



Programme du jour3

- Section14: Conception des mesures de sécurité et rédaction des politiques spécifiques et des procédures
- Section15: Mise en œuvre des mesures de sécurité
- Section16: Définition du processus de gestion de documents
- Section17: Plan de communication
- Section18: Plan de formation et de sensibilisation
- Section19: Gestion des opérations
- Section20: Gestion des incidents

© 2020 PECB. Tous droits réservés.

Version6.0

Numéro de document: ISMSLID3V6.0

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

Section 14

Conception des mesures de sécurité et rédaction des politiques spécifiques et des procédures

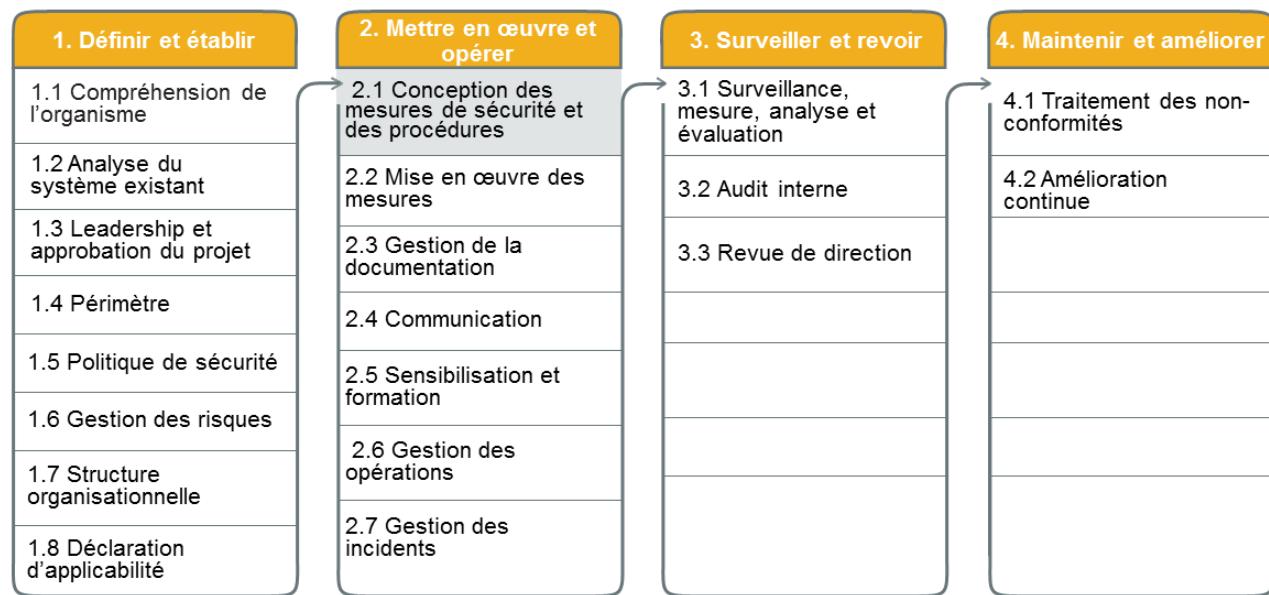
- Conception des processus et mesures de sécurité
- Description des processus et des mesures de sécurité
- Rédaction des politiques spécifiques
- Rédaction des procédures
- Définition des enregistrements

PECB

2

Cette section aidera le participant à acquérir des connaissances sur la conception des mesures de sécurité et la rédaction de politiques et de procédures spécifiques, y compris les procédures de rédaction et la définition des enregistrements.

2.1 Conception des mesures de sécurité et des procédures



PECB

3

Procédures

ISO 9000, article 3.4.5

manière spécifiée de réaliser une activité ou un processus

Note 1 à l'article: Les procédures peuvent ou non faire l'objet de documents.



PECB

4

Note terminologique:

Le document qui contient une procédure peut être appelé «document de procédure».

2.1 Conception des mesures de sécurité et des procédures

Liste des activités

2.1.1

Concevoir les processus et les mesures de sécurité

2.1.2

Définir les processus et les mesures

2.1.3

Rédiger les politiques spécifiques

2.1.4

Rédiger les procédures

2.1.5

Définir les enregistrements

2.1.1 Concevoir les processus et les mesures de sécurité

Avant de décrire les processus et les mesures, il convient de bien les concevoir. La phase de conception devrait d'abord identifier les éléments suivants :

- Objectifs
- Éléments d'entrée
- Rôles et responsabilités des parties intéressées
- Interfaces avec d'autres processus
- Ressources nécessaires aux opérations
- Listes des activités et des tâches à effectuer dans les opérations
- Liste des enregistrements
- Principaux indicateurs d'efficacité
- Éléments de sortie

2.1.2 Définir les processus et les mesures

Conseils pratiques

- Diverses mesures de sécurité liées au SMSI devraient être documentées.
- Aucune méthode n'est imposée par ISO/IEC 27001.
- Il est de bonne pratique de documenter les mesures de sécurité par groupe. Par exemple, on peut regrouper les mesures de sécurité concernant la gestion des incidents.
- La documentation doit être assez précise pour refléter la réalité, mais assez simple pour en assurer la surveillance.



7

PECB

Définir les processus et les mesures

Les 6 W

- Who (Qui) ?
- What (Quoi)?
- When (Quand) ?
- Where (Où) ?
- Why (Pourquoi)?
- How (Comment)?

Exemple :

L'administrateur réseau (qui ?) s'assure que les sauvegardes sont complétées (quoi ?) en révisant les journaux de sauvegarde (comment ?) chaque matin (quand ?). À la suite de la revue, il remplit et signe une liste de contrôles (où ?) qui est conservée comme référence future (pourquoi ?).

PECB

8

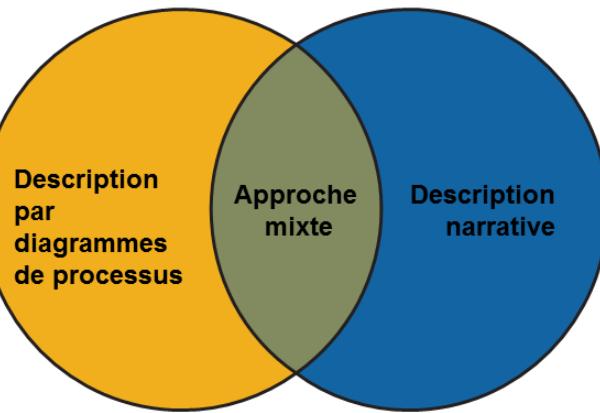
Note importante: Il n'y a aucune exigence de la norme ISO/IEC27001 qui oblige l'organisme à décrire de façon détaillée chaque mesure de sécurité en place. Un organisme peut fournir une documentation claire et concise décrivant le fonctionnement des processus et des mesures inclus dans le SMSI.

Plusieurs organismes incluent la description des mesures de sécurité dans leur déclaration d'applicabilité.

Définir les processus et les mesures

Types de méthodes

Représentation visuelle des processus et des mesures de sécurité



Description détaillée des processus et des mesures de sécurité

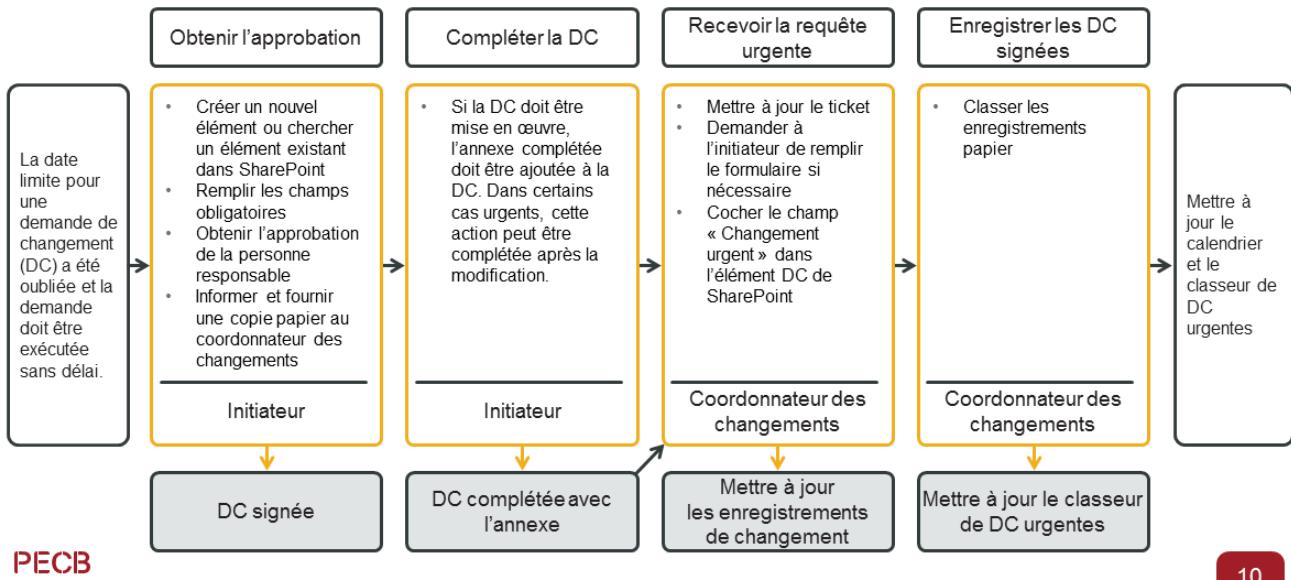
Description par diagrammes de processus complétés par des descriptions textuelles

PECB

9

Diagramme de processus

Exemple d'une demande de modification urgente



Les **diagrammes de processus** ou «logigrammes» permettent de visualiser l'enchaînement des actions. Le processus peut être documenté formellement dans une fiche de données processus comprenant une cartographie complète des processus de l'organisme. Il n'existe pas de norme pour représenter un processus. Il sera cependant nécessaire d'établir une symbolique (formes de base) pour représenter chaque caractéristique, boucle de décision et autres outils existants dans le processus de cartographie.

En résumé, la règle d'or: Penser simple et opérationnel et s'assurer que toute représentation demeure intelligible et utilisable par tous.

Description narrative

	Gestion des incidents	Nº :	MTR-CT01-131005RS		
	Type : Mesure narrative	Date de publication :	15/06/2019		
	Version : 1.2 (revue le 10/10/2017)	Page 1 de 2			
Émis par : Faton Aliu	Division : Siège social – Montréal	Approuvé par : Eric Lachapelle			
Processus	Technologies de l'information – Le processus de gestion des incidents doit garantir que les incidents sont signalés et résolus efficacement, en minimisant les impacts négatifs et en permettant un retour rapide à la normalité. Ce processus concerne les rapports d'incident, le suivi des incidents et l'escalade vers les niveaux de gestion appropriés.				
Sous-processus	Gestion des incidents				
Éléments d'entrée	Appels téléphoniques ou e-mails des utilisateurs, alertes des agents de surveillance de serveur, alertes des agents de surveillance du réseau				
Éléments de sortie	Rapports d'incident, réponses aux incidents, processus d'escalade d'incident, rapports des incidents traités remis au Service client, journaux des tâches effectuées pour résoudre les incidents				
Personnes impliquées :	Personnel du Service client, analystes TI, gestionnaires et le vice-président, GIT				
Responsabilité du processus	Vice-président et GIT				

PECB

11

Une deuxième méthode de documentation des processus et des mesures de sécurité consiste à rédiger des **narratifs** sur leur fonctionnement. L'objectif d'un processus narratif est de décrire le trajet de l'information et les mesures de sécurité reliées à ce processus. La description devrait permettre au lecteur de comprendre les différentes étapes liées aux opérations, à l'identification des acteurs (par le titre des fonctions) chargés d'exécuter les tâches, les éléments d'entrée et de sortie, la source d'information utilisée, les indicateurs, etc.

Conseils pratiques:

1. Éviter d'écrire un processus général de haut niveau, tel que «des sauvegardes sont effectuées périodiquement sur les systèmes d'information en fonction des besoins d'affaires de chaque unité administrative».
2. Utiliser des verbes d'action dans cet exemple: Le responsable du département revoit, approuve, valide, etc.
3. Éviter les tournures de verbe telles que pourrait ou devrait, qui laissent un doute quant à la réalisation de l'action si celle-ci est liée à une exigence de conformité
4. S'assurer de décrire les mesures de sécurité dans le contexte du processus métier lié
5. Décrire les processus et les mesures à partir des réponses aux questions des «6W»
6. Quand il y a une référence à un document, être aussi précis que possible et que nécessaire

Note importante: Il convient que la description reflète la réalité actuelle du fonctionnement du processus et des mesures de sécurité et non la situation souhaitée de l'organisme.

2.1.3 Rédiger les politiques spécifiques

- La publication d'une politique de sécurité de l'information est exigée
- Selon les mesures de sécurité sélectionnées, l'organisme doit publier des politiques spécifiques sur certains sujets tels que :
 - ▷ Appareils mobiles
 - ▷ Télétravail
 - ▷ Contrôle d'accès
 - ▷ Restriction d'accès à l'information
 - ▷ Contrôles et clés cryptographiques
 - ▷ Bureau propre et écran clair
 - ▷ Sauvegarde des informations
 - ▷ Développement sécurisé
 - ▷ Relations avec les fournisseurs

PECB

12

2.1.4 Rédiger les procédures

- Il est de bonne pratique d'écrire une première version des procédures avant de mettre en œuvre les mesures sélectionnées.
- Il convient d'impliquer les employés responsables des opérations dans la rédaction et la validation des procédures.
- Les procédures validées garantissent que les mesures de sécurité sont plus susceptibles d'être efficaces dans les opérations quotidiennes.



Information documentée requise

ISO/IEC 27001, articles 4 à 10

Voici la liste de l'information documentée explicitement exigée par ISO/IEC 27001

1. Périmètre du SMSI (4.3)
2. Politique de sécurité de l'information (5.2)
3. Processus et résultats de l'appréciation des risques de sécurité de l'information (6.1.2 et 8.2)
4. Processus et résultats du traitement des risques de sécurité de l'information (6.1.3 et 8.3)
5. Déclaration d'applicabilité (6.1.3 d)
6. Objectifs de sécurité de l'information (6.2)
7. Compétence des personnes (7.2 d)
8. Contrôles des informations documentées (7.5)
9. Planification et contrôles opérationnels (8.1)
10. Résultats de surveillance et de mesure (9.1)
11. Programme et résultats d'audit interne (9.2)
12. Revues de direction (9.3)
13. Non-conformités, actions correctives et résultats (10.1)

PECB

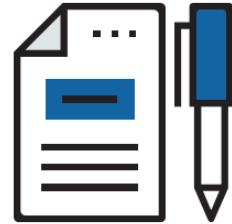
14

Exemple de procédures qui peuvent être incluses dans un SMSI documenté:

- Marquage des informations (A.8.2.2)
- Manipulation des actifs (A.8.2.3)
- Gestion des supports amovibles (A.8.3.1)
- Mise au rebut des supports (A.8.3.2)
- Sécuriser les procédures de connexion (A.9.4.2)
- Travail dans les zones sécurisées (A.11.1.5)
- Procédures d'exploitation documentées (A.12.1.1)
- Installation de logiciels sur des systèmes en exploitation (A.12.5.1)
- Politiques et procédures de transfert de l'information (A.13.2.1)
- Procédures de contrôle des changements de système (A.14.2.2)
- Gestion des incidents liés à la sécurité de l'information et améliorations (A.16.1)
- Collecte de preuves (A.16.1.7)
- Mise en œuvre de la continuité de la sécurité de l'information (A.17.1.2)
- Droits de propriété intellectuelle (A.18.1.2)

2.1.5 Définir les enregistrements

- La définition des processus et des mesures de sécurité exige la création d'une liste des enregistrements associés.
- Lors de la description des processus et mesures, il convient de se pencher sur le management des enregistrements.
- Lors de la rédaction des procédures, il convient de créer les formulaires et autres supports destinés à collecter et à conserver les enregistrements.



Questions ?

PECB

16

Section 15

Mise en œuvre des mesures de sécurité

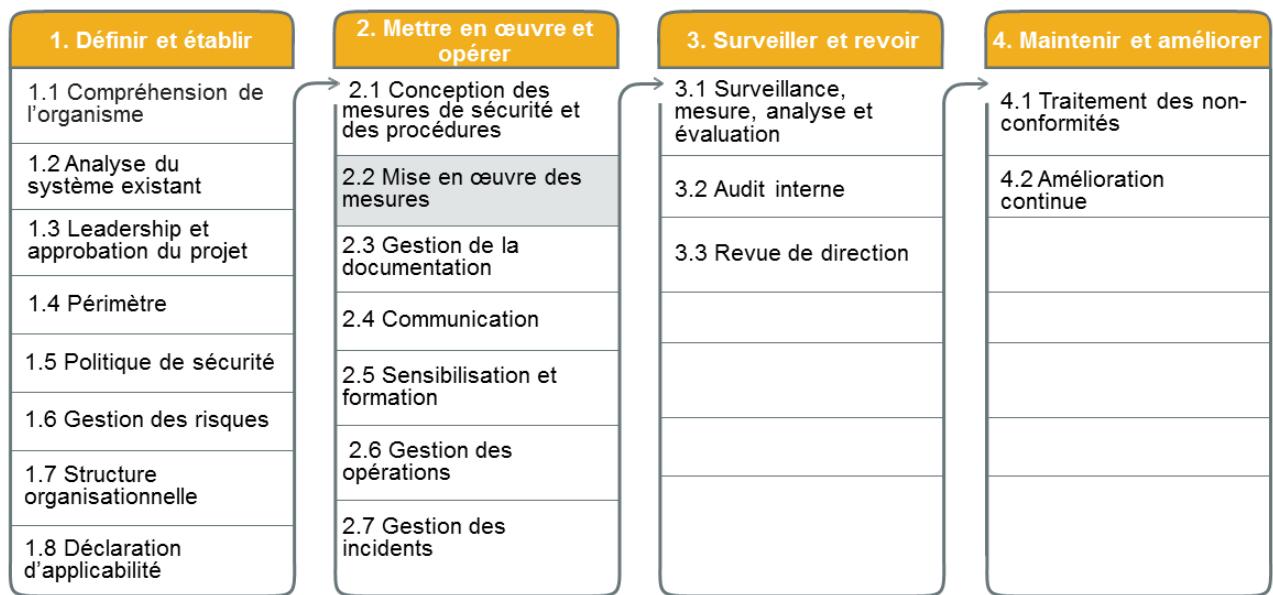
- Mise en œuvre des processus et des mesures de sécurité
- Introduction des mesures de l'Annexe A

PECB

17

La présente section aidera le participant à acquérir des connaissances sur la mise en œuvre des processus et des mesures de sécurité. Elle présente également les mesures de l'Annexe A.

2.2 Mise en œuvre des mesures



PECB

18

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

19

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

- Mettre en œuvre les mesures de sécurité détaillées dans le plan de traitement des risques et celles qui ont été déclarées applicables dans la déclaration d'applicabilité.

ISO/IEC27003, article 8.1 Planification et contrôle opérationnels

Les processus de conformité aux exigences de sécurité de l'information comprennent:

- a. les processus SMSI (par exemple: revue de direction, audit interne); et
- b. les processus requis pour la mise en œuvre du plan de traitement des risques liés à la sécurité de l'information.

La mise en œuvre des plans entraîne des processus exploités et contrôlés.

Ultimement, l'organisme est responsable de la planification et du contrôle de tout processus externalisé afin d'atteindre ses objectifs en matière de sécurité de l'information. Ainsi, l'organisme doit:

- c.déterminer les processus externalisés en tenant compte des risques de sécurité de l'information liés à la sous-traitance; et
- d.s'assurer que les processus externalisés sont contrôlés (c'est-à-dire planifiés, surveillés et examinés) de manière à garantir qu'ils fonctionnent comme prévu (en tenant compte des objectifs de sécurité de l'information et du plan de traitement des risques de sécurité de l'information).

Si une partie des fonctions ou des processus de l'organisme est externalisée aux fournisseurs, l'organisme devrait:

- q.déterminer toutes les relations de sous-traitance;
- r.établir des interfaces appropriées avec les fournisseurs;
- s.aborder les questions liées à la sécurité de l'information dans les accords avec les fournisseurs;
- t.surveiller et réviser les services du fournisseur afin de s'assurer qu'ils sont exploités comme prévu et que les risques de sécurité des informations sont en accord avec les critères de l'organisme; et
- u.gérer les changements apportés aux services du fournisseur si nécessaire.

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'appreciation des risques de sécurité de l'information.*

Traitement des risques de sécurité de l'information

- *L'organisation 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.*

PECB

20

ISO/IEC27003, article 8.2 Appréciation des risques de sécurité de l'information

Lignes directrices

Les organismes devraient avoir un plan pour effectuer des appréciations des risques de sécurité de l'information planifiées.

Lors de modifications importantes du SMSI (ou de son contexte) ou lors d'incidents de sécurité de l'information, l'organisme devrait déterminer:

- a. lesquels de ces changements ou incidents nécessitent une appréciation des risques de sécurité de l'information supplémentaire; et*
- b. comment ces appréciations seront générées.*

Le niveau de détail de l'identification des risques devrait être affiné étape par étape dans d'autres itérations de l'appreciation des risques de sécurité de l'information dans le contexte de l'amélioration continue du SMSI. Une appréciation des risques de sécurité de l'information générale devrait être effectuée au moins une fois par an.

ISO/IEC 27003, article8.3 Traitement des risques de sécurité de l'information

Explication

Afin de traiter les risques de sécurité de l'information, l'organisme doit exécuter le processus de traitement des risques de sécurité de l'information défini à l'article6.1.3. Pendant l'opération du SMSI, chaque fois que l'appreciation des risques est mise à jour conformément l'article8.2, l'organisme applique le traitement des risques selon l'article6.1.3 et met à jour le plan de traitement des risques. Le plan de traitement des risques mis à jour est de nouveau mis en œuvre.

Les résultats du traitement des risques de sécurité de l'information sont conservés dans l'information documentée comme preuve que le processus décrit à l'article6.1.3 a été exécuté tel que défini.

Lignes directrices

Le processus de traitement des risques devrait être effectué après chaque itération du processus d'appreciation des risques de sécurité de l'information de l'article8.2 ou lorsque la mise en œuvre du plan de traitement des

risques ou de certaines parties de celui-ci échoue.

L'avancement de la mise en œuvre du plan de traitement des risques de sécurité de l'information devrait être orienté et surveillé par cette activité.

2.2 Mise en œuvre des mesures

Liste des activités

2.2.1

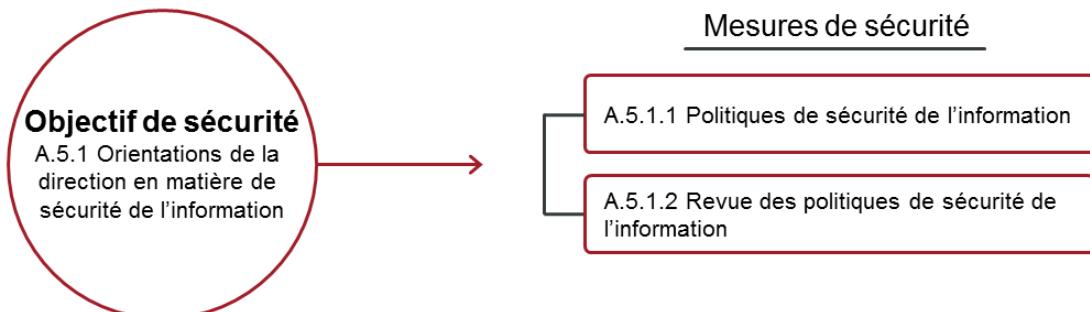
Sélection des mesures de sécurité appropriées

PECB

21

Orientations de la direction en matière de sécurité de l'information

ISO/IEC 27001, A.5.1



PECB

22

A.5.1 Orientations de la direction en matière de sécurité de l'information

Objectif: Apporter à la sécurité de l'information une orientation et un soutien de la part de la direction, conformément aux exigences de l'entreprise et aux lois et règlements en vigueur.

A.5.1.1 Politiques de sécurité de l'information

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.

A.5.1.2 Revue des politiques de sécurité de l'information

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.

Organisation interne

ISO/IEC 27001, A.6.1



Mesures de sécurité

- A.6.1.1 Fonctions et responsabilités liées à la sécurité de l'information
- A.6.1.2 Séparation des tâches
- A.6.1.3 Relations avec les autorités
- A.6.1.4 Relations avec des groupes de travail spécialisés
- A.6.1.5 Sécurité de l'information dans la gestion de projet

PECB

23

A.6.1 Organisation interne

Objectif: Établir un cadre de management pour lancer et vérifier la mise en place et le fonctionnement opérationnel de la sécurité de l'information au sein de l'organisation.

A.6.1.1 Fonctions et responsabilités liées à la sécurité de l'information

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

A.6.1.2 Séparation des tâches

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.

A.6.1.3 Relations avec les autorités

Des relations appropriées avec les autorités compétentes doivent être entretenues.

A.6.1.4 Relations avec des groupes de travail spécialisés

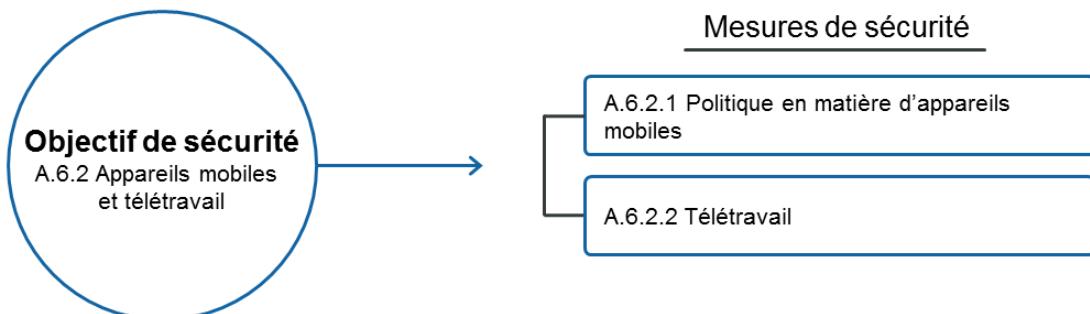
Des relations appropriées avec des groupes d'intérêt, des forums spécialisés dans la sécurité et des associations professionnelles doivent être entretenues.

A.6.1.5 La sécurité de l'information dans la gestion de projet

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

Appareils mobiles et télétravail

ISO/IEC 27001, A.6.2



PECB

24

A.6.2 Appareils mobiles et télétravail

Objectif: Assurer la sécurité du télétravail et de l'utilisation d'appareils mobiles.

