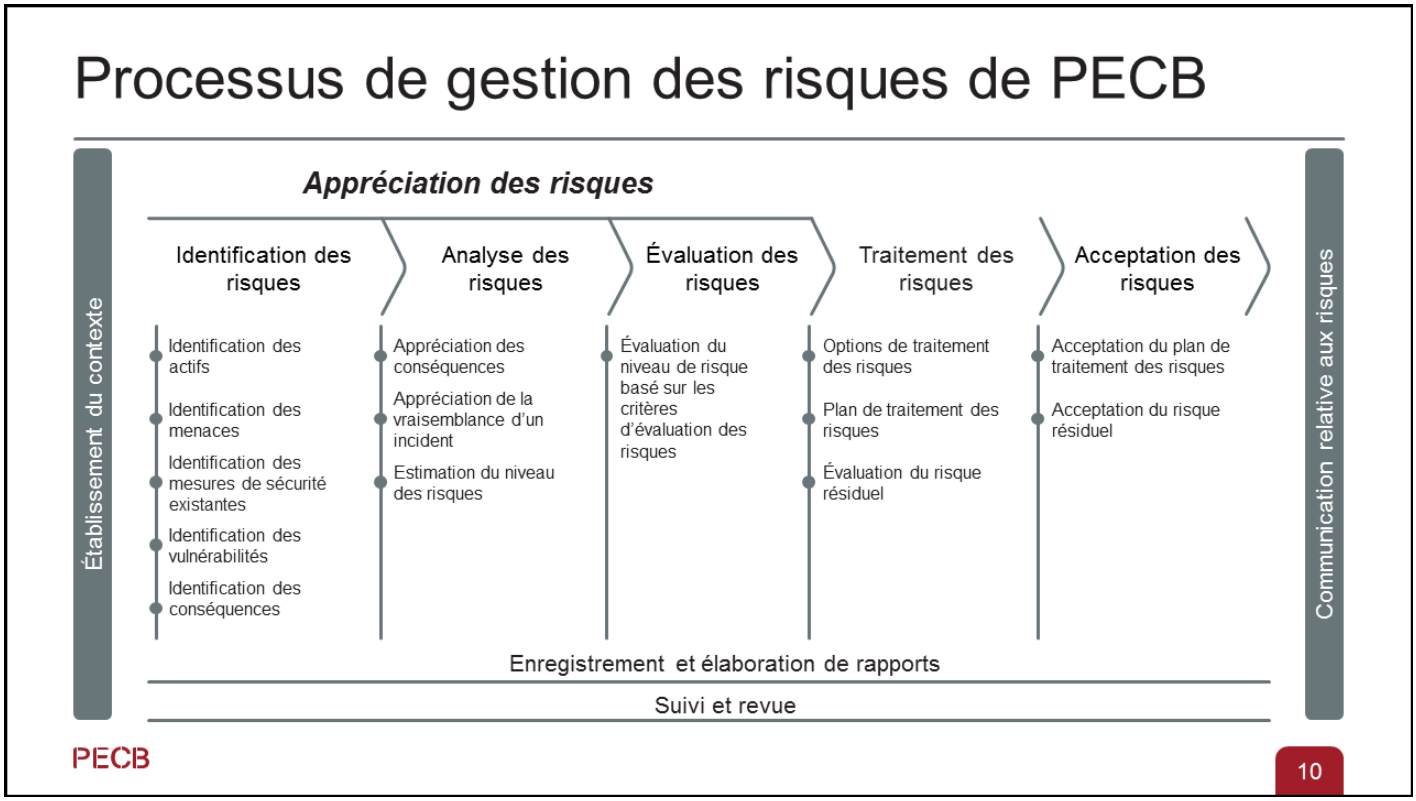
Basée sur le cadre de management du risque d'ISO 31000, la norme ISO/IEC 27005 explique en détail comment mener l'appréciation et le traitement des risques dans le cadre de la sécurité de l'information.



Comme l'illustre 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 planifiées 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 dépend des résultats 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'organisme et la surveillance des risques constituent des activités continues.



Note importante: Le processus de gestion des risques n'est pas un processus de fonctionnement indépendant (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.

Pour acquérir une connaissance plus approfondie de la mise en œuvre et de la gestion d'un programme de gestion des risques de sécurité de l'information, il est recommandé de suivre la formation " PECB Certified ISO/IEC 27005 Risk Manager.

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

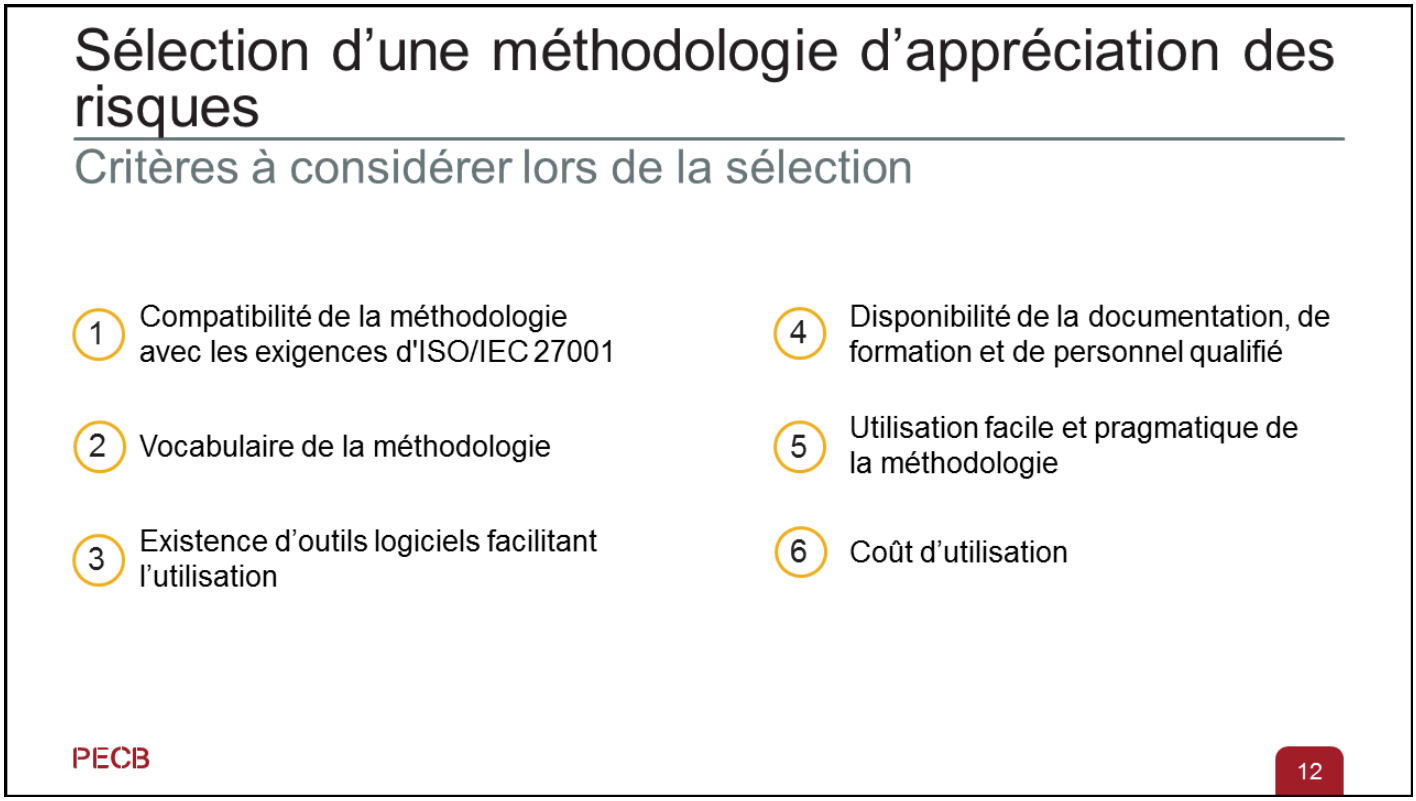
11

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:

a. *peuvent être préservés à l'avenir (voire être étendus à d'autres types de prise de décision);*
b. *nécessitent des modifications ou des améliorations;*
c. *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.



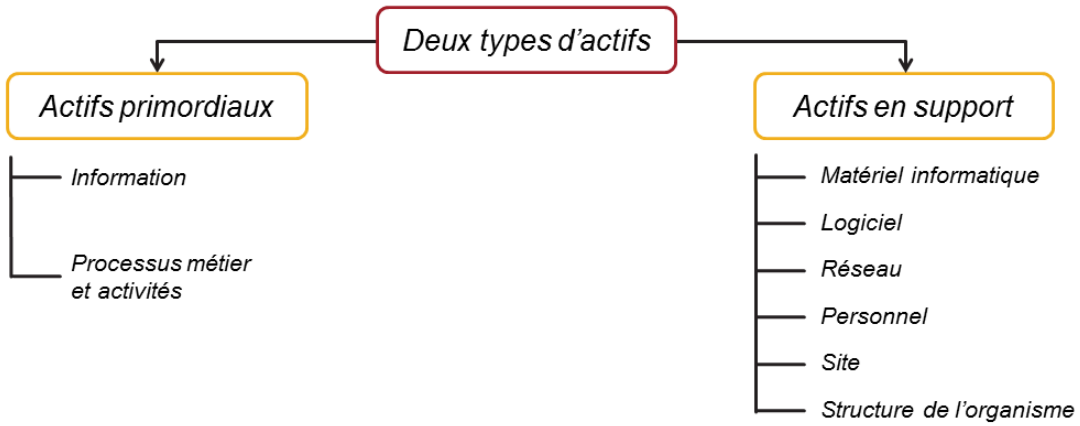
Toute méthodologie de gestion et d'appréciation des risques qui respecte les critères minimaux d'ISO/IEC 27001 est acceptable, même une méthode développée en interne, à condition de pouvoir démontrer qu'elle peut fournir des résultats comparables et reproductibles.

L'analyse des risques devrait au moins prendre en compte les critères d'évaluation définis par ISO/IEC 27001. Les mesures prises devraient produire les effets recherchés, prévenir et réduire les effets indésirables ainsi qu'améliorer les processus de l'organisme. En outre, l'analyse de risques doit permettre la sélection de critères objectifs pour déterminer un niveau de risque acceptable.

Identification des actifs

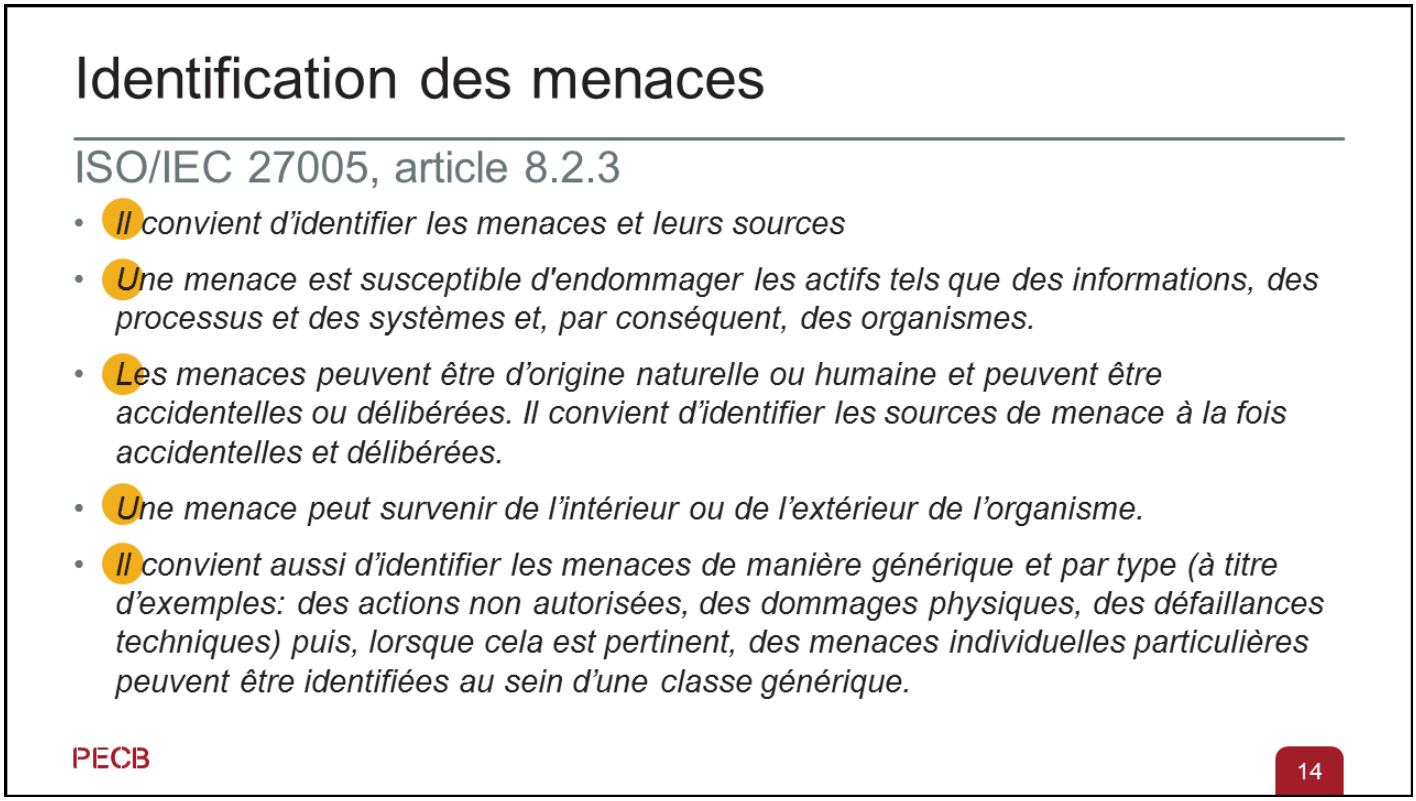
ISO/IEC 27005, article 8.2.2 et Annexe B.1.1

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



PECB

13



ISO/IEC 27005, article 8.2.3 Identification des menaces (suite)

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 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

15

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.

Identification des vulnérabilités

ISO/IEC 27005, article 8.2.5

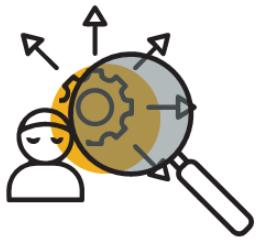
- *Il convient d'identifier les vulnérabilités susceptibles d'être exploitées par des menaces pour nuire aux actifs ou à l'organisme.*
- *La présence d'une vulnérabilité n'entraîne pas de dommage en elle-même, puisque la présence d'une menace est nécessaire pour l'exploiter.*
- *Une vulnérabilité à laquelle 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.*

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

17

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.

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».

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

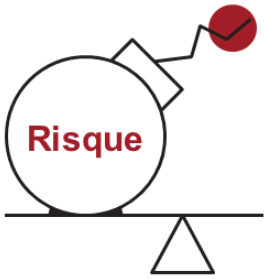
18

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.

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

19

ISO/IEC 27005, article 8.4 Évaluation du risque

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 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

20

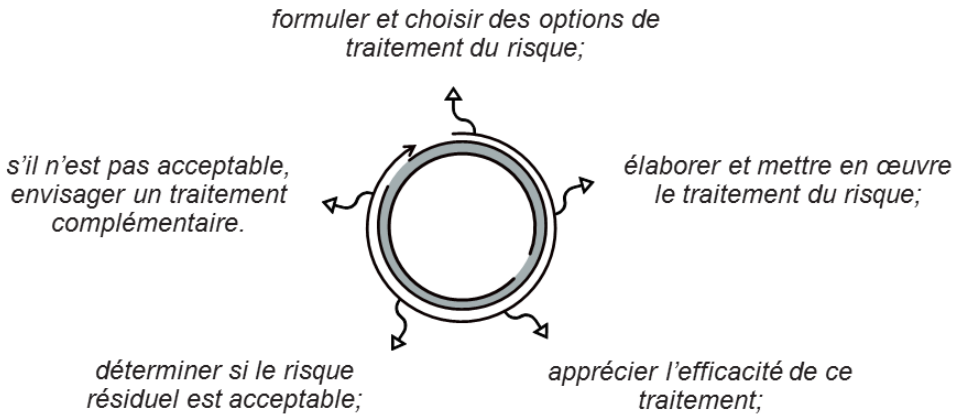
ISO/IEC 27005, Annexe E.2.3 Exemple 2 – Classement des menaces par mesures des risques

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 × c). Les menaces peuvent finalement être classées selon l’ordre de leur mesure des risques associée. Notez que dans cet exemple, 1 est considéré comme la conséquence et la vraisemblance la plus faible.

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

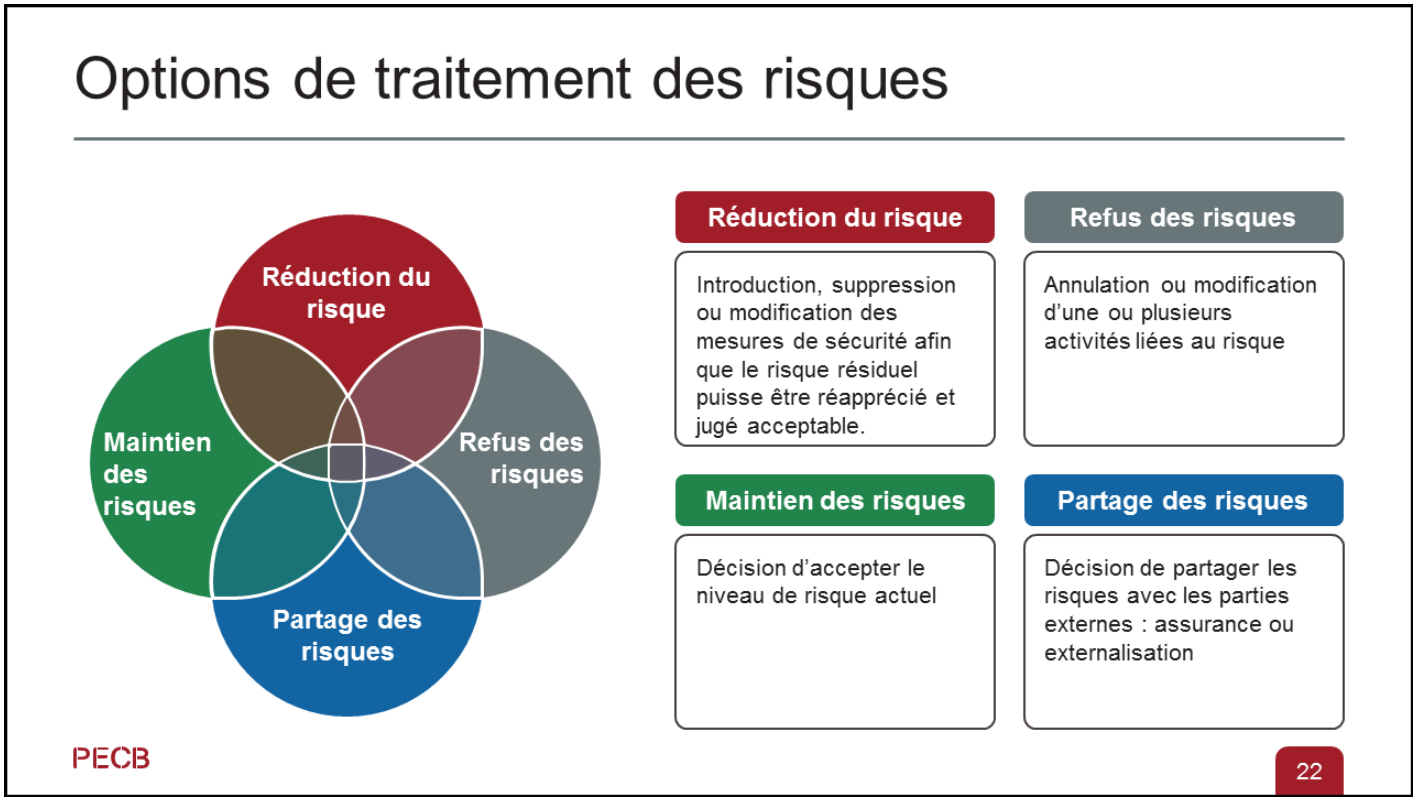
21

Le processus de traitement des risques comprend les activités suivantes :

1. Déterminer les options pour traiter les risques
2. Évaluer les options proposées pour traiter les risques
3. Élaborer et mettre en œuvre des plans d'action pour traiter 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 garantit que les coûts associés à la mise en œuvre de ces options n'excèdent pas les avantages qu'ils présentent. Conduire une analyse coûts-bénéfices est utile à cet égard.



La méthode d'appréciation des risques sélectionnée doit permettre à l'organisme de gérer les risques selon les 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

23

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

- Une fois que l'organisme a choisi l'option de traitement des risques la plus pertinente, il doit la planifier et la mettre en œuvre en conséquence.
- Les actions à entreprendre pour mettre en œuvre l'option de traitement des risques devraient être classées par ordre de priorité.
- L'organisme devrait allouer les ressources nécessaires à la mise en œuvre efficace de l'option de traitement des risques sélectionnée.

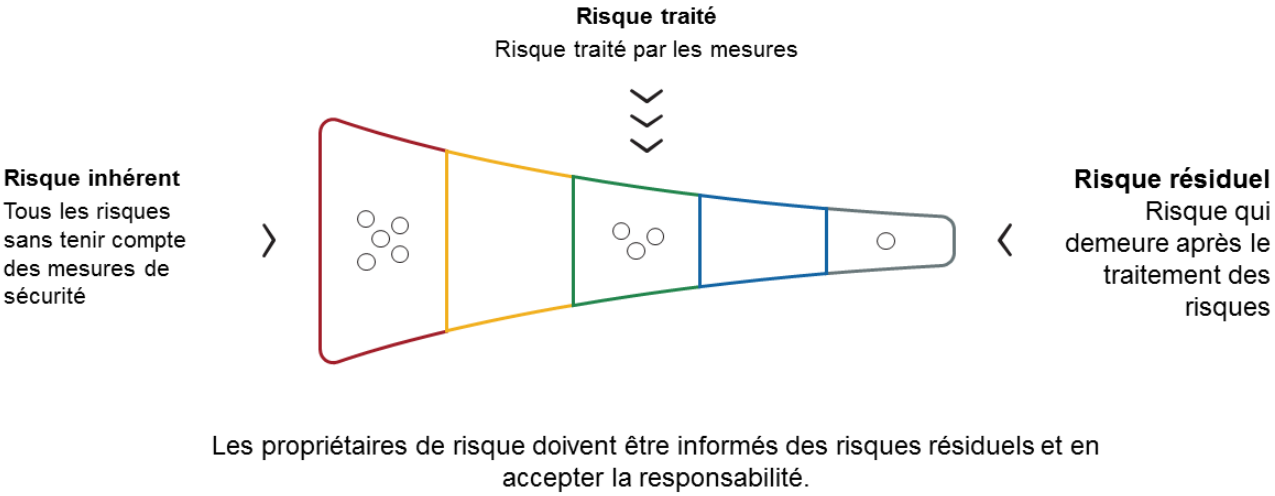
PECB

24

Lorsqu'elle détermine la priorité des actions à prendre pour mettre en œuvre l'option de traitement des risques sélectionnée, 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

Approbation du risque résiduel



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

PECB

25

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 :

Risque résiduel = risque inhérent – risque traité

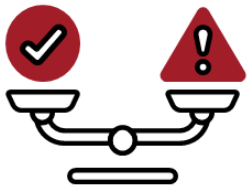
Après la mise en œuvre d'un plan de traitement des risques, il y a toujours des risques résiduels. **La valeur de la réduction des risques suivant le traitement des risques devrait être évaluée, calculée et documentée.** Le risque résiduel peut être difficile à évaluer, mais une évaluation devrait être 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.

Acceptation des risques

- L'acceptation des risques consiste à reconnaître les coûts et bénéfices potentiels auxquels un organisme s'expose en acceptant ces risques.
- L'acceptation des risques diffère suivant les secteurs d'activité, les organismes et les services d'un organisme.



PECB

26

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.

Exemples d'acceptation des risques :

Investissement :

La plupart des placements comportent un certain niveau de risque.

Assurance :

L'ensemble de l'industrie de l'assurance est basée sur des hypothèses de risques pour des frais définis.

Contrats dérivés :

Les contrats qui tirent leur valeur des taux de change ; le risque est transféré d'un organisme à l'autre.

Projets :

Les projets comportent un risque de dépassement de coûts.

Valeur nette (Business equity) :

Chaque actif détenu par un organisme est à risque.

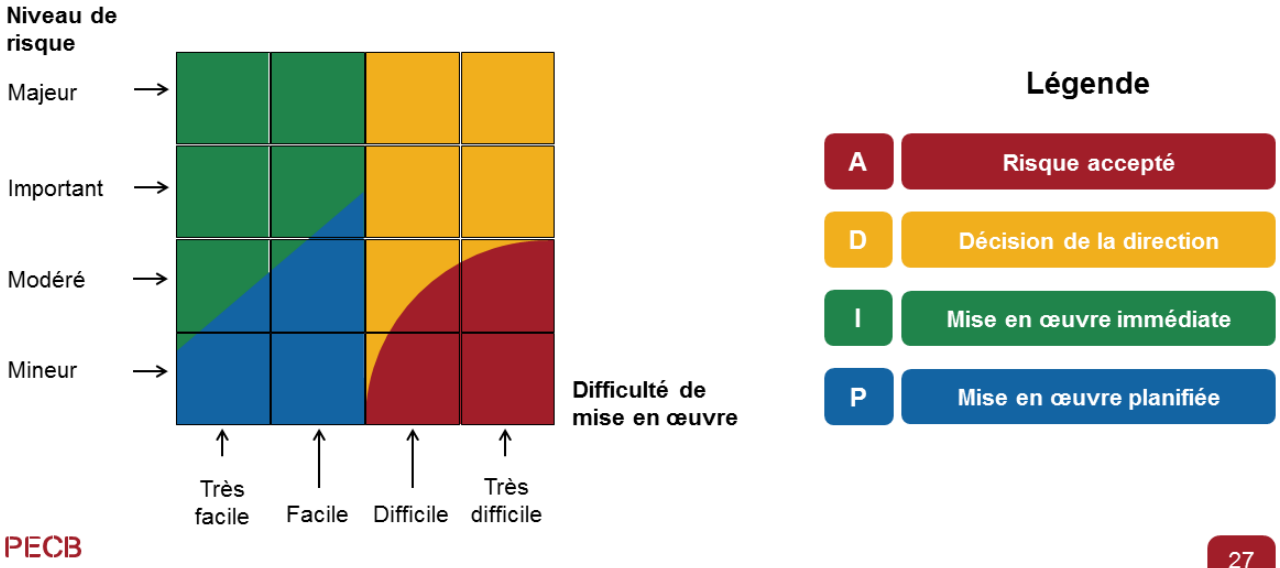
Ce risque est accepté en vertu de l'hypothèse que les rendements potentiels augmentent à mesure que le risque augmente.

Source :

Popov, Georgi, Bruce K. Lyon, and Bruce Hollcroft. Risk Assessment: A Practical Guide to Assessing Operational Risks. New Jersey: Wiley, 2016.

Acceptation du plan de traitement des risques

Présentation à la direction (exemple)



PECB

27

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.

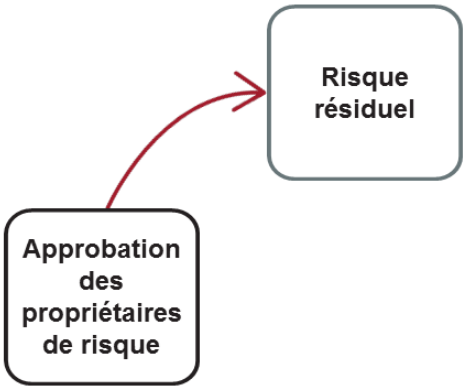
Toutefois, pour les risques mineurs ou modérés, le plan de traitement des risques pourrait être mis en œuvre immédiatement, ou le risque pourrait simplement être accepté en fonction de la difficulté de la mise en œuvre du plan.

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.*



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.*
- *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.*
- *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

29

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.

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.*

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.

Suivi et revue des risques

ISO 31000, article 6.6

- *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.*

PECB

31

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.

Quiz 2 : Planification

1. **Qu'est-ce qu'un actif ?**
   A. Tout élément ayant de la valeur pour l'organisme et nécessitant, par conséquent, une protection
   B. Tout élément que l'organisme a développé ou acheté
   C. Matériel informatique que l'organisme a développé ou acheté
2. **Quels types d'actifs sont les processus métier et activités ?**
   A. Actifs primordiaux
   B. Actifs secondaires
   C. Actifs en support
3. **Quel type d'actif est le matériel informatique ?**
   A. Secondaire
   B. Primordial
   C. Support
4. **Lequel des éléments suivants est un exemple de refus des risques ?**
   A. Annulation ou modification d'une ou plusieurs activités liées au risque
   B. Annulation ou modification du risque résiduel
   C. Annulation ou modification des critères d'acceptation des risques

5.Quel est le principal objectif de la phase de surveillance et revue du processus de management du risque ?

A. Faciliter l'interaction avec les parties prenantes, y compris celles ayant la responsabilité des activités de management du risque.
B. Assurer et améliorer la qualité et l'efficacité de la conception, de la mise en œuvre et des résultats des processus
C. Communiquer sur les activités de management du risque et leurs résultats au sein de l'organisme;

6.Quel est l'objectif de l'évaluation des risques ?