A.6.2.1 Politique en matière d'appareils mobiles

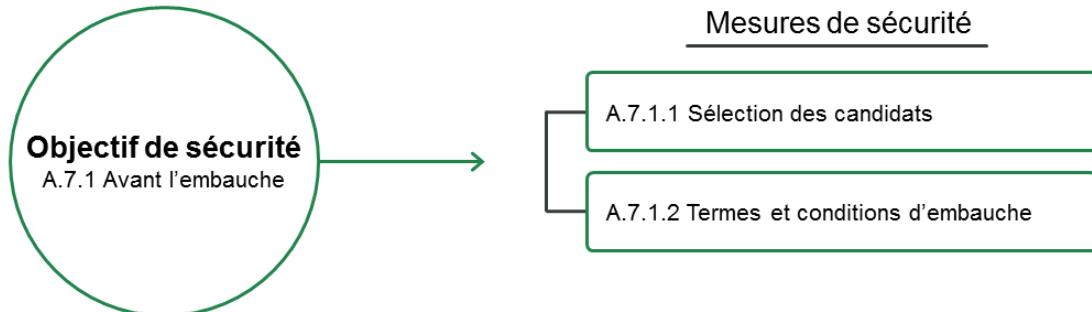
Une politique et des mesures de sécurité complémentaires doivent être adoptées pour gérer les risques découlant de l'utilisation des appareils mobiles.

A.6.2.2 Télétravail

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

Avant l'embauche

ISO/IEC 27001, A.7.1



PECB

25

A.7.1 Avant l'embauche

Objectif: S'assurer que les salariés et les sous-traitants comprennent leurs responsabilités et sont qualifiés pour les rôles qu'on envisage de leur donner.

A.7.1.1 Sélection des candidats

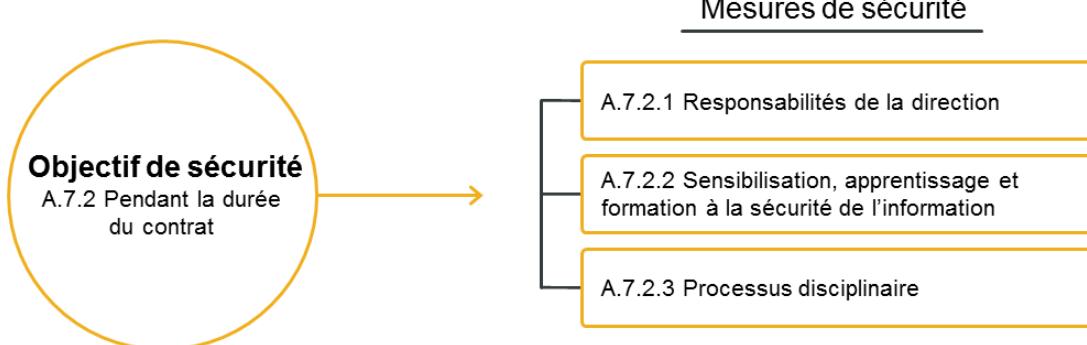
Des vérifications doivent être effectuées sur tous les candidats à l'embauche conformément aux lois, aux règlements et à l'éthique et être proportionnées aux exigences métier, à la classification des informations accessibles et aux risques identifiés.

A.7.1.2 Termes et conditions d'embauche

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.

Pendant la durée du contrat

ISO/IEC 27001, A.7.2



PECB

26

A.7.2 Pendant la durée du contrat

Objectif: S'assurer que les salariés et les sous-traitants sont conscients de leurs responsabilités en matière de sécurité de l'information et qu'ils assument ces responsabilités.

A.7.2.1 Responsabilités de la direction

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.

A.7.2.2 Sensibilisation, apprentissage et formation à la sécurité de l'information

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.

A.7.2.3 Processus disciplinaire

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.

Rupture, terme ou modification du contrat de travail

ISO/IEC 27001, A.7.3



PECB

27

A.7.3 Rupture, terme ou modification du contrat de travail

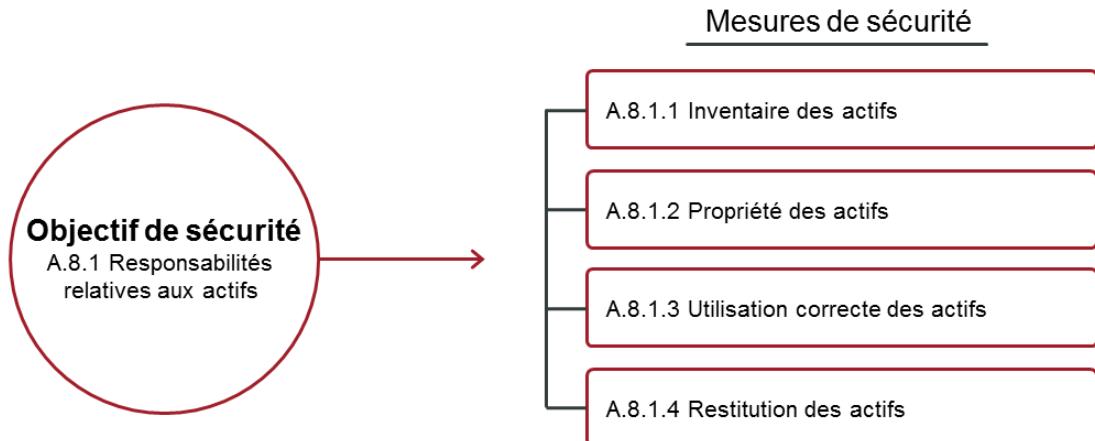
Objectif: Protéger les intérêts de l'organisation dans le cadre du processus de modification, de rupture ou de terme d'un contrat de travail.

A.7.3.1 Achèvement ou modification des responsabilités associées au contrat de travail

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.

Responsabilités relatives aux actifs

ISO/IEC 27001, A.8.1



PECB

28

A.8.1 Responsabilités relatives aux actifs

Objectif: Identifier les actifs de l'organisation et définir les responsabilités pour une protection appropriée.

A.8.1.1 Inventaire des actifs

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.

A.8.1.2 Propriété des actifs

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

A.8.1.3 Utilisation correcte des actifs

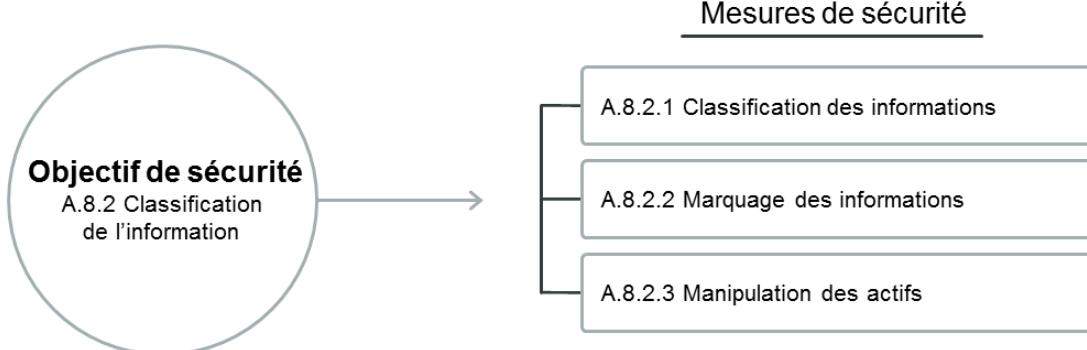
Les règles d'utilisation correcte de l'information, les actifs associés à l'information et les moyens de traitement de l'information doivent être identifiés, documentés et mis en œuvre.

A.8.1.4 Restitution des actifs

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.

Classification de l'information

ISO/IEC 27001, A.8.2



PECB

29

A.8.2 Classification de l'information

Objectif: S'assurer que l'information bénéficie d'un niveau de protection approprié et conforme à son importance pour l'organisation.

A.8.2.1 Classification des informations

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.

A.8.2.2 Marquage des informations

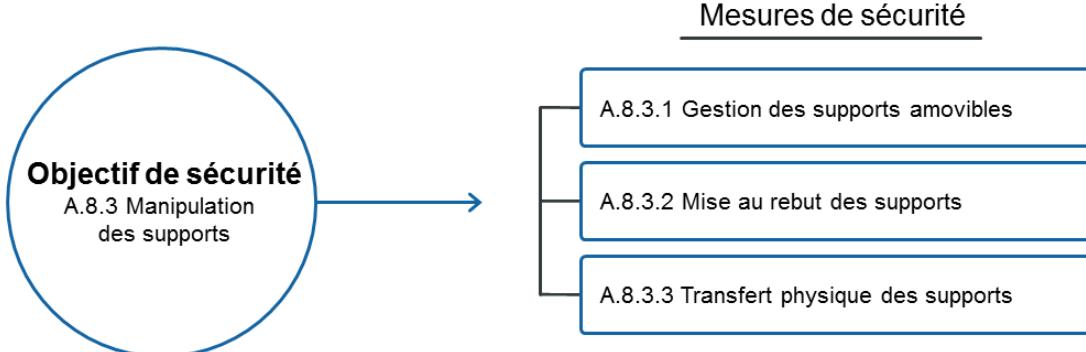
Un ensemble approprié de procédures pour le marquage de l'information doit être élaboré et mis en œuvre conformément au plan de classification adopté par l'organisation.

A.8.2.3 Manipulation des actifs

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

Manipulation des supports

ISO/IEC 27001, A.8.3



PECB

30

A.8.3 Manipulation des supports

Objectif: Empêcher la divulgation, la modification, le retrait ou la destruction non autorisé(e) de l'information de l'organisation stockée sur des supports.

A.8.3.1 Gestion des supports amovibles

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

A.8.3.2 Mise au rebut des supports

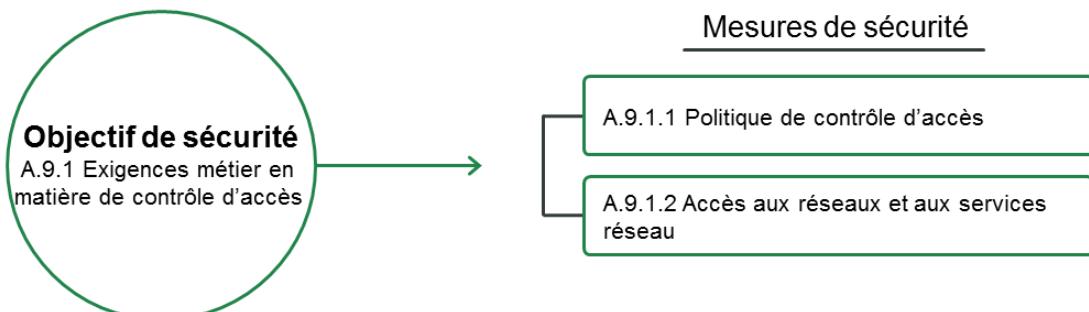
Les supports qui ne sont plus nécessaires doivent être mis au rebut de manière sécurisée en suivant des procédures formelles.

A.8.3.3 Transfert physique des supports

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

Exigences métier en matière de contrôle d'accès

ISO/IEC 27001, A.9.1



PECB

31

A.9.1 Exigences métier en matière de contrôle d'accès

Objectif: Limiter l'accès à l'information et aux moyens de traitement de l'information.

A.9.1.1 Politique de contrôle d'accès

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

A.9.1.2 Accès aux réseaux et aux services réseau

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

Gestion de l'accès utilisateur

ISO/IEC 27001, A.9.2

Mesures de sécurité



- A.9.2.1 Enregistrement et désinscription des utilisateurs
- A.9.2.2 Distribution des accès aux utilisateurs
- A.9.2.3 Gestion des droits d'accès à priviléges
- A.9.2.4 Gestion des informations secrètes d'authentification des utilisateurs
- A.9.2.5 Revue des droits d'accès utilisateurs
- A.9.2.6 Suppression ou adaptation des droits d'accès

PECB

32

A.9.2 Gestion de l'accès utilisateur

Objectif: Maîtriser l'accès utilisateur par le biais d'autorisations et empêcher les accès non autorisés aux systèmes et services d'information.

A.9.2.1 Enregistrement et désinscription des utilisateurs

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

A.9.2.2 Distribution des accès aux utilisateurs

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.

A.9.2.3 Gestion des droits d'accès à priviléges

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

A.9.2.4 Gestion des informations secrètes d'authentification des utilisateurs

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

A.9.2.5 Revue des droits d'accès utilisateurs

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

A.9.2.6 Suppression ou adaptation des droits d'accès

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.

Responsabilités des utilisateurs

ISO/IEC 27001, A.9.3



PECB

33

A.9.3 Responsabilités des utilisateurs

Objectif: Rendre les utilisateurs responsables de la protection de leurs informations d'authentification.

A.9.3.1 Utilisation d'informations secrètes d'authentification

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

Contrôle de l'accès au système et à l'information

ISO/IEC 27001, A.9.4

Mesures de sécurité



- A.9.4.1 Restriction d'accès à l'information
- A.9.4.2 Sécuriser les procédures de connexion
- A.9.4.3 Système de gestion des mots de passe
- A.9.4.4 Utilisation de programmes utilitaires à priviléges
- A.9.4.5 Contrôle d'accès au code source des programmes

PECB

34

A.9.4 Contrôle de l'accès au système et à l'information

Objectif: Empêcher les accès non autorisés aux systèmes et aux applications.

A.9.4.1 Restriction d'accès à l'information

L'accès à l'information et aux fonctions d'application système doit être restreint conformément à la politique de contrôle d'accès.

A.9.4.2 Sécuriser les procédures de connexion

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.

A.9.4.3 Système de gestion des mots de passe

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

A.9.4.4 Utilisation de programmes utilitaires à priviléges

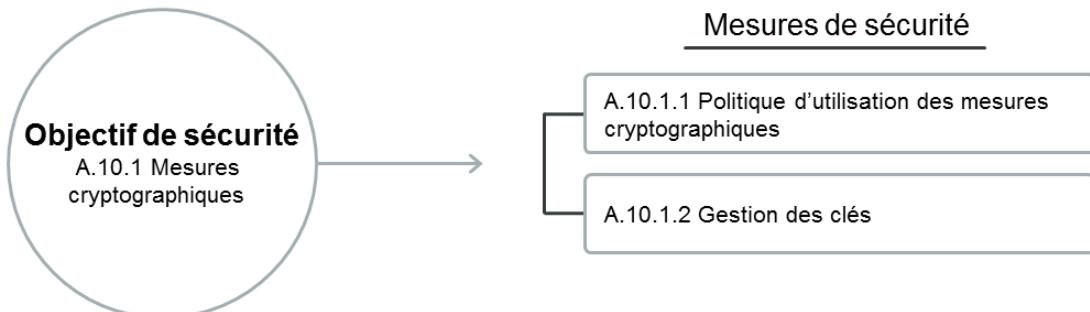
L'utilisation des programmes utilitaires permettant de contourner les mesures de sécurité d'un système ou d'une application doit être limitée et étroitement contrôlée.

A.9.4.5 Contrôle d'accès au code source des programmes

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

Mesures cryptographiques

ISO/IEC 27001, A.10.1



PECB

35

A.10.1 Mesures cryptographiques

Objectif: Garantir l'utilisation correcte et efficace de la cryptographie en vue de protéger la confidentialité, l'authenticité et/ou l'intégrité de l'information.

A.10.1.1 Politique d'utilisation des mesures cryptographiques

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

A.10.1.2 Gestion des clés

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.

Zones sécurisées

ISO/IEC 27001, A.11.1

Mesures de sécurité



- A.11.1.1 Périmètre de sécurité physique
- A.11.1.2 Contrôle d'accès physique
- A.11.1.3 Sécurisation des bureaux, des salles et des équipements
- A.11.1.4 Protection contre les menaces extérieures et environnementales
- A.11.1.5 Travail dans les zones sécurisées
- A.11.1.6 Zones de livraison et de chargement

PECB

36

11.1 Zones sécurisées

Objectif: Empêcher tout accès physique non autorisé, tout dommage ou intrusion portant sur l'information et les moyens de traitement de l'information de l'organisme.

A.11.1.1 Périmètre de sécurité physique

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.

A.11.1.2 Contrôle d'accès physique

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

A.11.1.3 Sécurisation des bureaux, des salles et des équipements

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

A.11.1.4 Protection contre les menaces extérieures et environnementales

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

A.11.1.5 Travail dans les zones sécurisées

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

A.11.1.6 Zones de livraison et de chargement

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.

Matériels

ISO/IEC 27001, A.11.2

Mesures de sécurité

- A.11.2.1 Emplacement et protection des matériels
- A.11.2.2 Services généraux
- A.11.2.3 Sécurité du câblage
- A.11.2.4 Maintenance des matériels

Objectif de sécurité A.11.2 Matériels

Mesures de sécurité

- A.11.2.5 Sortie des actifs
- A.11.2.6 Sécurité des matériels et des actifs hors des locaux
- A.11.2.7 Mise au rebut ou recyclage sécurisé(e) des matériels
- A.11.2.8 Matériels utilisateur laissés sans surveillance
- A.11.2.9 Politique du bureau propre et de l'écran verrouillé

PECB

37

A.11.2. Matériels

Objectif: Empêcher la perte, l'endommagement, le vol ou la compromission des actifs et l'interruption des activités de l'organisation.

A.11.2.1. Emplacement et protection des matériels

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.

A.11.2.2. Services généraux

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

A.11.2.3. Sécurité du câblage

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

A.11.2.4. Maintenance des matériels

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

A.11.2.5. Sortie des actifs

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

A.11.2.6. Sécurité des matériels et des actifs hors des locaux

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.

A.11.2.7 Mise au rebut ou recyclage sécurisé(e) des matériels

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.

A.11.2.8 Matériels utilisateur laissés sans surveillance

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

A.11.2.9 Politique du bureau propre et de l'écran verrouillé

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.

Procédures et responsabilités liées à l'exploitation

ISO/IEC 27001, A.12.1



Mesures de sécurité

A.12.1.1 Procédures d'exploitation documentées

A.12.1.2 Gestion des changements

A.12.1.3 Dimensionnement

A.12.1.4 Séparation des environnements de développement, de test et d'exploitation

PECB

38

A.12.1 Procédures et responsabilités liées à l'exploitation

Objectif: Assurer l'exploitation correcte et sécurisée des moyens de traitement de l'information.

A.12.1.1 Procédures d'exploitation documentées

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

A.12.1.2 Gestion des changements

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

A.12.1.3 Dimensionnement

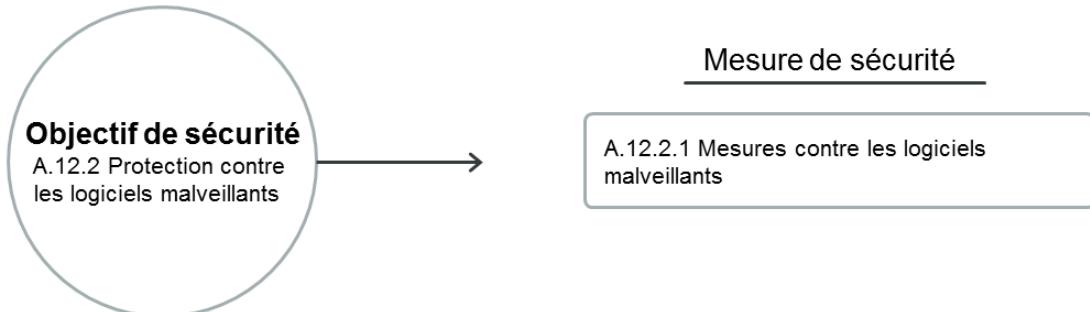
L'utilisation des ressources doit être surveillée et ajustée et des projections sur les dimensionnements futurs doivent être effectuées pour garantir les performances exigées du système.

A.12.1.4 Séparation des environnements de développement, de test et d'exploitation

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.

Protection contre les logiciels malveillants

ISO/IEC 27001, A.12.2



PECB

39

A.12.2 Protection contre les logiciels malveillants

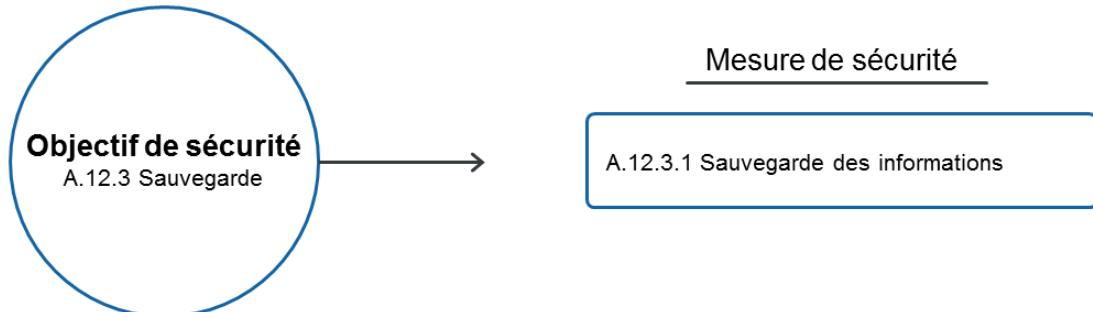
Objectif: S'assurer que l'information et les moyens de traitement de l'information soient protégés contre les logiciels malveillants.

A.12.2.1 Mesures contre les logiciels malveillants

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.

Sauvegarde

ISO/IEC 27001, A.12.3



PECB

40

A.12.3 Sauvegarde

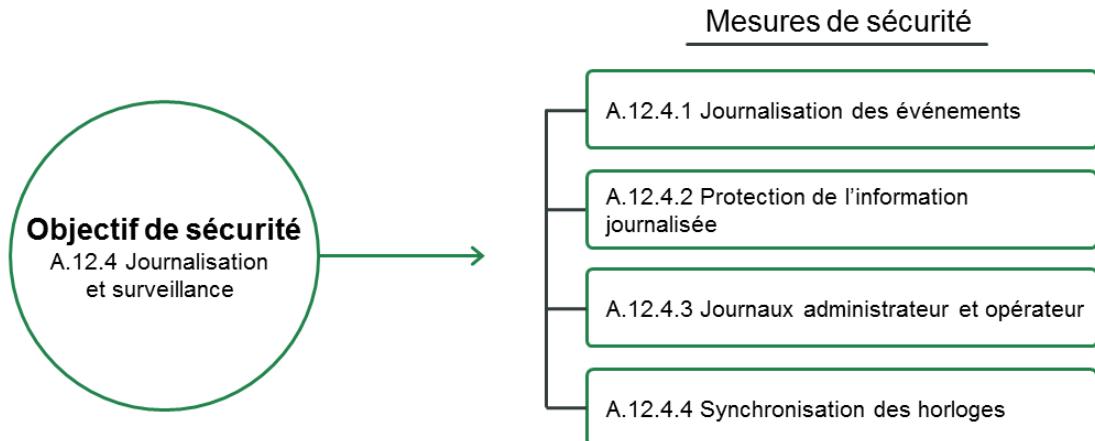
Objectif: Se protéger de la perte de données.

A.12.3.1 Sauvegarde des informations

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.

Journalisation et surveillance

ISO/IEC 27001, A.12.4



PECB

41

A.12.4 Journalisation et surveillance

Objectif: Enregistrer les événements et générer des preuves.

A.12.4.1 Journalisation des événements

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.

A.12.4.2 Protection de l'information journalisée

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

A.12.4.3 Journaux administrateur et opérateur

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

A.12.4.4 Synchronisation des horloges

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.

Maîtrise des logiciels en exploitation

ISO/IEC 27001, A.12.5



PECB

42

A.12.5 Maîtrise des logiciels en exploitation

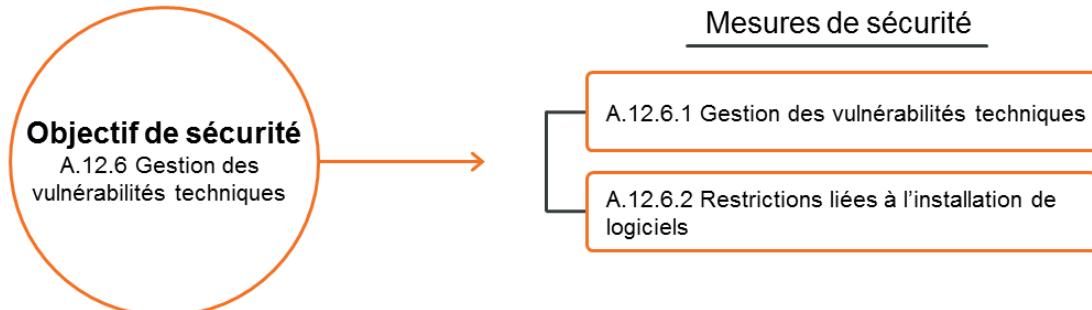
Objectif: Garantir l'intégrité des systèmes en exploitation.

A.12.5.1 Installation de logiciels sur des systèmes en exploitation

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

Gestion des vulnérabilités techniques

ISO/IEC 27001, A.12.6



PECB

43

A.12.6 Gestion des vulnérabilités techniques

Objectif: Empêcher toute exploitation des vulnérabilités techniques.

A.12.6.1 Gestion des vulnérabilités techniques

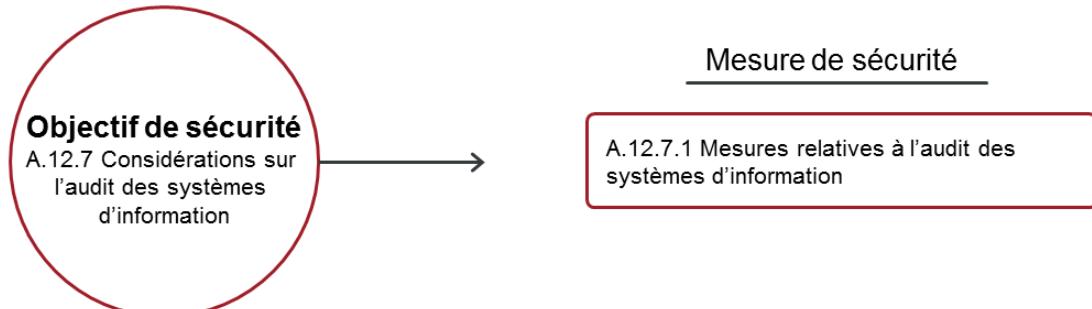
Des informations sur les vulnérabilités techniques des systèmes d'information en exploitation doivent être obtenues en temps opportun, l'exposition de l'organisation à ces vulnérabilités doit être évaluée et les mesures appropriées doivent être prises pour traiter le risque associé.

A.12.6.2 Restrictions liées à l'installation de logiciels

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

Considérations sur l'audit des systèmes d'information

ISO/IEC 27001, A.12.7



PECB

44

A.12.7 Considérations sur l'audit des systèmes d'information

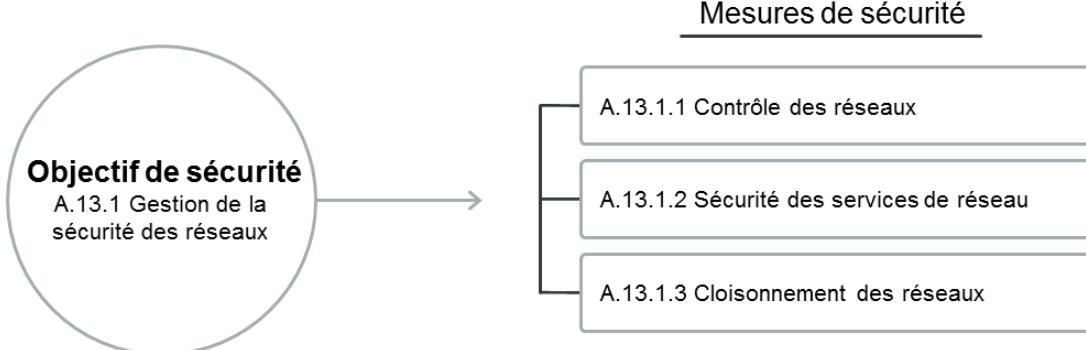
Objectif: Réduire au minimum l'impact des activités d'audit sur les systèmes en exploitation.