A. Soutenir les décisions qu'un organisme doit prendre
B. Créer une politique organisationnelle
C. Déterminer les acteurs de la menace

7.Quels sont les critères à considérer lors de la sélection d'une méthode d'appréciation des risques ?

A. Les menaces et les vulnérabilités identifiées
B. Le cadre de management du risque établi par la norme ISO 31000
C. Les critères d'évaluation établi par ISO/IEC 27001

8.À quoi se réfère le maintien des risques ?

A. Décision d'accepter le niveau de risque actuel
B. Décision de partager les risques avec les parties externes
C. Décision d'accepter les risques inhérents

9.Qu'est-ce que le risque résiduel ?

A. Risque que l'organisme ne peut éviter
B. Risque qui demeure après le traitement des risques
C. Risque inconnu de l'organisme

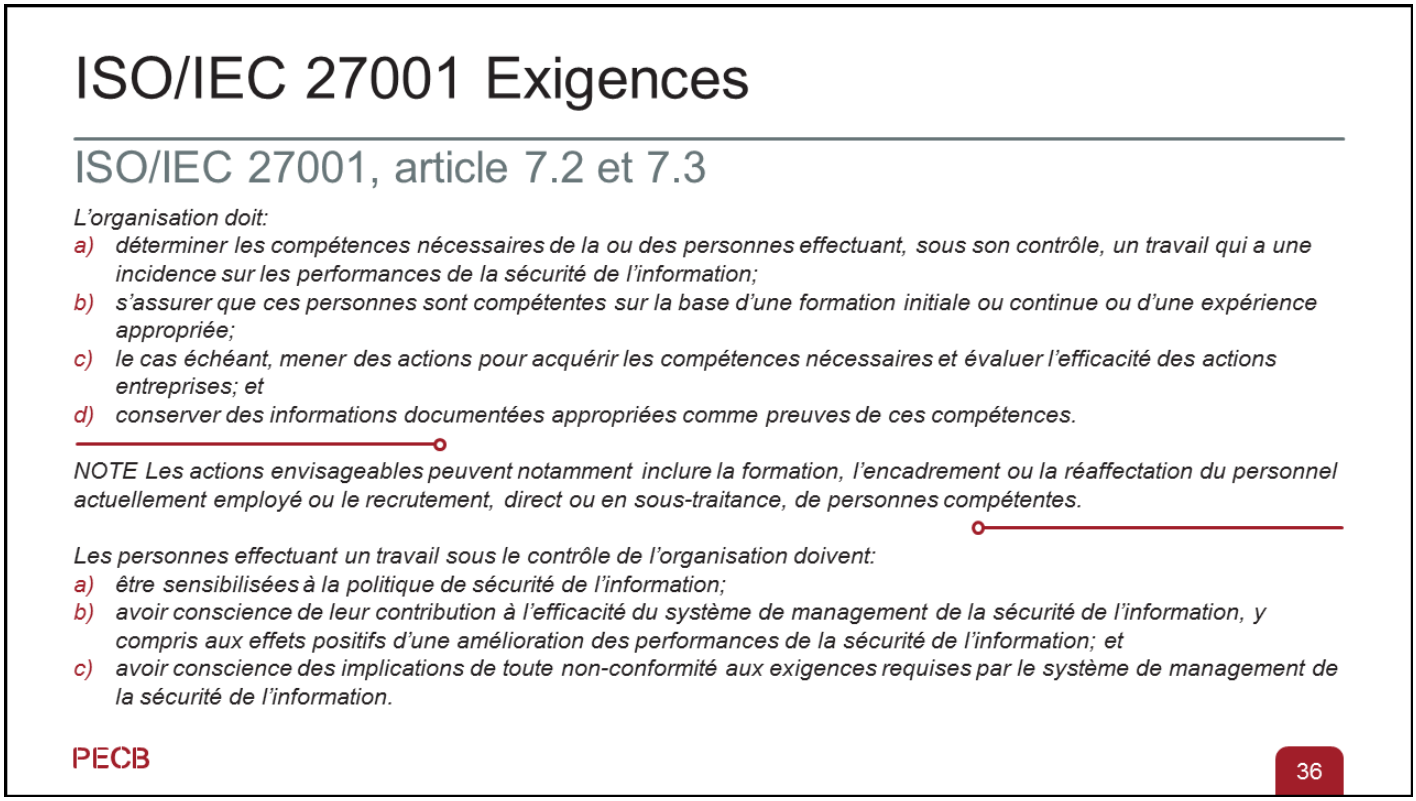
10.À quoi se réfère le scénario d'incident ?

A. Le scénario d'incident est la description des incidents potentiels susceptibles de nuire aux actifs de l'organisme
B. Le scénario d'incident est la description de mesures mal mises en œuvre ou de mauvais fonctionnements
C. Le scénario d'incident est la description d'une menace exploitant une vulnérabilité en termes de sécurité de l'information

Résumé de la section

- La norme ISO 31000 souligne l'importance d'intégrer la gestion des risques dans les processus, activités ou systèmes de l'organisation.
- Le processus de gestion des risques du PECB comprend l'établissement du contexte, l'appréciation des risques, le traitement des risques, l'acceptation des risques, la communication et la consultation, l'enregistrement et les rapports, ainsi que le suivi et la revue.
- L'appréciation des risques comprend l'identification, l'analyse et l'évaluation des risques.
- L'identification des risques consiste à trouver, reconnaître et décrire les risques.
- L'analyse des risques doit être aussi simple que possible.
- L'évaluation du risque compare les résultats de l'analyse du risque aux critères de risque établis.
- Les options de traitement des risques comprennent la modification, la rétention, l'évitement et le partage des risques.
- L'acceptation des risques est définie comme étant la décision informée de prendre un risque particulier.

Cette section fournit des informations qui aideront le participant à acquérir des connaissances sur la gestion des ressources, la formation, la compétence, la sensibilisation, la communication et l'information documentée du SMSI.



ISO/IEC 27003, article 7.2.3 (suite)

Lignes directrices

Il convient que l'organisation:

a. *définisse la compétence souhaitée pour chaque rôle dans le SMSI et décide si elle doit être documentée (p. ex. dans une description de poste);*
b. *attribue les rôles appartenant au sein du SMSI (voir 5.3) aux personnes ayant la compétence requise, soit en:*
    1. *identifiant les personnes au sein de l'organisation ayant la compétence appropriée (basée p. ex. sur leur éducation, leur expérience ou leurs certifications);*
    2. *planifiant et mettant en œuvre des actions pour que les personnes au sein de l'organisation obtiennent la compétence souhaitée (p. ex. par une formation, un mentorat, une réaffectation des employés actuels); ou*
    3. *engageant de nouvelles personnes qui ont la compétence (p. ex. en recrutant ou en contractant);*
c. *évalue l'efficacité des actions de l'alinéa b) ci-dessus;*
d. *vérifie que les personnes sont compétentes pour leurs rôles; et*
e. *s'assure que la compétence évolue au fil du temps, au besoin, et qu'elle répond aux attentes.*

Gestion des ressources

Afin de s'assurer du maintien et de l'amélioration continue du système de management de la sécurité de l'information, l'organisation doit allouer suffisamment de ressources à ses opérations :

Budget | Personnel qualifié | Outils

PECB

37

ISO/IEC 27021, article5.9 Compétence: Gestion des ressources

Résultats escomptés:

Veiller à ce que les ressources appropriées soient déterminées et fournies à temps pour l'établissement, la mise en œuvre, la maintenance et l'amélioration continue du SMSI.

Connaissances requises

- *Rapports financiers et mesure*
- *Techniques d'élaboration et de gestion budgétaire*
- *Techniques de gestion et de réduction des coûts*
- *Techniques de gestion du temps et des matériaux*
- *Revue de direction et processus d'actions correctives*

Compétences requises

- *Déterminer les ressources nécessaires à l'établissement, à la mise en œuvre, à la maintenance et à l'amélioration continue du SMSI*
- *Budgéter les éléments métier, y compris le coût de la mise en œuvre et du fonctionnement du SMSI*
- *Comprendre le rapport financier, y compris les flux de trésorerie et les profits et pertes*
- *Créer des études de faisabilité et d'investissement*
- *Indiquer le ROI (retour sur investissement), le ROSI (retour sur investissement en sécurité) et autres avantages financiers*
- *Appliquer les techniques de contrôle des coûts et de gestion budgétaire*
- *Fournir les ressources appropriées à temps et au bon endroit*

Compétences et développement du personnel

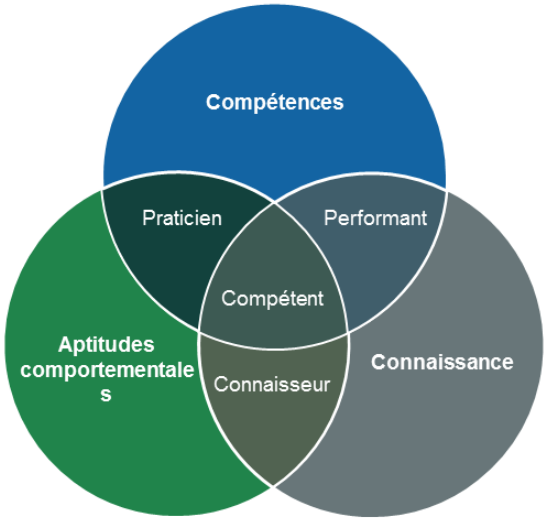
ISO 9000, article 3.10.4 et ISO 10015, article 3.2.1

Compétence

aptitude à mettre en pratique des connaissances et des savoir-faire pour obtenir les résultats escomptés

Développement du personnel

processus destiné à produire et à développer les connaissances, les savoir-faire et les comportements nécessaires à la satisfaction d'exigences



PECB

38

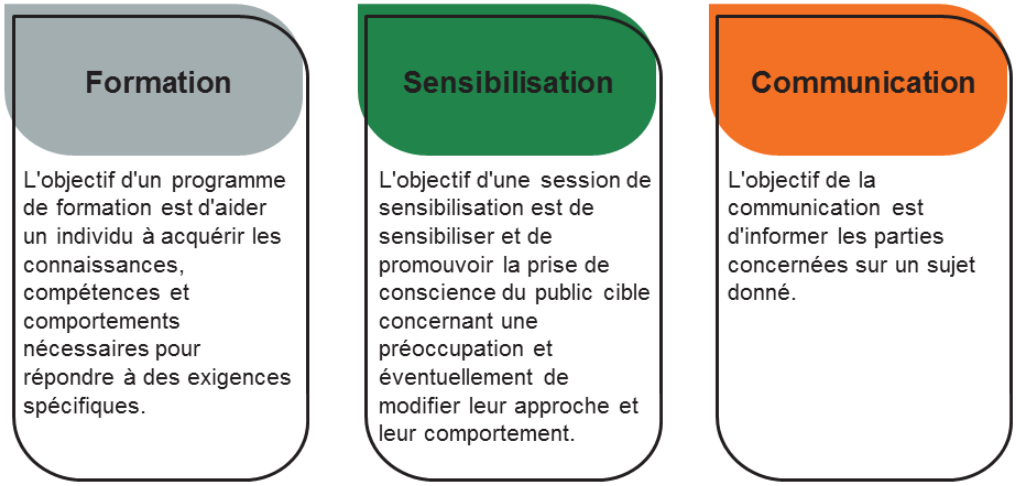
Un programme de formation planifié et systématique peut aider un organisme à augmenter ses capacités et à atteindre ses objectifs de sécurité de l'information.

ISO 10015, article 5.4.1

Les équipes, les groupes et les individus devraient être encouragés à s'engager dans des activités de gestion des compétences et de planification du développement des personnes afin d'accroître l'engagement et l'appropriation.

Formation, sensibilisation et communication

Différences



Programme de sensibilisation

Le programme de sensibilisation permet à un organisme :

- D'accroître la sensibilisation
- D'assurer une cohérence dans les pratiques de sécurité de l'information
- De contribuer à l'efficacité des politiques, directives et procédures.

Un employé qui n'est ni sensibilisé ni formé représente un risque potentiel.

PECB

40

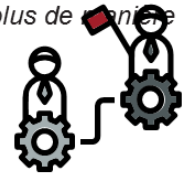
Le facteur technologique est l'un des paramètres clés dans le processus de mise en œuvre d'un système de management fonctionnel. Cependant, le facteur « humain » est tout aussi important pour assurer son efficacité. Les actifs humains peuvent être aussi bien une faiblesse qu'une force. Ils requièrent donc une attention considérable. Le personnel doit connaître et comprendre quelles sont ses responsabilités, comment il peut contribuer à l'efficacité du SMSI et comment il peut avoir une influence positive sur l'entreprise.

Gestion des compétences et développement du personnel

ISO 10015, article 5.4.2

La gestion des compétences et les activités de développement du personnel pour une équipe ou un groupe devraient aborder:

a) l'établissement et la mise en œuvre de programmes de formation d'équipe ou de groupe;
b) l'élaboration et la distribution d'une série de communications ciblées (p. ex., bulletins d'information, sites Web, apprentissage en ligne);
c) la participation à des conférences externes, des forums professionnels et des événements de réseautage;
d) assurer la liaison avec les organismes professionnels ou commerciaux concernés;
e) fournir des structures de soutien pour le partage des connaissances et des compétences;
f) recruter pour combler des lacunes spécifiques;
g) restructuration pour utiliser les compétences au sein de l'organisation dans un contexte plus de manière efficace et ciblée.



PECB

41

ISO 10015, article 5.4.3

Le développement d'activités au plan individuel peut inclure:

a. *des programmes d'apprentissage individuels;*
b. *le mentorat, l'encadrement et la supervision;*
c. *des plans de développement personnel;*
d. *des études formelles en vue de l'obtention de qualifications;*
e. *la participation à des conférences externes, etc.;*
f. *la formation (dans le rôle ou la fonction, en classe, en ligne);*
g. *les événements de réseautage.*

ISO 10015, article 5.5.1

Lors de la mise en œuvre du programme de développement, l'organisation doit déterminer et identifier les différents rôles et responsabilités.

L'organisation est responsable de:

a. *déterminer qui réalisera le programme de développement;*
b. *convenir du domaine d'application, de l'objectif et du public cible du programme de développement;*
c. *faciliter le programme de développement en fournissant les ressources nécessaires;*
d. *communiquer les exigences du programme aux parties intéressées concernées.*

ISO 10015, article 5.5.2

Les responsables du programme de développement du personnel et de ses activités sont chargés de:

a. *approuver le programme de développement du personnel;*
b. *veiller à ce que le programme de développement des ressources humaines comble les lacunes en matière de compétences;*
c. *s'assurer que les activités sont adaptées au public cible;*
d. *gérer et mettre en œuvre toutes les parties du programme dans les délais convenus;*
e. *veiller à ce que le suivi et l'évaluation se déroulent comme convenu.*

Communication

ISO/IEC 27001, article 7.4

L'organisation doit déterminer les besoins de communication interne et externe pertinents pour le système de management de la sécurité de l'information, et notamment:

a) sur quels sujets communiquer;

b) à quels moments communiquer;

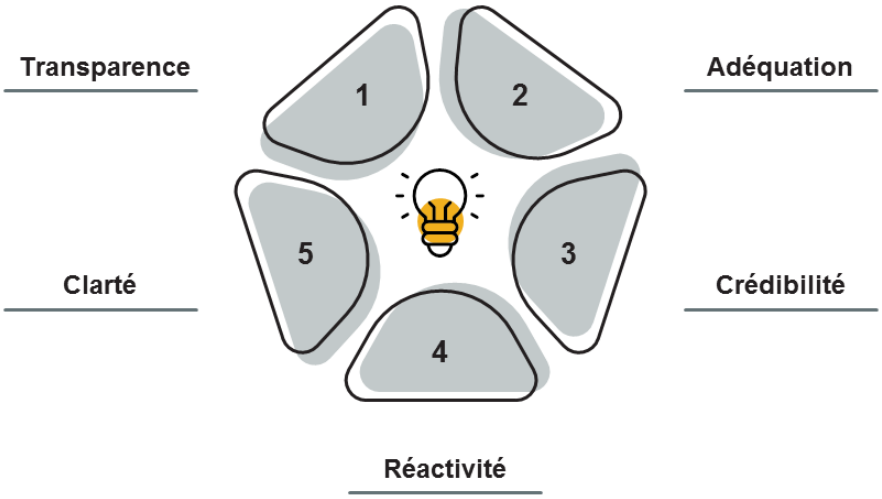
c) avec qui communiquer;

d) qui doit communiquer; et

e) les processus par lesquels la communication doit s'effectuer.

PECB

Principes pour une stratégie de communication efficace



PECB

43

Principes d'une stratégie de communication efficace

- **Transparence :** Communiquer correctement à toutes les parties intéressées les processus, procédures, méthodes, sources de données et hypothèses utilisés, en tenant compte du caractère confidentiel des informations.
- **Adéquation :** Fournir une information pertinente aux parties intéressées, en utilisant les formats, la langue et le support adaptés à leurs intérêts et leurs besoins, pour leur permettre de participer pleinement.
- **Crédibilité :** Gérer la communication de manière juste et honnête et fournir une information véridique, exacte, substantielle ; développer l'information et les données en utilisant des méthodes et des indicateurs reconnus et reproductibles.
- **Réactivité :** Répondre aux questions et aux préoccupations des parties intéressées de façon opportune ; rendre les parties intéressées conscientes de la façon dont leurs questions et leurs préoccupations ont été abordées.
- **Clarté :** S'assurer que les approches et la langue de communication soient compréhensibles par les parties intéressées afin de d'éviter l'ambiguité.

Information documentée

ISO/IEC 27001, article 7.5.1

Le système de management de la sécurité de l'information de l'organisation doit inclure:

a) les informations documentées exigées par la présente Norme internationale; et

b) les informations documentées que l'organisation juge nécessaires à l'efficacité du système de management de la sécurité de l'information.

NOTE L'étendue des informations documentées dans le cadre d'un système de management de la sécurité de l'information peut différer selon l'organisation en fonction de:

1) la taille de l'organisation, ses domaines d'activité et ses processus, produits et services;

2) la complexité des processus et de leurs interactions; et

3) la compétence des personnes.

PECB

44

ISO/IEC 27001, article 7.5.2 Création et mise à jour

Quand elle crée et met à jour ses informations documentées, l'organisation doit s'assurer que les éléments suivants sont appropriés:

a. *identification et description (par exemple titre, date, auteur, numéro de référence);*
b. *format (par exemple langue, version logicielle, graphiques) et support (par exemple, papier, électronique); et*
c. *examen et approbation du caractère approprié et pertinent des informations.*

ISO/IEC27001, article 7.5.3 Maîtrise des informations documentées

Les informations documentées exigées par le système de management de la sécurité de l'information et par la présente Norme internationale doivent être contrôlées pour s'assurer:

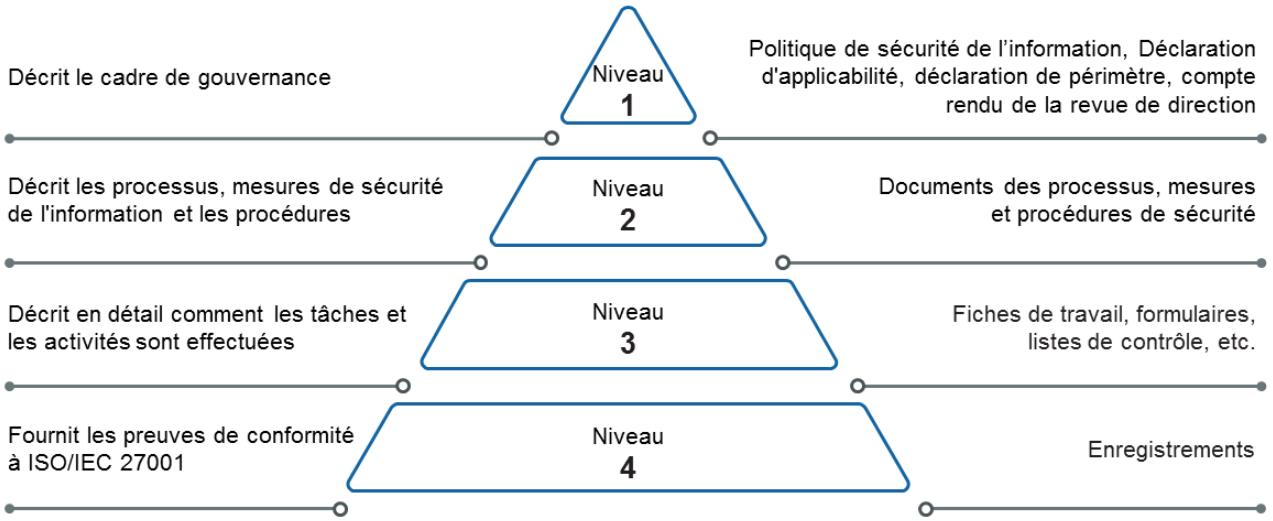
a. *qu'elles sont disponibles et conviennent à l'utilisation, où et quand elles sont nécessaires; et*
b. *qu'elles sont correctement protégées (par exemple, de toute perte de confidentialité, utilisation inappropriée ou perte d'intégrité).*

Pour contrôler les informations documentées, l'organisation doit traiter des activités suivantes, quand elles lui sont applicables:

c.distribution, accès, récupération et utilisation;
d.stockage et conservation, y compris préservation de la lisibilité;
e.contrôle des modifications (par exemple, contrôle des versions); et
f.durée de conservation et suppression.

Les informations documentées d'origine externe que l'organisation juge nécessaires à la planification et au fonctionnement du système de management de la sécurité de l'information doivent être identifiées comme il convient et maîtrisées.

Information documentée du SMSI



PECB

45

Il n'y a aucune exigence sur la façon de documenter les processus et les mesures de sécurité. L'organisme peut utiliser divers outils pour ce faire, p. ex. des diagrammes, descriptions textuelles, feuilles de calcul, etc.

Questions de discussion

1. Différence entre la formation, la sensibilisation et la communication
2. Quels sont les principes d'une stratégie de communication efficace ?
3. Quels sont certaines des principales informations documentées du SMSI ?

Questions ?

PECB

47

Cette section traite de la planification opérationnelle, de la gestion du changement et de la différence entre la continuité d'activité et la reprise d'activité après sinistre.

ISO/IEC 27001 Exigences

ISO/IEC 27001, article 8.1

- *L'organisation doit planifier, mettre en œuvre et contrôler les processus nécessaires à la satisfaction des exigences liées à la sécurité de l'information et à la réalisation des actions déterminées en 6.1. L'organisation doit également mettre en œuvre des plans pour atteindre les objectifs de sécurité de l'information définis en 6.2.*
- *L'organisation doit conserver des informations documentées dans une mesure suffisante pour avoir l'assurance que les processus ont été suivis comme prévu.*
- *L'organisation doit contrôler les modifications prévues, analyser les conséquences des modifications imprévues et, si nécessaire, mener des actions pour limiter tout effet négatif.*
- *L'organisation doit s'assurer que les processus externalisés sont définis et contrôlés.*

PECB

49

La déclaration d'applicabilité est un document décrivant les objectifs et les mesures pertinentes et applicables au SMSI de l'organisme. C'est un document clé du SMSI qui sert également de référence pour l'auditeur externe lors de l'audit de certification ainsi que l'un des documents que la direction générale doit valider et approuver avant le début des opérations du SMSI.

ISO/IEC 27001 Exigences

ISO/IEC 27001, article 8.2 et 8.3

Appréciation des risques de sécurité de l'information

- *L'organisation doit réaliser des appréciations des risques de sécurité de l'information à des intervalles planifiés ou quand des changements significatifs sont prévus ou ont lieu, en tenant compte des critères établis en 6.1.2 a).*
- *L'organisation doit conserver des informations documentées sur les résultats des processus d'appréciation des risques de sécurité de l'information.*

Traitement des risques de sécurité de l'information

- *L'organisme doit mettre en œuvre le plan de traitement des risques de sécurité de l'information.*
- *L'organisation doit conserver des informations documentées sur les résultats du traitement des risques de sécurité de l'information.*

Planification opérationnelle

- La norme ISO/IEC 27001 spécifie que les organismes devraient planifier, mettre en œuvre, contrôler et améliorer continuellement les processus nécessaires pour répondre aux exigences de sécurité de l'information.
- L'organisme devrait, à la suite du processus d'appréciation des risques, sélectionner les mesures et les mettre en œuvre.
- L'information documentée devrait être régulièrement tenue à jour afin de démontrer que les processus ont été exécutés comme prévu.
- Les changements planifiés et non planifiés devraient être contrôlés afin d'en atténuer les conséquences et les effets négatifs.
- L'organisme devrait aussi s'assurer que les processus externalisés sont contrôlés adéquatement.

Gestion des changements

- Fournir un plan de communication pour les utilisateurs avant la mise en œuvre des changements
- Éviter de mettre en œuvre trop de nouveaux processus en même temps
- Le cas échéant, assurer la formation du personnel avant de passer en mode opérationnel

PECB

52

Les étapes décrites ci-dessus s'appliquent à un changement qui a une incidence importante sur les éléments nouveaux du SMSI ou ceux ayant subi des changements importants. Dans d'autres cas, les changements peuvent nécessiter un minimum de communication ou de formation. Par exemple, lorsque le plan de mise en œuvre d'un SMSI est achevé avec succès, le SMSI sera officiellement transféré dans un mode opérationnel. L'importance relative de ce changement doit être décidée par la direction de l'organisme.