A.12.7.1 Mesures relatives à l'audit des systèmes d'information

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.

Gestion de la sécurité des réseaux

ISO/IEC 27001, A.13.1



PECB

45

A.13.1 Gestion de la sécurité des réseaux

Objectif: Garantir la protection de l'information sur les réseaux et des moyens de traitement de l'information sur lesquels elle s'appuie.

A.13.1.1 Contrôle des réseaux

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

A.13.1.2 Sécurité des services de réseau

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.

A.13.1.3 Cloisonnement des réseaux

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

Transfert de l'information

ISO/IEC 27001, A.13.2



Mesures de sécurité

- A.13.2.1 Politiques et procédures de transfert de l'information
- A.13.2.2 Accords en matière de transfert d'information
- A.13.2.3 Messagerie électronique
- A.13.2.4 Engagements de confidentialité ou de non-divulgation

PECB

46

A.13.2 Transfert de l'information

Objectif: Maintenir la sécurité de l'information transférée au sein de l'organisme et vers une entité extérieure.

A.13.2.1 Politiques et procédures de transfert de l'information

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.

A.13.2.2 Accords en matière de transfert d'information

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

A.13.2.3 Messagerie électronique

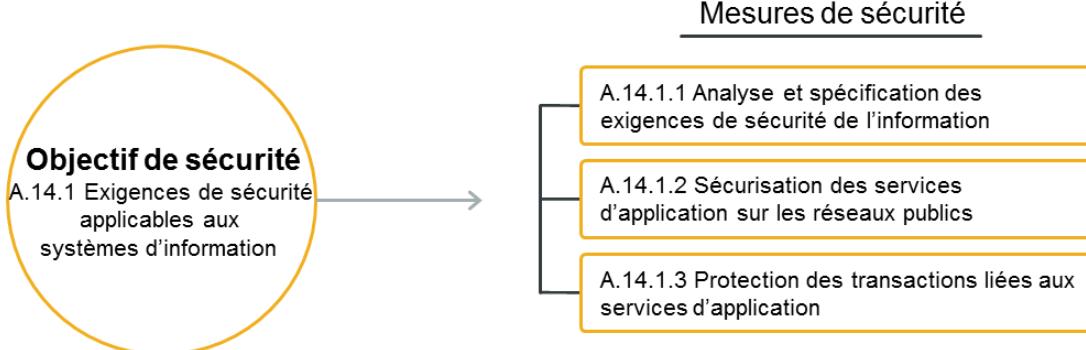
L'information transitant par la messagerie électronique doit être protégée de manière appropriée.

A.13.2.4 Engagements de confidentialité ou de non-divulgation

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.

Exigences de sécurité applicables aux systèmes d'information

ISO/IEC 27001, A.14.1



PECB

47

A.14.1 Exigences de sécurité applicables aux systèmes d'information

Objectif: Veiller à ce que la sécurité de l'information fasse partie intégrante des systèmes d'information tout au long de leur cycle de vie. Cela inclut également des exigences pour les systèmes d'information fournissant des services sur les réseaux publics.

A.14.1.1 Analyse et spécification des exigences de sécurité de l'information

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.

A.14.1.2 Sécurisation des services d'application sur les réseaux publics

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.

A.14.1.3 Protection des transactions liées aux services d'application

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.

Sécurité des processus de développement et d'assistance technique

ISO/IEC 27001, A.14.2

Mesures de sécurité

A.14.2.1 Politique de développement sécurisé

A.14.2.2 Procédures de contrôle des changements de système

A.14.2.3 Revue technique des applications après changement apporté à la plateforme d'exploitation

A.14.2.4 Restrictions relatives aux changements apportés aux progiciels

Objectif de sécurité

A.14.2 Sécurité des processus de développement et d'assistance technique

Mesures de sécurité

A.14.2.5 Principes d'ingénierie de la sécurité des systèmes

A.14.2.6 Environnement de développement sécurisé

A.14.2.7 Développement externalisé

A.14.2.8 Test de la sécurité du système

A.14.2.9 Test de conformité du système

PECB

48

A.14.2 Sécurité des processus de développement et d'assistance technique

Objectif: S'assurer que les questions de sécurité de l'information soient étudiées et mises en œuvre dans le cadre du cycle de développement des systèmes d'information.

A.14.2.1 Politique de développement sécurisé

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

A.14.2.2 Procédures de contrôle des changements de système

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

A.14.2.3 Revue technique des applications après changement apporté à la plateforme d'exploitation

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.

A.14.2.4 Restrictions relatives aux changements apportés aux progiciels

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

A.14.2.5 Principes d'ingénierie de la sécurité des systèmes

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.

A.14.2.6 Environnement de développement sécurisé

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.

A.14.2.7 Développement externalisé

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

A.14.2.8 Test de la sécurité du système

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

A.14.2.9 Test de conformité du système

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.

Données de test

ISO/IEC 27001, A.14.3



PECB

49

A.14.3 Données de test

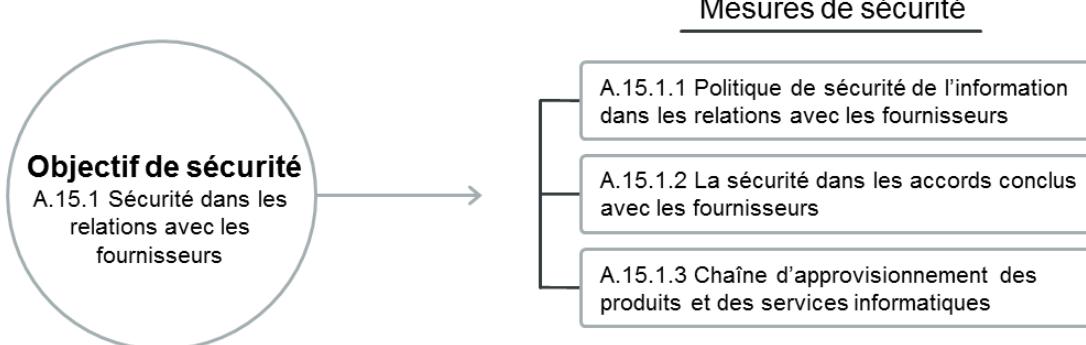
Objectif: Garantir la protection des données utilisées pour les tests.

A.14.3.1 Protection des données de test

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

Sécurité dans les relations avec les fournisseurs

ISO/IEC 27001, A.15.1



PECB

50

A.15.1 Sécurité dans les relations avec les fournisseurs

Objectif: Garantir la protection des actifs de l'organisation accessible aux fournisseurs.

A.15.1.1 Politique de sécurité de l'information dans les relations avec les fournisseurs

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.

A.15.1.2 La sécurité dans les accords conclus avec les fournisseurs

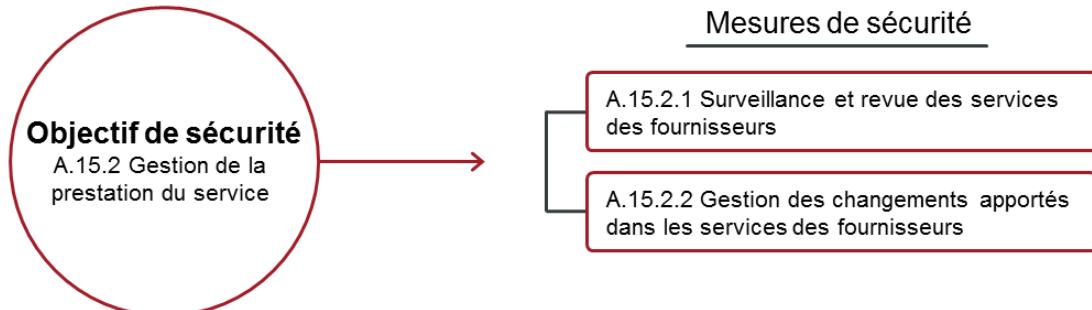
Les exigences applicables liées à la sécurité de l'information doivent être établies et convenues avec chaque fournisseur pouvant accéder, traiter, stocker, communiquer ou fournir des composants de l'infrastructure informatique destinés à l'information de l'organisation.

A.15.1.3 Chaîne d'approvisionnement des produits et des services informatiques

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.

Gestion de la prestation du service

ISO/IEC 27001, A.15.2



PECB

51

A.15.2 Gestion de la prestation du service

Objectif: Maintenir le niveau convenu de sécurité de l'information et de service conforme aux accords conclus avec les fournisseurs.

A.15.2.1 Surveillance et revue des services des fournisseurs

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

A.15.2.2 Gestion des changements apportés dans les services des fournisseurs

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.

Gestion des incidents liés à la sécurité de l'information et améliorations

ISO/IEC 27001, A.16.1

Mesures de sécurité

A.16.1.1 Responsabilités et procédures

A.16.1.2 Signalement des événements liés à la sécurité de l'information

A.16.1.3 Signalement des failles liées à la sécurité de l'information

Objectif de sécurité

A.16.1 Gestion des incidents liés à la sécurité de l'information et améliorations

Mesures de sécurité

A.16.1.4 Appréciation des événements liés à la sécurité de l'information et prise de décision

A.16.1.5 Réponse aux incidents liés à la sécurité de l'information

A.16.1.6 Tirer des enseignements des incidents liés à la sécurité de l'information

A.16.1.7 Collecte de preuves

PECB

52

A.16.1 Gestion des incidents liés à la sécurité de l'information et améliorations

Objectif: Garantir une méthode cohérente et efficace de gestion des incidents liés à la sécurité de l'information, incluant la communication des événements et des failles liés à la sécurité.

A.16.1.1 Responsabilités et procédures

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.

A.16.1.2 Signalement des événements liés à la sécurité de l'information

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

A.16.1.3 Signalement des failles liées à la sécurité de l'information

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.

A.16.1.4 Appréciation des événements liés à la sécurité de l'information et prise de décision

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.

A.16.1.5 Réponse aux incidents liés à la sécurité de l'information

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

A.16.1.6 Tirer des enseignements des incidents liés à la sécurité de l'information

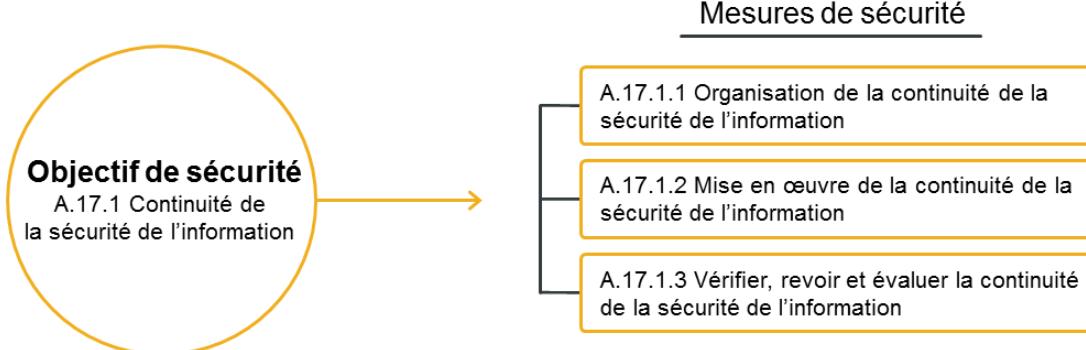
Les connaissances recueillies suite à l'analyse et la résolution d'incidents doivent être utilisées pour réduire la probabilité ou l'impact d'incidents ultérieurs.

A.16.1.7 Collecte de preuves

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

Continuité de la sécurité de l'information

ISO/IEC 27001, A.17.1



PECB

53

A.17.1 Continuité de la sécurité de l'information

Objectif: La continuité de la sécurité de l'information doit faire partie intégrante de la gestion de la continuité de l'activité.

A.17.1.1 Organisation de la continuité de la sécurité de l'information

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

A.17.1.2 Mise en œuvre de la continuité de sécurité de l'information

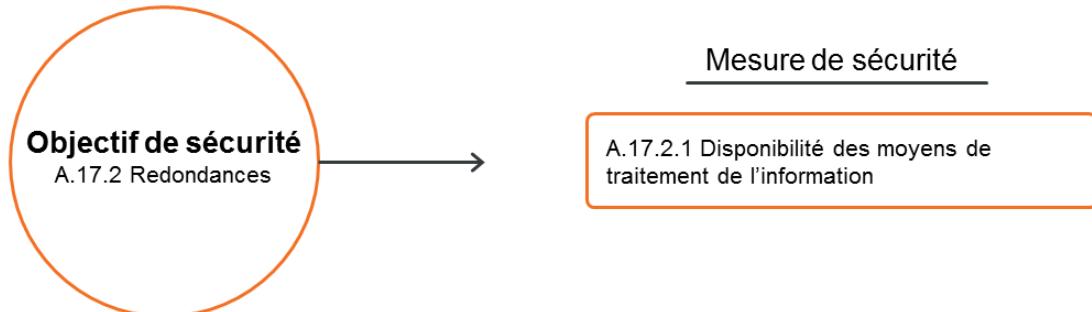
L'organisation doit établir, documenter, mettre en œuvre et tenir à jour des processus, des procédures et des mesures permettant de fournir le niveau requis de continuité de sécurité de l'information au cours d'une situation défavorable.

A.17.1.3 Vérifier, revoir et évaluer la continuité de la sécurité de l'information

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.

Redondances

ISO/IEC 27001, A.17.2



PECB

54

A.17.2 Redondances

Objectif: Garantir la disponibilité des moyens de traitement de l'information.

A.17.2.1 Disponibilité des moyens de traitement de l'information

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

Conformité aux obligations légales et réglementaires

ISO/IEC 27001, A.18.1



Mesures de sécurité

- A.18.1.1 Identification de la législation et des exigences contractuelles applicables
- A.18.1.2 Droits de propriété intellectuelle
- A.18.1.3 Protection des enregistrements
- A.18.1.4 Protection de la vie privée et protection des données à caractère personnel
- A.18.1.5 Réglementation relative aux mesures cryptographiques

PECB

55

A.18.1 Conformité aux obligations légales et réglementaires

Objectif: Éviter toute violation des obligations légales, statutaires, réglementaires ou contractuelles relatives à la sécurité de l'information, éviter toute violation des exigences de sécurité.

A.18.1.1 Identification de la législation et des exigences contractuelles applicables

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.

A.18.1.2 Droits de propriété intellectuelle

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.

A.18.1.3 Protection des enregistrements

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.

A.18.1.4 Protection de la vie privée et protection des données à caractère personnel

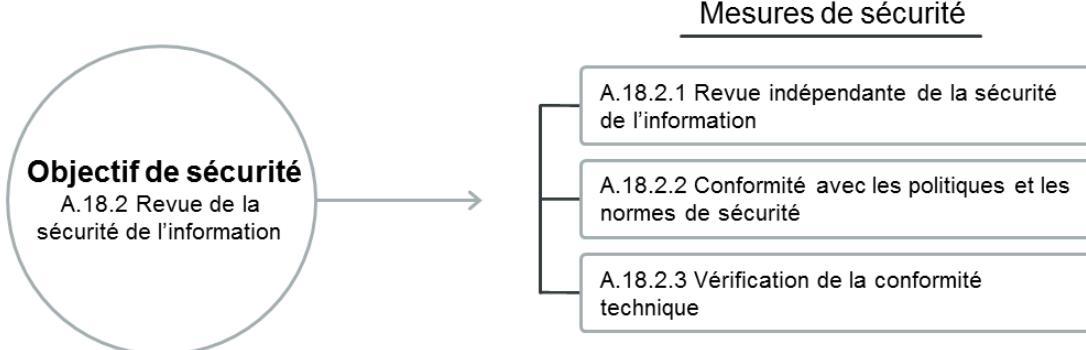
La protection de la vie privée et la protection des données à caractère personnel doivent être garanties telles que l'exigent la législation ou les réglementations applicables, et les clauses contractuelles le cas échéant.

A.18.1.5 Réglementation relative aux mesures cryptographiques

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

Revue de la sécurité de l'information

ISO/IEC 27001, A.18.2



PECB

56

A.18.2 Revue de la sécurité de l'information

Objectif: Garantir que la sécurité de l'information est mise en œuvre et appliquée conformément aux politiques et procédures organisationnelles.

A.18.2.1 Revue indépendante de la sécurité de l'information

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.

A.18.2.2 Conformité avec les politiques et les normes de sécurité

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.

A.18.2.3 Vérification de la conformité technique

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.

Exercice 8

PECB

57

Exercice8: Mesures de sécurité

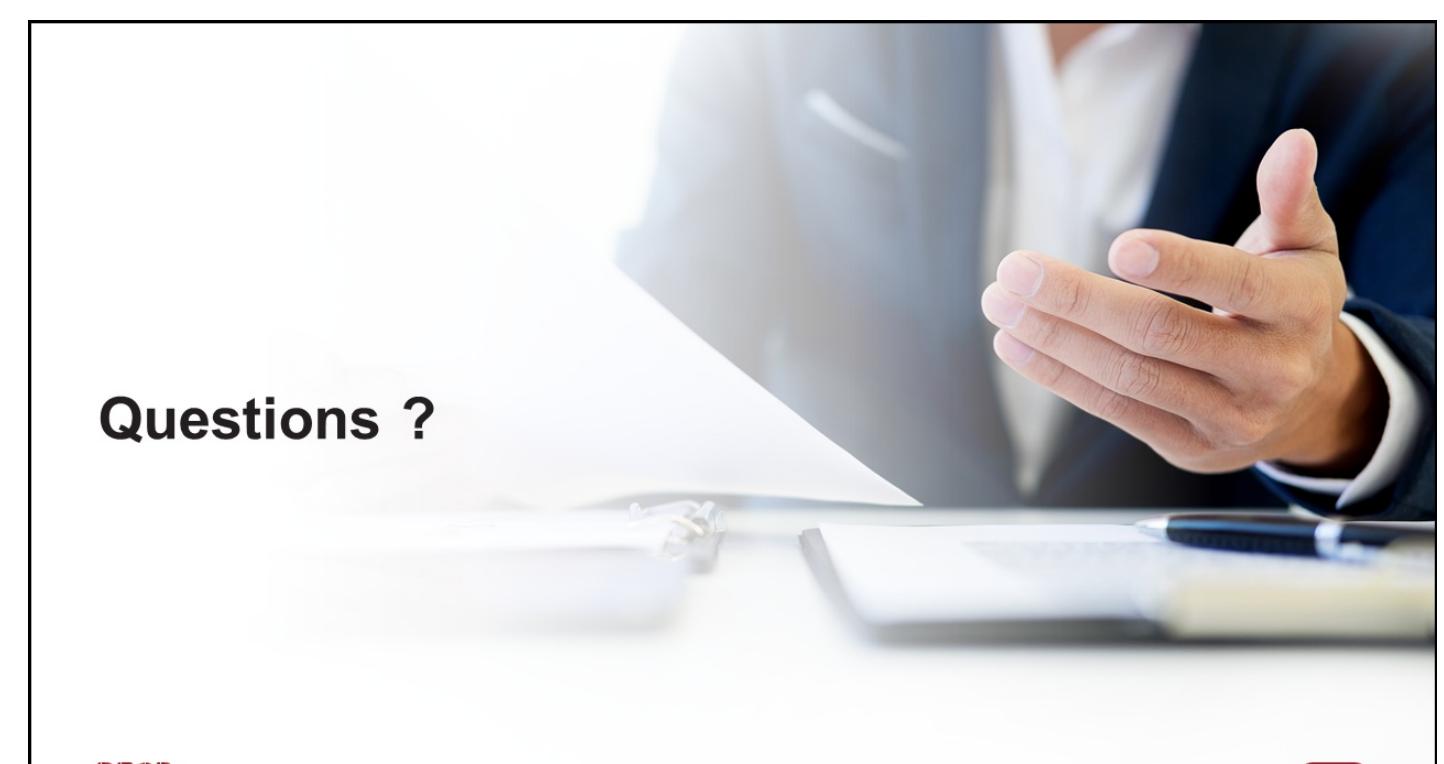
Pour chacun des articles suivants de la norme ISO/IEC27001 ou de son Annexe, définissez un plan d'action accompagné d'au moins deux actions concrètes qui permettraient d'assurer la conformité à l'article concerné et de satisfaire aux objectifs.

Exemple: Sécurité du câblage (MesureA.11.2.3)

- Utilisation de gaines de câblage réseau pour isoler et protéger de l'interception les communications réseau de l'organisation.
 - Liste documentée du matériel de câblage autorisé pour éviter l'utilisation de matériel non conforme.
1. Déterminer les compétences nécessaires de la ou des personnes effectuant, sous son contrôle, un travail qui a une incidence sur les performances de la sécurité de l'information (Article7.2 a)
 2. Réagir à la non-conformité (Article10.1 a)
 3. Dimensionnement (MesureA.12.1.3)
 4. Mesures contre les logiciels malveillants (MesureA.12.2.1)
 5. Messagerie électronique (MesureA.13.2.3)

Durée de l'exercice: 30 minutes

Commentaires: 15 minutes



Questions ?

PECB

58

Section 16

Définition du processus de gestion de documents

- Valeur et types de documents
- Création de modèles
- Gestion de documents
- Mise en œuvre d'un système de gestion de documents
- Gestion des enregistrements
- Liste maîtresse des documents

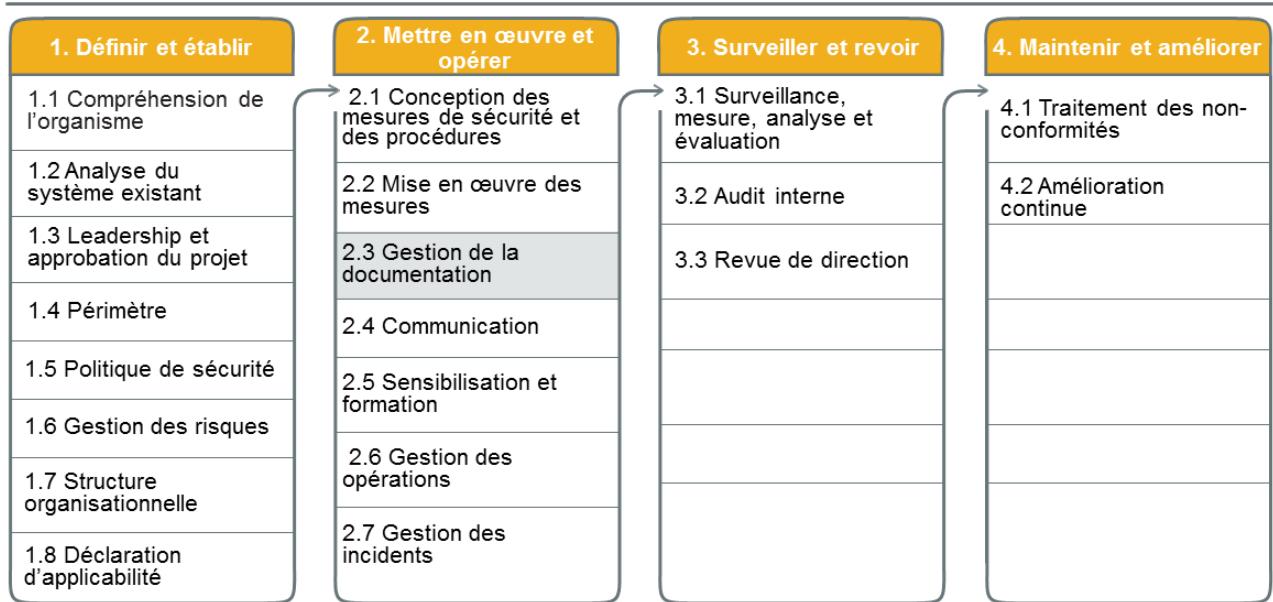
PECB

59



La présente section aidera le participant à acquérir des connaissances sur la définition du processus de gestion de documents, y compris la valeur et les types de documentation, la création de modèles, la gestion des documents et des enregistrements, la mise en œuvre d'un système de gestion de documents et la liste de référence des documents.

2.3 Gestion de la documentation



PECB

60

Le travail accompli au cours de cette étape permettra à l'organisation d'élaborer et de tenir à jour la documentation nécessaire pour assurer un système de management efficace et adapté aux besoins spécifiques de l'organisation. Il assurera également le contrôle et le caractère approprié de la documentation et des dossiers du SMSI.

ISO/IEC 27001 Exigences

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

61

La cohérence entre les documents principaux du SMSI est importante. L'organisme doit démontrer par la documentation que ses mesures de sécurité sont mises en œuvre selon les scénarios de risque identifiés dans l'appréciation des risques.

La documentation doit être développée de façon à être suffisante et appropriée dans le contexte particulier de l'organisme.

Page de notes

PECB

62

ISO/IEC27003, article 7.5.1 Généralités

Explication

Des informations documentées sont nécessaires pour définir et communiquer les objectifs, politiques, lignes directrices, instructions, mesures, processus, procédures liés à la sécurité de l'information ainsi que ce que les individus ou groupes d'individus sont censés faire et comment ils sont censés se comporter. Des informations documentées sont également nécessaires pour les audits du SMSI et pour maintenir un SMSI stable lorsque les personnes dans les rôles clés changent. En outre, les informations documentées sont nécessaires pour enregistrer les actions, les décisions et les résultats des processus et des mesures de sécurité du SMSI.

Lignes directrices

Voici des exemples d'informations documentées qui peuvent être considérées par l'organisation comme nécessaires pour assurer l'efficacité de son SMSI:

- les résultats de la définition du contexte (voir l'article4);
- les rôles, responsabilités et autorités (voir l'article5);
- les rapports sur les différentes phases de la gestion des risques (voir l'article6);
- les ressources déterminées et fournies (voir l'article7.1);
- la compétence attendue (voir l'article7.2);
- les plans et les résultats des actions de sensibilisation (voir l'article7.3);
- les plans et les résultats des actions de communication (voir l'article7.4);
- les informations documentées d'origine externe qui sont nécessaires pour le SMSI (voir l'article7.5.3);
- les processus de contrôle des informations documentées (voir l'article7.5.3);
- les politiques, règles et directives pour la gestion et l'opération des activités liées à la sécurité de l'information (voir l'article8);
- les processus et procédures utilisés pour mettre en œuvre, maintenir et améliorer le SMSI et l'état général de la sécurité de l'information (voir l'article9);
- les plans d'action; et
- la preuve des résultats des processus du SMSI (p. ex. gestion des incidents, contrôle d'accès, continuité de la sécurité de l'information, entretien de l'équipement, etc.).

ISO/IEC 27001 Exigences

ISO/IEC 27001, article 7.5.2

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.

PECB

63

Les documents exigés explicitement par ISO/IEC27001 sont:

1. Planification et contrôle opérationnels (article8.1)
2. Résultats de la surveillance et mesure du SMSI (article9.1)
3. Gestion des documents (articles7.5.2 et 7.5.3)
4. Programmes d'audit interne et résultats (article9.2)
5. Preuve de compétence (article7.2)
6. Revue de la direction (article9.3)
7. Non-conformités, actions correctives et résultats (article10.1)

La documentation suivante, même si elle n'est pas explicitement exigée, est implicitement requise pour démontrer la conformité du SMSI: La disponibilité de ces documents devrait soutenir les opérations et rendre la conformité plus facile à démontrer et à soutenir lors d'un audit de certification.

1. Tableau de bord ou autre documentation qui montre l'efficacité des processus et des mesures de sécurité mis en œuvre (article9.1)
2. Plan de communication pour communiquer avec les parties prenantes (parties intéressées) (article7.4)
3. Documentation sur les rôles et responsabilités (article5.3)
4. Budget de fonctionnement du SMSI (article5.1 c))
5. Politique/procédure d'amélioration continue (article10)

Page de notes

PECB

64

ISO/IEC27003, article 7.5 Création et mise à jour

Les informations documentées peuvent être conservées sous quelque forme que ce soit, p. ex. en tant que documents traditionnels (papier et électronique), pages Web, bases de données, journaux informatiques, rapports informatiques, audio et vidéo. En outre, les informations documentées peuvent être des spécifications d'intention (p. ex. politique de sécurité de l'information) ou des enregistrements de performance (p. ex. résultats d'une vérification) ou un mélange des deux. Les indications suivantes s'appliquent directement aux documents traditionnels et doivent être interprétées de manière appropriée lorsqu'elles s'appliquent à d'autres formes d'informations documentées.

Il convient que les organisations créent une bibliothèque d'informations documentées structurée, reliant différentes parties de l'information documentée en: déterminant la structure du cadre d'informations documentées; établissant la structure standard des informations documentées; fournissant des modèles pour différents types d'informations documentées; définissant les responsabilités pour la préparation, l'approbation, la publication et la gestion des informations documentées; et déterminant et documentant le processus de révision et d'approbation afin d'en assurer sa pertinence et son adéquation continue.

ISO/IEC 27001 Exigences

ISO/IEC 27001, article 7.5.3

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).*

PECB

65

Le contrôle des documents est assuré par la gestion efficace de leur cycle de vie, depuis leur création jusqu'à leur destruction.

ISO/IEC27003, article 7.5.3 Maîtrise des informations documentées

Lignes directrices

Une bibliothèque d'informations documentées structurée peut être utilisée pour faciliter l'accès aux informations.

Toutes les informations documentées devraient être classées (voir ISO/IEC27001:2013, A.8.2.1) conformément au système de classification de l'organisation. Les informations documentées devraient être protégées et traitées conformément à leur niveau de classification (voir ISO/IEC27001:2013, A.8.2.3).

Un processus de gestion de changement pour les informations documentées devrait garantir que seules les personnes autorisées aient le droit de les modifier et de les distribuer en fonction des besoins et selon des moyens appropriés et prédéfinis. Les informations documentées devraient être protégées afin de garantir leur validité et leur authenticité.

Les informations documentées devraient être distribuées et mises à la disposition des parties intéressées autorisées. Pour cela, l'organisation devrait identifier les parties intéressées concernées pour chaque information documentée (ou groupes d'informations documentées) et les moyens à utiliser pour la distribution, l'accès, la récupération et l'utilisation (p. ex. un site Web doté de mécanismes de contrôle d'accès appropriés). Il convient que la distribution soit conforme aux exigences relatives à la protection et à la gestion des informations privilégiées.

ISO/IEC 27001 Exigences

ISO/IEC 27001, article 7.5.3

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.

NOTE: L'accès implique une décision concernant l'autorisation de consulter les informations documentées uniquement, ou l'autorisation et l'autorité de consulter et modifier les informations documentées, etc.

PECB

66

ISO/IEC 27001 Exigences

Résumé



Contenu



Format



Cycle de vie du document

PECB

67

Page de notes

PECB

68

Définitions relatives à la gestion du document

ISO9000, article 3.8.2 Information

données porteuses de sens

ISO9000, article 3.8.5 Document

support d'information et l'information qu'il contient

ISO9000, article 3.8.7 Spécification

document formulant des exigences

ISO9000, article 3.6.13 Traçabilité

aptitude à retrouver l'historique, la mise en œuvre ou l'emplacement d'un objet

ISO9000, article 3.8.10 Enregistrement

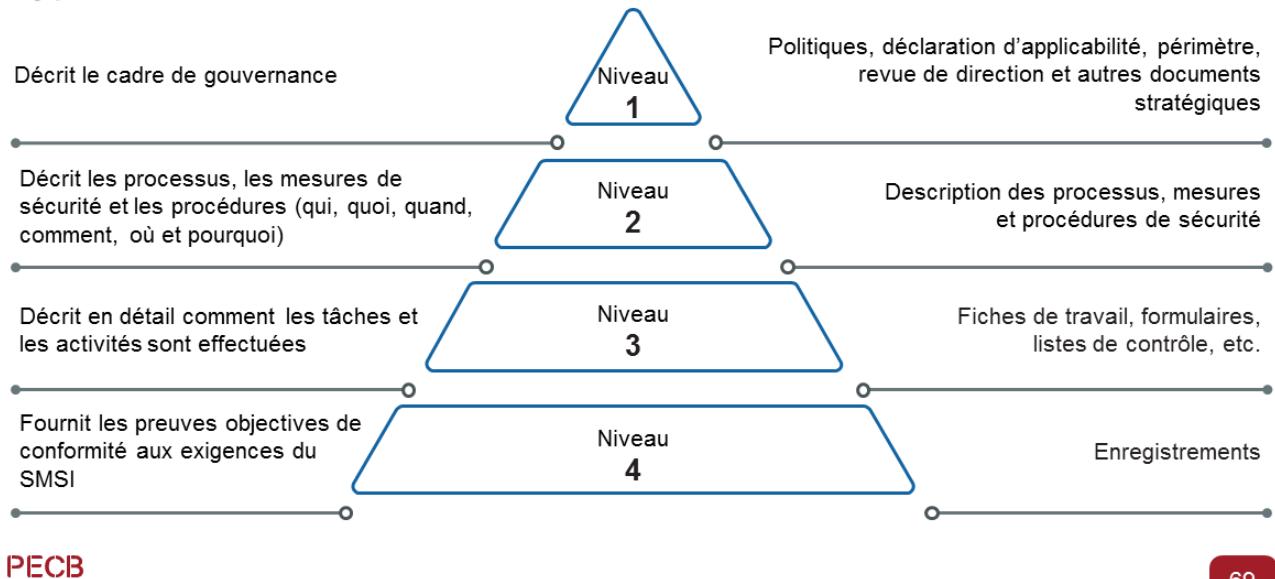
document faisant état de résultats obtenus ou apportant la preuve de la réalisation d'une activité

Note de terminologie:

1. Dans un système de management, il existe différents types de documents: politiques, procédures, enregistrements, spécifications, etc.
2. Un document est la combinaison de l'information avec son support. Le support peut être le papier, magnétique, électronique ou optique, photographie, etc. ou une combinaison de ceux-ci.
3. Un ensemble de documents est appelé couramment «documentation».

Documentation du SMSI

Types de documents



La documentation des processus clés et des mesures de sécurité peut prendre différentes formes: diagrammes, descriptions textuelles, feuilles de calcul, etc.

Il n'y a pas de prescription obligatoire sur la façon de documenter les processus et les mesures de sécurité.

Vocabulaire

Directives ISO/IEC, Partie 2

Terme	Explication
Exigence	Les termes « doit » (shall) et « ne doit pas » (shall not) indiquent des exigences qui doivent être strictement respectées afin de se conformer au document et pour lesquelles aucune déviation n'est autorisée.
Recommandation	Les termes « il convient de » ou « devrait » (should) et « il convient de ne pas » ou « ne devrait pas » (should not) indiquent que, parmi plusieurs possibilités, une est recommandée comme particulièrement appropriée, sans mentionner ou exclure les autres ou qu'une certaine ligne de conduite est préférable, mais pas nécessairement requise, ou que (dans la forme négative) une certaine possibilité ou ligne de conduite est dépréciée mais pas interdite.
Autorisation	Les termes « peut » (may) et « peut ne pas être » (need not) indiquent une ligne de conduite permise dans les limites du document.
Possibilité et capacité	Les termes « peut » (can) et « ne peut pas » (cannot) indiquent une possibilité que quelque chose se produise.

PECB

70

Lors de la mise en œuvre d'un système de management, il convient de porter une attention particulière à l'utilisation d'expressions verbales pour indiquer la nature des dispositions spécifiques.

L'organisme devra s'assurer que l'exigence d'une norme exprimée par l'utilisation du verbe «doit» (shall) est strictement suivie dans le système de management.

Dans le cas de recommandations, l'organisme n'est pas obligé d'en faire une exigence. Elles peuvent être formulées comme des lignes directrices que les utilisateurs **devraient** suivre.

Cependant, si un processus ou une mesure qui n'est pas une exigence de la norme est documenté par l'organisme avec le verbe « doit» (shall), cela devient une exigence du système de management de l'organisme. Une telle obligation peut être imposée, c'est-à-dire par la loi ou par contrat. Par exemple, si une procédure de l'organisme indique que les sauvegardes **doivent** (shall) être vérifiées chaque matin à 10heures, mais que l'auditeur a trouvé durant l'audit que ce n'est pas suivi, il en résulte une non-conformité. Cependant, si la même procédure était écrite avec le verbe «devrait» (should), il n'y aurait pas de non-conformité parce que cela serait vu comme une question de ligne directrice par l'organisme.

Exigence: expression, dans le contenu d'un document, formulant les critères objectivement vérifiables à respecter et avec lesquels aucun écart n'est permis afin de prétendre à la conformité avec le document

Référence: Directives ISO/IEC, Partie2, 2018article3.3.3

Recommandation: expression, dans le contenu d'un document, suggérant une possibilité de choix ou de mode de faire jugé particulièrement approprié sans pour autant en mentionner ou exclure d'autres

Référence: Directives ISO/IEC, Partie2, 2018article3.3.4

Valeur de la documentation

Notes importantes

- Dans plusieurs organismes, la création de la documentation est disproportionnée.
- L'élaboration de documents ne doit pas représenter une fin en soi. Elle doit être une activité à valeur ajoutée soutenant le SMSI.
- Une documentation trop lourde est difficile à gérer et souvent mal comprise par les utilisateurs, donc inutile.
- Les organismes devraient déterminer leurs propres besoins en matière de documentation et d'autres supports.



PECB

71

Chaque organisme devrait déterminer l'étendue de sa documentation et autres supports. Cela dépend de facteurs tels que le type et la taille de l'organisme, la complexité et les interactions des processus, les systèmes d'information et les technologies disponibles, les exigences des parties intéressées comme les clients et les fournisseurs, les exigences réglementaires applicables, etc.

La valeur première de la documentation est de permettre la communication de la mise en œuvre du SMSI et la cohérence des actions. Son utilisation contribue à:

- a. Réaliser la conformité aux exigences légales, réglementaires et contractuelles
- b. Réaliser la conformité avec la norme ISO/IEC27001 et autres normes
- c. Offrir un support adapté à la communication et à la formation
- d. Assurer la répétabilité et la traçabilité
- e. Fournir des éléments de preuve pour un audit de certification
- f. Évaluer l'efficacité et la pertinence continue du SMSI
- g. Améliorer les processus et les mesures de sécurité du SMSI

2.3 Gestion de la documentation

Liste des activités

2.3.1

Créer les modèles

2.3.2

Élaborer un processus de gestion de documents

2.3.3

Mettre en œuvre un système de gestion de documents

2.3.4

Gérer les enregistrements

2.3.5

Créer une liste maîtresse de documents

2.3.1 Créer les modèles

Type de documents

Type de documents	Objectifs
Politique	Intentions et orientations globales d'un organisme telles qu'exprimées formellement par la direction
Procédure	Instructions spécifiques qui expliquent clairement les étapes à suivre
Lignes directrices	Déclaration générale pour atteindre les objectifs de la politique en présentant des orientations sur les bonnes pratiques
Manuel de sécurité	Document décrivant ou faisant référence aux politiques, pratiques, processus, procédures et listes de contrôle liés à la sécurité de l'information
Charte	Description des conventions mises en place entre l'organisme et un groupe d'acteurs tels que les utilisateurs, employés, fournisseurs ou prestataires de services
Processus schématique	Schéma illustrant le fonctionnement d'un processus
Processus narratifs	Explication détaillée du fonctionnement d'un processus en tant que description narrative
Formulaire	Formulaire papier ou électronique conçu pour fournir ou enregistrer des informations sur une opération (demande de modification, demande d'autorisation, déclaration d'incident, etc.)
Guide	Document pratique décrivant en détail l'installation, l'utilisation, la maintenance, l'exploitation
Fiche technique	Document où sont résumées les informations techniques (spécifications) nécessaires à l'installation, l'utilisation, la maintenance, etc. d'un équipement, d'un logiciel, etc.

PECB

73

Politique: Représente les intentions et orientations générales d'un organisme telles qu'exprimées officiellement par la direction.

Procédure: Instructions spécifiques qui expliquent clairement les étapes à suivre afin de déterminer comment la politique, les lignes directrices et les normes correspondantes seront réellement mises en œuvre dans un environnement d'exploitation. La procédure décrit une suite d'actions ordonnées visant l'atteinte d'un objectif.

Ligne directrice: Déclaration générale permettant d'atteindre les objectifs d'une politique en fournissant des orientations sur les bonnes pratiques à suivre. C'est une directive importante qui devrait être respectée, bien qu'elle ne soit pas obligatoire.

Manuel de sécurité: Ensemble de descriptions réelles ou de renvois aux politiques, pratiques, processus, procédures et listes de contrôle relatifs à la sécurité de l'information, dans le cadre du SMSI. Contrairement à la norme ISO9001, qui mentionne la publication d'un manuel de qualité, ISO/IEC 27001 ne spécifie rien de similaire. Cependant, plusieurs organismes préfèrent regrouper la documentation du SMSI dans un seul manuel.

Processus schématique: Schéma illustrant le fonctionnement d'un processus.

Processus narratif: Explication détaillée du fonctionnement d'un processus en tant que description narrative.

Page de notes

PECB

74

Charte: Description des conventions mises en place entre l'organisme et un groupe d'acteurs tels que les utilisateurs, les employés, les fournisseurs ou les prestataires de services. Une charte définit les droits et les devoirs des parties.

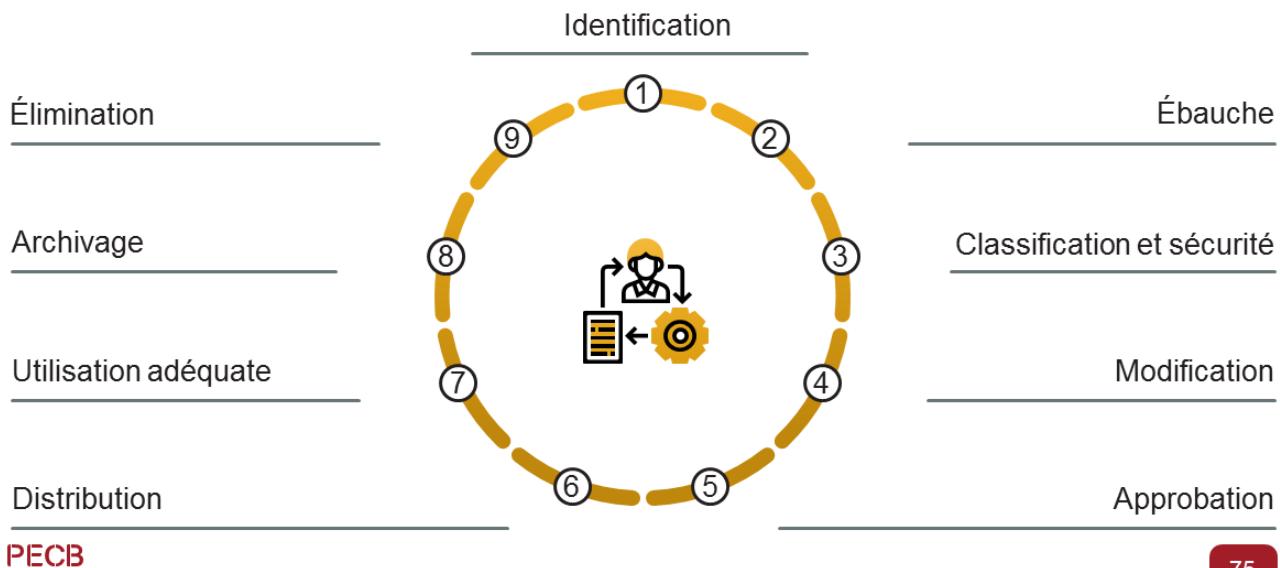
Guide: Document pratique décrivant en détail les modes l'installation, l'utilisation, la maintenance, l'exploitation. Dans la pratique, bien qu'ils désignent des concepts différents, les termes génériques «guide» et «manuel» sont souvent pris dans le même sens et donnent ainsi lieu à plusieurs expressions pratiquement synonymes. Le guide doit être adapté à la population visée (p. ex., un guide destiné à tous les utilisateurs doit contenir des termes simples et peu techniques).

Formulaire: Formulaire papier ou électronique conçu pour fournir ou enregistrer des informations sur une opération (demande de modification, demande d'autorisation, déclaration d'incident, etc.) L'utilisation de formulaires électroniques peut faciliter la saisie des éléments d'entrée, le contrôle des dossiers, les processus d'approbation et la réutilisation des informations. Synonyme: Modèle (*template*) ou pro forma

Fiche technique: Document sur lequel sont résumées les informations techniques (spécifications) nécessaires à l'installation, l'utilisation, la maintenance, etc. d'un équipement, d'un logiciel, etc. On l'utilise généralement pour les équipements techniques et les logiciels en séries simples et les normes qu'on retrouve dans l'organisme. Une fiche technique peut contenir, entre autres, une description physique, des informations sur les caractéristiques de fonctionnement du produit ainsi que les conditions d'installation.

2.3.2 Élaborer un processus de gestion de documents

Une procédure doit être établie pour gérer le cycle de vie d'un document.



75

Il est essentiel d'établir des documents et d'assurer un contrôle adéquat afin de maintenir, de communiquer et d'améliorer davantage les systèmes de management avec toutes les personnes impliquées.

1. **Identification:** Le document à créer a été identifié.
2. **Création d'une ébauche:** Une ébauche est créée.
3. **Classification et sécurité:** Le document est classifié et on détermine par qui il sera accessible.
4. **Révision:** Le document est distribué pour revue officielle ou révision. (Il peut s'écouler plusieurs cycles entre cette étape et l'étape2.)
5. **Approbation:** Le document est finalisé et signé.
6. **Distribution:** Le document est mis en circulation.
7. **Utilisation adéquate:** Le document est disponible pour utilisation et accessible au besoin.
8. **Archivage:** Le document est archivé.
9. **Élimination:** L'organisme élimine les documents inutiles et obsolètes à l'expiration de leur période de conservation.

2.3.3 Mettre en œuvre un système de gestion de documents

- Faciliter l'accès, le référencement, la diffusion et l'archivage des documents
- Gérer l'intégralité du cycle de vie du document
- Garantir la traçabilité
- Sécuriser l'accès aux documents



Optimiser la recherche et mettre à jour

PECB

76

Un système de gestion documentaire garantit la traçabilité et sécurise l'accès aux documents en gérant les différents niveaux d'autorisation à l'accès, à l'utilisation et à la diffusion des données.

Types de solutions disponibles:

1. **Système de gestion électronique de documents (GED):** La GED est un système informatisé d'acquisition, de classification, de stockage, d'archivage des documents (exemple d'utilisation: numérisation de masse de documents papier). Un exemple connu est SharePoint (Microsoft).
2. **Système de gestion de contenu:** Les systèmes de gestion de contenu, ou SGC, sont une famille de logiciels de conception et de mise à jour dynamique de site Web ou d'application multimédia permettant de gérer le contenu. Un exemple connu serait toutes les applications de type «Wiki» comme l'encyclopédie en ligne, Wikipédia.

2.3.4 Gérer les enregistrements

- L'identification, le stockage, la protection, la disponibilité, la conservation et l'élimination des enregistrements doivent être documentés et mis en œuvre.
- Les enregistrements doivent être protégés, rester lisibles, être faciles à identifier et accessibles.



The screenshot shows a Microsoft Notepad window with the title "*Untitled - Notepad". The content of the window is a log file from a Microsoft Windows Firewall. The log entries are in a standard text-based format, detailing network traffic such as drops, TCP connections, and ICMP events. The log starts with a header section and then lists numerous entries with timestamp, source IP, destination IP, port numbers, and various flags and status codes.

```
#Version: 1.5
#Software: Microsoft Windows Firewall
#Time Format: Local
#Fields: date time action protocol src-ip dst-ip src-port dst-port size tcpflags tcpsyn tcpack tcpwin icmptype icmpcode info path

2004-10-27 11:56:18 DROP TCP 192.168.1.100 192.168.1.101 2270 445 48 S 1584384258 0 65535 --- RECEIVE
2004-10-27 11:56:18 DROP TCP 192.168.1.100 192.168.1.101 2271 139 48 S 2322815226 0 65535 --- RECEIVE
2004-10-27 11:56:21 DROP TCP 192.168.1.100 192.168.1.101 2270 445 48 S 1584384258 0 65535 --- RECEIVE
2004-10-27 11:56:21 DROP TCP 192.168.1.100 192.168.1.101 2271 139 48 S 2322815226 0 65535 --- RECEIVE
2004-10-27 11:56:27 DROP TCP 192.168.1.100 192.168.1.101 2270 445 48 S 1584384258 0 65535 --- RECEIVE
2004-10-27 11:56:27 DROP TCP 192.168.1.100 192.168.1.101 2271 139 48 S 2322815226 0 65535 --- RECEIVE
2004-10-27 12:04:05 OPEN-INBOUND TCP 192.168.1.100 192.168.1.101 2276 445 -----
2004-10-27 12:04:05 OPEN-INBOUND TCP 192.168.1.100 192.168.1.101 2277 139 -----
2004-10-27 12:04:05 CLOSE TCP 192.168.1.101 192.168.1.100 139 2277 -----
2004-10-27 12:04:17 CLOSE TCP 192.168.1.101 192.168.1.100 445 2276 -----
```

PECB

VISITORS REGISTER				
Date	Visitors name	Email address	Time (in)	Time (out)
2019-02-08	Abbey Martin	abbey.martin@gmail.com	10:15	11:27
2019-02-10	Barren Miller	miller-b@gmail.com	09:07	10:41
2019-02-14	David Wilson	da.willson@gmail.com	12:10	13:44
2019-02-19	Lynda Brown	lyndaBrown@gmail.com	10:15	11:27
2019-02-26	Sofia Morris	ssofia@hotmail.com	14:22	15:15
2019-02-27	Tricia Zylker	tricia.Z@hotmail.com	10:15	11:27
2019-03-01	Jackson Rivera	jack-riv@gmail.com	15:20	16:20
2019-03-08	Peter Diaz	peter82@hotmail.com	09:50	10:30
2019-03-10	Jim Walker	walker.jim@gmail.com	10:58	11:40

77

Exemples d'enregistrements: Les enregistrements des systèmes d'information, le registre des visiteurs, les rapports d'audit et les formulaires d'autorisation d'accès remplis sont des exemples d'enregistrements.

Registre des enregistrements

Exemples

Identification	Stocké	Responsabilité	Maintien	Classification
Registre des visiteurs	Réception	Assistant(e) administratif(ve)	1 an	Usage interne
Fiche de rapport d'incidents	Centre de service	Directeur du centre de service	3 ans	Confidentiel
Dossier de l'employé	Service RH	Directeur RH	5 ans après la fin de l'emploi	Hautement confidentiel
Revue de direction	Comité exécutif	Secrétaire du comité exécutif	7 ans	Hautement confidentiel

PECB

78

2.3.5 Créer une liste maîtresse de documents

Il est de bonne pratique de créer une liste unique de l'ensemble de la documentation relative au SMSI avec les informations de base :

- Identificateur unique
- Titre
- Type de document
- Fonctions et noms des auteurs (ou des responsables)
- Fonction et nom de l'approbateur et date d'approbation
- Date d'émission
- Version et sa date de révision
- Numérotation des pages
- Classification

PECB

79

Plusieurs organismes intègrent la liste maîtresse des documents à la Déclaration d'applicabilité dans un document unique regroupant la description des mesures de sécurité ainsi que la documentation reliée.

Il est préférable de désigner les auteurs et les organismes d'approbation par leur rôle et non par leur nom. Il convient que leur rôle, leur nom et la date soient indiqués à chaque version ou publication officielle d'un document.

Aux fins du classement électronique, il est recommandé d'attribuer les dates dans le format 20aa-mm-jj (qui conservera les dossiers dans l'ordre des dates lorsque les recherches seront effectuées).

Gestion de la documentation

Problèmes les plus courants

Problèmes

- Difficulté à retrouver ou à gérer un document
- Incapacité d'extraire rapidement l'information utile d'un document
- Mise à jour des documents inefficace
- Différence entre les enregistrements et les processus de gestion actuels
- Textes ou graphiques ambigus ou incompréhensibles
- Prolifération des versions de documents

Cause potentielle

- Masse importante de documents mal classés et non indexés
- Document volumineux, trop littéraire, souvent muni d'annexes multiples
- Processus de gestion des documents non établis ou mal exploités
- Employés liés aux opérations non impliqués dans la rédaction des documents
- Pas de validation par les utilisateurs, manque de formation et de sensibilisation, rédacteur incompétent
- Pas de système de gestion de documents en place

PECB

80



Exercice 9

PECB

81

Exercice9: Liste maîtresse des documents

La direction de Scientia Online Library a décidé d'inclure toutes les mesures de sécurité relatives à la gestion de la continuité (mesureA.17) dans son organisme. Pour préparer la mise en œuvre, elle vous demande de compléter la liste maîtresse des documents.

Proposez une liste des documents et des enregistrements qui devraient être générés pour se conformer aux exigences des mesures de sécurité énoncées à la mesureA.17.

Durée de l'exercice: 30 minutes

Commentaires: 15 minutes

Questions ?