Continuité d’activité et reprise d’activité après sinistre

Différences

Continuité d’activité (CA)

- Définit les perturbations qui menacent la capacité d'un organisme à fournir ses services et produits
- Définit une réponse efficace aux perturbations
- Donne la priorité aux efforts de relance
- Protège les intérêts des différentes parties concernées

Reprise d’activité après sinistre (RA)

- Traite de l'impact direct d'un événement, comme les pannes de serveur, les failles de sécurité ou les ouragans
- Implique de réduire l'impact le plus rapidement possible et de s'attaquer immédiatement à ses conséquences

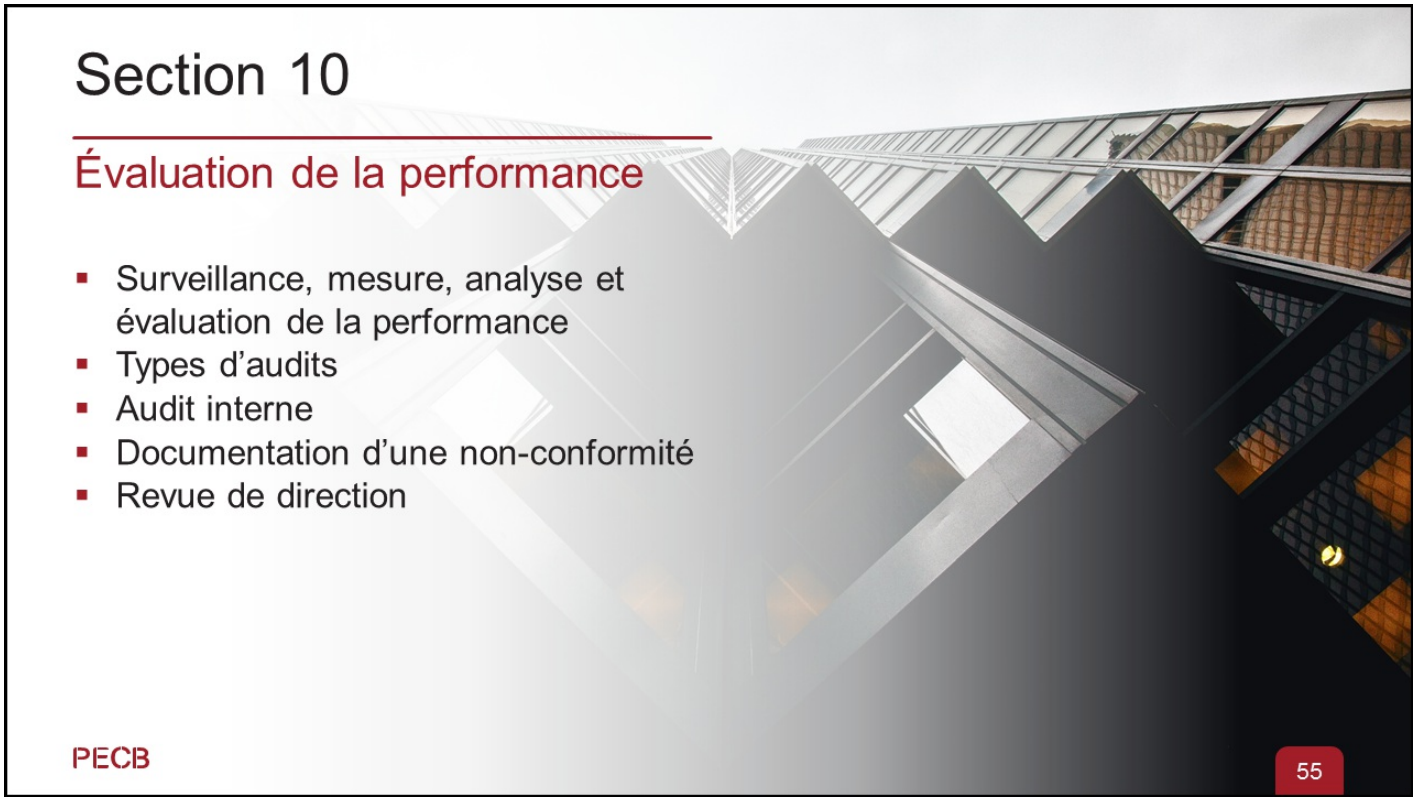
PECB

53

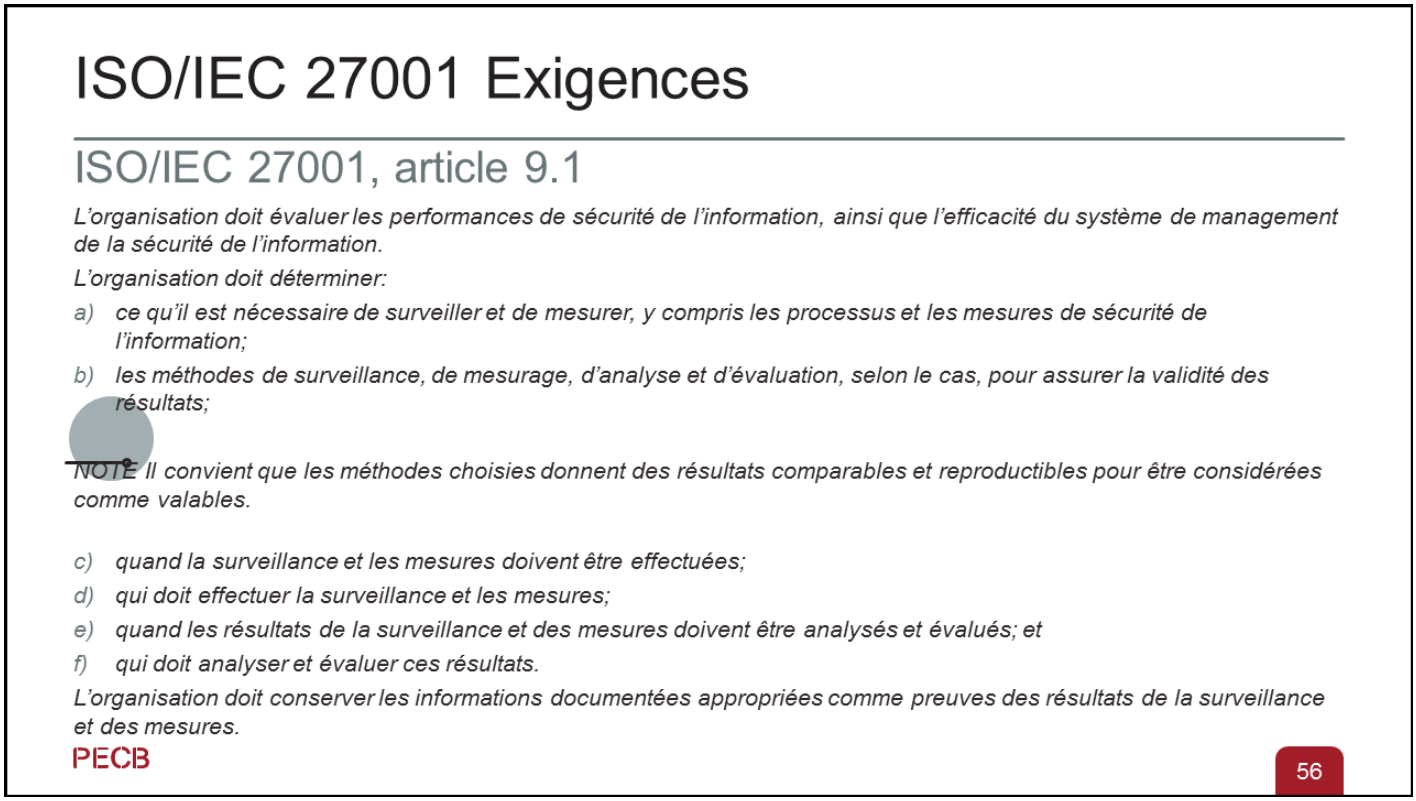
Bien que la différence entre la continuité d’activité (CA) et la reprise d’activité après sinistre (RA) puisse être floue pour certains, il est important de faire une distinction. La principale différence entre les deux est le moment où le plan est activé : La continuité d'activité vise à maintenir les opérations pendant une perturbation et immédiatement après qu'elle se soit produite, tandis que la reprise d'activité après sinistre vise à réagir après la perturbation et à rétablir le fonctionnement normal.

Résumé de la section

- Le document clé qui décrit les objectifs et les mesures ainsi que leur applicabilité dans le SMSI de l'organisme est défini comme la Déclaration d'applicabilité.
- La continuité d'activité définit les perturbations qui menacent la capacité d'un organisme à fournir ses services et ses produits, apporte une réponse efficace et protège les intérêts des parties concernées.
- La reprise d'activité après sinistre traite des impacts directs d'un événement.



Cette section fournit des informations qui aideront le participant à acquérir des connaissances sur l'évaluation des performances, y compris la surveillance, la mesure, l'analyse et l'évaluation, l'audit interne et la revue de direction.

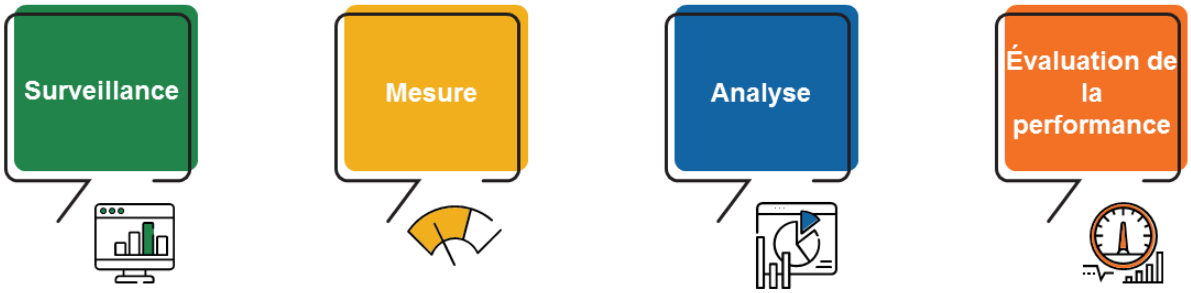


ISO/IEC 27003, clause 9.1 Surveillance, mesure, analyse et évaluation

Une bonne pratique consiste à définir le « besoin d'information » lors de la planification de la surveillance, de la mesure, de l'analyse et de l'évaluation. Un besoin d'information est généralement exprimé en tant qu'enjeu ou déclaration de sécurité d'information de haut niveau qui aide l'organisme à évaluer la performance en matière de sécurité de l'information et l'efficacité du SMSI. En d'autres termes, la surveillance et la mesure doivent être effectuées pour répondre à un besoin d'information défini.

Il convient d'être prudent lors de la détermination des attributs à mesurer. Il est irréaliste, coûteux et contreproductif de trop mesurer ou de s'intéresser aux mauvais attributs. En plus des coûts de mesure, d'analyse et d'évaluation de trop nombreux attributs, il est possible que les enjeux clés puissent être obscurcis ou complètement ignorés.

Surveillance, mesure, analyse et évaluation de la performance



Processus de détermination de l'état d'un système, d'un processus ou d'une activité

Processus de détermination d'une valeur

Processus d'examen de la nature d'une chose ou de détermination de ses caractéristiques essentielles et de leurs relations

Processus de détermination de résultats mesurables

PECB

57

La mesure des performances peut être définie comme un moyen systématique d'évaluer les réalisations actuelles d'une organisation par rapport à ses objectifs. Les mesures de performance sont d'une valeur minime en soi, à moins de les considérer dans le contexte des stratégies et des objectifs de l'organisme. C'est également vrai pour les systèmes de management, qui ne peuvent pas exister en vase clos et doivent contribuer aux objectifs de l'organisation pour être efficaces.

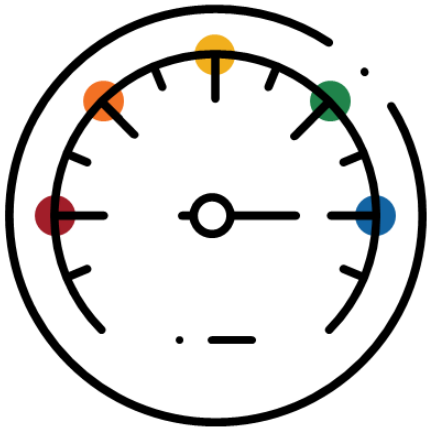
Surveillance et mesure

Qu'est-ce qui doit être surveillé et mesuré ?

1. Mesure dans laquelle les objectifs de l'organisme en matière de sécurité de l'information sont atteints

2. Processus, procédures et fonctions critiques

3. Preuves historiques de performance déficiente du SMSI (p. ex. non-conformités, fuite de données, défaillances, incidents)



4. Conformité aux exigences légales et réglementaires applicables, bonnes pratiques de l'industrie

5. Actions correctives et préventives appliquées pour traiter les non-conformités

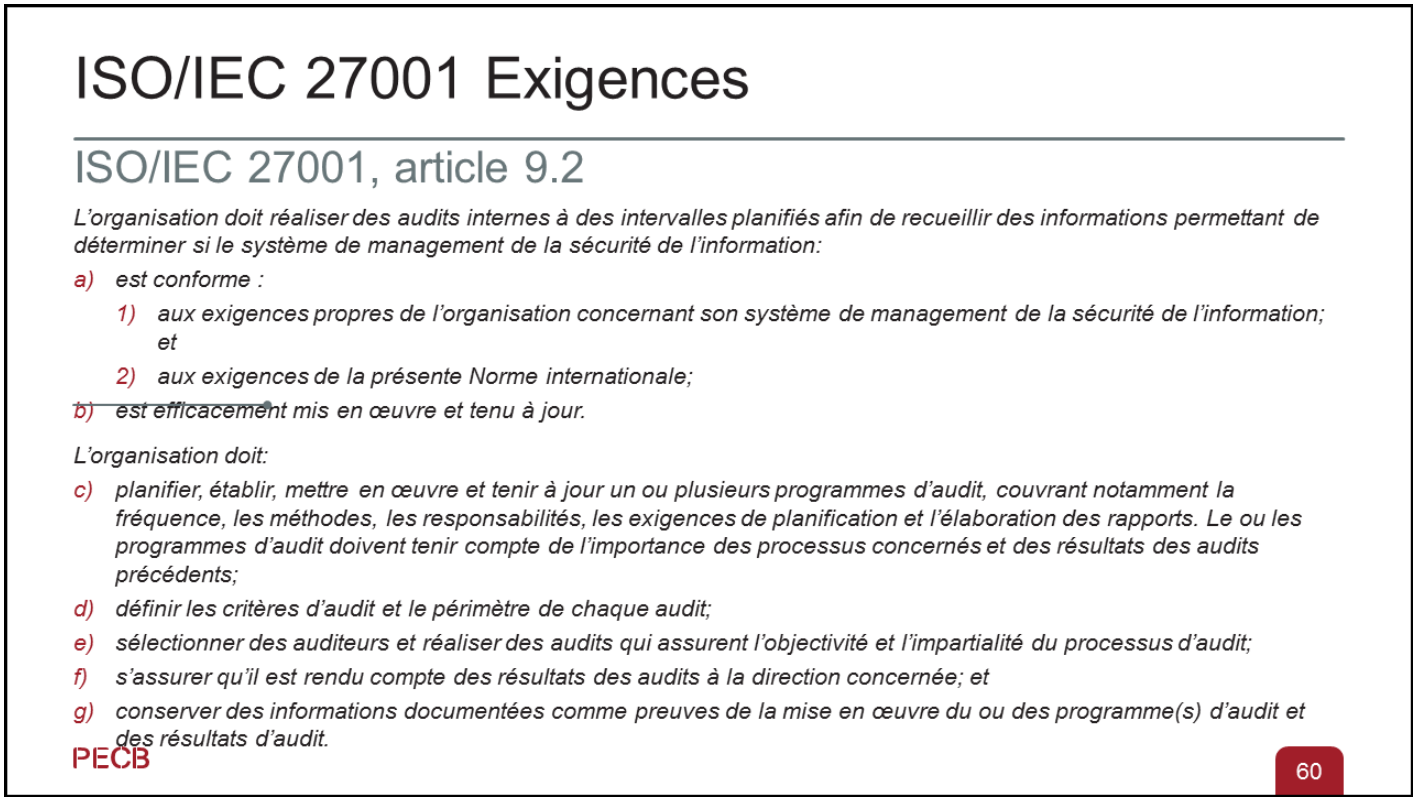
PECB

Déterminer la fréquence et la méthode de surveillance et de mesure

Comment et quand surveiller et mesurer ?

Pratiques

- La norme ISO/IEC 27001 n'indique pas comment ni à quelle fréquence la surveillance et la mesure doivent être effectuées.
- Il appartient à l'organisme de déterminer ce qui doit être surveillé et mesuré.
- Il est de bonne pratique d'utiliser des tableaux de bord pour enregistrer et rapporter les activités de surveillance et de mesure grâce à des indicateurs de performance.
- Les tableaux de bord devraient indiquer la performance réelle par rapport aux cibles de performance prédéterminées.



ISO/IEC27003, article9.2 Audit interne

Les auditeurs évaluent également si le SMSI est mis en œuvre et préservé de façon efficace. Un programme d'audit décrit le cadre général d'une série d'audits, planifiés selon des calendriers précis et orientés vers des objectifs spécifiques. Ceci est différent d'un plan d'audit, qui décrit les activités et les modalités d'un audit spécifique. Les critères d'audit sont un ensemble de politiques, de procédures ou d'exigences utilisées comme références auxquelles les données probantes sont comparées, c'est-à-dire que les critères d'audit décrivent ce que l'auditeur devrait constater.

Si le résultat de l'audit comprend des non-conformités, l'audité doit préparer un plan d'action pour chaque non-conformité, à convenir avec le chef de l'équipe d'audit. Un plan d'action de suivi comprend généralement:

i)*la description de la non-conformité détectée;*
j)*la description de la (des) cause(s) de non-conformité;*
k)*la description des actions correctives à court terme et à plus long terme afin d'éliminer une non-conformité détectée dans un délai défini; et*
l)*les personnes responsables de la mise en œuvre du plan.*

Les rapports d'audit, avec leurs résultats, devraient être remis à la direction.

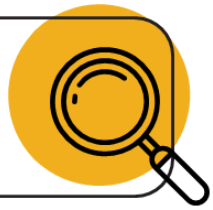
Les résultats des audits précédents devraient être revus et le programme d'audit devrait être adapté pour mieux gérer les zones présentant des risques plus élevés en raison de la non-conformité.

Qu’est-ce qu’un audit ?

ISO 19011, article 3.1

Processus méthodique, indépendant et documenté, permettant d’obtenir des preuves objectives et de les évaluer de manière objective pour déterminer dans quelle mesure les critères d’audit sont satisfaits

Autrement dit, l'audit est le processus qui consiste à demander à l'organisme audité ce qu'il fait et comment il le fait, afin de vérifier si ses pratiques sont conformes aux politiques, procédures et processus de l'organisme ainsi qu'aux exigences de la norme.

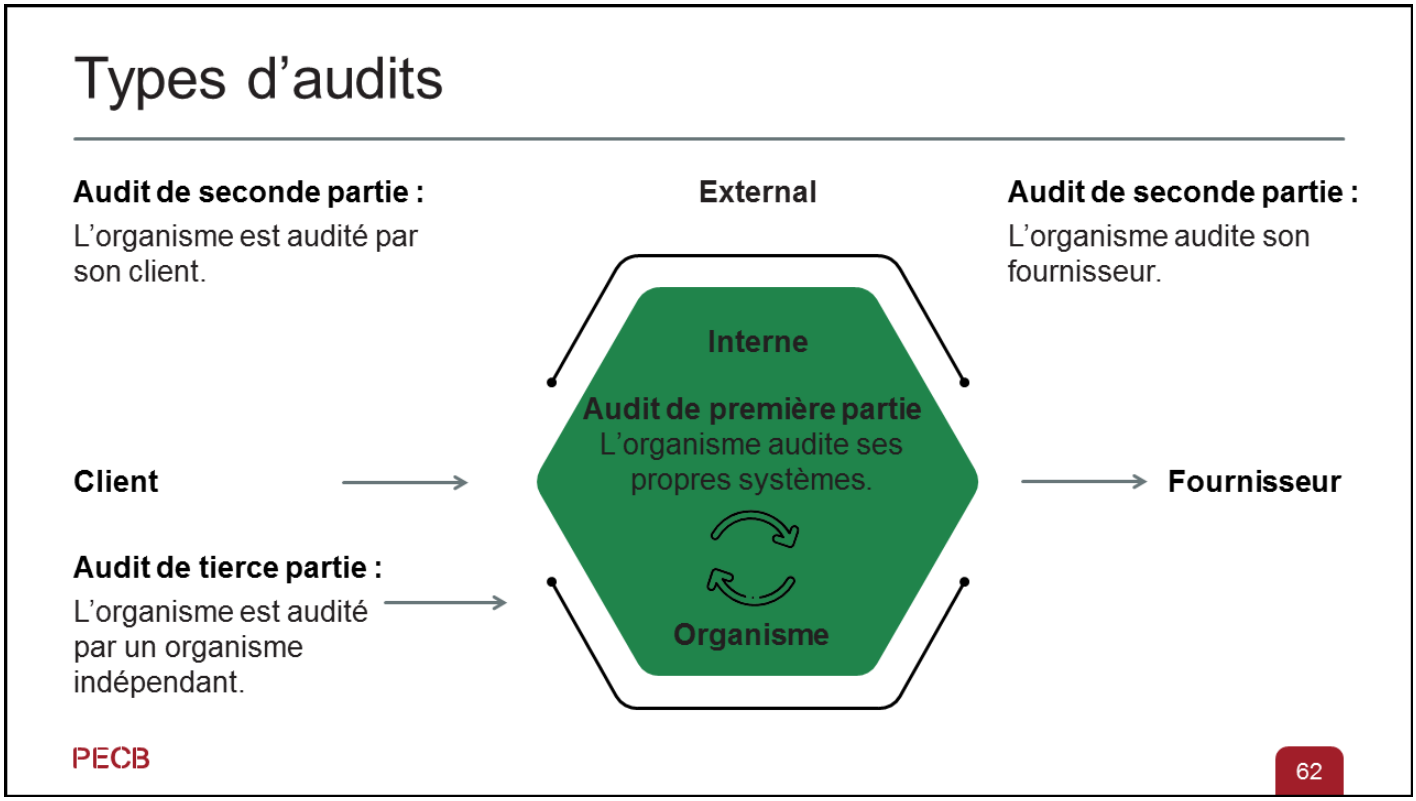


PECB

61

Un audit met en évidence les forces et les faiblesses de l’organisme ou du système audité. Les résultats de l'audit sont ensuite communiqués à la direction, qui prend alors les mesures appropriées.

- **Un audit financier** détermine si les pratiques comptables d'un organisme sont conformes aux exigences légales et aux principes reconnus.
- **Un audit administratif** détermine l'efficacité des pratiques administratives globales.
- **Un audit de sécurité de l'information** détermine si les actifs informationnels sont protégés de manière appropriée.



L'audit interne, parfois appelé audit de première partie, est une activité indépendante, objective et consultative conçue pour améliorer les fonctions de l'organisme. Les audits internes sont réalisés par l'organisme lui-même.

Les audits externes comprennent les audits de seconde et de tierce parties:

- **Les audits de deuxième partie** sont réalisés par des parties ayant un intérêt dans l'organisme audité, comme les clients, ou des personnes agissant en leur nom.
- **Les audits de tierce partie** sont réalisés par des organismes externes et indépendants qui octroient la certification et l'enregistrement de la conformité ou par des agences gouvernementales.

Note importante: L'audit de tierce partie est réalisé par des auditeurs externes indépendants de l'audité.

Différences entre audits internes et externes

Principales caractéristiques

Audit interne	Audit externe
1 Indépendant des activités auditées (pas de l'organisme)	1 Indépendant de l'organisme audité et de ses activités
2 Tient compte de l'efficacité et de l'efficience du SMSI	2 Tient compte uniquement de l'efficacité du SMSI
3 Rôle de conseil auprès de l'organisme pour l'amélioration du SMSI	3 Aucun rôle de conseil auprès de l'organisme
4 Peut être effectué en continu	4 Toujours mené de manière planifiée et en temps opportun

PECB

Non-conformité

Définition

- Selon la norme ISO 9000, une non-conformité est la « non-satisfaction d'une exigence ».
- Il existe deux types de non-conformités :
  - Non-conformité mineure
  - Non-conformité majeure

PECB

64

Les exigences peuvent provenir de plusieurs sources: normes nationales ou internationales, règles et politiques internes de l'organisme, lois et règlements du pays dans lequel l'organisme opère, contrats signés avec des clients ou des partenaires.

ISO9000, article3.6.9 Non-conformité

non-satisfaction d'une exigence

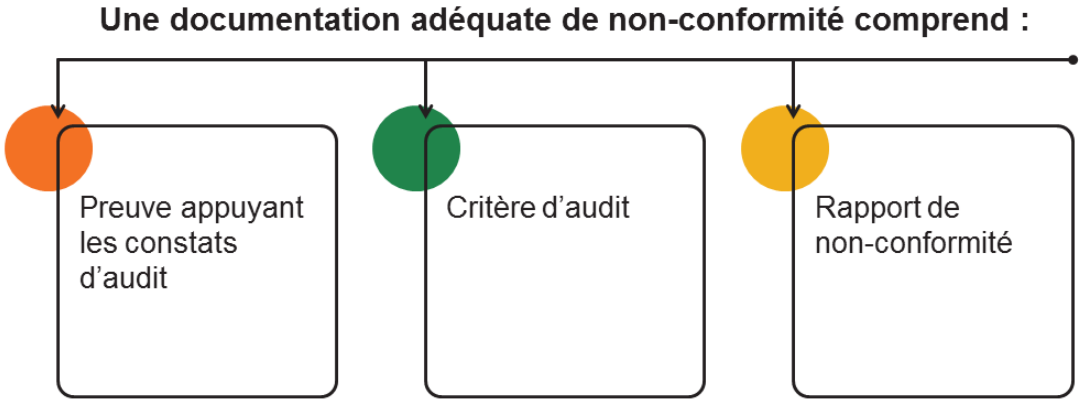
ISO9000, article3.6.11 Conformité

satisfaction d'une exigence

Voici des exemples de non-conformités:

- Documentation incomplète
- Mesure de sécurité absente ou ne remplissant pas ses fonctions
- Mesure de sécurité ne fournissant pas les résultats prévus

Documentation d'une non-conformité



PECB

65

Une fois la non-conformité confirmée, l'auditeur doit la documenter. L'enregistrement de cette non-conformité peut être aussi simple qu'une description de l'observation et la référence à l'article approprié.

Il est à noter qu'ISO/IEC 27001 contient des articles qui incluent plus d'une exigence. L'auditeur doit donc documenter les conditions spécifiques de la non-conformité en transcrivant l'exigence exacte de la norme.

Le rapport de non-conformité devrait:

- Explicite et concis
- Sans équivoque et linguistiquement correct

ISO/IEC 27001 Exigences

ISO/IEC 27001, article 9.3

À des intervalles planifiés, la direction doit procéder à la revue du système de management de la sécurité de l'information mis en place par l'organisation, afin de s'assurer qu'il est toujours approprié, adapté et efficace.

La revue de direction doit prendre en compte:

a) l'état d'avancement des actions décidées à l'issue des revues de direction précédentes;

b) les modifications des enjeux externes et internes pertinents pour le système de management de la sécurité l'information;

c) les retours sur les performances de sécurité de l'information, y compris les tendances concernant:

1) les non-conformités et les actions correctives;

2) les résultats de l'évaluation de la surveillance et des mesures;

3) les résultats d'audit; et

4) la réalisation des objectifs en matière de sécurité de l'information;

d) les retours d'information des parties intéressées;

e) les résultats de l'appréciation des risques et l'état d'avancement du plan de traitement des risques; et

f) les opportunités d'amélioration continue.

Les conclusions de la revue de direction doivent inclure les décisions relatives aux opportunités d'amélioration continue et aux éventuels changements à apporter au système de management de la sécurité de l'information. L'organisation doit conserver des informations documentées comme preuves des conclusions des revues de direction.

Revue de direction

Définition

Une revue de direction est un examen périodique effectué par la direction générale pour analyser la pertinence, l'adéquation et l'efficacité continues du SMSI.

Terme	Concept
Pertinence	Les résultats sont atteints de la meilleure manière possible.
Adéquation	Les éléments de sortie répondent aux critères établis.
Efficacité	Le SMSI répond aux besoins de l'organisme.

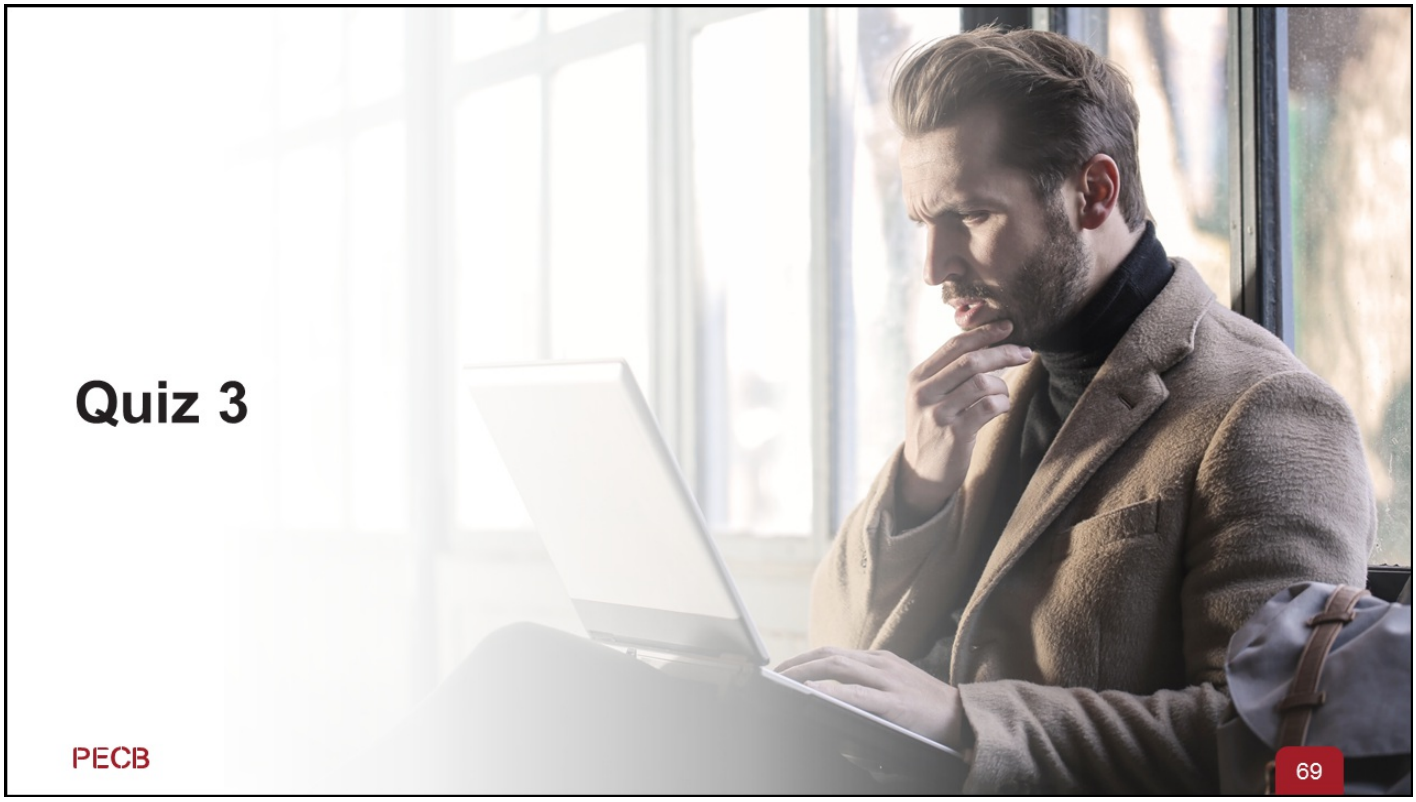
Revue de direction

- La revue de direction doit être effectuée à des intervalles planifiés.
- Elle peut être incluse dans une réunion générale de la direction et figurer à l'ordre du jour.
- Il est de bonne pratique d'envoyer toute la documentation pertinente au comité de gestion (rapport d'audit, résultats des revues, plans d'action) avant la réunion.

PECB

68

Il n'y a pas d'exigence spécifique pour la fréquence des réunions de revue de la direction. La pratique commune est d'une réunion tous les six mois. Avec une périodicité annuelle, l'organisme peut ne pas pouvoir prévenir ou résoudre les problèmes de façon ponctuelle.