PECB

82

Section 17

Plan de communication

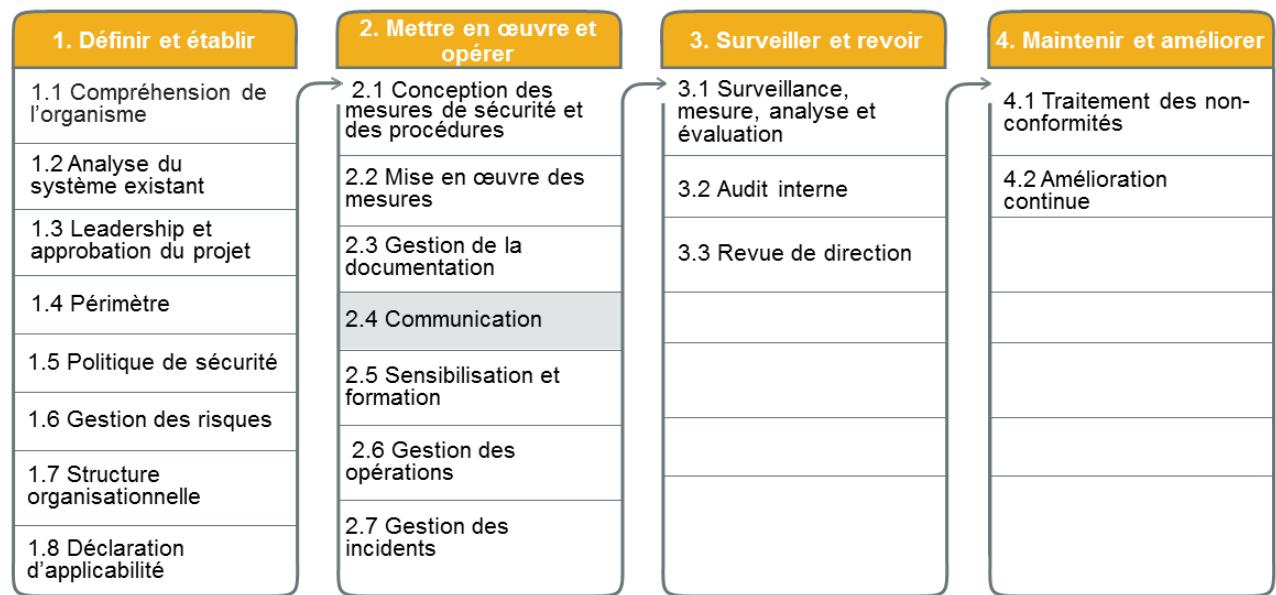
- Principes d'une stratégie de communication efficace
- Processus de communication de sécurité de l'information
- Définition des objectifs de communication
- Identification des parties intéressées
- Planification des activités de communication
- Réalisation d'une activité de communication
- Évaluation de la communication

PECB

83

Cette section aidera le participant à acquérir des connaissances sur le plan de communication y compris les principes d'une stratégie de communication efficace, comment définir des objectifs de communication et identifier les parties intéressées.

2.4 Plan de communication



PECB

84

ISO/IEC 27001 Exigences

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.*



85

PECB

Un organisme qui désire se conformer à ISO/IEC27001 doit:

1. Identifier les aptitudes nécessaires pour assurer le fonctionnement adéquat du SMSI
2. Mettre en œuvre un programme de formation pour le personnel qui exécute les tâches relatives au SMSI
3. Mettre en œuvre un programme de sensibilisation en sécurité de l'information adapté aux différentes parties prenantes
4. Mettre en œuvre un programme de communication pour informer les parties prenantes au sujet du SMSI – au sujet des changements qui pourraient les affecter
5. Évaluer l'efficacité des actions entreprises et conserver des enregistrements

ISO/CIE 27003, article 7.4 Communication

Lignes directrices

La communication repose sur les processus, les canaux et les protocoles. Ceux-ci devraient être choisis pour s'assurer que le message communiqué est intégralement reçu, correctement compris et, le cas échéant, qu'on y donne suite de manière appropriée.

Les organisations devraient déterminer quel contenu doit être communiqué, par exemple:

- a. les plans et les résultats de la gestion des risques aux parties intéressées, selon les besoins et le cas, dans l'identification, l'analyse, l'évaluation et le traitement des risques;*
- b. les objectifs de sécurité de l'information;*
- c. les objectifs de sécurité de l'information atteints, y compris ceux qui peuvent soutenir leur position sur le marché (p. ex. certification ISO/IEC 27001 octroyée; déclaration de conformité avec les lois sur la protection des données personnelles);*
- d. les incidents ou les crises, où la transparence est souvent essentielle pour préserver et accroître la confiance dans la capacité de l'organisation à gérer sa sécurité de l'information et à faire face aux situations imprévues;*
- e. les rôles, responsabilités et autorités;*

Page de notes

PECB

86

- f) les informations échangées entre les fonctions et rôles tel que requis par le processus du SMSI;
- g) les changements apportés au SMSI;
- h) d'autres questions relevées lors de la revue des mesures et des processus dans le cadre du SMSI;
- i) les enjeux (p. ex. avis d'incident ou de crise) qui nécessitent une communication aux organismes de réglementation ou à d'autres parties intéressées; et
- j) les demandes ou autres communications émanant de parties externes telles que les clients, les clients potentiels, les utilisateurs de services et les autorités.

L'organisation devrait déterminer les exigences en matière de communication sur les questions pertinentes:

- k) qui est autorisé à communiquer à l'externe et à l'interne (p. ex. dans des cas particuliers comme une atteinte à la protection des données), en attribuant des rôles précis à l'autorité compétente. Par exemple les chargés de communication officielle peuvent avoir l'autorité en la matière. Il pourrait s'agir d'un responsable des relations publiques pour la communication externe et d'un responsable de la sécurité pour la communication interne;
- l) les déclencheurs ou la fréquence des communications (p. ex. pour la communication d'un événement, le déclencheur est l'identification de l'événement);
- m) le contenu des messages destinés aux principales parties intéressées (p. ex. clients, régulateurs, grand public, utilisateurs internes importants) sur la base de scénarios d'impact de haut niveau. La communication peut être plus efficace si elle repose sur des messages préparés et approuvés au préalable par le niveau de gestion approprié dans le cadre d'un plan de communication, du plan de réponse aux incidents ou du plan de continuité d'activité;
- n) les personnes à qui la communication est destinée; dans certains cas, une liste devrait être tenue à jour (p. ex. pour communiquer les changements apportés aux services ou les crises);
- o) les moyens de communication et les canaux. La communication devrait utiliser des moyens et des canaux spécifiques, pour s'assurer que le message est officiel et qu'il porte l'autorité appropriée. Les canaux de communication devraient répondre à tout besoin de protection de la confidentialité et de l'intégrité de l'information transmise; et
- p) le processus conçu et la méthode pour s'assurer que les messages sont envoyés et qu'ils ont été correctement reçus et compris.

La communication devrait être classée et traitée conformément aux exigences de l'organisation.

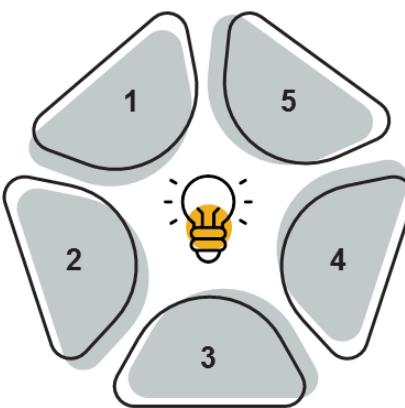
Principes pour une stratégie de communication efficace

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

Rendre l'information fournie dans la communication pertinente pour les parties intéressées, en utilisant des formats, un langage et un support adaptés à leurs intérêts et leurs besoins, afin de leur permettre de participer pleinement.



Clarté

S'assurer que les approches et la langue de communication sont compréhensibles par les parties intéressées afin de minimiser le risque d'ambiguïté.

Réactivité

Répondre aux questions et aux préoccupations des parties intéressées de façon totale et opportune. Rendre les parties intéressées conscientes de la façon dont leurs questions et leurs préoccupations ont été abordées.

2.4 Communication

2.4.1

Définir les objectifs de communication

2.4.2

Identifier les parties intéressées

2.4.3

Planifier les activités de communication

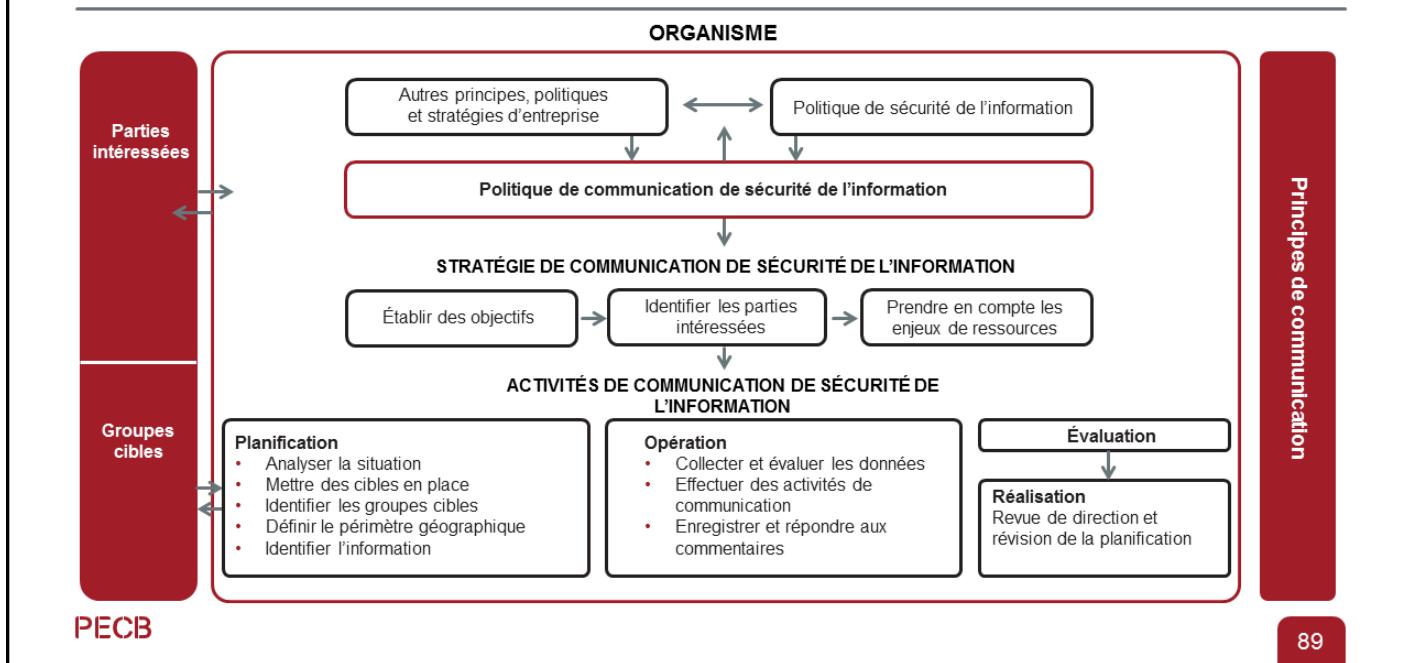
2.4.4

Réaliser une activité de communication

2.4.5

Évaluer la communication

Processus de communication de la sécurité de l'information



2.4.1 Définir les objectifs de communication

Exemples

- Améliorer la crédibilité et la réputation de l'organisme
- Établir un dialogue permanent avec les parties intéressées sur les enjeux de sécurité de l'information
- Se conformer aux exigences légales applicables et aux autres exigences auxquelles l'organisme adhère
- Influencer la politique publique sur les questions de sécurité de l'information
- Fournir de l'information et encourager la compréhension par les parties intéressées des activités de sécurité de l'information
- Satisfaire les attentes des parties intéressées en matière de sécurité de l'information



PECB

90

Un organisme devrait établir des objectifs de sécurité de l'information utiles, car ils peuvent offrir les bases d'une stratégie de communication efficace. Lorsqu'un organisme établit des objectifs de communication de sécurité de l'information, il devrait s'assurer que ces objectifs sont alignés sur la politique de communication, prennent en compte les points de vue des parties intéressées internes et externes et qu'ils sont cohérents avec les principes de communication. En établissant les objectifs pour ses activités de communication, l'organisme devrait évaluer ses priorités et les résultats souhaités de sorte que les objectifs définis soient exprimés de façon qu'aucune autre explication ne soit nécessaire.

La direction de l'organisme devrait développer une stratégie pour mettre en place un plan de communication. La stratégie devrait comprendre les objectifs de communication, l'identification des parties intéressées, une indication de la date et du contenu et un engagement de la direction pour allouer des ressources adéquates. Un organisme devrait préciser ce qui est possible, en tenant compte de ses ressources, afin de pouvoir répondre au mieux et de la manière la plus réaliste aux attentes des parties intéressées.

Une attention particulière devrait être accordée au fait que la communication sur la sécurité de l'information fait partie des activités de l'organisme en général et devrait être alignée sur les autres éléments des systèmes, politiques, stratégies ou activités de gestion pertinentes.

Page de notes

PECB

91

Au moment du développement de la stratégie de communication, les questions ci-dessous peuvent être utiles.

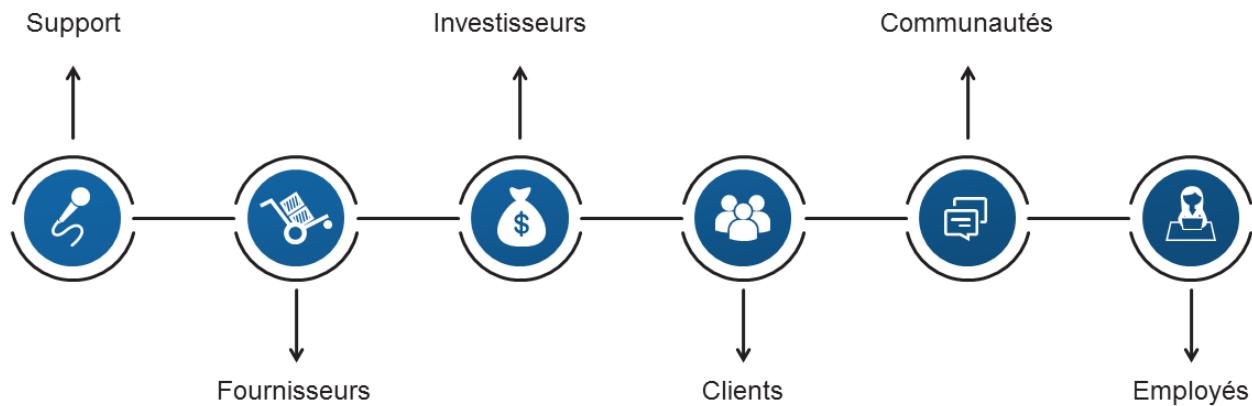
1. Pourquoi l'organisme engage-t-il une communication sur la sécurité de l'information et quels sont ses buts?
2. Quel est le public cible?
3. Quels sont les principaux enjeux et impacts de l'organisme en matière de sécurité de l'information?
4. Quels sont les principaux points à couvrir, les messages à véhiculer, les techniques de communication, les approches, les outils et les canaux à utiliser?
5. Combien de temps est nécessaire pour mettre en œuvre la stratégie?
6. Comment la stratégie engage-t-elle et coordonne-t-elle les responsables de la sécurité de l'information, les parties intéressées, les responsables des mesures de sécurité de l'information et les responsables de la communication interne et externe de l'organisme?
7. Quelles sont les limites locales, régionales, nationales et internationales de la stratégie?

Une fois définie, la stratégie devrait être approuvée par la direction et utilisée comme base pour les activités de communication de l'organisme en matière de sécurité de l'information.

Les activités de communication en matière de sécurité de l'information d'un organisme dépendent des ressources disponibles. La stratégie de communication sur la sécurité de l'information devrait comprendre une répartition des ressources humaines, techniques et financières, des responsabilités et des pouvoirs désignés ainsi que des actions définies. Les expériences et les besoins de formation des employés devraient également être pris en considération.

2.4.2 Identifier les parties intéressées

Adaptation du plan de communication



PECB

92

L'engagement avec les parties intéressées donne à un organisme l'occasion de comprendre leurs enjeux et leurs préoccupations ; il peut mener à une meilleure connaissance par les deux parties et peut influencer les opinions et les perceptions. Quand elle est effectuée correctement, toute approche peut être réussie et peut satisfaire les besoins de l'organisme et des parties intéressées.

Dans certains cas, la compréhension du modèle/comportement de communication de chaque partie intéressée (ou groupe cible) est également importante dans les communications. Un processus de communication efficace implique un contact continu entre l'organisme et les parties intéressées internes et externes qui s'inscrit dans le cadre d'une stratégie globale de communication des organismes.

En développant la stratégie de communication de sécurité de l'information et la définition des objectifs, l'organisme devrait identifier les parties intéressées internes et externes qui ont exprimé un intérêt dans ses activités, produits et services. Il devrait aussi identifier les autres parties intéressées potentielles avec lesquelles communiquer pour réaliser les objectifs globaux de sa stratégie de communication de sécurité de l'information.

2.4.3 Planifier les activités de communication

Clés du succès

- Un organisme devrait décider de l'objectif à atteindre pour une activité de communication de sécurité de l'information.
- Les objectifs fixés devraient être compatibles avec les objectifs de communication de sécurité de l'information et devraient également être spécifiques, mesurables, réalisables, réalistes et limités dans le temps.
- L'organisme devrait anticiper les enjeux de sécurité de l'information qui préoccupent les parties intéressées.

Cela permettra à l'organisme d'évaluer l'activité de communication de sécurité de l'information et de déterminer si l'objectif a été atteint.

PECB

93

Les organismes utiliseront une large gamme d'activités de communication dans la mise en œuvre de leur plan de communication sur la sécurité de l'information. En définissant la stratégie et les objectifs de communication de sécurité de l'information, les activités spécifiques de communication devraient être développées en tenant compte des différentes thématiques, des limites géographiques et des parties intéressées.

Le développement ou l'amélioration d'une activité de communication de sécurité de l'information commence par une compréhension du contexte.

Dans l'analyse de la situation, l'organisme devrait tenir compte des questions suivantes:

- a. L'identification et compréhension des questions préoccupantes pour les parties intéressées ;
- b. Les attentes et les perceptions des parties intéressées au sujet de l'organisme ;
- c. La sensibilisation à la sécurité de l'information des parties intéressées, telles que les communautés locales ;
- d. Les supports de communication et les activités qui se sont révélées les plus efficaces pour communiquer avec les parties intéressées dans des situations similaires ;
- e. L'identification des leaders d'opinion et leur influence sur les questions relatives à la communication sur la sécurité de l'information ;
- f. Image publique (ou interne) de l'organisation sur un point spécifique ;
- g. Les derniers développements et les tendances sur les points de sécurité de l'information relatifs au contexte spécifique de l'organisme.

Lors de l'évaluation d'une activité de communication de sécurité, il est important d'évaluer les coûts potentiels et les conséquences de la non-communication. Ils peuvent être réels, coûter, à la longue, plus que la communication et peuvent même imposer des coûts supplémentaires à un organisme, par exemple des atteintes à la réputation.

En planifiant une activité de communication, il convient qu'un organisme identifie les groupes cibles parmi ses parties intéressées. Une bonne communication implique un éventail de groupes cibles possibles.

Page de notes

PECB

94

Il n'est pas inhabituel d'identifier les conflits d'intérêts parmi différents groupes cibles. En conséquence, les activités de communication doivent traiter et répondre aux différentes demandes souvent contradictoires des groupes cibles, en particulier ceux qui sont les plus influents et qui peuvent avoir un impact négatif sur les résultats d'une activité de communication.

L'organisme devrait anticiper les problèmes de sécurité de l'information qui préoccupent les parties intéressées. Cela aidera à collecter les impacts et des performances de sécurité de l'information au sujet de ses produits, ses services, ses processus et ses activités. En fonction des objectifs fixés pour une activité de communication de sécurité de l'information, des données et des informations quantitatives et qualitatives appropriées peuvent être sélectionnées ou générées. Il convient que ces informations soient alignées sur les normes et directives actuelles relatives à la sécurité de l'information et leurs indicateurs de performance.

2.4.4 Réaliser une activité de communication

Approches et outils de communication

- Site Web
- Rapport
- Brochure et newsletter
- Affiche
- E-mail
- Articles de journaux
- Communiqué de presse
- Publicité
- Réunion publique
- Groupe de discussion
- Sondage
- Visite guidée de l'organisme
- Atelier et conférence
- Entrevue avec les médias
- Présentation aux groupes



PECB

95

L'approche d'un organisme en matière de communication de sécurité de l'information sera influencée par sa volonté de consulter, comprendre, informer, persuader ou impliquer les groupes cibles.

Il est important de noter que la communication est un processus dynamique et qu'il y a un changement continu entre les groupes cibles et les organismes.

En choisissant ses approches de la communication, il est important de prendre en compte les besoins et le degré d'intérêt des groupes cibles impliqués dans l'activité de communication. De plus, il est également important de considérer le degré d'activité que l'organisation souhaite avoir dans sa communication. Il existe différentes approches de la communication selon que l'organisation et les groupes cibles sont actifs ou passifs, selon les objectifs de communication de sécurité de l'information, ainsi que selon les groupes cibles et les ressources organisationnelles disponibles pour la communication.

Un organisme devrait adapter l'information qu'il fournit, conformément à la planification initiale, aux groupes cibles. L'information devrait:

- a. Prendre en considération les aspects comportementaux et les intérêts sociaux, culturels, éducatifs, économiques et politiques des groupes cibles
- b. Utiliser un langage approprié
- c. Utiliser des images ou des supports électroniques, le cas échéant, et
- d. Être cohérent avec l'approche choisie et, le cas échéant, avec d'autres informations sur les questions de sécurité de l'information communiquées précédemment par l'organisme.

Un organisme peut vouloir tester ses moyens de diffusion de l'information avant de procéder à toute communication publique. Une étude d'opinion visant à tester la diffusion de l'information peut aider à identifier les domaines qui nécessitent plus d'explications ou de précisions, les questions clés, les questions à traiter, etc.

Page de notes

PECB

96

1. Site Web: Support de communication électronique, accessible en ligne à toutes les parties intéressées externes et internes

- Peut inclure des rapports téléchargeables, du matériel pédagogique ou des liens vers les sites Web où les utilisateurs peuvent fournir des commentaires à l'organisme.
- Offre un grand potentiel pour atteindre plusieurs personnes sur de multiples enjeux (et offrir une information adaptée).
- Facile à mettre à jour, avec la possibilité d'effectuer une communication dans les deux sens.

2. Rapport: Présentation détaillée de l'implication et de la performance d'un certain nombre de points clés Les extraits ou les résumés de ces rapports peuvent être inclus dans une autre communication de l'organisme, p. ex. les rapports financiers.

- Opportunité d'aborder en profondeur de multiples questions ; approche de base pour bâtir la confiance et la crédibilité.
- Assurer une transparence interne au sujet de tous les enjeux pertinents d'un organisme.
- Demande beaucoup de travail pour être produit et peut être difficile à mettre à jour fréquemment

3. Matériel imprimé (brochure et newsletter): Résumé de l'installation ou du projet d'intérêt, des questions clés et de la façon dont les gens peuvent participer

- Informe et entretient les relations avec les parties intéressées.
- Peut ne couvrir qu'un seul point, si nécessaire.
- Peu coûteux et rapide à produire.
- Informe un grand nombre de personnes.

4. Affiche/Panneau: Description d'un projet, mettant en évidence les enjeux et mis en place dans un lieu public.

- Fournit l'information générale à des coûts relativement bas.
- Donne l'information plutôt que de la recevoir.
- S'en tenir aux points principaux ; utiliser des photos et des cartes ; peut être mis à jour régulièrement.

5. E-mail: Méthode électronique d'envoi d'informations et de messages

- Offre une occasion d'envoyer des copies électroniques de publications papier.

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

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

100/163

- Peu coûteux et méthode facile pour envoyer et recevoir des messages et de l'information.
- Échange rapide, dissémination immédiate.
- Opportunité de joindre rapidement un grand nombre de personnes.
- Peut être supprimé avant même d'être lu si les gens pensent que ce n'est pas important.
- Lors de l'envoi de pièces jointes, s'assurer que le destinataire ait accès à un logiciel compatible.

6.Article de fond dans les médias/journaux: Explique les caractéristiques d'un service ou d'un projet

- Peut joindre un large public.
- Pratique pour le public.
- Excellent véhicule pour l'éducation.
- Probablement édité par le journal, donc seule une partie de l'histoire est racontée.
- Support local et national qui peut exiger des approches, un style et un niveau de détail différents.

7.Commiqué de presse: Information préparée et distribuée aux médias pour leur utilisation

- Façon efficace et économique de faire de la publicité et de générer de l'intérêt.
- Les médias ne couvriront que si l'histoire est jugée digne d'intérêt.

Page de notes

PECB

97

8. Publicité: Matériel promotionnel payant, par exemple une publicité directe dans un journal ou le parrainage d'une rubrique (comme le « dossier spécial » du journal régional).

- Atteint une large audience.
- Peut être coûteux et avoir une durée de vie limitée
- Possibilité limitée de décrire des questions complexes.

9. Réunion publique: Façon de présenter l'information et l'échange de points de vue et opinions Présentations et sessions de questions-réponses ou de témoignages formels minutés.

- Traite les agendas spécifiques ou l'aspect projet.
- Est vue comme une consultation légitime.
- L'information est fournie à un nombre relativement important de personnes. Les coûts sont faibles.
- Les interactions peuvent être limitées. Ne garantit pas que tous les points de vue soient entendus.
- Peut se transformer en champ de bataille émotif.
- Une minorité vocale peut dominer.
- Dans la mesure du possible, faites appel à un président indépendant ou à un animateur ou à un modérateur.

10. Groupe de discussion: Réunion en petit comité constitué des parties intéressées qui présentent des caractères communs (p. ex. des représentants gouvernementaux ou des nationaux) pour discuter d'un sujet particulier

- Permet un libre échange d'idées parce que les gens se sentent à l'aise en compagnie de leurs pairs.
- Permet souvent d'arriver à un consensus sur les points les plus importants.
- Demande beaucoup de temps pour organiser des groupes avec toutes les parties intéressées importantes.
- Souvent utilisé après des entrevues initiales avec les parties intéressées pour identifier les principaux enjeux qui peuvent être soulevés.

11. Sondage: Questionnaire utilisé avec les parties intéressées (peuvent être réalisés par un organisme indépendant si nécessaire) pour recueillir de l'information de la part des répondants et identifier leurs attentes et problèmes

- Utile lorsqu'une entreprise planifie de s'établir dans une communauté ou si un changement majeur dans ses opérations est envisagé.
- Constitue également une bonne mise à jour si régulier (tous les 2ans).
- La création d'une enquête peut inclure de nombreuses personnes selon la complexité du questionnaire, la manière dont les questions sont posées (personnellement ou via le Web par exemple), le nombre de personnes dans l'échantillon et le nombre et la taille des lieux géographiques choisis.
- Le sondage peut être réalisé porte à porte ou par téléphone. Il peut aussi être écrit ou réalisé sur Internet.