Quiz 3 : Évaluation de la performance

1. **À quoi se réfère la surveillance ?**
   A. Processus d'examen de la nature d'une chose ou de détermination de ses caractéristiques essentielles et de leurs relations
   B. Processus de détermination de l'état d'un système, d'un processus ou d'une activité
   C. Processus de détermination de la valeur des actifs d'un organisme
2. **Qu'est-ce que l'évaluation des performances ?**
   A. Processus de détermination de résultats mesurables
   B. Processus qui consiste à examiner la nature d'une chose
   C. Processus de détermination de l'état d'un système, d'un processus ou d'une activité
3. **Que comprend le processus de surveillance et de mesure ?**
   A. Mesure dans laquelle un organisme atteint ses objectifs en matière de sécurité de l'information
   B. Processus, procédures et fonctions critiques
   C. Toutes ces réponses
4. **Laquelle des affirmations suivantes est vraie en ce qui concerne les audits externes ?**
   A. Les audits externes sont également connus sous le nom d'audits de première partie
   B. Les audits externes n'ont pas de rôle consultatif au sein de l'organisme
   C. Les audits externes sont conçus pour actualiser et améliorer les fonctions de l'organisme

5.Que doivent indiquer les tableaux de bord de surveillance et de mesure ?

A. Performance réelle par rapport à l'historique des performances
B. Performance réelle par rapport à des objectifs de performance prédéterminés
C. Historique des performances comparée à des objectifs de performance prédéterminés

6.Quel type d'audit est l'audit interne ?

A. Audit de première partie
B. Audit de seconde partie
C. Audit de tierce partie

7.Qu'est-ce qu'un audit de tierce partie ?

A. L'organisme est audité par son client
B. L'organisme audite ses propres systèmes
C. L'organisme est audité par un organisme indépendant

8.Quel type d'audit a lieu lorsque l'organisme audite son fournisseur ?

A. Audit interne
B. Audit externe
C. Audit client

9.Quelle est la meilleure définition de l'adéquation en matière de revue de direction ?

A. Les résultats de la production satisfont aux critères établis
B. Les résultats obtenus répondent aux besoins de l'organisme
C. Les résultats obtenus satisfont aux actions correctives

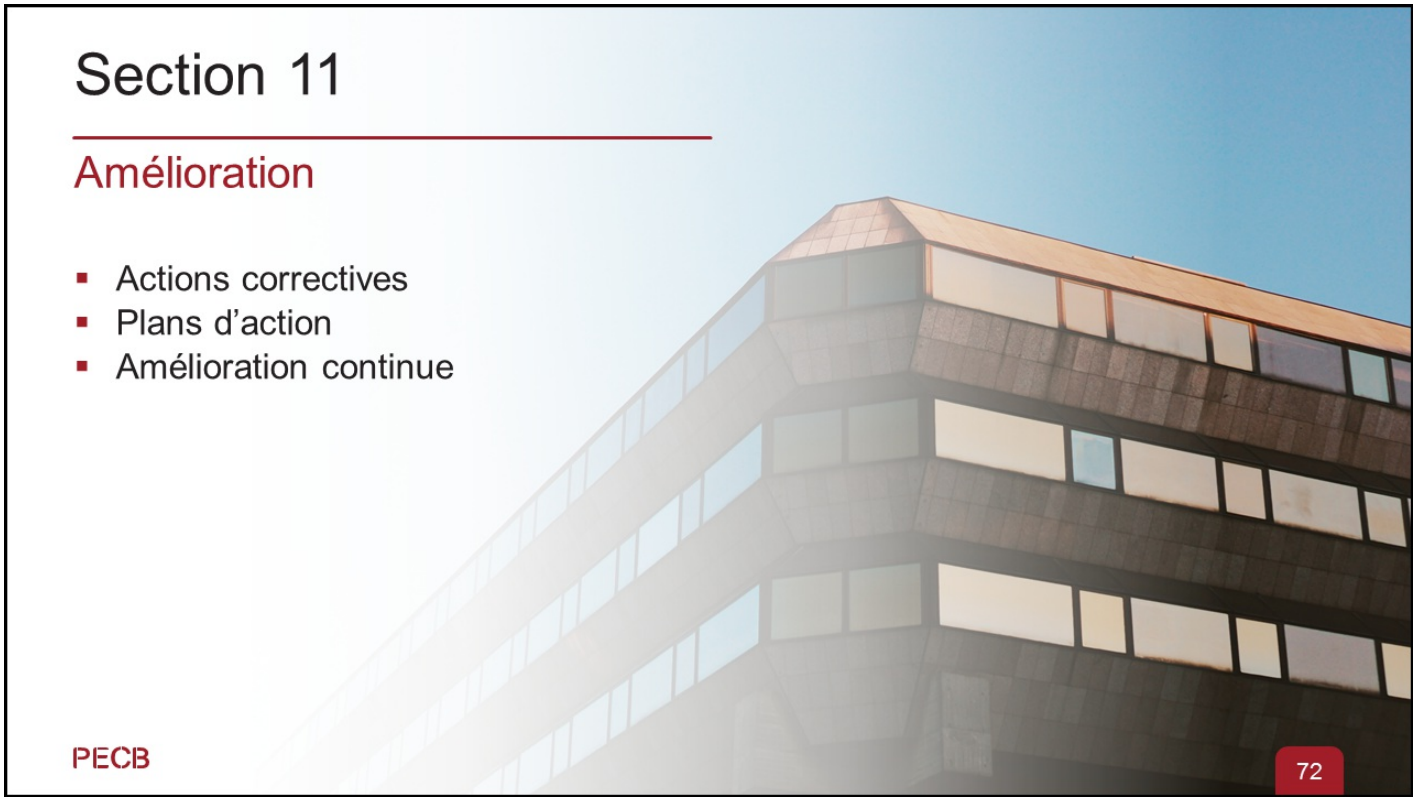
10.Parmi les éléments suivants, lequel reflète l'objectif de procéder à un examen périodique du système de management ?

A. Analyse des opportunités d'amélioration continue du système
B. Analyse des résultats de la surveillance et des mesures du système

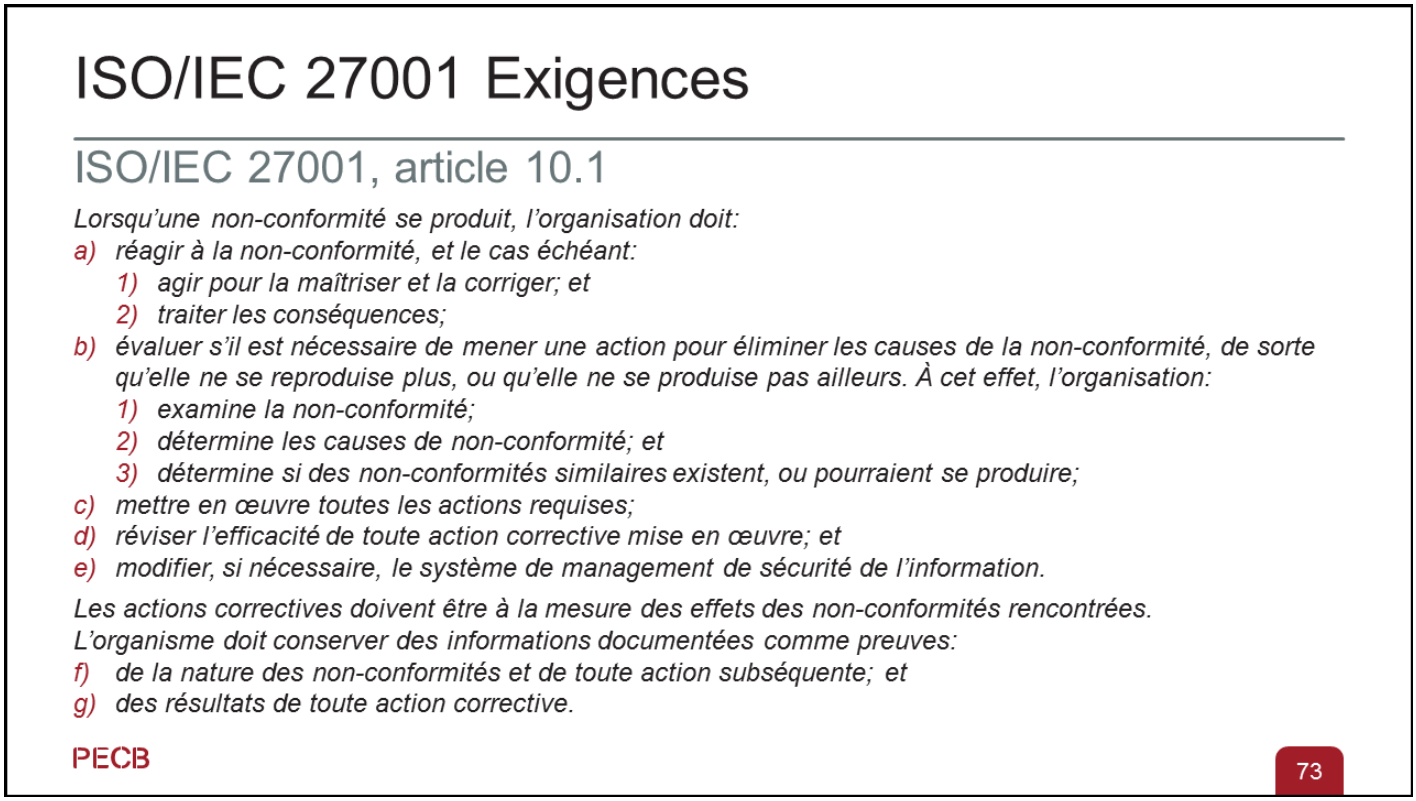
C. Analyse de la pertinence, de l'adéquation et de l'efficacité continues du système

Résumé de la section :

- La surveillance, la mesure, l'analyse et l'évaluation visent à améliorer le SMSI.
- L'organisme devrait identifier les objectifs de mesure, sélectionner les objets à mesurer, créer des indicateurs de performance et évaluer si les objectifs ont été atteints.
- L'organisme devrait déterminer comment et à quelle fréquence doit être surveillé et mesuré le SMSI.
- Les audits internes aident les organismes à évaluer si leur SMSI est efficacement mis en œuvre et tenu à jour, ainsi que leur conformité aux exigences d'ISO/IEC 27001.
- L'audit interne est un type d'audit lors duquel les organismes auditent leurs propres systèmes.
- La revue de direction doit inclure, entre autres, des informations sur les résultats d'audit, les non-conformités et les actions correctives, la revue des actions nouvelles et en cours, les résultats de la surveillance et de la mesure, l'appréciation des risques et l'état du plan de traitement des risques.
- La revue de direction doit être effectuée à des intervalles planifiés.



Cette section fournit des informations qui aideront le participant à acquérir des connaissances sur les actions correctives, les plans d'action et l'amélioration continue.



ISO/IEC27003, article 10.1, Non-conformité et actions correctives

Une non-conformité est le non-respect d'une exigence du SMSI. Les exigences sont les besoins ou les attentes énoncés, implicites ou obligatoires. Il existe donc plusieurs types de non-conformités telles que:

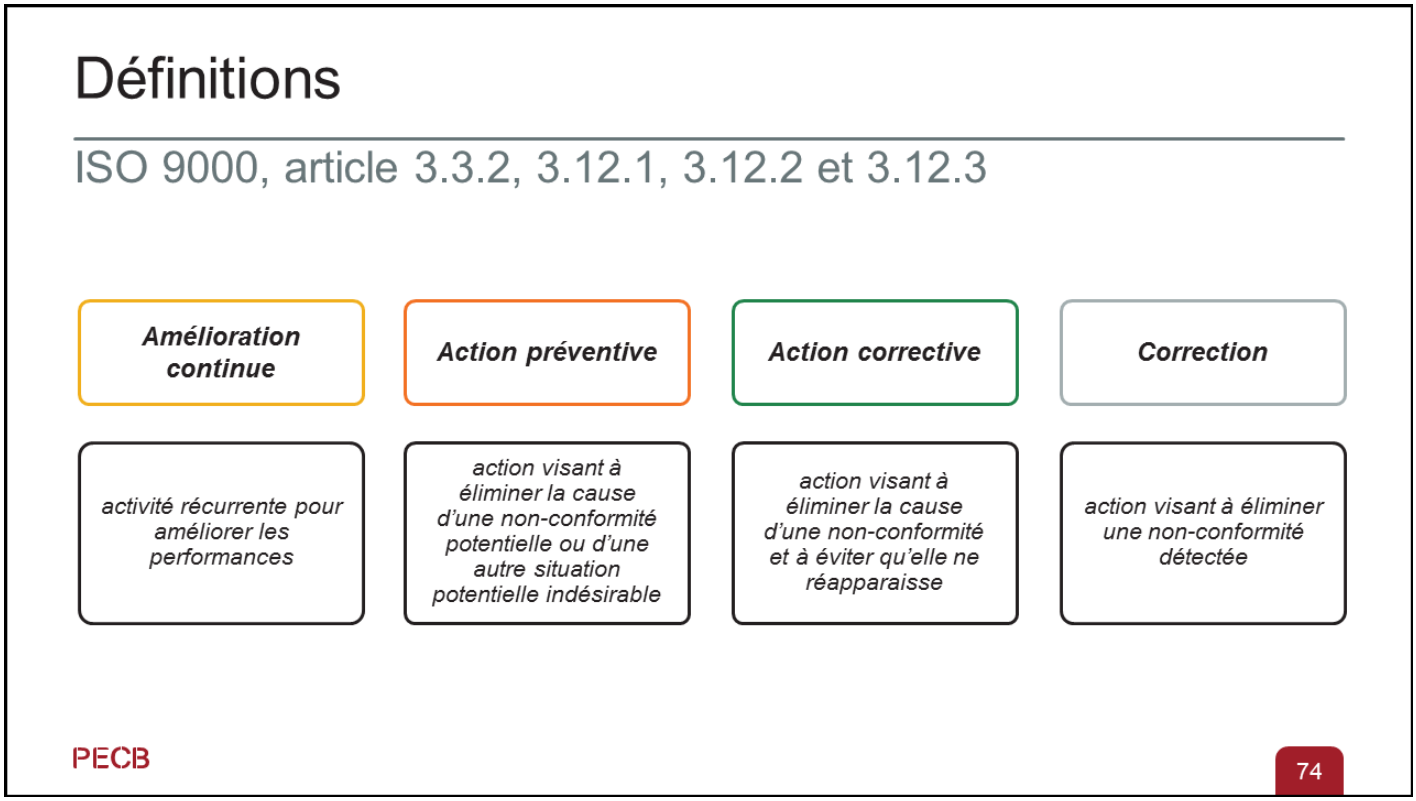
a. *l'incapacité de satisfaire à une exigence (totalement ou partiellement) d'ISO/IEC27001 dans le SMSI;*
b. *l'échec de la mise en œuvre ou de la conformité à une exigence, à une règle ou à une mesure énoncées par le SMSI; et*
c. *l'incapacité partielle ou totale de se conformer aux exigences légales, contractuelles ou convenues avec des clients.*

Les faits suivants peuvent constituer des non-conformités:

d.*les personnes qui ne se comportent pas comme prévu par les procédures et les politiques;*
e.*les fournisseurs qui ne fournissent pas les produits ou les services convenus;*
f. l*es projets qui ne dispensent pas les résultats escomptés; et*
g.*les mesures qui ne fonctionnent pas comme prévu.*

Les non-conformités peuvent être identifiées par:

h.*les déficiences des activités réalisées dans le périmètre du système de management;*
i.*les mesures inefficaces qui ne sont pas corrigées de manière appropriée;*
j.*l'analyse des incidents de sécurité de l'information, montrant le non-respect d'une exigence du SMSI;*
k.*les réclamations des clients;*
l.*les alertes d'utilisateurs ou de fournisseurs;*
m.*les résultats de surveillance et de mesure ne répondant pas aux critères d'acceptation; et*
n.*les objectifs non atteints.*



Note de terminologie:

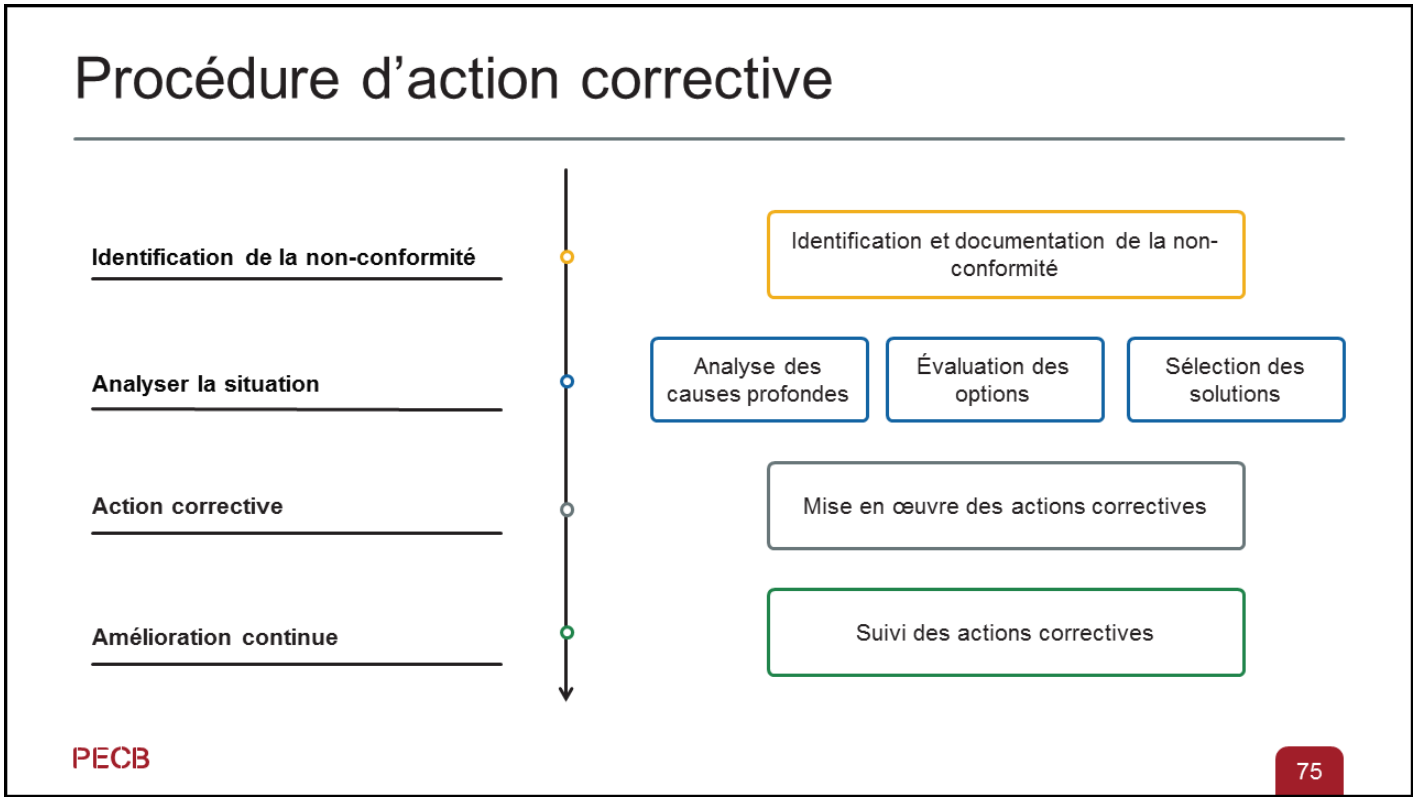
1. Le processus de définition des objectifs et de recherche d'opportunités d'amélioration est un processus continu utilisant les constatations et les conclusions d'audit, l'analyse des données, les revues de direction et d'autres moyens. Ce processus mène généralement à des actions correctives ou préventives.
2. Une action préventive est entreprise pour empêcher l'occurrence, alors qu'une action corrective est entreprise afin d'éviter sa réapparition.

ISO9000, article3.7.10 Efficience

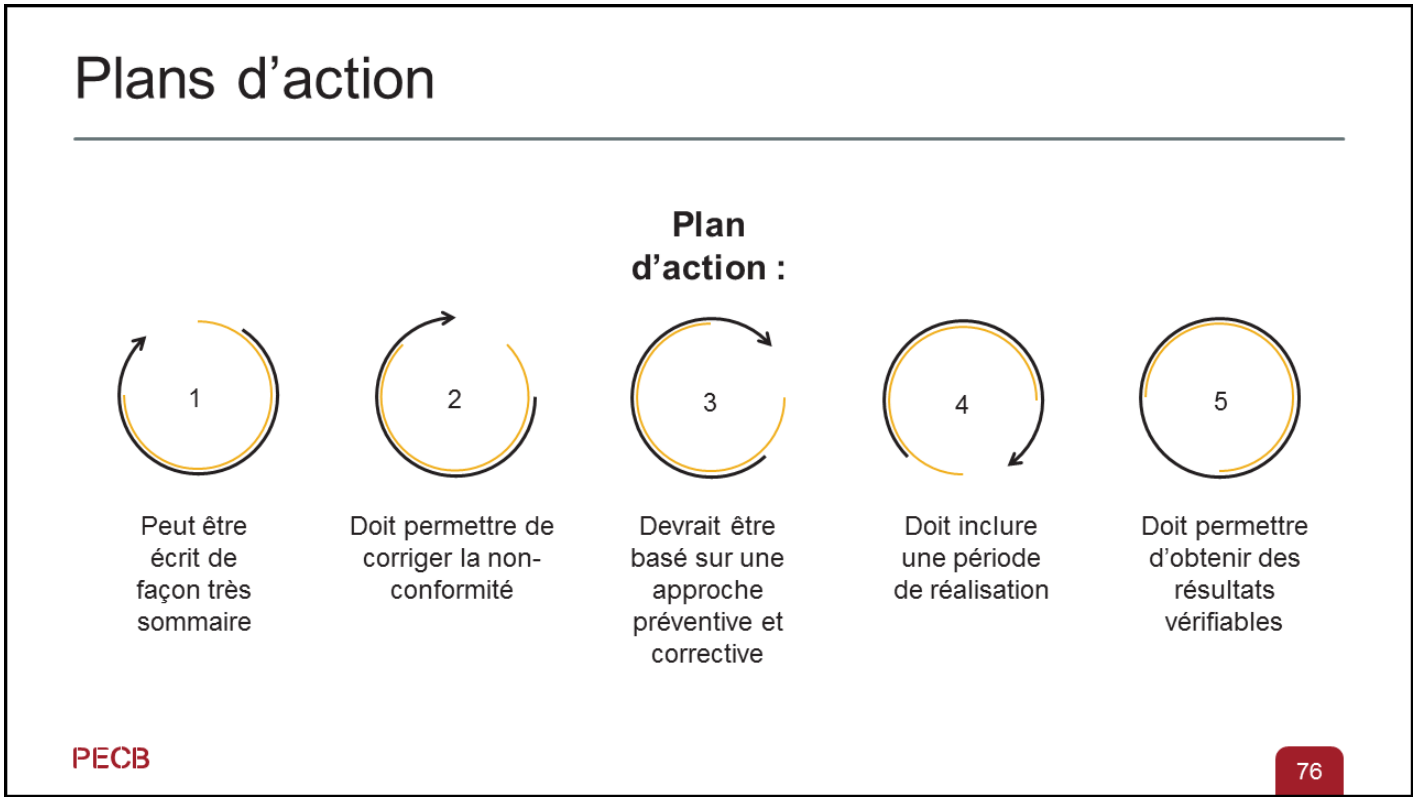
rapport entre le résultat obtenu et les ressources utilisées

ISO9000, article3.7.11 Efficacité

niveau de réalisation des activités planifiées et d'obtention des résultats escomptés



Une action corrective est une action entreprise pour éliminer les causes fondamentales d'un problème et pour empêcher sa récurrence.



Un plan d'action doit être soumis pour chaque non-conformité dans des délais précis.

Exemples de plans d'action :

- Un accord de confidentialité doit être signé avec les personnes impliquées dans le traitement des informations sensibles (délai : dans les deux mois).
- Une nouvelle version de la politique de sauvegarde doit être publiée afin d'inclure les exigences relatives à la récupération des informations (délai : immédiatement).

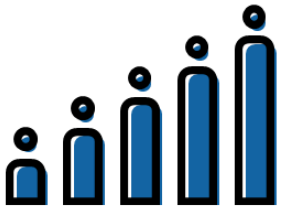
ISO/IEC 27001 Exigences

ISO/IEC 27001, article 10.2

L'organisation doit continuellement améliorer la pertinence, l'adéquation et l'efficacité du système de management de la sécurité de l'information.

Amélioration continue

L'amélioration continue est un processus visant à augmenter l'efficacité et l'efficience de l'organisme à répondre à sa politique et à ses objectifs.



Les grandes transformations se font à petits pas.

PECB

78

L'amélioration continue est obtenue en fixant des objectifs de performance organisationnelle, en mesurant et révisant, et en apportant les modifications nécessaires aux processus, systèmes, ressources, etc.

Les avantages de l'amélioration continue

Efficacité accrue

L'amélioration continue permet d'accroître la productivité, puisque

les changements peuvent conduire à des résultats positifs à long terme.

Collaboration au sein de l'équipe

Travailler continuellement ensemble pour atteindre un objectif commun aidera à construire et à renforcer les relations existantes au sein de l'équipe.

Satisfaction accrue de la clientèle

Tout en recherchant activement des moyens d'améliorer leurs processus, les organismes augmentent aussi la valeur et la qualité des produits et services qu'ils offrent.

Réduction des erreurs

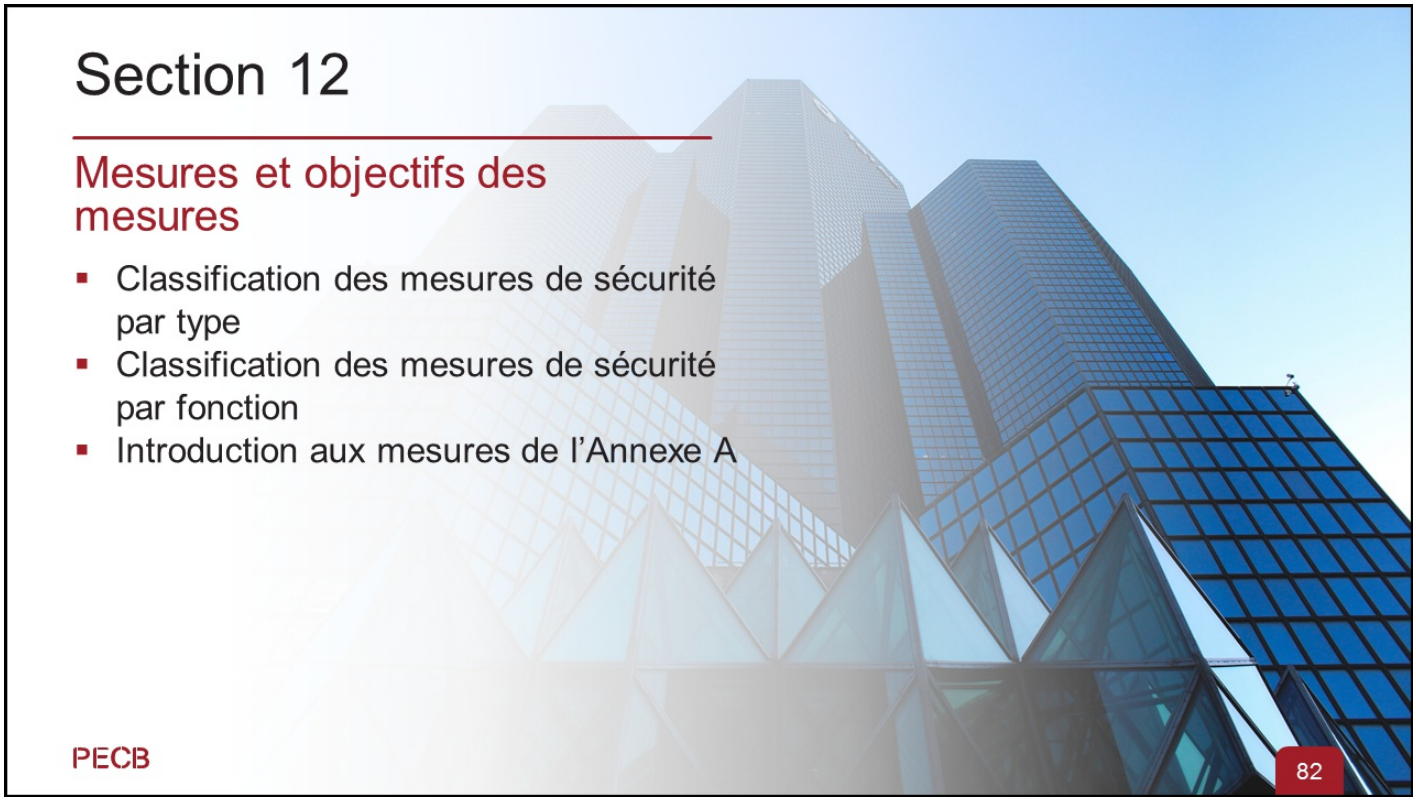
Si les processus s'améliorent continuellement, le nombre d'erreurs dans ces processus va également diminuer.