12. Visite guidée de l'organisme: Visite proposée aux groupes cibles dans des zones ou des installations présentant un intérêt pour l'organisme

- Fournit l'occasion de prises de contact entre le personnel de l'organisme et les visiteurs.
- Fournit l'occasion immédiate de montrer les activités de l'organisme.
- Peut être interprété comme un exercice de relations publiques si seuls les bons aspects sont montrés.
- Est limité en termes de nombre de personnes touchées par l'effort.
- Peut être coûteux et nécessiter de nombreuses heures de travail du personnel. S'appuyer sur les connaissances et les compétences du personnel.

Page de notes

PECB

98

13. Atelier et conférence: Événement de dialogue

- Occasion pour les parties intéressées de débattre des idées, des préoccupations et des problèmes.
- Très productif et utile pour parvenir à un consensus sur des questions hautement prioritaires.
- Peut prendre beaucoup de temps à organiser pour que toutes les parties intéressées soient présentes.
- Il est habituellement plus efficace d'organiser ce type d'événement après des entrevues spécifiques afin d'obtenir des informations sur les questions qui pourront émerger.

14. Entrevue avec les médias: Programme court qui vise généralement à discuter ou à répondre à des problématiques très restreintes ou ciblées.

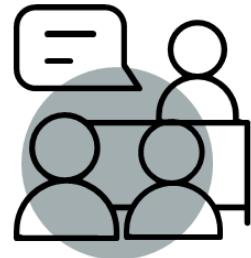
- Possibilité d'atteindre plusieurs personnes.
- Il n'est pas possible de contrôler les questions qui seront posées.
- À moins que la station de radio permette aux auditeurs de téléphoner, il est difficile d'avoir tout type d'échange.
- Garder les messages précis, clairs et simples.
- Participer à ces entrevues si la décision majeure prise est d'un intérêt commun à toute la communauté.

15. Présentation aux groupes: Discussion avec les groupes intéressés, généralement une courte présentation suivie d'une session de questions et de réponses.

- Peut être utilisée pour les groupes internes ou externes.
- Les groupes peuvent être ciblés, l'information peut être adaptée aux besoins du groupe et l'information peut être passée aux autres.
- Fournir des documents écrits à examiner avant la réunion.
- Permettre d'apporter à domicile les documents écrits.

2.4.5 Évaluer la communication

- Un organisme devrait consacrer une période de temps adéquate pour que la communication soit efficace.
- Le temps nécessaire dépend de la nature de la communication, du nombre de parties intéressées, de leurs préoccupations et du type de support utilisé.
- L'organisme devrait revoir et évaluer l'efficacité de sa communication sur la sécurité de l'information.



En évaluant l'efficacité de la communication, l'organisme devrait tenir compte des éléments suivants:

- a. Sa politique de sécurité de l'information
- b. Comment il a appliqué les principes de communication
- c. Si ses objectifs et ses buts ont été atteints
- d. La qualité et l'adéquation de l'information fournie aux groupes cibles et de l'activité de communication sur la sécurité de l'information
- e. La façon dont la communication de sécurité de l'information a été réalisée
- f. Les réponses des parties intéressées
- g. Si le programme de communication a favorisé l'efficacité et un dialogue significatif avec les groupes cibles
- h. Si les procédures et l'approche ont été transparentes
- i. Si la communication de sécurité de l'information a traité les besoins des groupes cibles
- j. Si les groupes cibles sentent qu'ils ont été entendus et ont été informés de la manière dont leur contribution sera utilisée
- k. Si les groupes cibles ont compris le but et le contenu de la communication de sécurité de l'information
- l. Si un suivi approprié a été assuré pour les questions posées par les groupes cibles

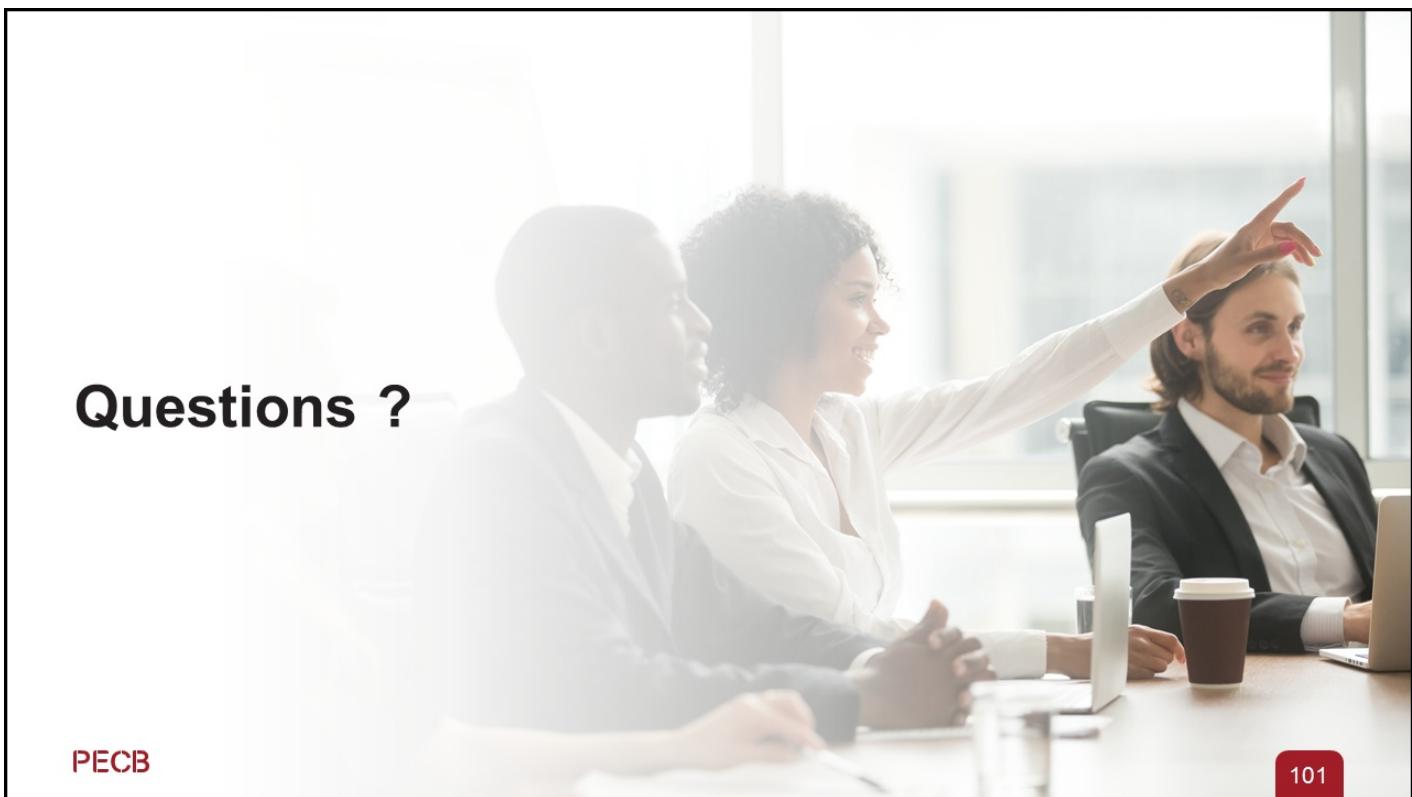
Communication et rapport

Exemple de formulaire

Nom du projet		Numéro de projet		
Responsable	<Nom>	Date	2019-02-21	
Communication		Partie prenante 1	Partie prenante 2	Partie prenante 3
Approche de la communication				
Intérêt et sujets principaux				
Statut actuel (Sympathisant/Neutre/Opposant)				
Soutien désiré (Élevé/Moyen/Faible)				
Rôle du projet prévu (le cas échéant)				
Actions proposées				
Avis requis				
Actions et autres canaux de communication				

PECB

100



Questions ?

PECB

101

Section 18

Plan de formation et de sensibilisation

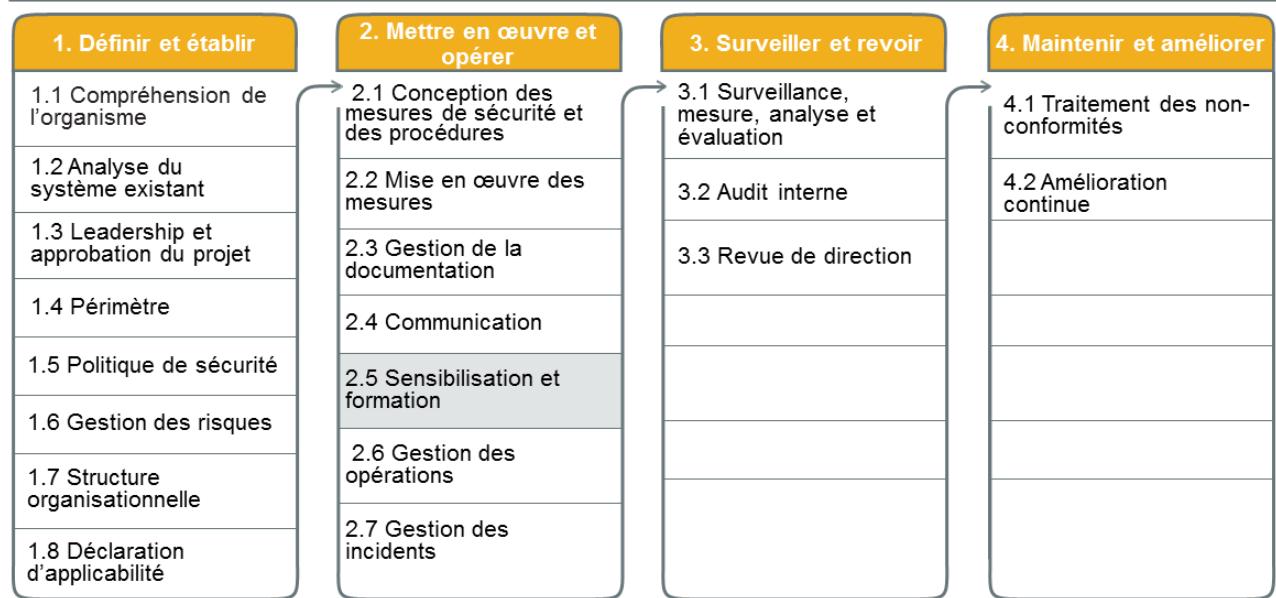
- Définition de la compétence et de la formation
- Différence entre la formation, la sensibilisation et la communication
- Définition des besoins de formation
- Conception et planification de la formation
- Session de formation
- Évaluation des résultats de la formation

PECB

102

La présente section aidera le participant à acquérir des connaissances sur le plan de formation et de sensibilisation, y compris sur la façon de sensibiliser les parties intéressées de l'organisation aux défis de la sécurité de l'information et d'assurer l'adoption des comportements souhaités sur le terrain et d'informer les parties intéressées de l'organisation des actions, améliorations et changements liés au management du SMSI avec le niveau de détail approprié.

2.5 Plan de formation et de sensibilisation



PECB

103

ISO/IEC 27001 Exigences

ISO/IEC 27001, article 7.2 et 7.3

L'organisation doit:

- a) déterminer les compétences nécessaires de la ou des personnes effectuant, sous son contrôle, un travail qui a une incidence sur les performances de la sécurité de l'information;
- b) s'assurer que ces personnes sont compétentes sur la base d'une formation initiale ou continue ou d'une expérience appropriée;
- c) le cas échéant, mener des actions pour acquérir les compétences nécessaires et évaluer l'efficacité des actions entreprises; et
- d) conserver des informations documentées appropriées comme preuves de ces compétences.

NOTE: Les actions envisageables peuvent notamment inclure la formation, l'encadrement ou la réaffectation du personnel actuellement employé ou le recrutement, direct ou en sous-traitance, de personnes compétentes.

Les personnes effectuant un travail sous le contrôle de l'organisation doivent:

- a) être sensibilisées à la politique de sécurité de l'information;
- b) avoir conscience de leur contribution à l'efficacité du système de management de la sécurité de l'information, y compris aux effets positifs d'une amélioration des performances de la sécurité de l'information; et
- c) avoir conscience des implications de toute non-conformité aux exigences requises par le système de management de la sécurité de l'information.

PECB

104

Un organisme qui désire se conformer à ISO/IEC27001 doit:

1. Déterminer ses besoins en compétences pour assurer le bon fonctionnement du SMSI
2. Mettre en œuvre un programme de formation du personnel effectuant un travail ayant une incidence sur le SMSI
3. Mettre en œuvre un programme de sensibilisation en sécurité de l'information adapté aux différentes parties prenantes
4. Mettre en œuvre un programme de communication afin d'informer les parties prenantes des changements au SMSI qui peuvent les concerner
5. Évaluer l'efficacité des actions entreprises et conserver des enregistrements

ISO/IEC 27003, article 7.2 Compétence

Lignes directrices

Il convient que l'organisation:

- a. définitisse 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.

Page de notes

PECB

105

ISO/IEC 27003, article 7.3 Sensibilisation

Lignes directrices

Il convient que l'organisme:

- c) prépare un programme contenant des messages spécifiques axés sur chaque audience (p. ex. les personnes internes et externes);
- d) inclue les besoins et les attentes en matière de sécurité de l'information dans les documents de sensibilisation et de formation relevant d'autres sujets, afin de placer les besoins en matière de sécurité de l'information dans des contextes opérationnels pertinents;
- e) prépare un plan pour communiquer les messages à des intervalles préétablis;
- f) teste la connaissance et la compréhension des messages à la fin d'une session de sensibilisation et de manière aléatoire entre les sessions; et
- g) vérifie si les personnes agissent selon les messages communiqués et utilise des exemples de comportements «bons» et «mauvais» pour renforcer le message.

Compétence et formation

ISO 9000, article 3.10.4 et ISO 10015, article 3.1

Compétence

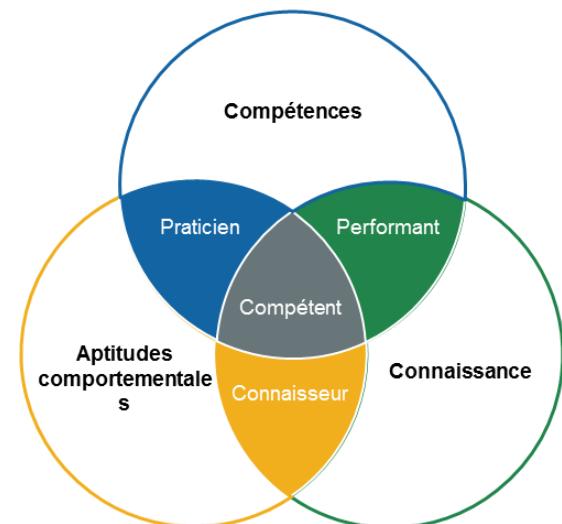
aptitude à mettre en pratique des connaissances et des savoir-faire pour obtenir les résultats escomptés

Formation

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

PECB

106



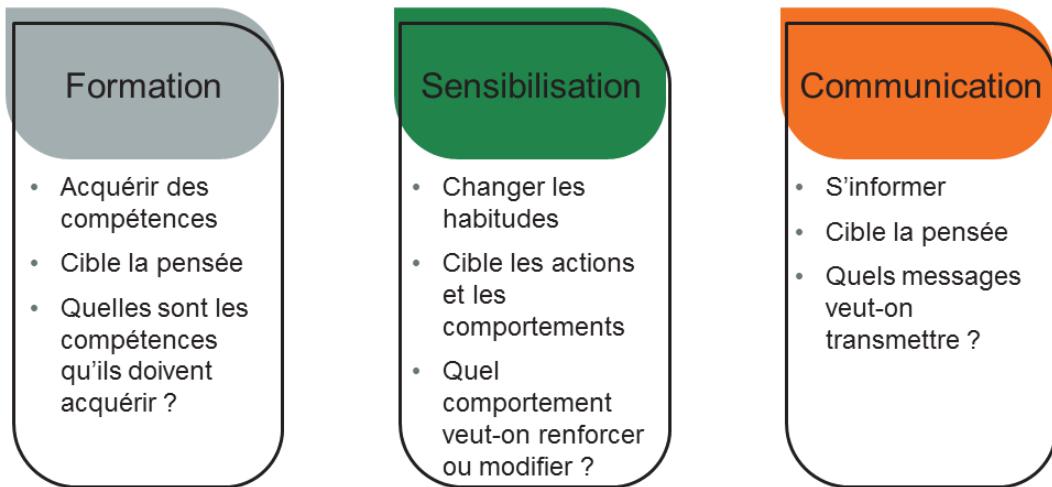
Un processus de formation planifié et systématique peut contribuer à aider un organisme à améliorer ses capacités et à atteindre ses objectifs en matière de sécurité de l'information.

ISO10015:1999, article 4.1.3 Implication du personnel

Le personnel qui s'implique dans le développement de ses compétences au cours d'un processus de formation est susceptible de mieux s'approprier ce processus et, par conséquent d'accroître sa part de responsabilité dans la réussite de la formation.

Formation, sensibilisation et communication

Différences



PECB

107

La grande différence entre formation et sensibilisation est que la formation vise à fournir des compétences permettant à une personne de remplir ses fonctions, tandis que la sensibilisation vise à attirer l'attention sur une ou plusieurs préoccupations individuelles en matière de sécurité de l'information.

La communication permet d'informer les parties prenantes sur un sujet donné.

2.5 Sensibilisation et formation

Liste des activités

2.5.1 Définir les besoins de formation

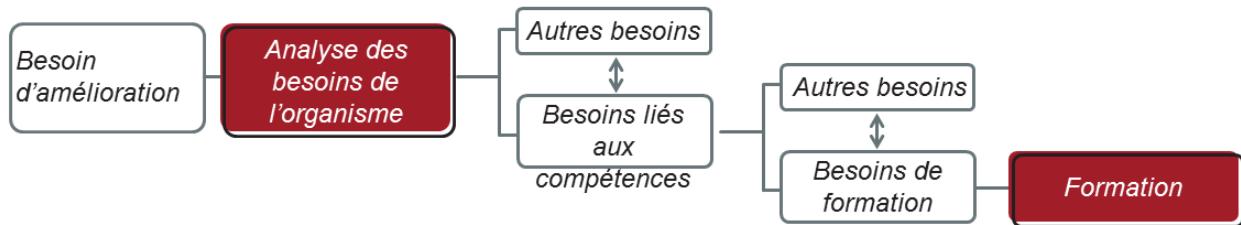
2.5.2 Concevoir et planifier la formation

2.5.3 Pourvoir à la formation

2.5.4 Évaluer les résultats de la formation

2.5.1 Définir les besoins de formation

ISO 10015, article 4.2



PECB

109

ISO10015, article4.2.1 Généralités

Le processus de formation devrait être engagé à l'issue de l'étape d'analyse des besoins de l'organisme et de la description des besoins reliés aux compétences.

4.2.3 Définir et analyser les exigences de compétences

Il convient de formaliser par écrit les exigences de compétences. Cette formalisation peut être révisée périodiquement ou chaque fois que nécessaire, lorsque les tâches sont attribuées ou les performances évaluées.

Les politiques de l'organisme en matière de sécurité de l'information et de formation, les exigences de management de la sécurité de l'information, la gestion des ressources et la conception des processus devraient être prises en compte lors du lancement de la formation afin de garantir que la formation requise sera orientée vers la satisfaction des besoins de l'organisme.

Déterminer les compétences requises

Documenter les besoins de formation spécifiés par fonction

Fonctions	Politique s	Incident	Risque	Audit	Légal
Fonction A	●		●		
Fonction B	■	▲	▲		▲
Fonction C		■		●	
Fonction D			■		▲
Fonction E	●		▲	●	

- Niveau de sensibilisation
- Connaissance
- ▲ Expertise

PECB

110

ISO10015, article4.2.1 Généralités

Il convient que les organismes définissent les compétences nécessaires à chaque tâche ayant un impact sur la qualité des produits, évaluent les compétences du personnel pour accomplir les tâches et planifient des actions pour réduire tout écart existant.

Il convient que cette définition s'appuie sur une analyse des besoins actuels et anticipés de l'organisme par comparaison avec les compétences existantes de son personnel.

L'objectif de cette étape consiste à

- définir les écarts entre les compétences existantes et les compétences requises;*
- définir la formation nécessaire aux personnels dont les compétences existantes ne correspondent pas aux compétences requises par les tâches;*
- spécifier par écrit les besoins de formation.*

Il convient d'analyser les écarts entre les compétences existantes et les compétences requises pour déterminer s'ils peuvent être éliminés par la formation ou si d'autres actions s'avèrent nécessaires.

ISO10015, article4.2.4 Effectuer la revue des compétences

Il convient de mener régulièrement une revue de tous les documents identifiant les compétences requises par chaque processus ainsi que les enregistrements qui répertorient les compétences de chaque membre du personnel.

Les méthodes utilisées pour effectuer la revue des compétences peuvent être les suivantes:

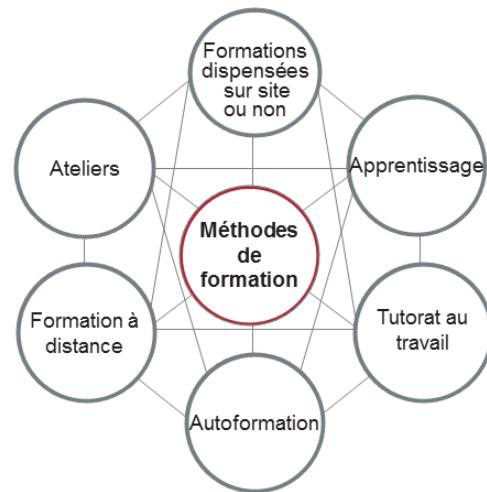
- *les entretiens et questionnaires avec les employés, l'encadrement et la direction;*
- *l'observation;*
- *les discussions de groupe;*
- *les contributions d'experts sur des sujets spécifiques.*

La revue porte sur les exigences des tâches et leur réalisation.

2.5.2 Concevoir et planifier la formation

ISO 10015, article 4.2.7 et 4.3.3

- Quand la formation est une solution pour réduire les écarts de compétences, il convient de spécifier les besoins de formation et de les formaliser par écrit.
- Il convient d'énumérer les méthodes de formation susceptibles de répondre aux besoins de formation. Les types de formation appropriés dépendront des ressources, des contraintes et des objectifs identifiés.



PECB

111

ISO10015, article 4.2.6 Identifier les solutions pour réduire les écarts de compétence (suite)

Les solutions qui permettent de réduire les écarts de compétences peuvent consister en des actions de formation ou bien en d'autres actions conduites par l'organisme comme, par exemple, une reconfiguration de processus, le recrutement d'un personnel déjà formé, une externalisation, une optimisation des autres ressources, la rotation des postes ou la modification des procédures de travail.

4.2.7 Définir la spécification des besoins de formation

Quand la formation est choisie en tant que solution pour réduire les écarts de compétences, il convient de spécifier les besoins de formation et de les formaliser par écrit.

Il convient que la spécification des besoins de formation formalise les objectifs ainsi que les résultats attendus de la formation. Il convient que la liste des exigences de compétences établie en 4.2.3, les résultats des formations antérieures, les écarts de compétences existants et les demandes d'actions correctives fournissent les éléments d'entrée pour l'élaboration de la spécification des besoins de formation. Il convient que cette formalisation soit intégrée dans la spécification du dispositif de formation et qu'elle contienne l'enregistrement des objectifs de l'organisme. Ceux-ci serviront de données d'entrée pour la conception et la planification de la formation ainsi que pour le pilotage du processus de formation.

Page de notes

PECB

112

4.3.3 Modes de formation et critères de sélection

Il convient de définir les modes pertinents de formation susceptibles de répondre aux besoins de formation. Les types appropriés de formation qui sont fonction des ressources, des contraintes et des objectifs identifiés peuvent consister en Les méthodes de formation pourraient inclure:

- cours ou formations dispensés sur site ou au-dehors;
- apprentissage;
- tutorat, coaching et conseil sur le tas;
- autoformation; et
- formation à distance.

Il convient de définir et de formaliser les critères retenus pour choisir au mieux parmi les différents modes possibles de formation. Ces critères peuvent être:

- date et lieu;
- locaux;
- coûts;
- les objectifs de la formation;
- population d'apprenants visés (par exemple, situation professionnelle actuelle ou visée; expertise et/ou expérience spécifique; nombre maximal de participants);
- durée de la formation et séquence de mise en œuvre; et
- modalités d'appréciation, d'évaluation et de certification.

ISO10015, article4.3.4 Cahier des charges du dispositif de formation

Pour négocier les clauses de la proposition d'une formation spécifique avec un prestataire de formation potentiel, il convient d'établir le cahier des charges du dispositif de la formation. Un cahier des charges du dispositif de formation est nécessaire pour établir de façon claire et compréhensible les besoins de l'organisme, ses besoins de formation et les objectifs qui définiront ce que les apprenants seront capables de réaliser après la formation.

Pour garantir une prestation efficace de formation et créer les conditions d'une communication claire et ouverte, il convient que les objectifs de la formation s'appuient sur les compétences attendues et décrites dans le document de spécification des besoins de formation.

Il convient que le cahier des charges du dispositif de formation comprenne une description des éléments suivants:

- a. *les objectifs et les exigences de l'organisme;*
- b. *la spécification des besoins de formation;*
- c. *les objectifs de la formation;*
- d. *les personnes à former (groupes ou populations de personnel visés);*
- e. *les modes de formation et contenus indicatifs;*
- f. *la chronologie des exigences, par exemple: durée, dates, étapes clés;*
- g. *les ressources nécessaires, par exemple: supports de cours et formateurs;*
- h. *les contraintes financières;*
- i. *les critères et les méthodes pour l'évaluation des résultats de la formation.*

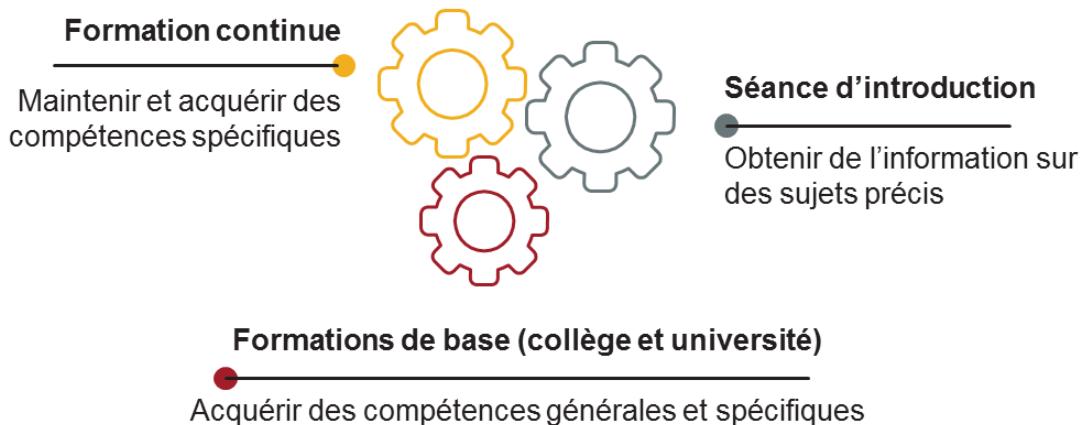
4.3.5 Sélectionner un prestataire de formation

Il convient que tout prestataire de formation interne ou externe fasse l'objet d'un examen critique avant d'être choisi. Cet examen peut porter sur la documentation écrite du prestataire (catalogues, dépliants) et sur des rapports d'évaluation. Il convient que cet examen s'appuie sur le cahier des charges du dispositif de formation et qu'il tienne compte des contraintes identifiées.