Questions de discussion

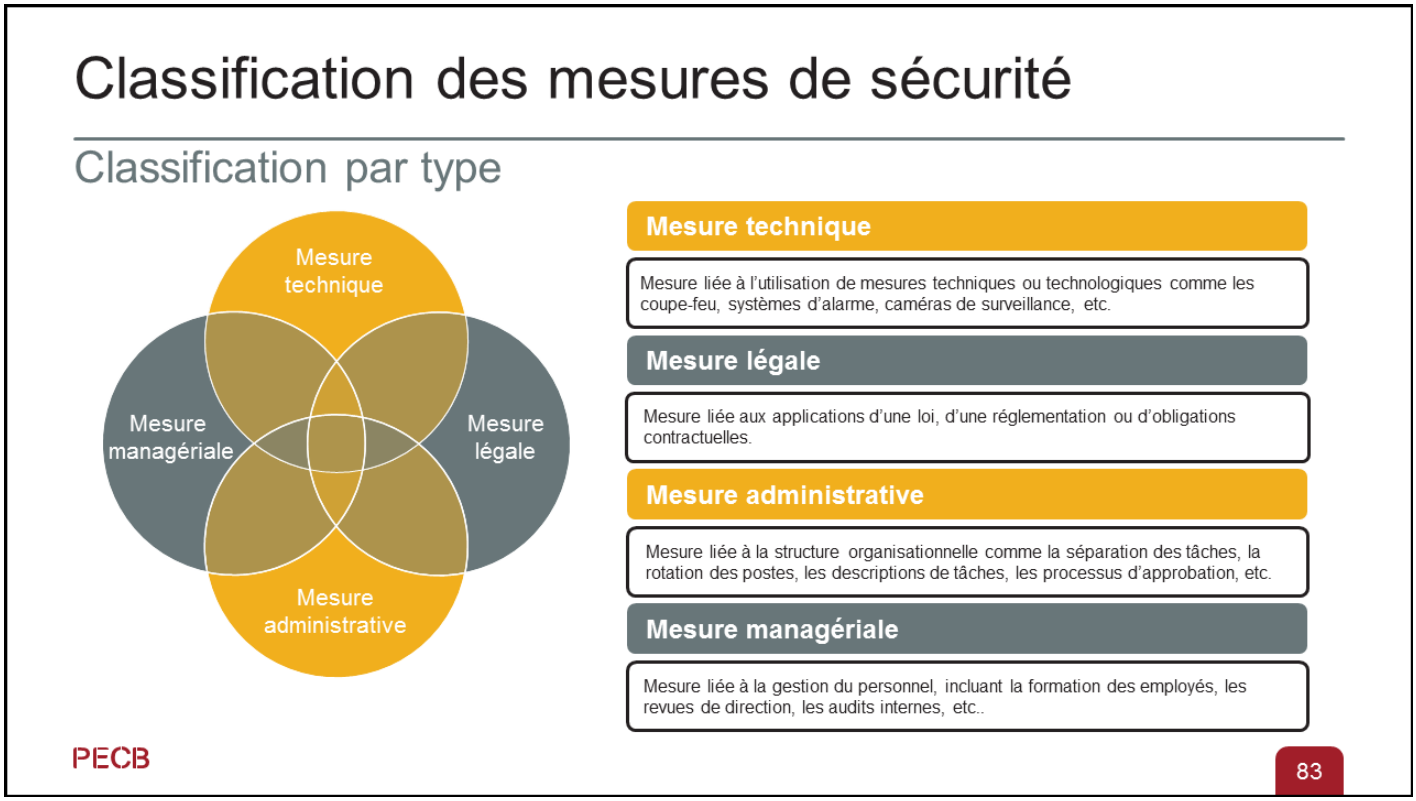
1. Que devrait comprendre le processus d'action corrective ?
2. Qu'est-ce que l'amélioration continue ?
3. Quels sont les avantages d'une amélioration continue ?

Résumé de la section

- Les organismes doivent définir un processus pour réagir efficacement aux non-conformités et les examiner, les évaluer et les traiter en conséquence.
- Le traitement des non-conformités nécessite la définition d'un processus pour les résoudre, la détermination des actions correctives et préventives, et l'élaboration d'un plan d'action.
- Un plan d'action doit être soumis pour chaque non-conformité dans des délais précis.



Cette section fournit de précieuses informations sur la classification des mesures de sécurité par type et par fonction, ainsi que sur les contrôles de l'annexe A.



ISO/IEC 27000, article 3.14 Mesure

mesure qui modifie un risque

ISO/IEC 27000, article3.15 Objectif d'une mesure de sécurité

déclaration décrivant ce qui est attendu de la mise en œuvre des mesures de sécurité

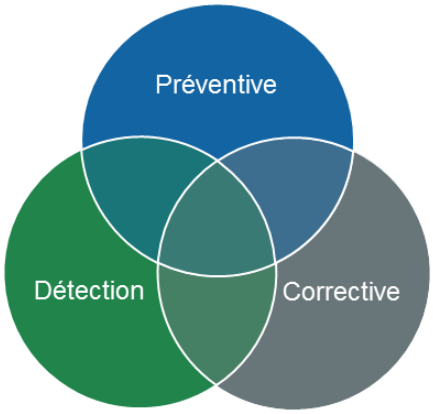
Les mesures de sécurité de l'information comprennent tout processus, politique, procédure, ligne directrice, pratique , ou structure organisationnelle qui peuvent être de nature administrative, technique managériale ou légale, et qui modifient les risques liés à la sécurité de l'information.

Note:

- Une mesure administrative est plus liée à la structure de l'organisme comme un tout, sans être appliquée par une personne en particulier, tandis que la mesure managériale doit être appliquée par les directeurs.
- Les différences entre les types de mesures de sécurité ne sont expliquées que pour une meilleure compréhension. Un organisme n'a pas besoin de qualifier la nature des différentes mesures mises en œuvre.

Classification des mesures de sécurité

Classification par fonction



Mesure préventive

Mesures pour éviter ou prévenir les incidents

Mesure de détection

Mesures pour rechercher, détecter et identifier les incidents

Mesure corrective

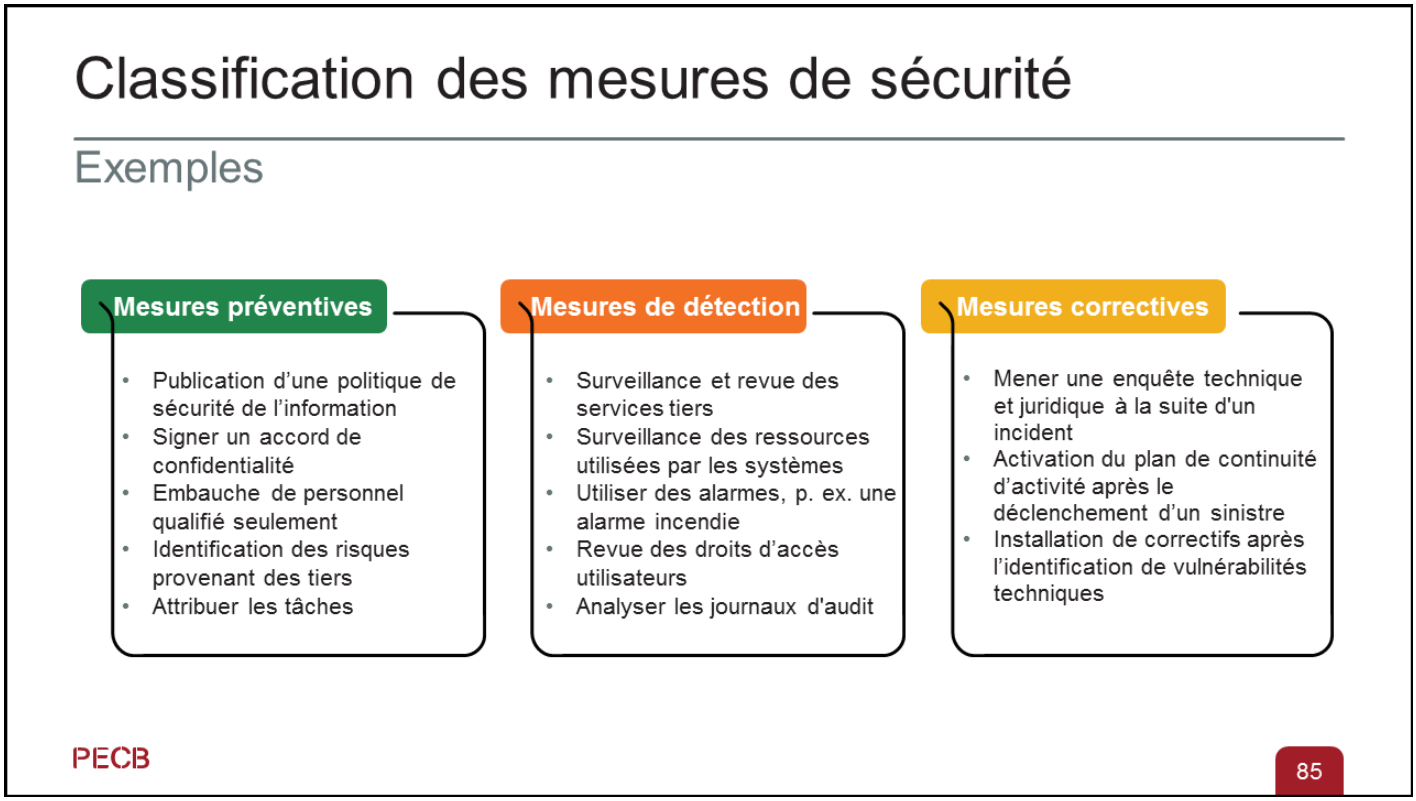
Mesures pour résoudre les incidents et prévenir leur récurrence

PECB

84

Les mesures de sécurité peuvent être classées en trois catégories: préventives, de détection et correctives. Plusieurs structures de référence en sécurité de l'information définissent une classification avec plus de catégories.

Note importante: Ces différents types de mesures sont intereliés. Par exemple, l'établissement d'un antivirus est une mesure préventive parce qu'il protège l'information contre les programmes malveillants. En même temps, l'antivirus sert de mesure de détection lorsqu'il détecte un virus potentiel et fournit une mesure corrective lorsqu'un fichier suspect est mis en quarantaine ou supprimé.



1.Mesure préventive
But: Éviter ou prévenir la survenance d'incidents

- Détecter les incidents avant qu'ils ne se produisent
- Contrôler les opérations
- Prévenir une erreur, une omission ou des actes malveillants

Exemples :

- Séparer les environnements de développement, de test et d'exploitation
- Sécuriser les bureaux, les salles et l'équipement
- Utiliser des procédures clairement définies (pour éviter les erreurs)
- Utiliser la cryptographie
- Utiliser un logiciel de contrôle d'accès qui permet uniquement au personnel autorisé d'accéder aux fichiers sensibles

Page de notes

PECB

86

2.Mesure de détection
But: Rechercher, détecter et identifier les incidents

- Utiliser les mesures qui détectent et rapportent la possibilité d'une erreur, d'une omission ou d'un acte malveillant.

Exemples :

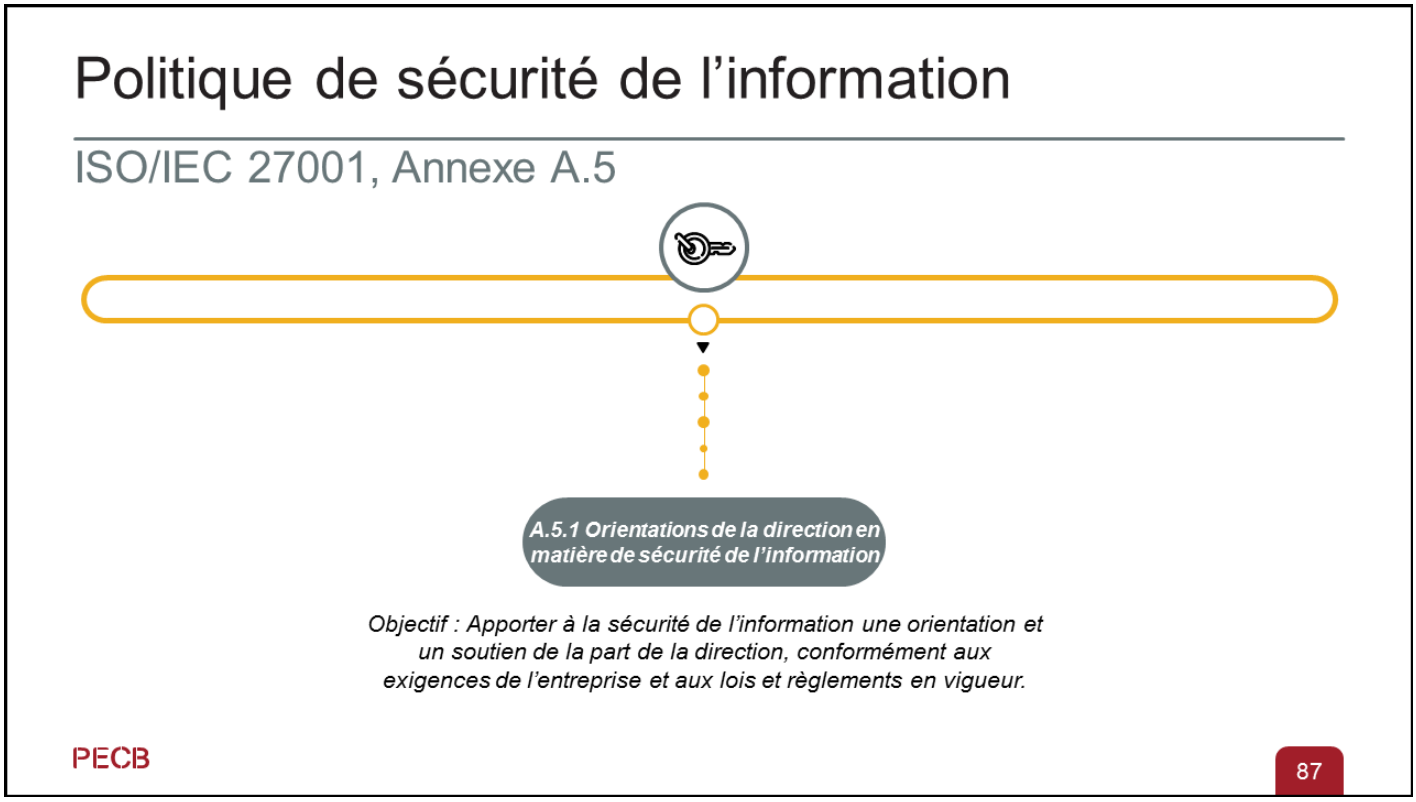
- Intégrer des points de contrôle dans les applications en cours d'élaboration
- Contrôler l'écho dans les télécommunications
- Créer des alarmes pour détecter les risques liés à la chaleur, à la fumée, au feu ou à l'eau
- Vérifier les doublons de calculs dans le traitement des données
- Détecter les pannes au moyen de caméras vidéo
- Détecter les intrusions potentielles sur les réseaux avec un système de détection d'intrusion (IDS)
- Revoir les droits d'accès utilisateurs
- Faire une revue technique des applications après une modification du système d'exploitation

3.Mesure corrective
But: Résoudre les incidents identifiés et prévenir leur récurrence

- Minimiser l'impact d'une menace
- Résoudre les incidents découverts par les mesures de détection
- Identifier les causes d'un incident
- Modifier le système de traitement pour réduire au minimum la présence d'incidents futurs

Exemples :

- Revoir la politique de sécurité après l'intégration d'une nouvelle division à l'organisme
- En appeler aux autorités pour signaler un crime informatique
- Changer tous les mots de passe de tous les systèmes lorsqu'une intrusion sur le réseau a été détectée
- Récupérer les transactions grâce à la procédure de sauvegarde après la découverte que des données ont été corrompues
- Déconnecter automatiquement les sessions inactives
- Installer des correctifs après l'identification de vulnérabilités techniques



ISO/IEC 27001, Annexe A.5.1.1 Politiques de sécurité de l'information

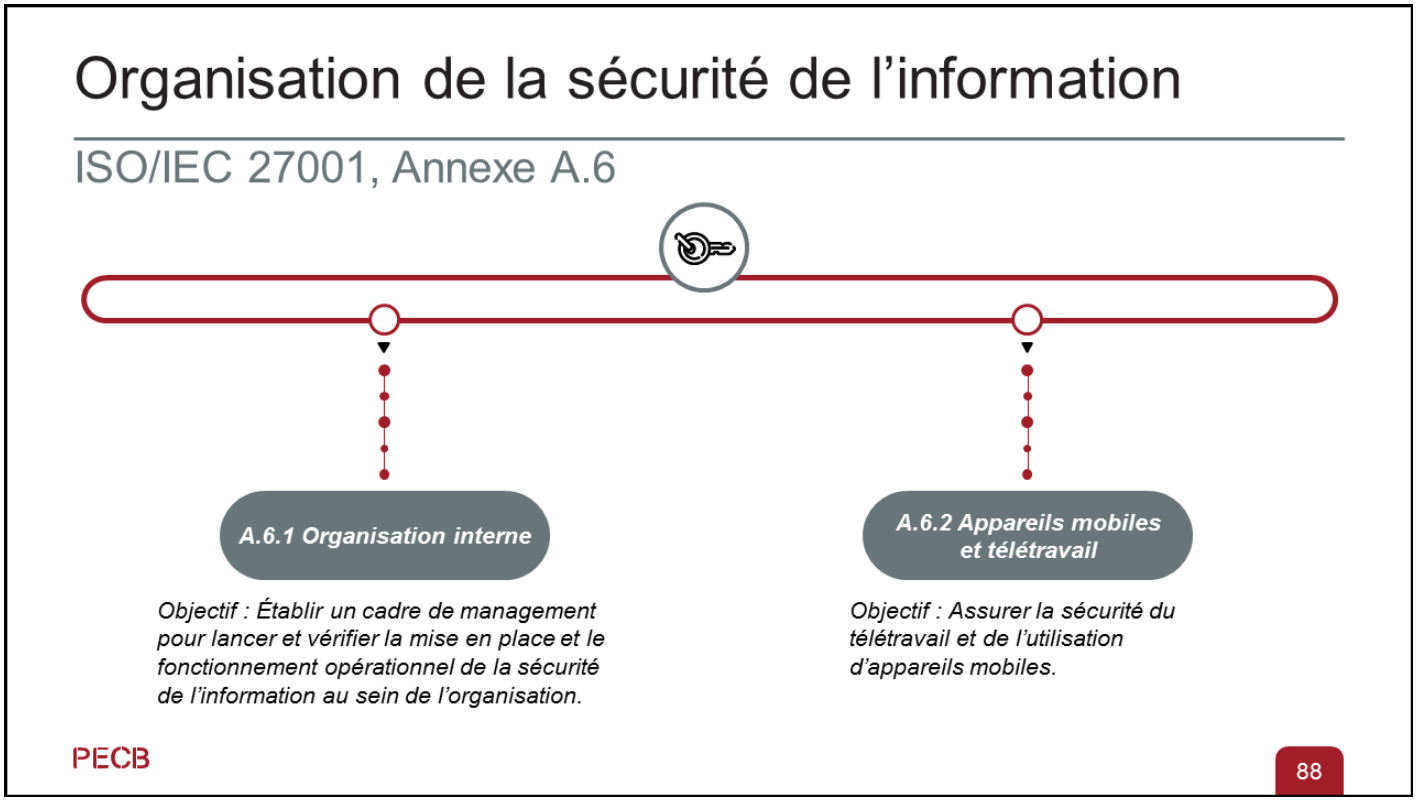
Mesure

Un ensemble de politiques de sécurité de l'information doit être défini, approuvé par la direction, diffusé et communiqué aux salariés et aux tiers concernés.

ISO/IEC 27001, Annexe A.5.1.2 Revue de la politiques de sécurité de l'information

Mesure

Les politiques de sécurité de l'information doivent être revues à intervalles programmés ou en cas de changements majeurs pour garantir leur pertinence, leur adéquation et leur effectivité dans le temps.



ISO/IEC 27001, AnnexeA.6.1.1 Fonctions et responsabilités liées à la sécurité de l'information

Mesure

Toutes les responsabilités en matière de sécurité de l'information doivent être définies et attribuées.

ISO/IEC 27001, Annexe A.6.1.2 Séparation des tâches

Mesure

Les tâches et les domaines de responsabilité incompatibles doivent être cloisonnés pour limiter les possibilités de modification ou de mauvais usage, non autorisé(e) ou involontaire, des actifs de l'organisation.

ISO/IEC 27001, AnnexeA.6.1.3 Relations avec les autorités

Mesure

Des relations appropriées avec les autorités compétentes doivent être entretenues.

ISO/IEC 27001, AnnexeA.6.1.4 Relations avec les groupes de travail spécialisés

Mesure

Des relations appropriées avec des groupes d'intérêt, des forums spécialisés dans la sécurité et des associations professionnelles doivent être entretenues.

ISO/IEC27001, AnnexeA.6.1.5 La sécurité de l'information dans la gestion de projet

Mesure

La sécurité de l'information doit être considérée dans la gestion de projet, quel que soit le type de projet concerné.

ISO/IEC 27001, AnnexeA.6.2.1 Politique en matière d'appareils mobiles

Mesure

Une politique et des mesures de sécurité complémentaires doivent être adoptées pour gérer les risques découlant de l'utilisation des appareils mobiles.

Page de notes

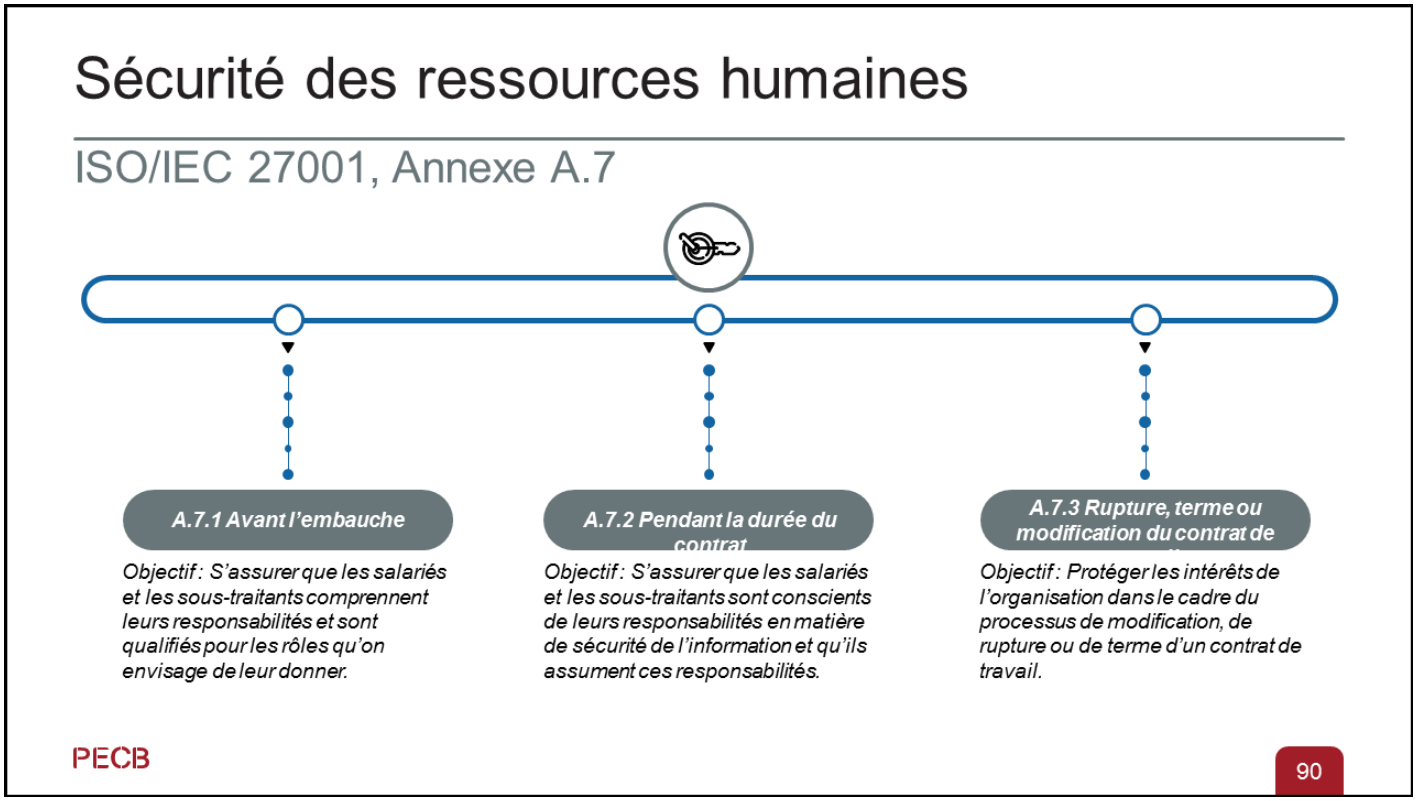
PECB

89

ISO/IEC 27001, Annexe A.6.2.2 Télétravail

Mesure

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.



ISO/IEC 27001, Annexe A.7.1.1 Sélection des candidats

Mesure

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.

ISO/IEC 27001, Annexe A.7.1.2 Termes et conditions d'embauche

Mesure

Les accords contractuels entre les salariés et les sous-traitants doivent préciser leurs responsabilités et celles de l'organisation en matière de sécurité de l'information.

ISO/IEC 27001, Annexe A.7.2.1 Responsabilités de la direction des candidats

Mesure

La direction doit demander à tous les salariés et sous-traitants d'appliquer les règles de sécurité de l'information conformément aux politiques et aux procédures en vigueur dans l'organisation.

ISO/IEC 27001, Annexe A.7.2.2 Sensibilisation, apprentissage et formation à la sécurité de l'information

Mesure

L'ensemble des salariés de l'organisation et, quand cela est pertinent, des sous-traitants, doit bénéficier d'une sensibilisation et de formations adaptées et recevoir régulièrement les mises à jour des politiques et procédures de l'organisation s'appliquant à leurs fonctions.

ISO/IEC 27001, AnnexeA.7.2.3 Processus disciplinaire

Mesure

Un processus disciplinaire formel et connu de tous doit exister pour prendre des mesures à l'encontre des salariés ayant enfreint les règles liées à la sécurité de l'information.

Page de notes

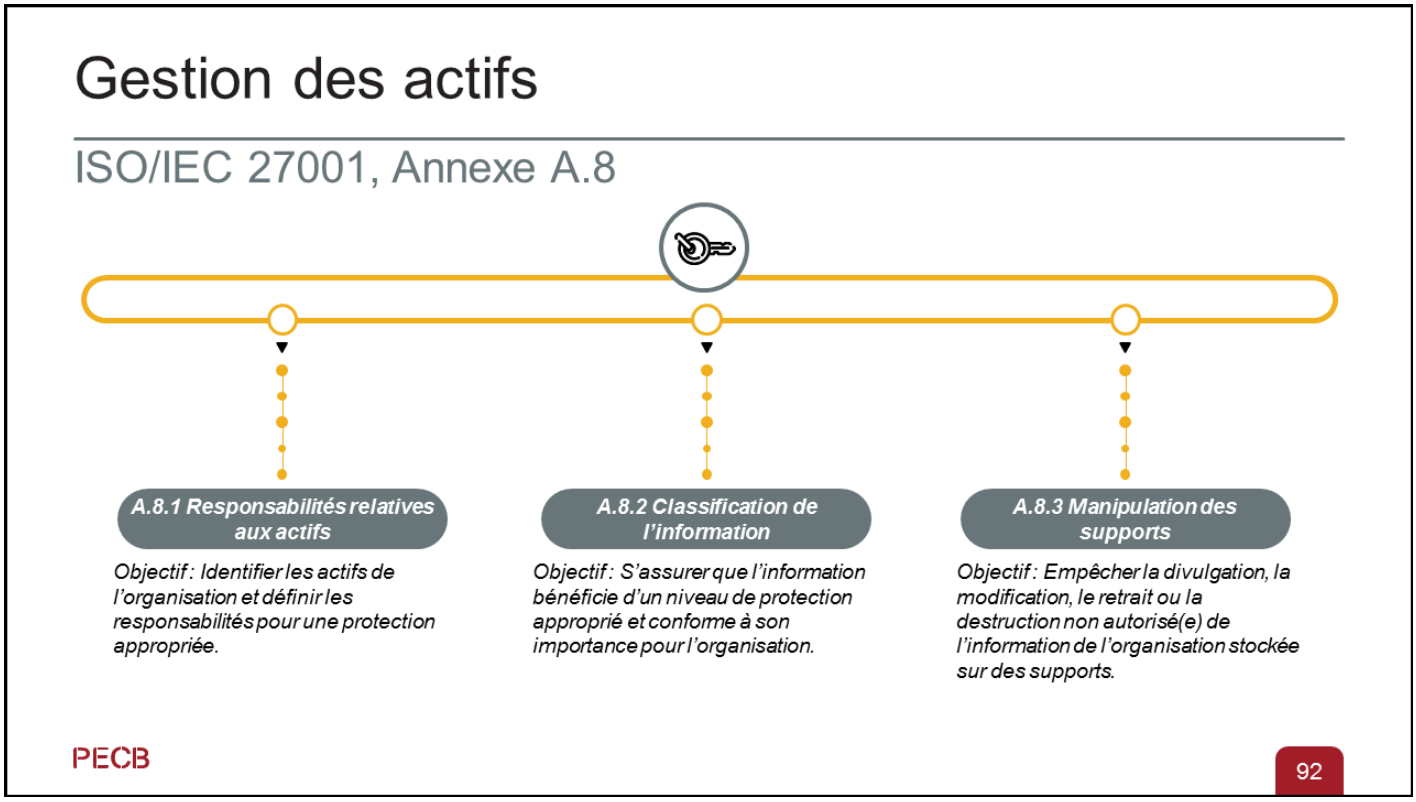
PECB

91

ISO/IEC 27001, Annexe A.7.3.1 Achèvement ou modification des responsabilités associées au contrat de travail

Mesure

Les responsabilités et les missions liées à la sécurité de l'information qui restent valables à l'issue de la rupture, du terme ou de la modification du contrat de travail, doivent être définies, communiquées au salarié ou au sous-traitant, et appliquées.