Il convient que le choix du prestataire fasse l'objet d'un contrat formel établissant les droits de propriété et les responsabilités relatives au processus de formation.

Programme de formation

Types de programme et objectifs



PECB

113

L'objectif fondamental de l'éducation est de permettre aux individus d'acquérir des compétences générales et spécifiques. Les programmes d'éducation sont habituellement offerts par les collèges et les universités.

La formation continue comprend toutes les activités formelles et informelles qui aident à entretenir et à acquérir des compétences spécifiques.

Une séance d'introduction est une courte séance de formation qui fournit des informations générales sur un sujet spécifique. La durée varie d'une heure à quelques jours, en fonction de l'objet et de la portée à laquelle elle s'adresse.

Une formation à plus long terme permet de développer une large expertise en sécurité de l'information. Ces dernières années, plusieurs universités et collèges offrent des formations spécialisées complètes en sécurité de l'information.

Les formations à long terme peuvent apporter une expertise et une spécialisation supplémentaire à certains employés responsables de la sécurité de l'information dans des domaines spécifiques.

La formation de base permet à tous les employés et autres parties prenantes de l'organisme, quel que soit leur domaine de spécialisation ou leur niveau de responsabilité, d'améliorer leurs compétences de base en matière de sécurité de l'information.

Des entreprises technologiques comme Microsoft, CheckPoint ou Cisco ont popularisé les certifications dites professionnelles, qui sont généralement obtenues après avoir suivi un cours suivi d'un examen. Au cours des dernières années, des certifications professionnelles en sécurité de l'information ont été développées, indépendamment de tout éditeur. Ces certifications peuvent contribuer au développement personnel et à la reconnaissance du marché.

Page de notes

PECB

114

Les principales certifications indépendantes en sécurité de l'information sont:

1. Pour les professionnels ISO/IEC27001: ISO/IEC 27001 Lead Auditor, ISO/IEC 27001 Lead Implementer et ISO/IEC 27005 Certified Risk Manager
2. Pour une expérience professionnelle en sécurité de l'information: CISSP, CISA, CISM
3. Pour les nouveaux diplômés: Security+, SSCP, ISMS Foundation, COBIT Foundation

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 la diffusion et à la mise en œuvre des politiques, directives et procédures

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



Le facteur technologique est l'un des paramètres clés dans le processus de mise en place d'un système de management fonctionnel ; cependant, le facteur « humain » est tout aussi important pour garantir son efficacité. Si l'humain est la clé, il est aussi le maillon faible, et il faut prêter attention à cet « actif ». Le personnel doit connaître et comprendre quelles sont ses responsabilités, comment il peut contribuer à la sécurité de l'information (management) et comment il peut avoir une influence positive sur l'entreprise.

En ce qui concerne la sensibilisation des parties prenantes, l'objectif majeur consiste à renforcer ou modifier leurs comportements et attitudes ainsi qu'à les amener à adhérer aux valeurs de l'organisme.

Programme de sensibilisation

Principaux domaines qui doivent être abordés

- | | |
|--|--|
|  Politique de sécurité |  Gestion des incidents de sécurité |
|  Utilisation de mots de passe |  Utilisation d'outils de chiffrement |
|  Protection contre les virus |  Sécurité des ordinateurs portables et <i>smartphones</i> |
|  Bon usage d'Internet |  Utilisation au travail de logiciels/systèmes d'ordre privé |
|  Risques associés aux e-mails (<i>SPAM, phishing, code malveillant</i>) |  Respect de la propriété intellectuelle |
|  Sauvegarde et stockage de données |  Problèmes liés au contrôle d'accès |
|  Ingénierie sociale |  Rôles et responsabilités individuels |

2.5.3 Pourvoir à la formation

ISO 10015, article 4.4

Il incombe au prestataire de formation de réaliser toutes les activités en rapport avec l'action de formation telles que spécifiées dans le cahier des charges du dispositif de formation.

Cependant, outre la mise à disposition des ressources nécessaires au prestataire de formation, le rôle assumé par l'organisme pour encadrer et faciliter la formation pourraient inclure les opérations suivantes:

- *apporter son appui au formateur et à l'apprenant; et*
- *piloter la qualité de la formation.*



PECB

117

ISO10015, article 4.4.2.1 Appui précédent l'action de formation

Une aide précédant l'action de formation peut inclure les activités suivantes:

- *donner au prestataire les informations appropriées (voir 4.2);*
- *informer l'apprenant sur la nature de la formation et sur les écarts de compétences que celle-ci vise à réduire; et*
- *permettre le contact entre le formateur et l'apprenant.*

4.4.2.2 Appui au cours de l'action de formation

Un appui au cours de l'action de formation peut inclure les activités suivantes:

- *fournir à l'apprenant, au formateur ou aux deux, les outils, les équipements, les documents et les logiciels appropriés;*
- *offrir à l'apprenant les possibilités adéquates de mise en œuvre des compétences en cours d'acquisition; et*
- *donner au formateur, à l'apprenant ou aux deux les appréciations relatives aux travaux réalisés.*

4.4.2.3 Appui suivant l'action de formation

Un appui suivant l'action de formation peut inclure les activités suivantes:

- *obtenir un retour d'information de l'apprenant;*
- *obtenir un retour d'information du formateur; et*
- *fournir un retour d'information au personnel concernés par le processus de formation.*

2.5.4 Évaluer les résultats de la formation

ISO 10015, article 4.5

Les buts de l'évaluation sont de confirmer que la formation a bien permis d'atteindre les objectifs de l'organisme et ceux du dispositif de formation, en d'autres termes que la formation a été efficace.



PECB

118

ISO10015, article4.5.1 Généralités

Les données d'entrée de l'évaluation des résultats de la formation sont la spécification des besoins de formation, le cahier des charges du dispositif de formation et les données enregistrées à l'issue de la réalisation de la formation.

Il est souvent impossible d'analyser et de valider intégralement les résultats de la formation avant que les personnes formées ne soient en situation d'être observées ou testées en situation de travail.

Dans un délai donné suivant la fin de la formation, il convient que la direction de l'organisme s'assure qu'une évaluation destinée à vérifier le niveau de compétences atteint a bien été effectuée.

Il convient que l'évaluation intervienne à la fois à court terme et à long terme:

- à court terme pour recueillir le retour d'information sur les méthodes et les ressources utilisées, ainsi que sur les progrès dans les connaissances et les capacités issues de la formation; et
- à long terme pour apprécier la performance dans le travail et l'amélioration de la productivité.

Il convient que l'évaluation s'appuie sur les critères préétablis.

Il convient que le processus d'évaluation intègre la collecte des données et la préparation du rapport d'évaluation qui fournit également des données d'entrée du processus de pilotage.



Questions ?

PECB

119

Section 19

Gestion des opérations

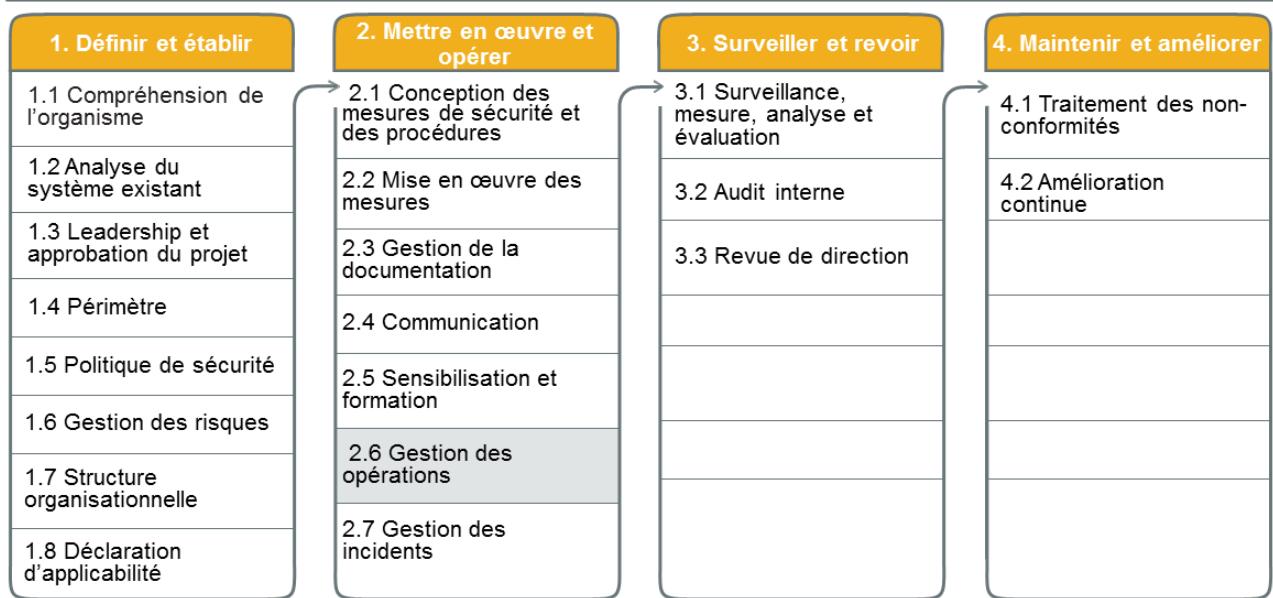
- Planification de la gestion du changement
- Transfert aux opérations
- Gestion des ressources nécessaire au maintien du SMSI

PECB

120

Cette section aidera le participant à acquérir des connaissances sur la gestion des opérations, y compris la planification de la gestion du changement et la gestion des ressources nécessaires au maintien du SMSI.

2.6 Gestion des opérations



PECB

121

Exigences ISO/IEC 27001

8.1 Planification et contrôle opérationnels

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.

5.1 Leadership et engagement

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

- c) s'assurant que les ressources nécessaires pour le système de management de la sécurité de l'information sont disponibles;

7.1 Ressources

L'organisation doit identifier et fournir les ressources nécessaires à l'établissement, la mise en œuvre, la tenue à jour et l'amélioration continue du système de management de la sécurité de l'information.



PECB

122

Un organisme qui désire se conformer à ISO/IEC27001 doit:

1. S'assurer de la gestion efficace des opérations liées au SMSI
2. Assurer la mise à disposition de ressources adéquates pour le fonctionnement du SMSI

ISO/IEC27003, article 8.1 Planification et contrôles opérationnels

Explication

Les processus de conformité aux exigences de sécurité de l'information comprennent:

- a. les processus SMSI (par exemple: revue de direction, audit interne); et
- b. les processus requis pour la mise en œuvre du plan de traitement des risques liés à la sécurité de l'information.

La mise en œuvre des plans entraîne des processus exploités et contrôlés.

Ultimement, l'organisme est responsable de la planification et du contrôle de tout processus externalisé afin d'atteindre ses objectifs en matière de sécurité de l'information. Ainsi, l'organisme doit:

- c.déterminer les processus externalisés en tenant compte des risques de sécurité de l'information liés à la sous-traitance; et
- d.s'assurer que les processus externalisés sont contrôlés (c'est-à-dire planifiés, surveillés et examinés) de manière à garantir qu'ils fonctionnent comme prévu (en tenant compte des objectifs de sécurité de l'information et du plan de traitement des risques de sécurité de l'information).

Page de notes

PECB

123

ISO/IEC27003, article5.1 Leadership et engagement

Lignes directrices

Il convient que la direction fournisse un leadership et fasse preuve d'engagement par le biais de ce qui suit:

- a. *il convient que la direction veille à ce que la politique de sécurité de l'information et ses objectifs soient établis et compatibles avec la stratégie de l'organisme;*
- b. *il convient que la direction s'assure que les exigences et les mesures SMSI soient intégrées dans les processus de l'organisme. La manière d'y parvenir devrait être adaptée au contexte spécifique de l'organisme. Par exemple, un organisme qui a désigné des propriétaires de processus peut déléguer la responsabilité de la mise en œuvre des exigences applicables à ces personnes ou groupes de personnes. Le soutien de la direction peut également être nécessaire pour surmonter la résistance organisationnelle aux changements de processus et de mesures;*
- c. *il convient que la direction s'assure de la disponibilité des ressources nécessaires à un SMSI efficace. Les ressources sont nécessaires à la mise en place du SMSI, à sa mise en œuvre, à sa maintenance et à son amélioration, ainsi qu'à la mise en œuvre des mesures de sécurité de l'information. Les ressources nécessaires au SMSI comprennent:*
 1. *les ressources financières;*
 2. *le personnel;*
 3. *les installations; et*
 4. *l'infrastructure technique.*
 - *Les ressources nécessaires dépendent du contexte de l'organisme, comme la taille, la complexité, ainsi que les exigences internes et externes. La revue de direction devrait fournir des renseignements qui indiquent si les ressources sont adéquates pour l'organisme;*
- d. *il convient que la direction communique la nécessité du management de la sécurité de l'information au sein de l'organisme et la nécessité de se conformer aux exigences du SMSI. Cela peut se faire en donnant des exemples pratiques qui illustrent le besoin réel dans le contexte de l'organisme et en communiquant les exigences de sécurité de l'information;*

ISO/IEC 27003, article7.1 Ressources

Explication

Les ressources sont essentielles pour effectuer tout type d'activité. Les catégories de ressources peuvent inclure:

- a. des personnes pour mener et exploiter les activités;
- b. le temps nécessaire pour réaliser les activités puis pour que les résultats s'installent avant de franchir une nouvelle étape;
- c. les ressources financières pour acquérir, développer et mettre en œuvre ce qui est nécessaire; et
- d. de l'information pour appuyer les décisions, mesurer la performance des actions et améliorer les connaissances; et
- e. l'infrastructure et les autres moyens qui peuvent être acquis ou construits, tels que la technologie, les outils et les supports, indépendamment du fait qu'ils soient ou non des produits de la technologie de l'information.

Lignes directrices

Il convient que l'organisme:

- f.estime les ressources nécessaires pour toutes les activités liées au SMSI en termes de quantité et qualité (compétences et aptitudes);
- g.acquière les ressources nécessaires;
- h.fournisse les ressources;
- i.maintienne les ressources tout au long des processus SMSI et des activités spécifiques; et
- j.examine les ressources qui vont à l'encontre des besoins du SMSI et les modifie selon les besoins.

2.6 Gestion des opérations

Liste des activités

2.6.1

Planifier la gestion du changement

2.6.2

Transférer aux opérations

2.6.3

Assurer la gestion des ressources

2.6.1 Planifier la gestion du changement

- Fournir un plan de communication pour les utilisateurs avant le transfert aux opérations
- Éviter de mettre en œuvre trop de nouveaux processus en même temps
- Assurer la formation du personnel, le cas échéant, avant de transférer à un mode de fonctionnement



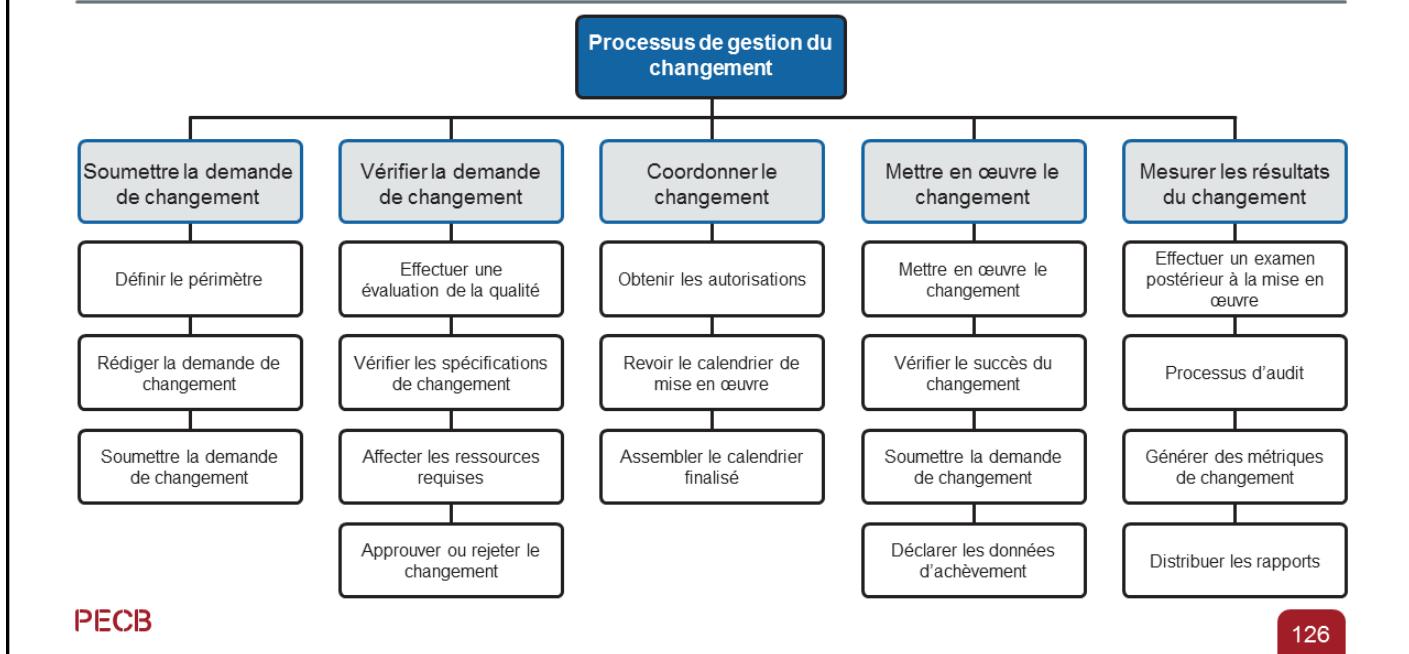
PECB

125

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. Toutefois, l'ampleur d'un changement peut nécessiter un minimum de communication ou de formation. Chaque changement doit donc être jugé en fonction de ses mérites propres.

Bien entendu, il pourrait s'agir d'un changement très important: un SMSI dans son ensemble passant officiellement en mode opérationnel pour la première fois, auquel cas il convient que cela soit l'aboutissement d'un plan de mise en œuvre.

Processus de gestion du changement



Soumettre une demande de changement: Avant la préparation d'une demande de changement, le demandeur et le personnel (potentiellement) responsable de la mise en œuvre du changement devraient coordonner tous les aspects techniques du changement. Les changements inclus dans la demande de changement devraient être testés.

Vérifier la demande de changement: Après la soumission d'une demande de changement, un processus de vérification devrait être mené.

Coordonner le changement: Le groupe responsable de la mise en œuvre d'un changement est chargé d'affiner le calendrier final des changements.

Mettre en œuvre le changement: La mise en œuvre du changement relève de la responsabilité de l'exécutant. Toutefois, il peut y avoir un autre niveau d'autorité pour la mise en œuvre du changement (prouvé) dans un mode opérationnel (p. ex. le coordonnateur du SMSI). La portée et la nature du changement (et peut-être de l'organisation) devraient déterminer qui, et à quel niveau, autorise un changement réalisé.

Mesurer les résultats du changement: Cette phase comprend la revue des éléments suivants:

- Documentation de la demande de changement
- État final de la mise en œuvre
- Métriques

2.6.2 Transférer aux opérations

Gestion des opérations

Lorsque la mise en œuvre du SMSI est terminée, que le SMSI soit mis en œuvre pour la première fois ou que le système existant soit modifié, la transition vers les opérations quotidiennes devrait se faire en douceur sans interrompre le processus opérationnel principal.

PECB

127

Dans la pratique, bien qu'il y ait peut-être un lancement officiel du SMSI (p. ex., il passe officiellement en mode opérationnel) il est beaucoup plus probable que le passage en mode opérationnel se fasse progressivement. Au fur et à mesure que les éléments du SMSI sont terminés et validés (p. ex. approuvés), il convient de les mettre en mode opérationnel – le SMSI doit assurément être en cours de mise en œuvre, car l'organisation pourra en tirer des avantages. Il semble peu judicieux de retarder la réalisation de ces avantages jusqu'à ce qu'un événement catastrophique se produise. Les processus et les mesures visant à réduire les risques organisationnels ne le feront pas avant leur mise en service.

Ainsi, bien qu'il faille gérer le transfert aux opérations, le processus devrait être continu.

2.6.3 Assurer la gestion des ressources

Afin de s'assurer du maintien et de l'amélioration du système de management, l'organisation doit allouer suffisamment de ressources aux activités de maintien du SMSI :



Budget



Personnel qualifié



Matériel nécessaire

PECB

128

ISO/IEC 27021, article 5.9 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
- Budgérer 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

Questions ?



PECB

129

Section 20

Gestion des incidents

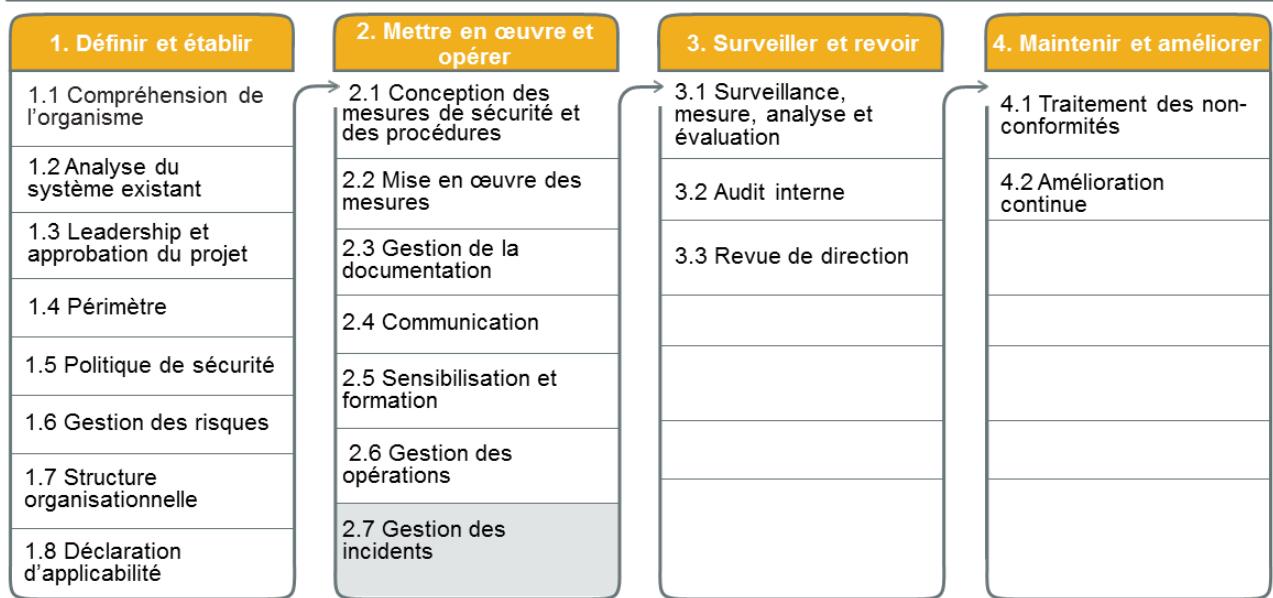
- ISO/IEC 27035
- Politique de gestion des incidents en sécurité de l'information
- Processus et procédure de gestion des incidents
- Équipe de réponse aux incidents
- Mesures de sécurité liées à la gestion des incidents
- Processus de cyberenquête
- Enregistrements des incidents de sécurité
- Mesure et revue du processus de gestion des incidents

PECB

130

Cette section aidera le participant à acquérir des connaissances sur la gestion des incidents, y compris la politique de gestion des incidents de sécurité de l'information et l'équipe de réponse aux incidents.

2.7 Gestion des incidents



PECB

131

Page de notes

PECB

132

Définitions relatives aux incidents de sécurité de l'information

ISO/IEC27000, article 3.30 Événement lié à la sécurité de l'information

occurrence identifiée de l'état d'un système, d'un service ou d'un réseau indiquant une faille possible dans la politique de sécurité de l'information ou un échec des mesures de sécurité, ou encore une situation inconnue jusqu'alors et pouvant relever de la sécurité

ISO/IEC 27035-1, article 3.3 Événement lié à la sécurité de l'information

occurrence indiquant une possible violation de la sécurité de l'information ou l'échec des mesures

ISO/IEC27000, article 3.31 Incident lié à la sécurité de l'information

un ou plusieurs événements liés à la sécurité de l'information, indésirables ou inattendus, présentant une probabilité forte de compromettre les opérations liées à l'activité de l'organisme et de menacer la sécurité de l'information

ISO/IEC27035-1, article3.4 Incident de sécurité de l'information

un ou plusieurs événements de sécurité de l'information reliés et identifiés, qui peuvent nuire aux actifs d'un organisme ou compromettre ses opérations

ISO/IEC27000, article 3.32 Gestion des incidents liés à la sécurité de l'information

ensemble de processus visant à détecter, rapporter, apprécier, gérer et résoudre les incidents liés à la sécurité de l'information, ainsi qu'à en tirer des enseignements

ISO/IEC 27035-1, article 3.5 Gestion des incidents de sécurité de l'information

exercice d'une approche cohérente et efficace pour le traitement des incidents de sécurité de l'information

ISO/IEC27035-1, article3.1 Enquête sur la sécurité de l'information

application de vérifications, d'analyses et d'interprétations pour faciliter la compréhension d'un incident de sécurité de l'information

ISO/IEC27035-1, article3.2 Équipe de réponse aux incidents ERI

équipe composée de membres de l'organisme ayant les compétences et la confiance nécessaires pour gérer les incidents au cours de leur cycle de vie

Note de terminologie:

1. ISO/IEC 27035 distingue un incident de sécurité d'un événement de sécurité. **Un incident de sécurité possède une forte probabilité** de compromettre l'activité de l'organisme alors qu'un événement pointe vers une **possible faille** de sécurité. Un incident de sécurité est la concrétisation d'un risque qui impacte la confidentialité, l'intégrité ou la disponibilité des ressources informationnelles et menace, selon son degré de sévérité, la poursuite des activités de votre organisme.
2. ISO/IEC 27005 définit un scénario d'incident comme toute menace qui exploiterait une ou plusieurs vulnérabilités durant un incident de sécurité de l'information.
3. ISO/IEC27001 décrit l'occurrence d'un scénario d'incident comme étant une «faille de sécurité».
4. Ne confondez pas la définition des incidents de sécurité avec la définition de «défaut» telle que définie dans ITIL: «Tout événement qui ne fait pas partie du fonctionnement standard d'un service et qui cause, ou peut causer, une interruption ou une diminution de la qualité de ce service».