ISO/IEC 27001, AnnexeA.8.1.1 Inventaire des actifs

Mesure

Les actifs associés à l'information et aux moyens de traitement de l'information doivent être identifiés et un inventaire de ces actifs doit être dressé et tenu à jour.

ISO/IEC 27001, AnnexeA.8.1.2 Propriété des actifs

Mesure

Les actifs figurant à l'inventaire doivent être attribués à un propriétaire.

ISO/IEC 27001, AnnexeA.8.1.3 Utilisation correcte des actifs

Mesure

Les règles d'utilisation correcte de l'information, les actifs associés à l'information et les moyens de traitement de l'information doivent être identifiés, documentés et mis en œuvre.

ISO/IEC 27001, AnnexeA.8.1.4 Restitution des actifs

Mesure

Tous les salariés et les utilisateurs tiers doivent restituer la totalité des actifs de l'organisation qu'ils ont en leur possession au terme de la période d'emploi, du contrat ou de l'accord.

Page de notes

PECB

93

ISO/IEC 27001, AnnexeA.8.2.1 Classification des informations

Mesure

Les informations doivent être classifiées en termes d'exigences légales, de valeur, de caractère critique et de sensibilité au regard d'une divulgation ou modification non autorisée.

ISO/IEC 27001, AnnexeA.8.2.2 Marquage des informations

Mesure

Un ensemble approprié de procédures pour le marquage de l'information doit être élaboré et mis en œuvre conformément au plan de classification adopté par l'organisation.

ISO/IEC 27001, AnnexeA.8.2.3 Manipulation des actifs

Mesure

Des procédures de traitement de l'information doivent être élaborées et mises en oeuvre conformément au plan de classification de l'information adopté par l'organisation.

ISO/IEC 27001, Annexe A.8.3.1 Gestion des supports amovibles

Mesure

Des procédures de gestion des supports amovibles doivent être mises en œuvre conformément au plan de classification adopté par l'organisation.

ISO/IEC 27001, Annexe A.8.3.2 Mise au rebut des supports

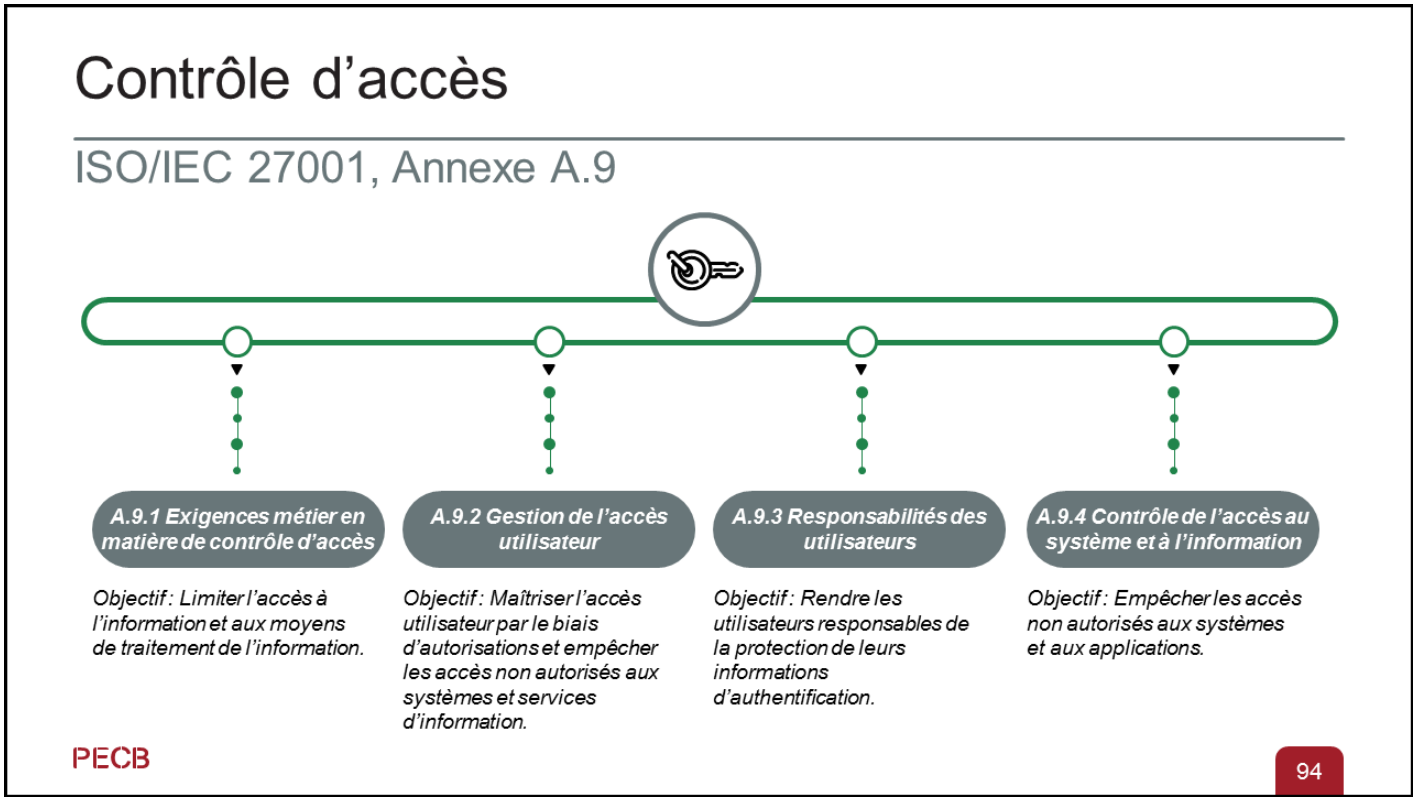
Mesure

Les supports qui ne sont plus nécessaires doivent être mis au rebut de manière sécurisée en suivant des procédures formelles.

ISO/IEC 27001, Annexe A.8.3.3 Transfert physique des supports

Mesure

Les supports contenant de l'information doivent être protégés contre les accès non autorisés, les erreurs d'utilisation et l'altération lors du transport.



ISO/IEC 27001, Annexe A.9.1.1 Politique de contrôle d'accès

Mesure

Une politique de contrôle d'accès doit être établie, documentée et revue sur la base des exigences métier et de sécurité de l'information.

ISO/IEC 27001, Annexe A.9.1.2 Accès aux réseaux et aux services réseau

Mesure

Les utilisateurs doivent avoir uniquement accès au réseau et aux services réseau pour lesquels ils ont spécifiquement reçu une autorisation.

ISO/IEC 27001, Annexe A.9.2.1 Enregistrement et désinscription des utilisateurs

Mesure

Un processus formel d'enregistrement et de désinscription des utilisateurs doit être mis en œuvre pour permettre l'attribution des droits d'accès.

ISO/IEC 27001, Annexe A.9.2.2 Distribution des accès aux utilisateurs candidats

Mesure

Un processus formel de distribution des accès aux utilisateurs doit être mis en œuvre pour attribuer et retirer des droits d'accès à tous types d'utilisateurs sur l'ensemble des services et des systèmes.

ISO/IEC 27001, Annexe A.9.2.3 Gestion des droits d'accès à privilèges

Mesure

L'allocation et l'utilisation des droits d'accès à privilèges doivent être restreintes et contrôlées.

ISO/IEC 27001, Annexe A.9.2.4 Gestion des informations secrètes d'authentification des utilisateurs

Mesure

L’attribution des informations secrètes d’authentification doit être réalisée dans le cadre d’un processus de gestion formel.

Page de notes

PECB

95

ISO/IEC 27001, Annexe A.9.2.5 Revue des droits d'accès utilisateurs

Mesure

Les propriétaires des actifs doivent vérifier les droits d'accès des utilisateurs à intervalles réguliers.

ISO/IEC 27001, Annexe A.9.2.6 Suppression ou adaptation des droits d'accès

Mesure

Les droits d'accès aux informations et aux moyens de traitement des informations de l'ensemble des salariés et utilisateurs tiers doivent être supprimés à la fin de leur période d'emploi, ou adaptés en cas de modification du contrat ou de l'accord.

ISO/IEC 27001, Annexe A.9.3.1 Utilisation d'informations secrètes d'authentification

Mesure

Les utilisateurs doivent suivre les pratiques de l'organisation pour l'utilisation des informations secrètes d'authentification.

ISO/IEC 27001, Annexe A.9.4.1 Restriction d'accès à l'information

Mesure

L'accès à l'information et aux fonctions d'application système doit être restreint

conformément à la politique de contrôle d'accès.

ISO/IEC 27001, Annexe A.9.4.2 Sécuriser les procédures de connexion

Mesure

Lorsque la politique de contrôle d'accès l'exige, l'accès aux systèmes et aux applications doit être contrôlé par une procédure de connexion sécurisée.

ISO/IEC 27001, Annexe A.9.4.3 Système de gestion des mots de passe

Mesure

Les systèmes qui gèrent les mots de passe doivent être interactifs et doivent garantir la qualité des mots de passe.

ISO/IEC 27001, Annexe A.9.4.4 Utilisation de programmes utilitaires à privilèges

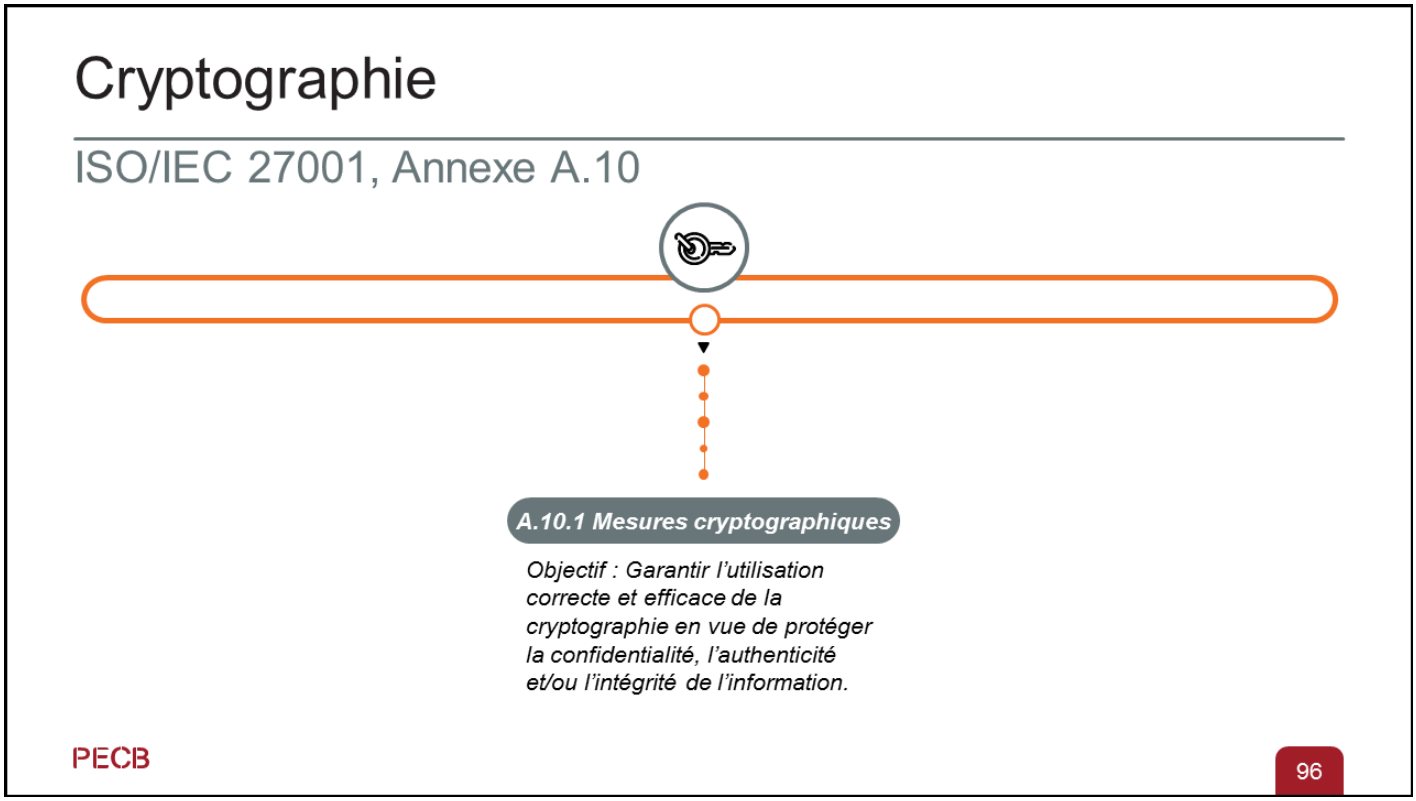
Mesure

L'utilisation des programmes utilitaires permettant de contourner les mesures de sécurité d'un système ou d'une application doit être limitée et étroitement contrôlée.

ISO/IEC 27001, Annexe A.9.4.5 Contrôle d'accès au code source des programmes

Mesure

L'accès au code source des programmes doit être restreint.



ISO/IEC 27001, AnnexeA.10.1.1 Politique d'utilisation des mesures cryptographiques

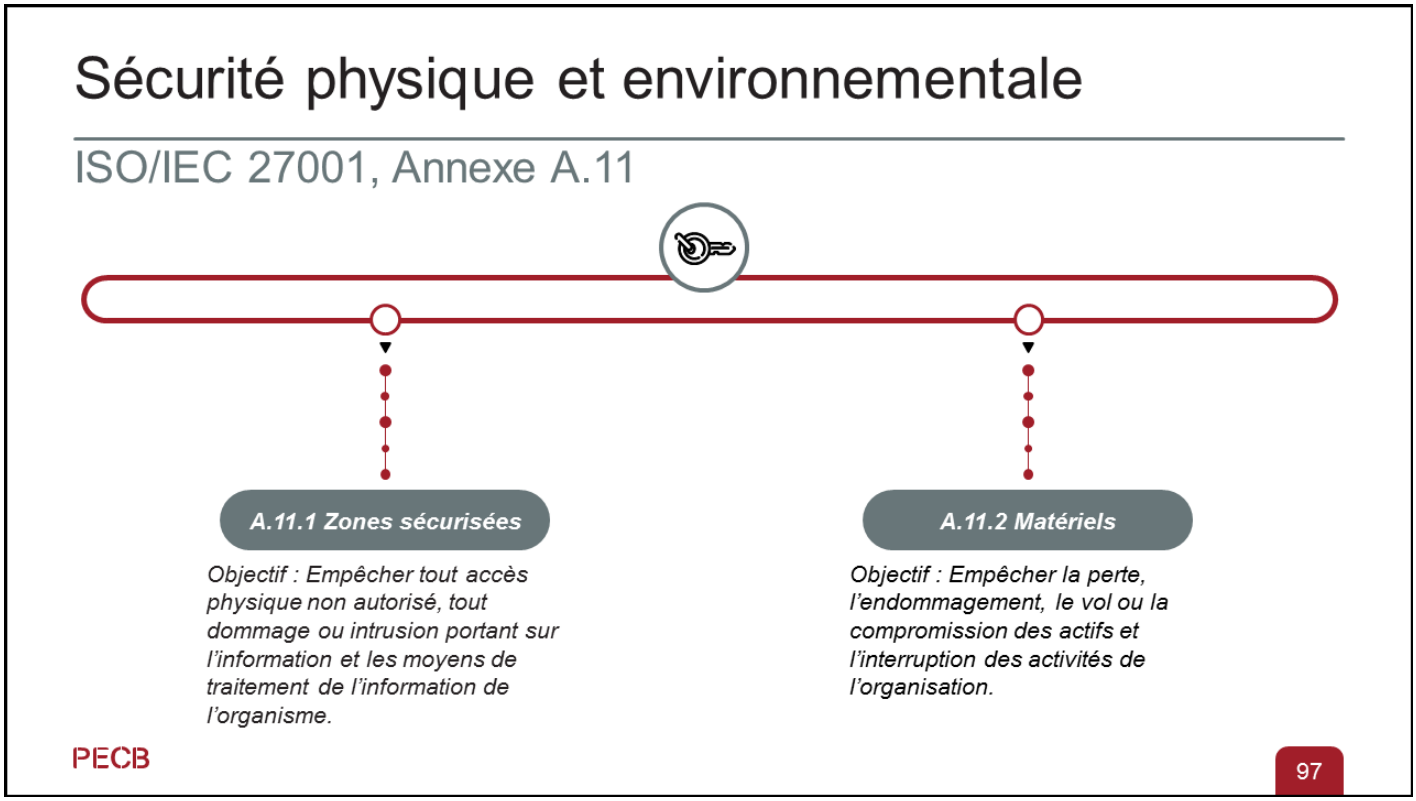
Mesure

Une politique d'utilisation des mesures cryptographiques en vue de protéger l'information doit être élaborée et mise en œuvre.

ISO/IEC 27001, Annexe A.10.1.2 Gestion des clés

Mesure

Une politique sur l'utilisation, la protection et la durée de vie des clés cryptographiques doit être élaborée et mise en œuvre tout au long de leur cycle de vie.



ISO/IEC 27001, Annexe A.11.1.1 Périmètre de sécurité physique

Mesure

Des périmètres de sécurité doivent être définis et utilisés pour protéger les zones contenant l'information sensible ou critique et les moyens de traitement de l'information.

ISO/IEC 27001, Annexe A.11.1.2 Contrôle d'accès physique

Mesure

Les zones sécurisées doivent être protégées par des contrôles adéquats à l'entrée pour s'assurer que seul le personnel autorisé est admis.

ISO/IEC 27001, Annexe A.11.1.3 Sécurisation des bureaux, des salles et des équipements

Mesure

Des mesures de sécurité physique aux bureaux, aux salles et aux équipements doivent être conçues et appliquées.

ISO/IEC 27001, Annexe A.11.1.4 Protection contre les menaces extérieures et environnementales

Mesure

Des mesures de protection physique contre les désastres naturels, les attaques malveillantes ou les accidents doivent être conçues et appliquées.

ISO/IEC 27001, Annexe A.11.1.5 Travail dans les zones sécurisées

Mesure

Des procédures pour le travail dans les zones sécurisées doivent être conçues et appliquées.

ISO/IEC 27001, Annexe A.11.1.6 Zones de livraison et de chargement

Mesure

Les points d'accès tels que les zones de livraison et de chargement et les autres points par lesquels des personnes non autorisées peuvent pénétrer dans les locaux doivent être contrôlés et, si possible, isolés des moyens de traitement de l'information, de façon à éviter l'accès non autorisé.

Page de notes

PECB

98

ISO/IEC 27001, Annexe A.11.2.1 Emplacement et protection des matériels

Mesure

Les matériels doivent être localisés et protégés de manière à réduire les risques liés à des menaces et des dangers environnementaux et les possibilités d'accès non autorisé.

ISO/IEC 27001, AnnexeA.11.2.2 Services généraux

Mesure

Les matériels doivent être protégés des coupures de courant et autres perturbations dues à une défaillance des services généraux.

ISO/IEC 27001, AnnexeA.11.2.3 Sécurité du câblage

Mesure

Les câbles électriques ou de télécommunication transportant des données ou supportant les services d'information doivent être protégés contre toute interception ou tout dommage.

ISO/IEC 27001, AnnexeA.11.2.4 Maintenance des matériels

Mesure

Les matériels doivent être entretenus correctement pour garantir leur disponibilité permanente et leur intégrité.

ISO/IEC 27001, Annexe A.11.2.5 Sortie des actifs

Mesure

Les matériels, les informations ou les logiciels des locaux de l'organisation ne doivent pas sortir sans autorisation préalable.

ISO/IEC 27001, Annexe 11.2.6 Sécurité des matériels et des actifs hors des locaux

Mesure

Des mesures de sécurité doivent être appliquées aux matériels utilisés hors des locaux de l'organisation en tenant compte des différents risques associés au travail hors site.

ISO/IEC 27001, Annexe A.11.2.7 Mise au rebut ou recyclage sécurisé(e) des matériels

Mesure

Tous les composants des matériels contenant des supports de stockage doivent être vérifiés pour s'assurer que toute donnée sensible a bien été supprimée et que tout logiciel sous licence a bien été désinstallé ou écrasé de façon sécurisée, avant leur mise au rebut ou leur réutilisation.

ISO/IEC 27001, AnnexeA.11.2.8 Matériels utilisateur laissés sans surveillance

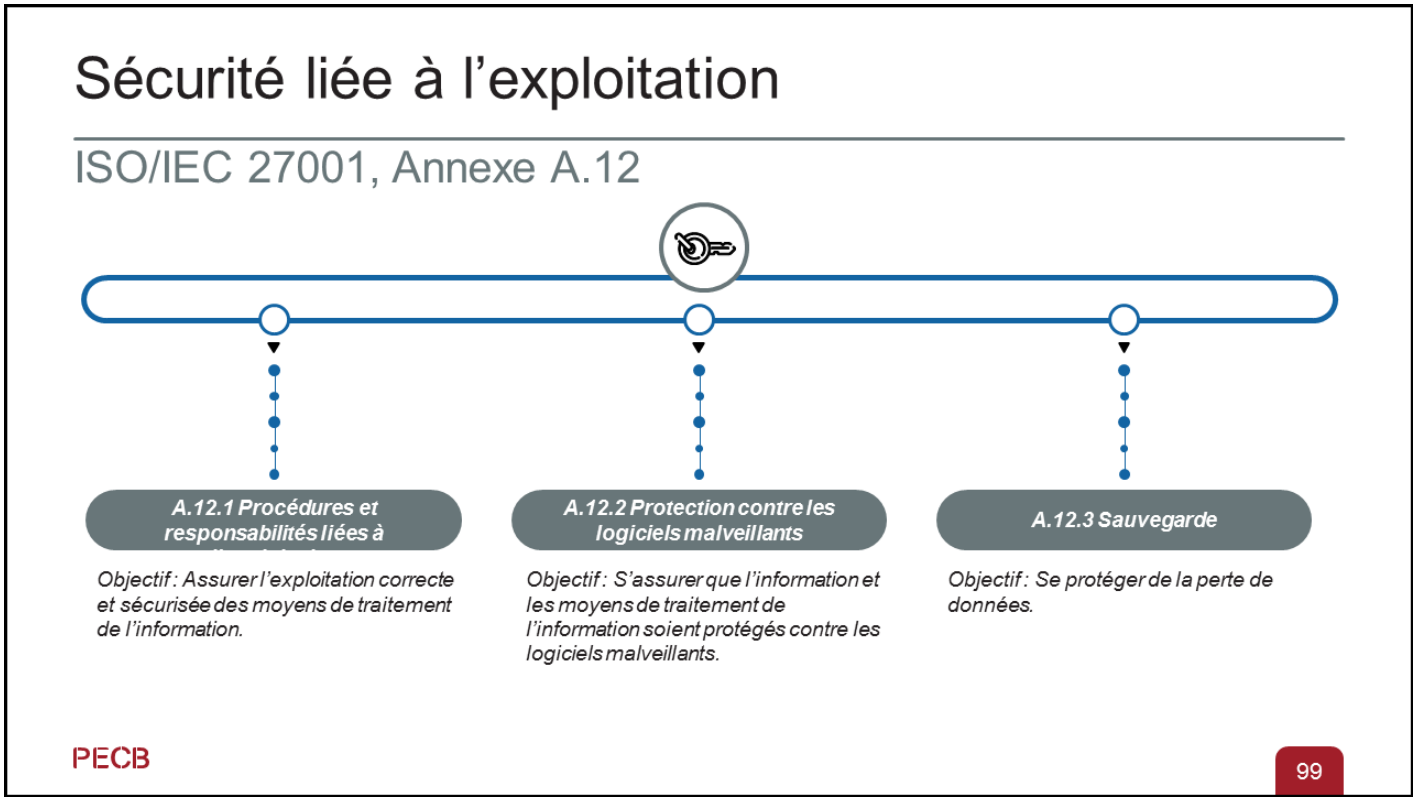
Mesure

Les utilisateurs doivent s'assurer que les matériels non surveillés sont dotés d'une protection appropriée.

ISO/IEC 27001, AnnexeA.11.2.9 Politique du bureau propre et de l'écran verrouillé

Mesure

Une politique du bureau propre pour les documents papier et les supports de stockage amovibles, et une politique de l'écran verrouillé pour les moyens de traitement de l'information doivent être adoptées.



ISO/IEC 27001, AnnexeA.12.1.1 Procédures d'exploitation documentées

Mesure

Les procédures d'exploitation doivent être documentées et mises à disposition de tous les utilisateurs concernés.

ISO/IEC 27001, AnnexeA.12.1.2 Gestion des changements

Mesure

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.

ISO/IEC 27001, AnnexeA.12.1.3 Dimensionnement

Mesure

L'utilisation des ressources doit être surveillée et ajustée et des projections sur les dimensionnements futurs doivent être effectuées pour garantir les performances exigées du système.

ISO/IEC 27001, AnnexeA.12.1.4 Séparation des environnements de développement, de test et d'exploitation

Mesure

Les environnements de développement, de test et d'exploitation doivent être séparés pour réduire les risques d'accès ou de changements non autorisés dans l'environnement en exploitation.

ISO/IEC 27001, AnnexeA.12.2.1 Mesures contre les logiciels malveillants

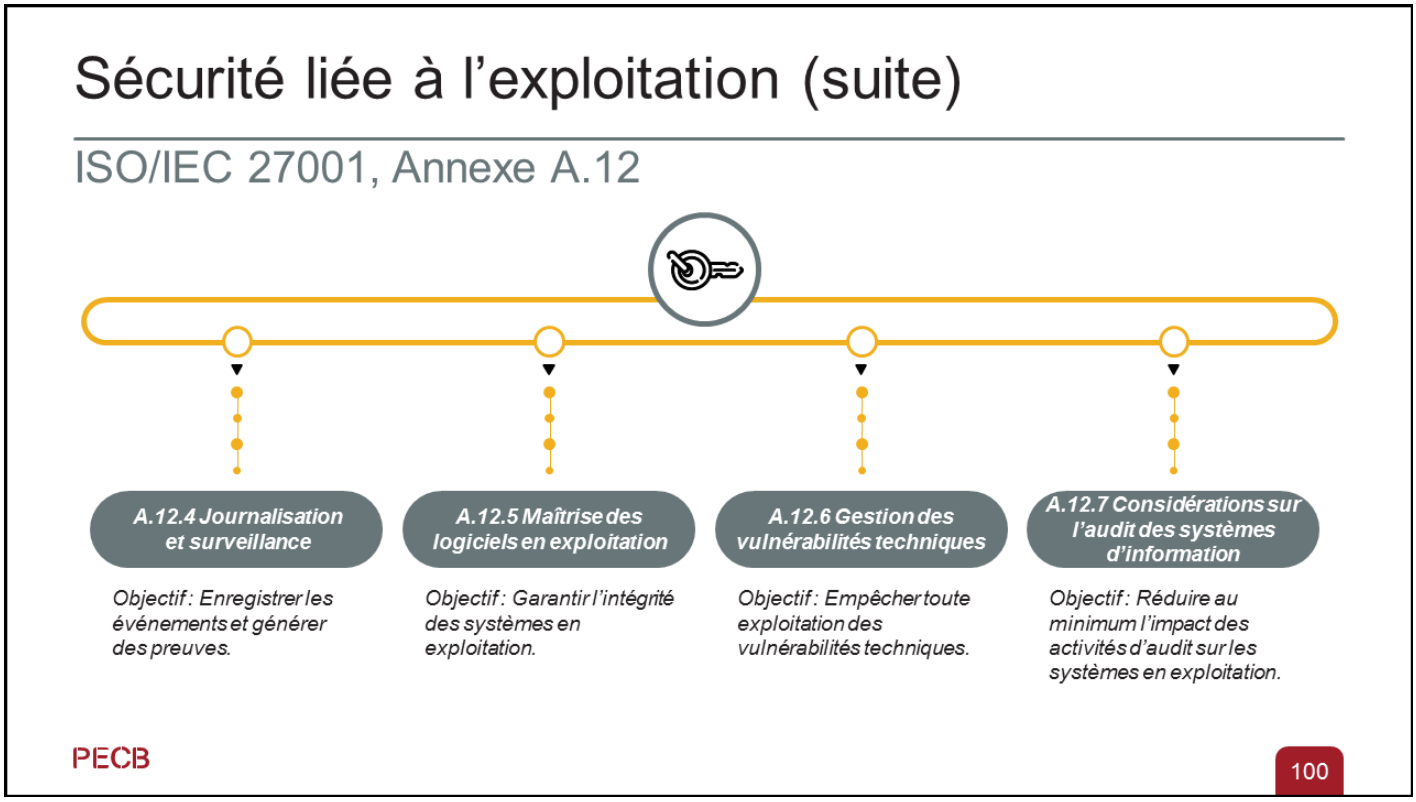
Mesure

Des mesures de détection, de prévention et de récupération conjuguées à une sensibilisation des utilisateurs adaptée, doivent être mises en œuvre pour se protéger contre les logiciels malveillants.

ISO/IEC 27001, AnnexeA.12.3.1 Sauvegarde des informations

Mesure

Des copies de sauvegarde de l'information, des logiciels et des images systèmes doivent être réalisés et testés régulièrement conformément à une politique de sauvegarde convenue.



ISO/IEC 27001, AnnexeA.12.4.1 Journalisation des événements

Mesure

Des journaux d'événements enregistrant les activités de l'utilisateur, les exceptions, les défaillances et les événements liés à la sécurité de l'information doivent être créés, tenus à jour et vérifiés régulièrement.

ISO/IEC 27001, Annexe A.12.4.2 Protection de l'information journalisée

Mesure

Les moyens de journalisation et d'information journalisée doivent être protégés contre les risques de falsification ou d'accès non autorisé.

ISO/IEC 27001, AnnexeA.12.4.3 Journaux administrateur et opérateur

Mesure

Les activités de l'administrateur système et de l'opérateur système doivent être journalisées, protégées et vérifiées régulièrement.

ISO/IEC 27001, AnnexeA.12.4.4 Synchronisation des horloges

Mesure

Les horloges de l'ensemble des systèmes de traitement de l'information concernés d'une organisation ou d'un domaine de sécurité doivent être synchronisées sur une source de référence temporelle unique.

ISO/IEC 27001, AnnexeA.12.5.1 Installation de logiciels sur des systèmes en exploitation

Mesure

Des procédures doivent être mises en œuvre pour contrôler l'installation de logiciels sur des systèmes en exploitation.

Page de notes

PECB

101

ISO/IEC 27001, Annexe A.12.6.1 Gestion des vulnérabilités techniques

Mesure

Des informations sur les vulnérabilités techniques des systèmes d'information en exploitation doivent être obtenues en temps opportun, l'exposition de l'organisation à ces vulnérabilités doit être évaluée et les mesures appropriées doivent être prises pour traiter le risque associé.

ISO/IEC 27001, AnnexeA.12.6.2 Restrictions liées à l'installation de logiciels

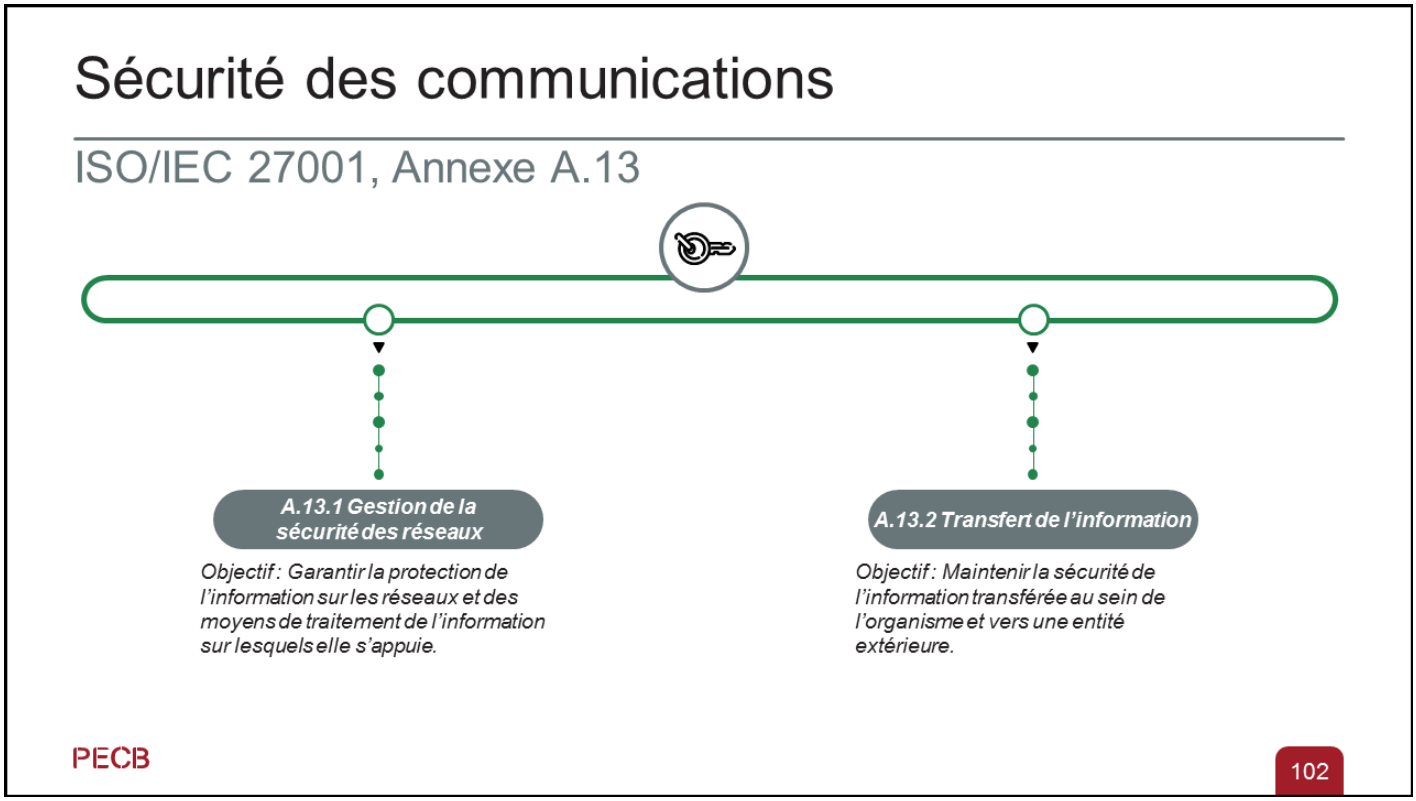
Mesure

Des règles régissant l'installation de logiciels par les utilisateurs doivent être établies et mises en œuvre.

ISO/IEC 27001, AnnexeA.12.7.1 Mesures relatives à l'audit des systèmes d'information

Mesure

Les exigences et activités d'audit impliquant des vérifications sur des systèmes en exploitation doivent être prévues avec soin et validées afin de réduire au minimum les perturbations subies par les processus métier.



ISO/IEC 27001, AnnexeA.13.1.1 Contrôle des réseaux

Mesure

Les réseaux doivent être gérés et contrôlés pour protéger l'information contenue dans les systèmes et les applications.

ISO/IEC 27001, Annexe A.13.1.2 Sécurité des services de réseau

Mesure

Pour tous les services de réseau, les mécanismes de sécurité, les niveaux de service et les exigences de gestion doivent être identifiés et intégrés dans les accords de services de réseau, que ces services soient fournis en interne ou externalisés.

ISO/IEC 27001, Annexe A.13.1.3 Cloisonnement des réseaux

Mesure

Les groupes de services d'information, d'utilisateurs et de systèmes d'information doivent être cloisonnés sur les réseaux.

ISO/IEC 27001, Annexe A.13.2.1 Politiques et procédures de transfert de l'information

Mesure

Des politiques, des procédures et des mesures de transfert formelles doivent être mises en place pour protéger les transferts d'information transitant par tous types d'équipements de communication.

ISO/IEC 27001, Annexe A.13.2.2 Accords en matière de transfert d'information

Mesure

Des accords doivent traiter du transfert sécurisé de l'information liée à l'activité entre l'organisation et les tiers.

ISO/IEC 27001, AnnexeA.13.2.3 Messagerie électronique

Mesure

L’information transitant par la messagerie électronique doit être protégée de manière appropriée.

Page de notes

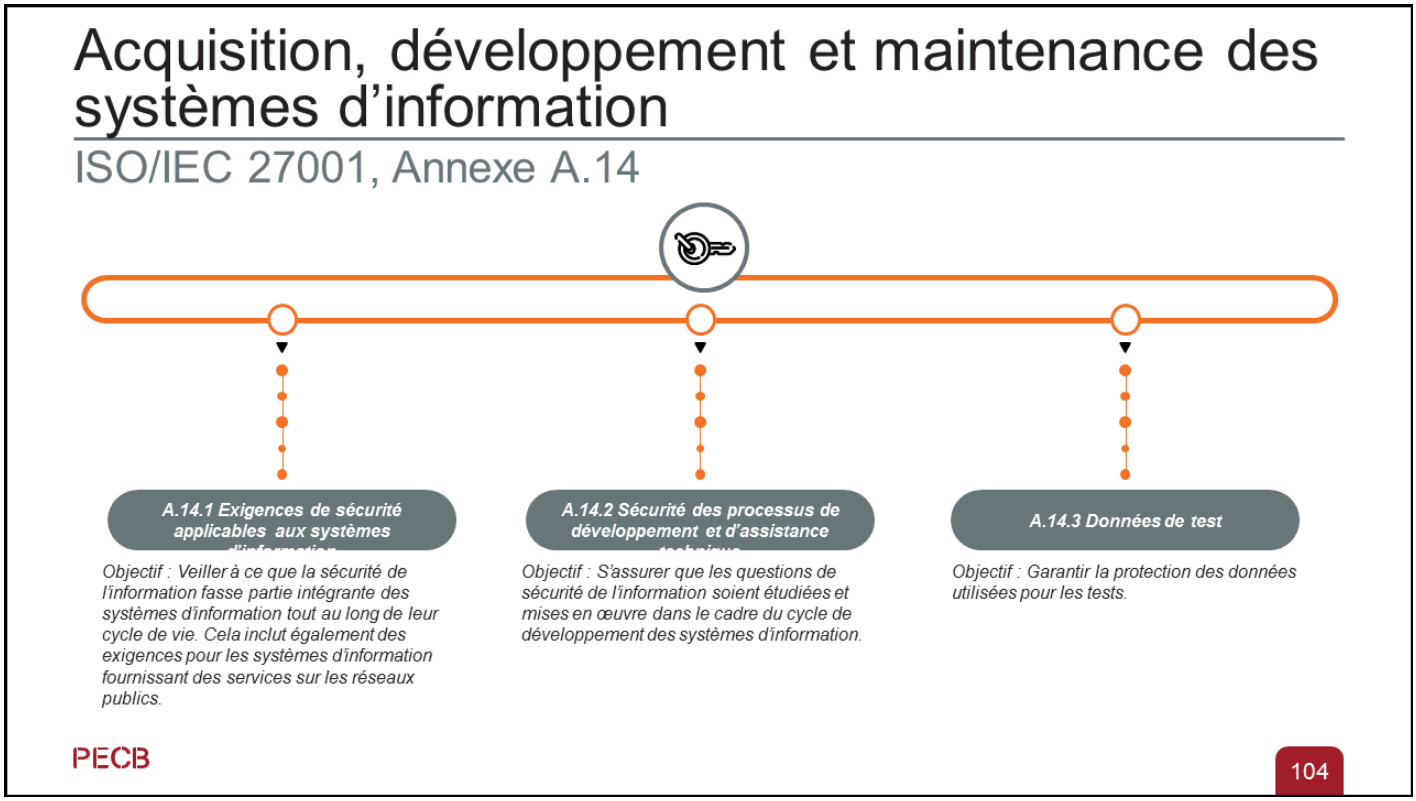
PECB

103

ISO/IEC 27001, Annexe A.13.2.4 Engagements de confidentialité ou de non-divulgation

Mesure

Les exigences en matière d'engagements de confidentialité ou de non-divulgation, doivent être identifiées, vérifiées régulièrement et documentées conformément aux besoins de l'organisation.



ISO/IEC 27001, AnnexeA.14.1.1 Analyse et spécification des exigences de sécurité de l'information

Mesure

Les exigences liées à la sécurité de l'information doivent être intégrées aux exigences des nouveaux systèmes d'information ou des améliorations de systèmes d'information existants.

ISO/IEC 27001, AnnexeA.14.1.2 Sécurisation des services d'application sur les réseaux publics

Mesure

Les informations liées aux services d'application transmises sur les réseaux publics doivent être protégées contre les activités frauduleuses, les différents contractuels, ainsi que la divulgation et la modification non autorisées.

ISO/IEC 27001, AnnexeA.14.1.3 Protection des transactions liées aux services d'application

Mesure

Les informations impliquées dans les transactions liées aux services d'application doivent être protégées pour empêcher une transmission incomplète, des erreurs d'acheminement, la modification non autorisée, la divulgation non autorisée, la duplication non autorisée du message ou sa réémission.

ISO/IEC 27001, AnnexeA.14.2.1 Politique de développement sécurisé

Mesure

Des règles de développement des logiciels et des systèmes doivent être établies et appliquées aux développements de l'organisation.

ISO/IEC 27001, AnnexeA.14.2.2 Procédures de contrôle des changements de système

Mesure

Les changements des systèmes dans le cadre du cycle de développement doivent être contrôlés par le biais de procédures formelles.

Page de notes

PECB

105

ISO/IEC 27001, AnnexeA.14.2.3 Revue technique des applications après changement apporté à la plateforme d'exploitation

Mesure

Lorsque des changements sont apportés aux plateformes d'exploitation, les applications critiques métier doivent être vérifiées et testées afin de vérifier l'absence de tout effet indésirable sur l'activité ou sur la sécurité.

ISO/IEC 27001, AnnexeA.14.2.4 Restrictions relatives aux changements apportés aux progiciels

Mesure

Les modifications des progiciels ne doivent pas être encouragées, être limitées aux changements nécessaires et tout changement doit être strictement contrôlé.

ISO/IEC 27001, AnnexeA.14.2.5 Principes d'ingénierie de la sécurité des systèmes

Mesure

Des principes d'ingénierie de la sécurité des systèmes doivent être établis, documentés, tenus à jour et appliqués à tous les travaux de mise en œuvre des systèmes d'information.

ISO/IEC 27001, AnnexeA.14.2.6 Environnement de développement sécurisé

Mesure

Les organisations doivent établir des environnements de développement sécurisés pour les tâches de développement et d'intégration du système, qui englobe l'intégralité du cycle de vie du développement du système, et en assurer la protection de manière appropriée.

ISO/IEC 27001, AnnexeA.14.2.7 Développement externalisé

Mesure

L'organisation doit superviser et contrôler l'activité de développement du système externalisée.

ISO/IEC 27001, AnnexeA.14.2.8 Test de la sécurité du système

Mesure

Les tests de fonctionnalité de la sécurité doivent être réalisés pendant le développement.

ISO/IEC 27001, AnnexeA.14.2.9 Test de conformité du système

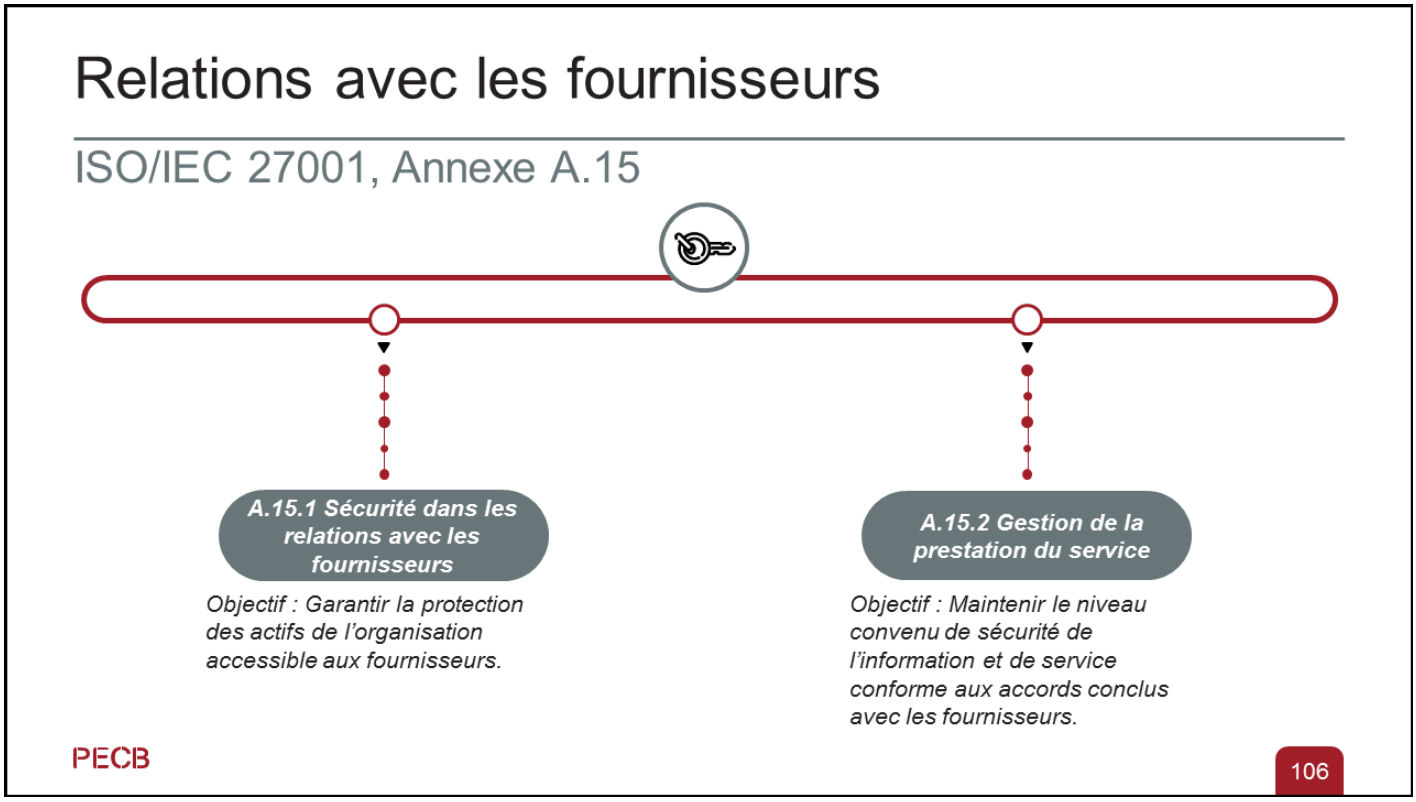
Mesure

Des programmes de test de conformité et des critères associés doivent être déterminés pour les nouveaux systèmes d'information, les mises à jour et les nouvelles versions.

ISO/IEC 27001, Annexe A.14.3.1 Protection de données de test

Mesure

Les données de test doivent être sélectionnées avec soin, protégées et contrôlées.



ISO/IEC 27001, Annexe A.15.1.1 Politique de sécurité de l'information dans les relations avec les fournisseurs

Mesure

Des exigences de sécurité de l'information pour limiter les risques résultant de l'accès des fournisseurs aux actifs de l'organisation doivent être acceptées par le fournisseur et documentées.

ISO/IEC 27001, Annexe A.15.1.2 La sécurité dans les accords conclus avec les fournisseurs

Mesure

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.

ISO/IEC 27001, Annexe A.15.1.3 Chaîne d'approvisionnement des produits et des services informatiques

Mesure

Les accords conclus avec les fournisseurs doivent inclure des exigences sur le traitement des risques liés à la sécurité de l'information associé à la chaîne d'approvisionnement des produits et des services informatiques.

ISO/IEC 27001, Annexe A.15.2.1 Surveillance et revue des services des fournisseurs

Mesure

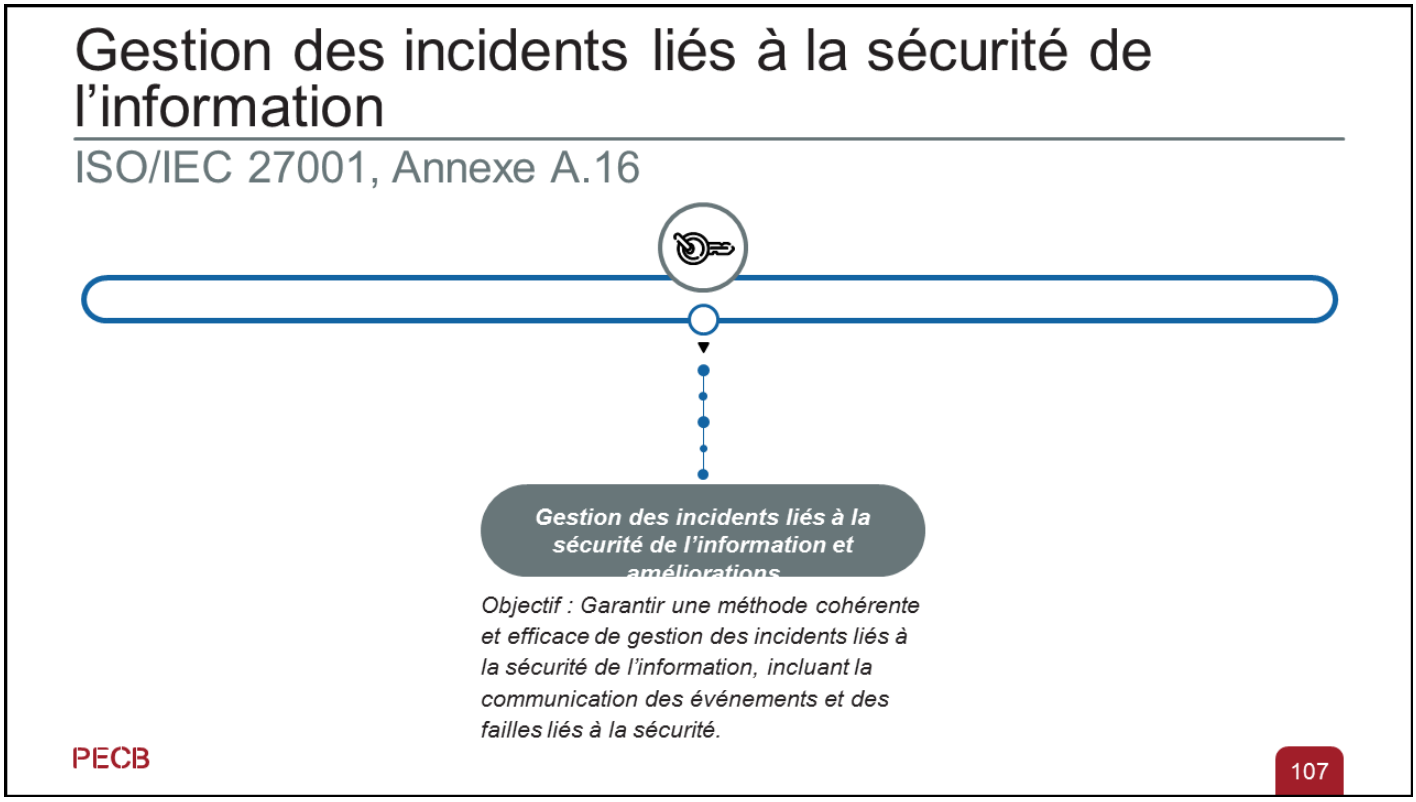
Les organisations doivent surveiller, vérifier et auditer à intervalles réguliers la prestation des services assurés par les fournisseurs.

ISO/IEC 27001, Annexe A.15.2.2 Gestion des changements apportés dans les services des fournisseurs

Mesure

Les changements effectués dans les prestations de service des fournisseurs, comprenant le maintien et l'amélioration des politiques, procédures et mesures existant en matière de sécurité de l'information, doivent être

gérés en tenant compte du caractère critique de l'information, des systèmes et des processus concernés et de la réappréciation des risques.



ISO/IEC 27001, AnnexeA.16.1.1 Responsabilités et procédures

Mesure

Des responsabilités et des procédures permettant de garantir une réponse rapide, efficace et pertinente doivent être établies en cas d'incident lié à la sécurité de l'information.

ISO/IEC 27001, AnnexeA.16.1.2 Signalement des événements liés à la sécurité de l'information

Mesure

Les événements liés à la sécurité de l'information doivent être signalés dans les meilleurs délais par les voies hiérarchiques appropriées.

ISO/IEC 27001, AnnexeA.16.1.3 Signalement des failles liées à la sécurité de l'information

Mesure

Les salariés et les sous-traitants utilisant les systèmes et services d'information de l'organisation doivent noter et signaler toute faille de sécurité observée ou soupçonnée dans les systèmes ou services.

ISO/IEC 27001, AnnexeA.16.1.4 Appréciation des événements liés à la sécurité de l'information et prise de décision

Mesure

Les événements liés à la sécurité de l'information doivent être appréciés et il doit être décidé s'il faut les classer comme incidents liés à la sécurité de l'information.

ISO/IEC 27001, Annexe A.16.1.5 Réponse aux incidents liés à la sécurité de l'information

Mesure

Les incidents liés à la sécurité de l'information doivent être traités conformément aux procédures documentées.

Page de notes

PECB

108

ISO/IEC 27001, Annexe A.16.1.6 Tirer des enseignements des incidents liés à la sécurité de l'information

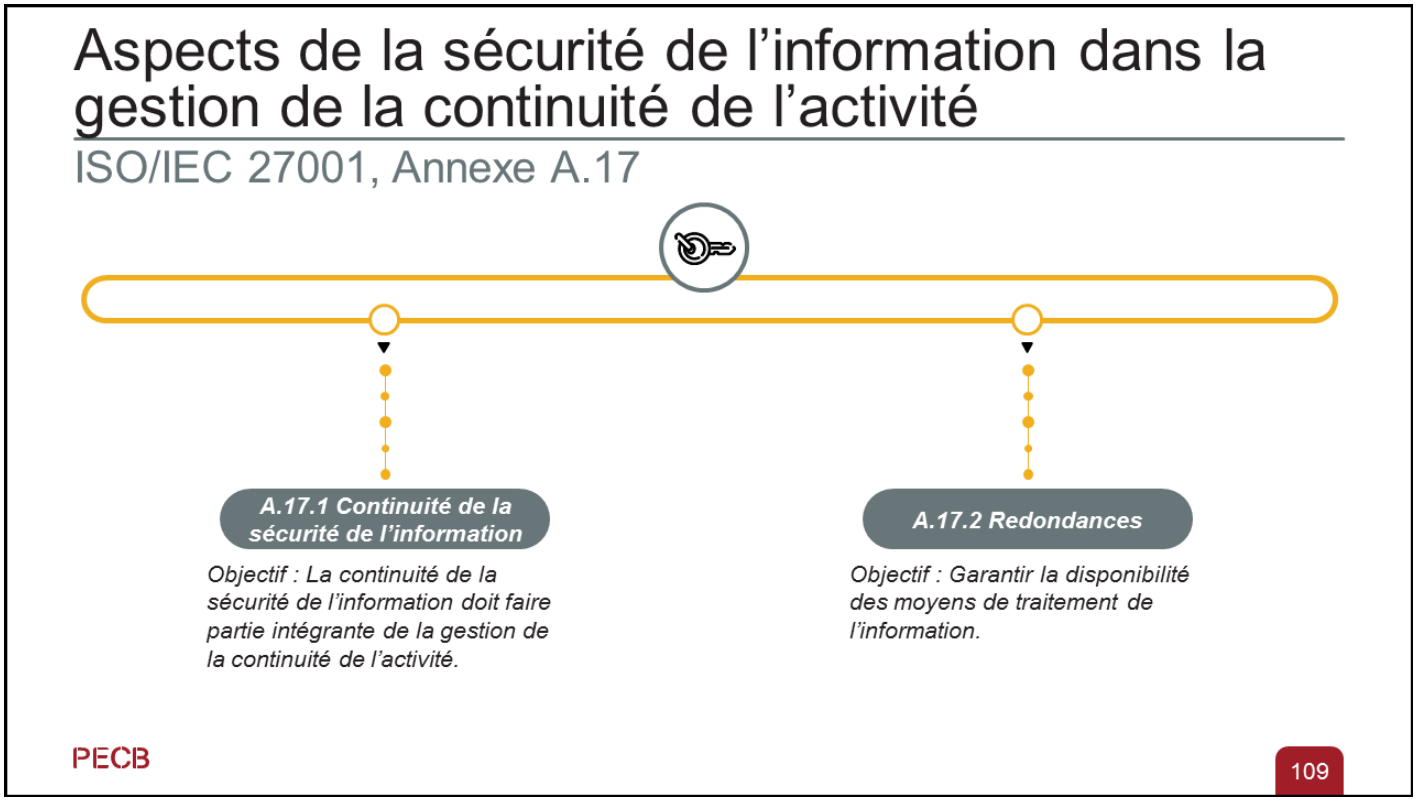
Mesure

Les connaissances recueillies suite à l'analyse et la résolution d'incidents doivent être utilisées pour réduire la probabilité ou l'impact d'incidents ultérieurs.

ISO/IEC 27001, Annexe A.16.1.7 Collecte de preuves

Mesure

L'organisation doit définir et appliquer des procédures d'identification, de collecte, d'acquisition et de protection de l'information pouvant servir de preuve.



ISO/IEC 27001, Annexe A.17.1.1 Organisation de la continuité de la sécurité de l'information

Mesure

L'organisation doit déterminer ses exigences en matière de sécurité de l'information et de continuité de management de la sécurité de l'information dans des situations défavorables, comme lors d'une crise ou d'un sinistre

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

Mesure

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.

ISO/IEC 27001, Annexe A.17.1.3 Vérifier, revoir et évaluer la continuité de la sécurité de l'information

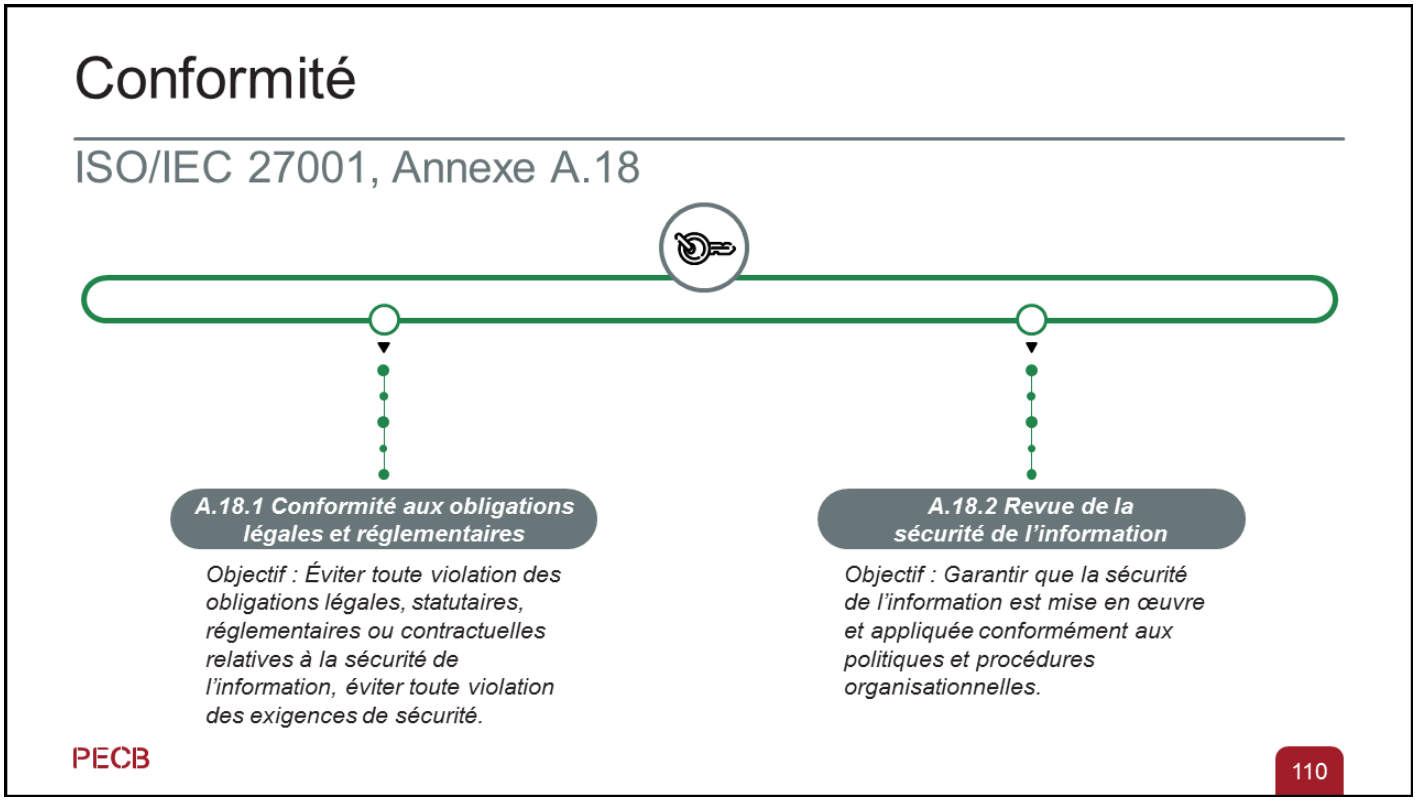
Mesure

L'organisation doit vérifier les mesures de continuité de la sécurité de l'information mises en œuvre à intervalles réguliers afin de s'assurer qu'elles sont valables et efficaces dans des situations défavorables.

ISO/IEC 27001, Annexe A.17.2.1 Disponibilité des moyens de traitement de l'information

Mesure

Des moyens de traitement de l'information doivent être mis en œuvre avec suffisamment de redondances pour répondre aux exigences de disponibilité.



ISO/IEC 27001, Annexe A.18.1.1 Identification de la législation et des exigences contractuelles applicables

Mesure

Toutes les exigences légales, statutaires, réglementaires et contractuelles en vigueur, ainsi que l'approche adoptée par l'organisation pour satisfaire à ces exigences, doivent être explicitement définies, documentées et mises à jour pour chaque système d'information et pour l'organisation elle-même.

ISO/IEC 27001, AnnexeA.18.1.2 Droits de propriété intellectuelle

Mesure

Des procédures appropriées doivent être mises en œuvre pour garantir la conformité avec les exigences légales, réglementaires et contractuelles relatives à la propriété intellectuelle et à l'usage des licences de logiciels propriétaires.

ISO/IEC 27001, Annexe A.18.1.3 Protection des enregistrements

Mesure

Les enregistrements doivent être protégés de la perte, de la destruction, de la falsification, des accès non autorisés et des diffusions non autorisées, conformément aux exigences légales, réglementaires, contractuelles et aux exigences métier.

ISO/IEC 27001, AnnexeA.18.1.4 Protection de la vie privée et protection des données à caractère personnel

Mesure

La protection de la vie privée et la protection des données à caractère personnel doivent être garanties telles que l'exigent la législation ou les réglementations applicables, et les clauses contractuelles le cas échéant.

ISO/IEC 27001, Annexe A.18.1.5 Réglementation relative aux mesures cryptographiques

Mesure

Des mesures cryptographiques doivent être prises conformément aux accords, législation et réglementations applicables.

Page de notes

PECB

111

ISO/IEC 27001, Annexe A.18.2.1 Revue indépendante de la sécurité de l'information

Mesure

Des revues régulières et indépendantes de l'approche retenue par l'organisme pour gérer et mettre en œuvre la sécurité de l'information (à savoir le suivi des objectifs de sécurité, les mesures, les politiques, les procédures et les processus relatifs à la sécurité de l'information) doivent être effectuées à intervalles définis ou lorsque des changements importants sont intervenus.

ISO/IEC 27001, Annexe A.18.2.2 Conformité avec les politiques et les normes de sécurité

Mesure

Les responsables doivent régulièrement vérifier la conformité du traitement de l'information et des procédures dont ils sont chargés au regard des politiques, des normes de sécurité applicables et autres exigences de sécurité.

ISO/IEC 27001, Annexe A.18.2.3 Vérification de la conformité technique

Mesure

Les systèmes d'information doivent être examinés régulièrement quant à leur conformité avec les politiques et les normes de sécurité de l'information de l'organisation.

Exercice2: Classification des mesures de sécurité

Déterminez le type (administratif, technique, managérial ou juridique) et la fonction (préventive, corrective ou de détection) de chacune des mesures de sécurité de l'information suivantes. Justifiez votre réponse.

Exemple: L'installation d'une clôture en fil de fer autour du site de l'entreprise

Par fonction, l'installation d'une clôture métallique est une mesure préventive qui contribue à sécuriser le site de l'organisme, en particulier les installations de traitement de l'information, contre tout accès physique non autorisé. Par type, il s'agit d'une mesure technique.

1. Séparation des fonctions de sécurité de l'information
2. Mise en place d'un système d'alarme incendie
3. Cryptage des communications électroniques
4. Enquête sur un incident de sécurité
5. Identification de la législation applicable

Durée de l'exercice: 30 minutes

Commentaires : 15 minutes

Résumé de la section

- Les mesures de sécurité de l'information comprennent tout processus, politique, procédure, ligne directrice, pratique ou structure organisationnelle susceptible de modifier les risques.
- Par type, les mesures de sécurité de l'information sont classées ainsi : techniques, juridiques, administratives et managériales.
- Par fonction, les mesures de sécurité de l'information sont classées en trois catégories : prévention, détection et correction.
- Plusieurs structures de référence en sécurité de l’information définissent une classification avec plus de catégories.

Cette section fournit des informations sur le programme de certification PECB et le processus de certification.

Programme de certification PECB ISO/IEC 27001

Principales exigences

Certification professionnelle	Examen	Expérience professionnelle	Expérience d'audit SMSI	Expérience de projet SMSI
ISO/IEC 27001 Foundation	Examen ISO/IEC 27001 Foundation	----------	----------	----------
ISO/IEC 27001 Provisional Auditor	ISO/IEC 27001 Examen Lead Auditor	----------	----------	----------
ISO/IEC 27001 Auditor		2 ans (1 en sécurité de l'information)	200 heures	----------
ISO/IEC 27001 Lead Auditor		5 ans (2 en sécurité de l'information)	300 heures	----------
ISO/IEC 27001 Senior Lead Auditor		10 ans (7 en sécurité de l'information)	1 000 heures	----------
ISO/IEC 27001 Provisional Implementer	ISO/IEC 27001 Examen Lead Implementer	----------	----------	----------
ISO/IEC 27001 Implementer		2 ans (1 en sécurité de l'information)	----------	200 heures
ISO/IEC 27001 Lead Implementer		5 ans (2 en sécurité de l'information)	----------	300 heures
ISO/IEC 27001 Senior Lead Implementer		10 ans (7 en sécurité de l'information)	----------	1 000 heures
ISO/IEC 27001 Master	Examens ISO/IEC 27001 LA+LI (4 examens Foundation supplémentaires)	15 ans (10 en sécurité de l'information)	700 heures	700 heures

PECB

115

La certification **Foundation** reconnaît que la personne comprend les concepts de base, les approches, méthodes et techniques permettant la gestion efficace d'un système de management.

Les principales certifications d'auditeur:

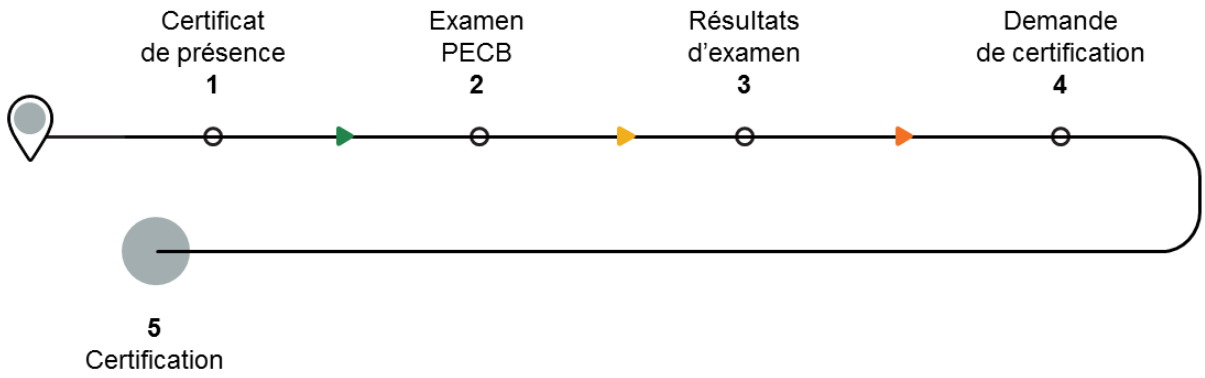
1. La certification **Certified Provisional Auditor** reconnaît que le candidat possède les connaissances de base en audit et peut intégrer une équipe d'audit en tant que membre.
2. La certification **Certified Auditor** reconnaît que le candidat possède les connaissances nécessaires pour participer à un audit et les compétences de base pour conduire un audit de certification d'un système de management, ayant déjà été membre d'une équipe d'audit.
3. La certification **Certified Lead Auditor** reconnaît que le candidat maîtrise les connaissances de l'audit et démontre des compétences en audit et en gestion d'une équipe d'audit.
4. La certification **Certified Senior Lead Auditor** s'adresse aux professionnels qui ont une vaste expérience en audit.

Les principales certifications d'Implementer:

1. La certification **Certified Provisional Implementer**reconnaît que le candidat possède les connaissances de base pour participer à la mise en œuvre et la gestion d'un système de management.
2. La certification **Certified Implementer**reconnaît que le candidat possède les connaissances nécessaires pour participer à la mise en œuvre et la gestion d'un système de management.
3. La certification **Certified Lead Implementer**reconnaît que le candidat maîtrise les connaissances nécessaires pour mettre en œuvre un système de management et démontre des compétences en gestion d'une équipe d'implémentation d'un cadre de conformité.
4. La certification **Certified Senior Lead Implementer** s'adresse aux professionnels qui ont une grande expérience dans les projets de mise en œuvre.

La certification **Master** reconnaît que le candidat maîtrise à la fois les concepts de base, les approches, méthodes et techniques pour réaliser et diriger une équipe d'audit ainsi que pour diriger un projet de mise en œuvre d'un système de management.

Processus de certification PECB



PECB

1. Certificat de présence

Unités de formation professionnelle continue (FPC)

Après avoir assisté à la formation et soumis le ***Formulaire d'évaluation*** de la formation, un certificat de présence sera généré dans votre tableau de bord ***monPECB*****,** sous l'onglet ***Mes formations***. Le certificat de participations est valable pour 14unités de FPC.

2. Examen PECB

- L'objectif de l'examen de certification est de s'assurer que les candidats comprennent les concepts de bases d'un système de management de la sécurité de l'information selon ISO/IEC 27001.
- L'examen est disponible en plusieurs langues.
- Pour plus d'informations sur le processus d'examen, veuillez visiter les Politiques et règlement relatifs à l'examen.

PECB

118

Le Comité d'examen de PECB s'assure que l'élaboration et le caractère adéquat des questions d'examen sont maintenus en fonction des pratiques professionnelles actuelles.

L'examen est disponible en plusieurs langues. Pour passer l'examen dans une langue autre que le français, veuillez demander au formateur, ou nous contacter en envoyant un e-mail à examination@pecb.com.

Tous les domaines de compétence sont couverts par l'examen. Pour obtenir une description détaillée de chaque domaine de compétence, veuillez consulter le site Web de PECB: www.pecb.com.

3. Résultats d'examen

Il y a deux résultats possibles :

- Vous recevrez par e-mail un numéro d'examen pour faire une demande de certification.
- Ce numéro d'examen est important pour faire votre demande de certification PECB.

- Vous pouvez reprendre l'examen une fois gratuitement dans les douze mois suivant l'examen initial.
- Veuillez contacter le prestataire de la formation pour déterminer la date de reprise de l'examen.

Note importante : Aucune note numérique ne sera envoyée au candidat.

PECB

119

Les examens sont corrigés par des correcteurs qualifiés qui sont assignés de façon anonyme.

Afin de garantir l'indépendance et l'impartialité et éviter les conflits d'intérêts, les formateurs et les surveillants ne participent pas au processus de correction des examens ni au processus de certification.

Si le candidat échoue à l'examen, une explication lui sera fournie sur les domaines dans lesquels il n'a pas démontré les compétences requises. Pour reprendre l'examen, le candidat doit communiquer avec le responsable de l'organisme de formation.

4. Demande de certification

Processus général

Après avoir réussi l'examen, vous pouvez faire la demande en ligne pour obtenir votre certification PECB au www.pecb.com.

PECB

120

Après avoir réussi l'examen, le candidat dispose d'un délai maximum de trois ans pour soumettre un dossier professionnel afin d'obtenir une certification professionnelle.

Lors de votre demande, vous devrez fournir vos coordonnées. Veuillez écrire votre nom tel que vous souhaitez qu'il apparaisse sur votre certificat (en format ASCII). Avant de soumettre votre demande de certification, veuillez vérifier l'exactitude des coordonnées que vous avez fournies. Le certificat sera délivré avec le nom que vous avez fourni lorsque vous avez créé le compte PECB. Pour mettre à jour votre nom dans votre compte PECB, veuillez nous contacter à l'adresse customer@pecb.com.

5. Certification

- Une fois votre demande approuvée, PECB délivrera un certificat professionnel en format PDF qui peut être téléchargé à partir de votre compte PECB.
- Ce certificat comporte un numéro de certification qu'il est possible de valider sur le site de PECB www.pecb.com sous l'onglet ***Valider un certificat***.
- Pour plus d'informations sur le processus de certification, veuillez consulter les Politiques et règlement relatifs à la certification.

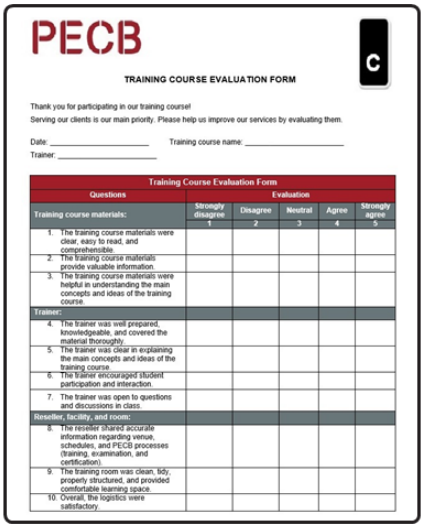
PECB

121

Lorsque le candidat est certifié, il reçoit un avis du système afin de télécharger le certificat à partir de son compte PECB.

Évaluation de la formation

Formulaire d'évaluation de la formation



PECB

TRAINING COURSE EVALUATION FORM

Thank you for participating in our training course!
Serving our clients is our main priority. Please help us improve our services by evaluating them.

Date: _____ Training course name: _____
Trainer: _____

Training Course Evaluation Form					
Questions	Evaluation				
Training course materials:	Strongly disagree 1	Disagree 2	Neutral 3	Agree 4	Strongly agree 5
1. The training course materials were clear, easy to read, and comprehensible.					
2. The training course materials provide valuable information.					
3. The training course materials were helpful in understanding the main concepts and ideas of the training course.					
Trainer:					
4. The trainer was well prepared, knowledgeable, and covered the material thoroughly.					
5. The trainer was clear in explaining the main concepts and ideas of the training course.					
6. The trainer encouraged student participation and interaction.					
7. The trainer was open to questions and discussions in class.					
Reseller, facility, and room:					
8. The reseller shared accurate information regarding venue, schedules, and PECB processes (training, examination, and certification).					
9. The training room was clean, tidy, properly structured, and provided comfortable learning space.					
10. Overall, the logistics were satisfactory.					

PECB

122

Nous nous efforçons d'améliorer constamment la qualité et la pertinence pratique de nos formations. Dans cette optique, votre opinion quant à la formation que vous venez de suivre a pour nous une grande valeur.

Nous vous serions très reconnaissants de bien vouloir donner votre appréciation de la formation et des formateurs.

De plus, si vous avez des suggestions pour améliorer le matériel de formation de PECB, n'hésitez pas à nous en faire part. Veuillez ouvrir un ticket à l'intention du département de formation sur le site Web de PECB (www.pecb.com) dans la section ***Contactez-nous***. Nous lisons et évaluons attentivement les commentaires que nous recevons de nos membres.

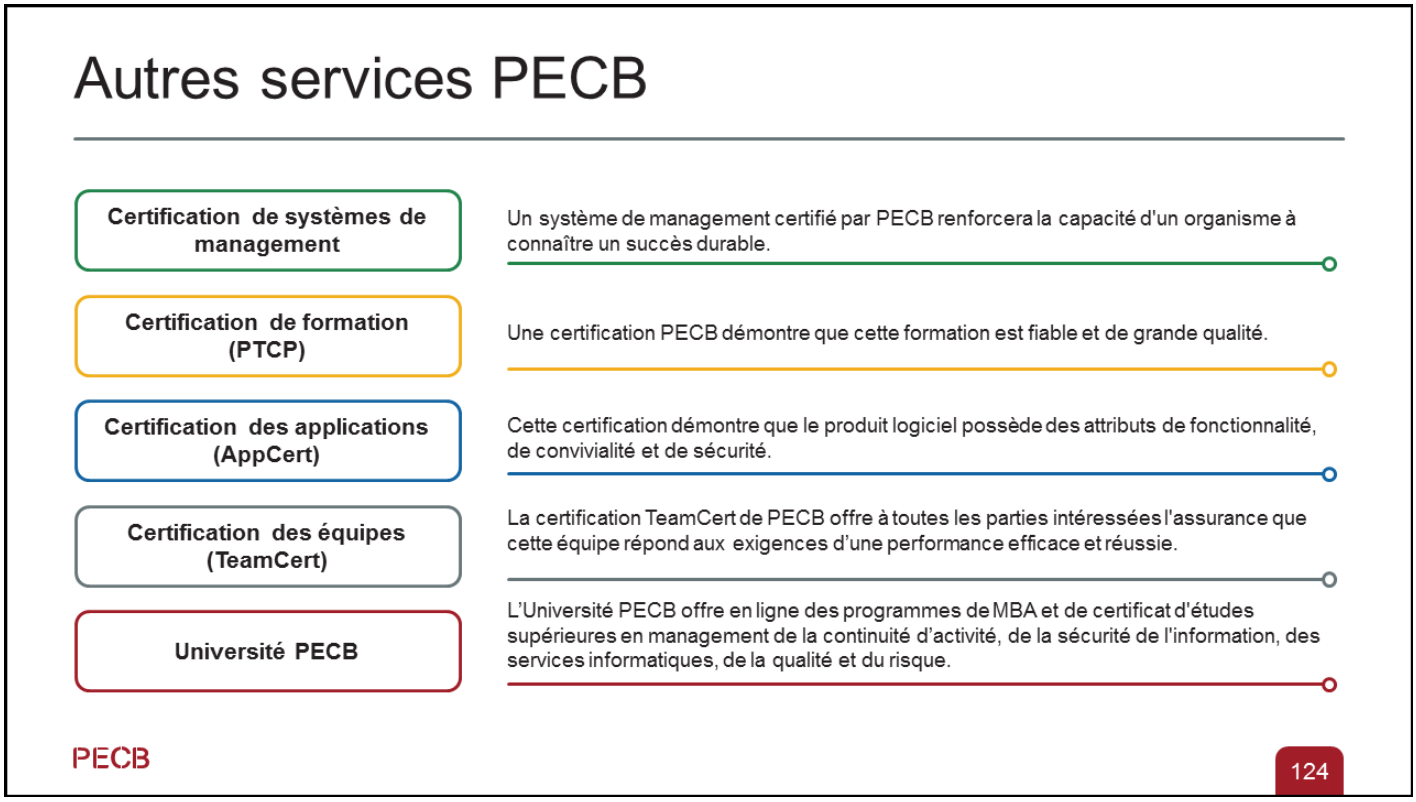
En cas d'insatisfaction à l'égard de la formation (formateur, salle de formation, équipement, etc.), de l'examen ou des processus de certification, veuillez ouvrir un ticket dans la catégorie ***Déposer une plainte*** du site Web de PECB (www.pecb.com), dans la section ***Contactez-nous***.

Certification de personnes PECB

- Une certification personnelle est une reconnaissance officielle délivrée par PECB qui stipule que le titulaire possède les compétences et la compréhension d'un domaine de connaissances donné.
- Les individus peuvent faire la demande de diverses certifications professionnelles parmi les programmes de certification de PECB. Chaque certification PECB requiert une formation et une expérience spécifiques.

Exemple :

PECB Certified ISO 9001 Lead Implementer



Certification de systèmes de management

Alors que les organismes cherchent continuellement des moyens d'obtenir un avantage concurrentiel sur le marché, avoir un système de management certifié en place est la meilleure solution. Les avantages sont multiples: amélioration de la qualité des produits et des services, reconnaissance internationale accrue, réduction des coûts, amélioration de la satisfaction client, etc.

Certification de formation:

Les organismes ou les personnes qui cherchent à faire certifier leur formation (aussi appelés «développeurs de formation») doivent se conformer aux exigences du programme de certification de formation établi par PECB.

Certification des applications:

Compte tenu de l'augmentation considérable du nombre d'utilisateurs d'applications logicielles dans le monde, PECB a développé un programme de certification d'applications logicielles. Ce programme vise à définir les règles qualitatives et quantitatives communes, les caractéristiques et les conditions minimales applicables aux produits logiciels à respecter par les sociétés de développement de logiciels pour attester de leur conformité.

Certification des équipes:

PECB offre des certifications des équipes qui aident les organismes à améliorer l'efficacité et la productivité de leurs équipes. Les équipes cherchant à obtenir la certification feront l'objet d'une évaluation et d'une appréciation afin de vérifier la conformité aux exigences et aux critères.

Toutes les certifications mentionnées ci-dessus sont valables pour une période de trois ans. PECB examinera périodiquement la performance des personnes, des systèmes de management, des équipes, des produits et applications pour s'assurer qu'ils sont conformes aux exigences et que l'amélioration continue est en place.

Page de notes

PECB

125

Université PECB :

L'objectif de l'Université PECB est de fournir un enseignement supérieur de haute qualité et des services complets qui inspirent l'amélioration continue, démontrent une reconnaissance et profitent à une organisation, à une communauté, à un état et à la société dans son ensemble.

Note importante:

1. Afin de compléter l'un des programmes de MBA, les candidats doivent accumuler un total de 48 crédits. Les programmes sont composés de trois ensembles de cours classés par catégorie: cours de base, de spécialisation et facultatifs – plus la thèse de MBA. Chaque cours des trois catégories mentionnées ci-dessus vaut trois crédits, tandis que la thèse vaut 12 crédits.
2. Chacun des programmes de certificat d'études supérieures est un programme d'une valeur de douze crédits. Les candidats devront suivre quatre cours qui s'inscrivent dans les domaines respectifs. Si un candidat décide de poursuivre ses études et d'obtenir un MBA, il peut suivre deux programmes de certificat d'études supérieures de son choix, combinés au certificat d'études supérieures en administration des affaires, soumettre sa thèse et obtenir son diplôme.

Les candidats qui détiennent un certificat valide de PECB et qui répondent aux exigences du programme universitaire qui les intéresse peuvent transférer ces crédits pour obtenir des crédits valides pour le cours correspondant de l'université. Pour de plus amples informations sur l'Université PECB ou le transfert des crédits de certification, veuillez contacter university@pecb.com.

Autres formations et certifications PECB

- Principes et concepts fondamentaux d'un système de management de la sécurité de l'information (SMSI)
- Concepts et principes fondamentaux de l'audit
- Préparer un audit ISO/IEC 27001
- Réaliser un audit ISO/IEC 27001
- Clore un audit ISO/IEC 27001
- Gérer un programme d'audit ISO/IEC 27001

- Classification des actifs
- Identification et analyse des risques
- Approche quantitative et qualitative de l'évaluation des risques
- Traitement des risques
- Gestion du risque résiduel
- Gouvernance et gestion des risques
- Connaissance des méthodes compatibles (CRAMM, OCTAVE, etc.)

PECB

126

PECB Certified ISO/IEC 27001 Lead Auditor (5 jours)

La formation ISO/IEC 27001Lead Auditor permet aux participants de développer l'expertise nécessaire à la réalisation d'un audit de système de management de la sécurité de l'information (SMSI) en appliquant des principes, procédures et techniques largement reconnus en audit. Au cours de cette formation, le participant acquerra les connaissances et les compétences nécessaires pour planifier et réaliser des audits internes et externes conformément à ISO19011.

PECB Certified ISO/IEC 27005Risk Manager (3 jours)

La formation ISO/IEC 27005Certified Risk Manager permet aux participants de maîtriser la gestion des risques liés à la sécurité de l'information, incluant la planification d'un programme de gestion des risques, l'analyse, l'appréciation, le traitement des risques, la communication et la surveillance des risques.

Page de notes

PECB

128

Résumé du jour 2

Les sujets suivants ont été abordés lors de la première journée de cette formation :

- Processus de gestion des risques et méthodologie d'appréciation des risques
- Identification, estimation, évaluation et traitement des risques
- Gestion des ressources
- Formation, sensibilisation et communication
- Gestion des changements
- Surveillance, mesure, analyse et évaluation de la performance
- Actions correctives et amélioration continue
- Audits interne et externe
- Revue de direction
- Non-conformités
- Classification des mesures de sécurité de l'information par type et par fonction
- Introduction aux mesures de sécurité de l'annexe A

Suivez-nous sur les médias sociaux

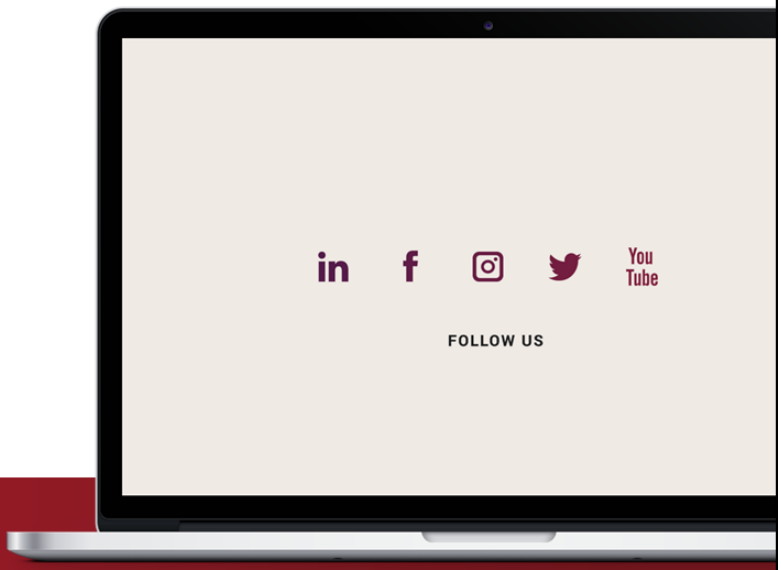
www.pecb.com/facebook

www.pecb.com/linkedin

www.pecb.com/twitter

www.pecb.com/youtube

www.instagram.com/pecb.official



PECB

Page de notes

Page de notes