La norme ISO/IEC 27035-1

- Concepts et phases de base pour la gestion des incidents de sécurité de l'information
- Combine ces concepts avec des principes dans une approche structurée
- Document de référence à utiliser comme complément des normes ISO/IEC 27001 et ISO/IEC 27002
- Ne mène pas à la certification



PECB

133

ISO/IEC27035-1 présente les lignes directrices pour planifier, mettre en œuvre, gérer et améliorer un processus de gestion des incidents pour un organisme dans le contexte de la mise en œuvre d'un SMSI. Cette norme fournit des informations supplémentaires sur les mesures de sécurité décrites dans ISO/IEC27001 et ISO/IEC27002. Il convient de noter qu'un organisme n'a aucune obligation de suivre ses recommandations pour se préparer à la certification ISO/IEC27001.

ISO/IEC27035-1, article1 Domaine d'application

Cette première de deux parties d'ISO/IEC27035 est le fondement de cette norme internationale. Elle présente les concepts de base et les phases de la gestion des incidents de sécurité de l'information et combine ces concepts avec les principes dans une approche structurée pour détecter, déclarer, apprécier et répondre aux incidents et appliquer les leçons apprises.

Les principes énoncés dans cette partie d'ISO/IEC27035 sont génériques et destinés à tous les organismes, quels que soient leur type, leur taille ou leur nature. Les organismes peuvent ajuster les directives données dans cette partie d'ISO/IEC27035 en fonction de leur type, leur taille et de la nature de leurs activités par rapport à la situation de risque en sécurité de l'information. Cette partie d'ISO/IEC27035 s'applique également aux organismes externes qui fournissent des services de gestion des incidents de sécurité de l'information.

La norme ISO/IEC 27035-2

- Lignes directrices pour planifier et préparer une réponse aux incidents
- Document de référence à utiliser comme complément des normes ISO/IEC 27001 et ISO/IEC 27002
- Un nouveau modèle : Phases de gestion des incidents de sécurité de l'information : Planification et préparation, Leçons à retenir,
- Ne mène pas à la certification



PECB

134

ISO/IEC 27035-2 fournit des lignes directrices afin de planifier, mettre en œuvre, gérer et améliorer un processus de gestion des incidents d'un organisme dans le cadre de la mise en œuvre d'un système de management de la sécurité de l'information (SMSI). Cette norme fournit des informations supplémentaires sur les mesures de sécurité décrites dans ISO/IEC27001 et ISO/IEC27002. Il convient de noter qu'un organisme n'a aucune obligation de suivre ses recommandations en vue de la certification ISO/IEC27001.

ISO/IEC27035-2, article1 Domaine d'application

Cette seconde partie d'ISO/IEC27035 fournit les lignes directrices pour planifier et préparer la réponse aux incidents. Les lignes directrices sont basées sur la phase « Planification et préparation » et la phase « Leçons à retenir » du modèle « Phase de gestion des incidents de sécurité de l'information » présenté dans ISO/IEC27035-1.

La phase « Planification et préparation » comprend les éléments suivants:

- politique de gestion des incidents de sécurité de l'information et engagement de la direction;
- politiques de sécurité de l'information, y compris celles relatives à la gestion des risques, mises à jour tant pour l'entreprise que sur le plan du système, du service et du réseau;
- plan de gestion des incidents de sécurité de l'information;
- établissement d'une équipe de réponse aux incidents de sécurité (ERI);
- établissement des relations et des liens avec des organismes internes et externes;
- soutien technique et autres formes de soutien (y compris le soutien organisationnel et opérationnel);
- activités d'information et de sensibilisation à la gestion des incidents de sécurité de l'information;
- test du plan de gestion des incidents de sécurité de l'information.

Les principes énoncés dans cette partie d'ISO/IEC27035 sont génériques et destinés à tous les organismes, quels que soient leur type, leur taille ou leur nature. Les organismes peuvent ajuster les lignes directrices d'ISO/IEC27035 en fonction du type, de la taille et de la nature des activités de la sécurité de l'information. Cette partie d'ISO/IEC27035 s'applique également aux organismes externes qui fournissent des services de gestion des incidents de sécurité de l'information.

ISO/IEC 27035-1

ISO/IEC 27035-1, article 5

PLANIFICATION ET PRÉPARATION

- politique de gestion des incidents de sécurité de l'information et engagement de la direction
- politiques de sécurité de l'information, y compris celles liées à la gestion des risques, mises à jour tant pour l'entreprise que sur le plan du système, du service et du réseau;
- plan de gestion des incidents de sécurité de l'information
- établissement de l'ERI (équipe de réponse aux incidents)
- relations et liens avec les organismes internes et externes
- appui technique et autres formes de soutien (y compris le soutien organisationnel et opérationnel)
- sensibilisation et formation à la gestion des incidents de la sécurité de l'information
- test du plan de gestion des incidents de sécurité de l'information

DÉTECTION ET SIGNALLEMENT

- collecte d'informations sur la situation de l'environnement local et des sources de données externes ainsi que des flux d'actualités
- suivi des systèmes et des réseaux de circonscription
- détection et signalement d'activités anormales, suspectes ou malveillantes
- collecte de rapports sur les événements liés à la sécurité de l'information provenant de constituants, de revendeurs, d'autres ERI ou d'organismes de sécurité et de détecteurs automatisés
- rapport des événements de sécurité de l'information

PECB

135



ISO/IEC 27035-1

ISO/IEC 27035-1, article 5 (suite)

APPRÉCIATION ET DÉCISION

- évaluation de la sécurité de l'information et détermination de l'incident de sécurité de l'information



INTERVENTIONS

- enquêtes visant à déterminer si les incidents liés à la sécurité de l'information sont maîtrisées
- confinement et éradication des incidents de sécurité de l'information
- mesures de reprise après les incidents de sécurité de l'information
- résolution et clôture des incidents de sécurité de l'information

LEÇONS À RETENIR

- identification des leçons à retenir
- identification et amélioration de la sécurité de l'information
- identification et amélioration de l'appréciation des risques de sécurité de l'information et des résultats de revue de direction
- identification et amélioration du plan de gestion des incidents de sécurité de l'information
- évaluation de la performance et de l'efficacité de l'ERI

ACTIVITÉ POST-INCIDENT

- Une enquête plus approfondie, si nécessaire

PECB

136

2.7 Gestion des incidents

Liste des activités

2.7.1

Créer une politique de gestion des incidents

2.7.6

Enregistrer les informations relatives aux incidents de sécurité

2.7.2

Définir le processus et rédiger les procédures

2.7.7

Mesurer et revoir le processus de gestion des incidents

2.7.3

Mettre sur pied une équipe de réponse aux incidents

2.7.4

Mettre en œuvre les mesures de sécurité

2.7.5

Définir un processus de cyberenquête

PECB

137

2.7.1 Créer une politique de gestion des incidents

ISO/IEC 27035-2, article 4.3

Il convient que la politique de gestion des incidents de sécurité de l'information inclue les éléments suivants :

- Engagement de la direction
- Définition d'un incident de sécurité de l'information
- Rôles et responsabilités
- Collecte et conservation des enregistrements
- Formation et sensibilisation
- Référence aux exigences légales, réglementaires et contractuelles



PECB

138

L'article 4.3 d'ISO/IEC 27035-2 souligne l'importance d'une politique claire et efficace en matière de gestion des incidents de sécurité de l'information.

La politique devrait tenir compte des éléments suivants:

Engagement de la direction: La direction générale doit soutenir les initiatives énoncées dans la politique et s'assurer que tous les membres de l'organisme inclus dans le périmètre comprennent la valeur et l'importance d'une politique et de processus associés efficaces dans ce domaine. Lorsqu'un incident survient, personne ne doit douter de l'importance de la politique et tous doivent travailler en conformité avec les exigences clairement énoncées.

Définition d'un incident de sécurité de l'information: Ceci devrait être clair et sans ambiguïté. Tout membre de l'organisme devrait être en mesure d'identifier si un événement ou un ensemble d'événements constitue un incident. Une telle clarté est vitale à la rédaction de rapports précis et détaillés, mais aussi pour une réponse efficace.

Rôles et responsabilités: Il convient que toutes les personnes impliquées dans l'organisme comprennent leur rôle et leur position de manière claire lorsqu'il s'agit d'identifier, de signaler et de répondre aux incidents.

Collecte et conservation des enregistrements: Au cours du rapport, de l'intervention et de l'analyse d'un incident, divers enregistrements seront générés. Il doit être clair pour quiconque est impliqué lesquels des documents devraient être créés, où ces documents doivent être conservés, et le format et le contenu des types d'enregistrement spécifiques.

Page de notes

PECB

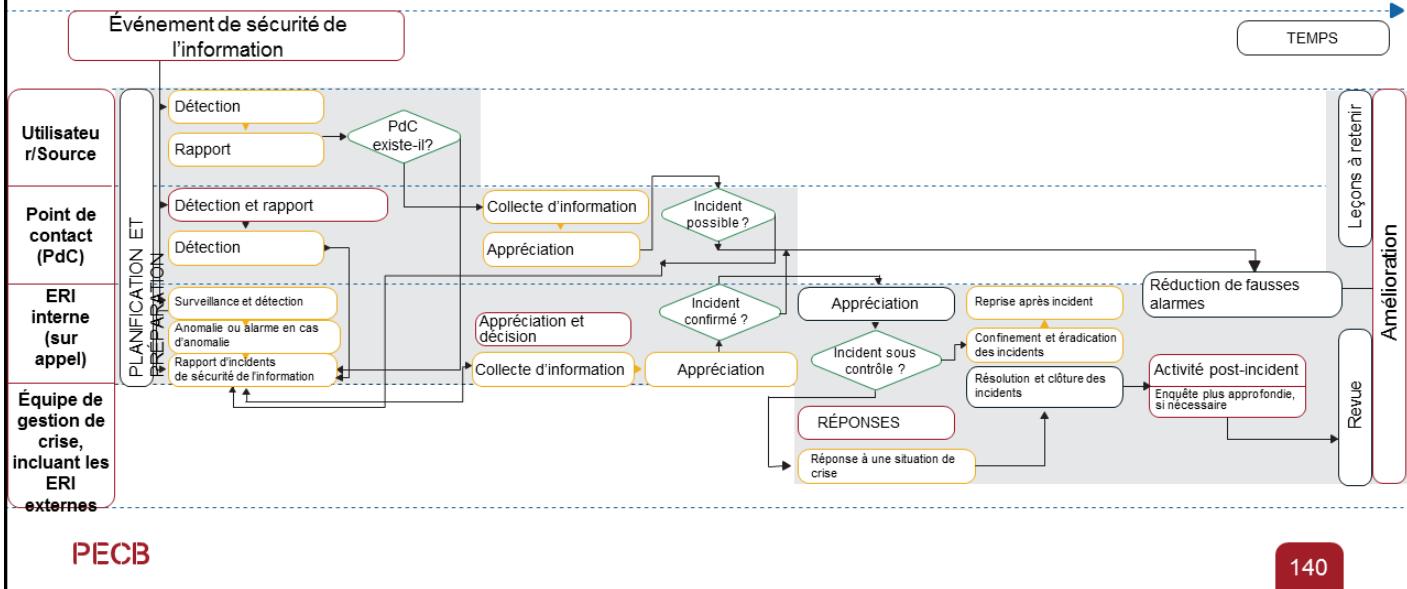
139

Formation et sensibilisation: En général, la sensibilisation à la sécurité de l'information est essentielle à la posture globale de sécurité d'un organisme. Une partie importante de ce processus de sensibilisation doit inclure une description claire de ce qu'est un incident, l'importance de signaler l'incident et le dispositif de signalement.

Référence aux exigences légales, réglementaires et contractuelles: S'assurer que les personnes impliquées dans la gestion des incidents comprennent les lois et réglementations pertinentes est essentiel à tout processus efficace de gestion des incidents. Certaines lois et réglementations exigent que les incidents soient abordés et signalés dans un délai déterminé. D'un point de vue contractuel, les organismes peuvent avoir l'obligation de signaler ou de traiter les incidents dans certains délais dictés par les clients.

Cette politique peut être intégrée à la politique globale de sécurité de l'information ou à une politique globale de gestion des incidents intégrant différents aspects tels que les incidents environnementaux, de santé et de sécurité.

2.7.2 Définir le processus et rédiger les procédures



Note importante :

Notez que la figure de la diapositive est expliquée dans les pages de notes suivantes.

Page de notes

PECB

141

1.Détection et rapport

Lorsqu'un événement lié à la sécurité de l'information est détecté, la personne responsable lance le processus de détection et de rapport. Cette personne doit suivre les procédures et utiliser le formulaire de rapport pour le type d'événement, comme indiqué dans la procédure appropriée, afin de porter l'événement à l'attention du groupe de soutien opérationnel. Tout le personnel devrait être informé des procédures de rapport des événements liés à la sécurité de l'information et y avoir accès.

2.Évaluation initiale et décision

À la réception d'un rapport d'événement, le groupe de soutien aux opérations doit remplir le ticket d'événement de sécurité de l'information, l'analyser (triage) et lui attribuer une priorité. Au besoin, la personne recevant le rapport devrait demander des éclaircissements à la personne qui l'a produit et recueillir toute information complémentaire, en sollicitant éventuellement des éléments d'entrée d'autres sources.

Après la réception initiale de l'événement, une évaluation visant à déterminer si le rapport d'événement doit faire l'objet d'une analyse plus approfondie devrait être faite, essentiellement pour déterminer si l'événement doit être classé comme incident de sécurité de l'information ou s'il s'agit d'une fausse alerte.

S'il est déterminé que l'événement de sécurité de l'information peut être un incident et si le soutien opérationnel du groupe a le niveau de compétence approprié, une évaluation supplémentaire peut être effectuée. Cela peut entraîner des actions correctives ; par exemple, les mesures de protection d'urgence sont identifiées et renvoyées aux personnes compétentes afin que des actions puissent être prises.

3.Deuxième évaluation et confirmation d'un incident

La deuxième évaluation et la confirmation ou non de la décision de clore ou non l'incident dans la catégorie de la sécurité de l'information devraient relever du CSIRT (Computer Security Incident Response Team), si un CSIRT a été mis en place. S'il est déterminé que l'incident de sécurité de l'information est réel, alors un membre du CSIRT, impliquant des collègues au besoin, devrait effectuer une évaluation plus approfondie. L'objectif est de confirmer la nature de l'incident de sécurité de l'information, comment il a été causé – et ce qu'il pourrait affecter ou qui, l'impact ou l'impact potentiel de l'incident sur les activités de l'organisme, une indication si l'incident de sécurité de l'information est jugé important ou pas (à l'aide de la matrice préalable de l'organisme).

Page de notes

PECB

142

4.Réponse

Dans la plupart des cas, pour le membre CSIRT, l'activité suivante consistera à identifier les actions de réponse immédiate pour traiter l'incident de sécurité de l'information, enregistrer les détails sur le formulaire d'incident de sécurité de l'information et dans la base de données d'événements/incidents de sécurité de l'information, et informer les personnes ou groupes appropriés des actions requises. Cela peut se traduire par des mesures de protection d'urgence (par exemple, l'isolement ou l'arrêt d'un système d'information, d'un service ou d'un réseau affecté, avec l'approbation préalable des responsables concernés), ou par l'identification de contrôles de protection et la présentation de rapports supplémentaires permanents à la personne ou au groupe approprié pour action.

Si ce n'est pas déjà fait, la gravité de l'incident de sécurité de l'information devrait être déterminée à l'aide de la grille de sévérité prédéterminée de l'organisme, et si elle est suffisamment importante, les membres appropriés de la direction générale devraient être avisés directement. S'il est clair qu'une situation de crise doit être déclarée, par exemple, le directeur de la continuité de l'activité doit être informé de l'activation éventuelle du plan de continuité de l'activité ; le directeur du CSIRT et la direction générale doivent également être informés.

Une fois que le membre du CSIRT a entamé les réponses immédiates et que l'analyse forensique et la communication sont complétées, une opinion doit être formulée rapidement pour déterminer si l'incident de sécurité de l'information est maîtrisé. Si nécessaire, le membre du CSIRT peut consulter des collègues, le directeur du CSIRT ou d'autres personnes ou groupes.

Si l'on obtient la confirmation que l'incident de sécurité de l'information est maîtrisé, le membre du CSIRT devrait amorcer toutes les actions, l'analyse forensique et les communications ultérieures requises pour isoler l'incident de sécurité de l'information et restaurer les opérations normales du système d'information affecté.

Ayant déterminé qu'un incident de sécurité de l'information est maîtrisé et qu'il ne doit pas être soumis à des activités de « crise », le membre du CSIRT doit alors déterminer si des réponses supplémentaires sont nécessaires et quelles réponses supplémentaires sont requises pour résoudre le problème de sécurité de l'information.

Ceci pourrait comprendre la restauration des systèmes, services et réseaux d'information affectés afin qu'ils reprennent leurs opérations normales. Il devrait alors enregistrer les détails liés à l'incident de sécurité de l'information sur le formulaire de rapport d'incidents de sécurité de l'information et dans la base de données d'événements/incidents de sécurité de l'information et aviser les personnes responsables pour qu'ils complètent les actions liées. Une fois que ces actions ont été menées à bien, les détails doivent être enregistrés sur le formulaire de rapport d'incident de sécurité de l'information et dans la base de données des événements/incidents de sécurité de l'information, puis l'incident de sécurité de l'information doit être clos et le personnel approprié doit en être informé.

2.7.3 Mettre sur pied une équipe de réponse aux incidents

ISO/IEC 27035-2, article 7.1

- *L'objectif de la création de l'ERI est de doter l'organisme des capacités appropriées pour évaluer les incidents de sécurité de l'information, y répondre et en tirer des enseignements, et pour assurer la coordination, la gestion, le retour d'information et la communication nécessaires.*
- *Une ERI contribue à la réduction des dommages physiques et pécuniaires, ainsi qu'à la réduction des dommages à la réputation de l'organisme qui sont parfois associés aux incidents de sécurité de l'information.*
- *Les ERI peuvent être structurées différemment selon la taille de l'organisation, les membres de son personnel et le secteur d'activité.*

PECB

143

Tout au long du cours, l'acronyme ERI sera utilisé pour désigner l'équipe de réponse aux incidents. Cependant, il peut y avoir d'autres termes comme indiqué ci-dessous.

Il existe des distinctions entre «équipes de sécurité», «CSIRT interne» et «CSIRT de coordination»:

- Dans une **équipe de sécurité**, la responsabilité formelle du traitement des activités liées à l'incident a été attribuée à tout groupe ou section de l'organisation. Aucun CSIRT (Équipe de réponse aux incidents de sécurité informatique – Computer Security Incident Response Team) n'a été établi; au lieu du CSIRT, le personnel disponible (généralement des administrateurs système, réseau ou de sécurité) ou une filiale locale traite les événements de sécurité de manière ad hoc et parfois, en cas d'incident isolé, dans le cadre de leurs responsabilités globales ou de leurs missions.
- Dans un **CSIRT interne**, la responsabilité du traitement des incidents est généralement attribuée à un groupe de personnes spécifiquement qualifiées. «Le CSIRT est dans la même organisation que le groupe, comme un CSIRT commercial dont le groupe est l'organisation commerciale dans laquelle le CSIRT est situé.» (Alberts, Dorofee, Ruefle et Zajicek 2004)
- Dans le modèle **CSIRT de coordination**, le CSIRT coordonne et facilite le traitement des incidents, vulnérabilités et information globale dans une variété d'organismes externes et internes, qui peuvent inclure d'autres CSIRT, des organismes de fournisseurs, des experts en sécurité, voire des organismes d'application de la loi.

Source: Brown, Moira West., Stikvoort, Don., Kossakowski, Klaus-Peter., Killcrece, Georgia., Ruefle, Robin et Zajicek, Mark. *Handbook for Computer Security Incident Response Teams (CSIRTs)*. Software Engineering Institute, Pittsburgh: 2003.

Page de notes

PECB

144

- La taille de l'organisme dans son ensemble par rapport au SMSI peut impliquer que la mise sur pied d'un CSIRT sur une base constante n'est pas une proposition réaliste. Dans un tel cas, le personnel spécifique pourrait être défini comme étant la première ligne de défense en cas d'incident de sécurité de l'information. Il convient que cette ERI de base ait accès à d'autres membres du personnel et à d'autres disciplines (TI, services juridiques, RH, opérations, relations publiques, etc.) au besoin.
- L'ERI a également besoin d'une délégation de pouvoirs de la part de la direction pour être en mesure de s'acquitter rapidement de ses responsabilités dans l'éventualité où un événement constituerait un incident grave en matière de sécurité informatique.

Note de terminologie:

ISO/IEC 27035-1, article 3.2 Équipe d'intervention en cas d'incident

équipe composée de membres de l'organisme ayant les compétences et la confiance nécessaires pour gérer les incidents au cours de leur cycle de vie

Note 1 à l'article: CERT (Computer Emergency Response Team) et CSIRT (Computer Security Incident Response Team) sont des termes couramment utilisés pour les ERI.

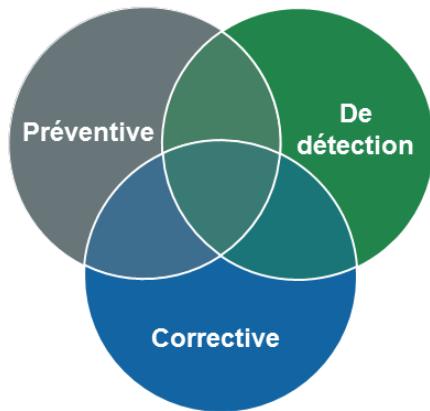
L'ERI peut choisir d'offrir plusieurs services. Les services offerts par chaque ERI devraient être basés sur la mission, le but, et la composition de l'équipe. Les services des ERI peuvent se regrouper à l'intérieur de trois catégories:

1. **Services réactifs:** Ces services sont déclenchés par un événement ou une requête tels que le signalement d'un hôte compromis, un code malveillant généralisé, une vulnérabilité logicielle, ou quelque chose qui a été identifié par une détection d'intrusion ou un système d'enregistrement. Les services réactifs sont la composante fondamentale du travail de l'ERI.
2. **Services proactifs:** Ces services fournissent assistance et information pour aider à préparer, protéger et sécuriser les systèmes en prévision d'attaques, de problèmes ou d'événements. L'exécution de ces services réduira directement le nombre d'incidents dans l'avenir.
3. **Service de gestion de la qualité de la sécurité:** Ces services renforcent les services existants et bien établis, indépendants du traitement d'incidents et exécutés de façon traditionnelle par d'autres secteurs d'une organisation tels que les services de TI, d'audit ou de formation. Si le CSIRT exécute ou collabore avec ces services, le point de vue et l'expertise du CSIRT peuvent fournir une vision approfondie pour

aider à améliorer la sécurité globale et identifier les risques, menaces et faiblesses du système. Ces services sont généralement proactifs, mais contribuent indirectement à la diminution du nombre d'incidents.

Source: Brown, Moira West., Stikvoort, Don., Kossakowski, Klaus-Peter., Killcrece, Georgia., Ruefle, Robin., et Zajicek, Mark. *Handbook for Computer Security Incident Response Teams (CSIRTs)*. Software Engineering Institute, Pittsburgh: 2003

2.7.4 Mettre en œuvre des mesures de sécurité



Exemples de mesures préventives

- Formation, sensibilisation des utilisateurs, zone démilitarisée (DMZ), réseau privé virtuel (VPN), sélection du personnel, etc.

Exemples de mesures de détection

- Système de détection d'intrusion (IDS), garde de sécurité, alertes de sécurité, etc.

Exemples de mesures correctives

- Groupe de réponse aux incidents, procédure de traitement des incidents, processus forensique, etc.

PECB

145

ISO/IEC 27001 mentionne explicitement la nécessité de mettre en œuvre des mesures de détection et de réponse (donc, de correction) aux incidents de sécurité. Il est également exigé d'établir un certain nombre de mesures préventives telles que la formation des principaux intervenants et la sensibilisation des utilisateurs.

Sans prétendre à l'exhaustivité, voici les principales mesures de sécurité relatives à la gestion des incidents:

Exemples de mesures de prévention des incidents

- Formation adéquate du personnel
- Contrôle de l'accès physique à l'équipement
- Utilisation de documents bien conçus (éviter des erreurs)
- Authentification et autorisation (mots de passe)
- Cryptographie

Exemples de mesures de détection des incidents

- Alertes configurées sur des équipements de télécommunications
- Système de détection d'intrusion (IDS)
- Alarmes de détection de la chaleur, de la fumée, du feu ou des risques liés à l'eau
- Vérification de duplicité de calculs
- Caméras vidéo

Exemples de mesures de correction des incidents

- Mise sur pied de plans d'urgence avec toute la formation, la sensibilisation, la mise à l'essai et les activités de maintenance nécessaires
- Création d'une équipe de réponse aux incidents
- Processus d'investigation des incidents

2.7.5 Définir un processus de cyberenquête

ISO/IEC 27002, article 16.1.7

- *Il convient de mettre au point et d'appliquer des procédures internes de traitement des preuves dans le cadre d'une action judiciaire et disciplinaire.*
- *Il convient, en général, que les procédures relatives aux preuves prévoient des processus d'identification, de recueil, d'acquisition et de protection selon les différents types de supports, de dispositifs et d'état des dispositifs, par exemple allumé ou éteint.*



Personnel compétent



Processus défini



Outil spécialisé

PECB

146

Le concept de «cyberenquête» (enquête informatique, correspondant à l'anglais « computer forensic ») est construit sur le modèle plus ancien de la science légale (médicale).

On désigne par cyberenquête l'application de techniques et de protocoles d'investigation respectant les procédures légales et destinées à apporter des preuves numériques admissibles devant la justice. On peut également la définir comme l'ensemble des connaissances et méthodes qui permettent de collecter, conserver et analyser des preuves issues de supports électroniques en vue de les présenter dans le cadre d'une action en justice.

Il y a quatre étapes dans une cyberenquête:

1. Préparation (les enquêteurs doivent détenir les aptitudes nécessaires à ce genre d'enquête)
2. Collecte et archivage des données (en respectant les procédures requises d'admissibilité)
3. Revue et analyse (interprétation de l'information avec pour but de recherche de preuves)
4. Rapport (incluant conclusions et commentaires)

Également, une cyberenquête nécessite:

- Outils techniques (outils d'audit, équipement d'analyse, etc.)
- Procédures
- Personnel qualifié

Note importante: Un organisme qui veut se conformer à l'article A.16.1.3 de la norme ISO/IEC27001 peut soit développer les compétences de cyberenquête en interne, soit avoir recours à des consultants externes.

2.7.6 Enregistrer les informations relatives aux incidents de sécurité

Toute information pertinente relative à l'incident devrait être enregistrée, incluant :

- Identificateur d'enregistrement unique
- Catégorisation et priorité
- Date/heure d'enregistrement
- Identification de la personne ayant signalé l'incident
- Identification de la personne ayant créé l'enregistrement de l'incident
- Description des symptômes
- État de l'incident (actif, en attente, clos)
- Actifs affectés
- Information de clôture (résolution, date/heure de clôture)
- Groupes/individus affectés par l'incident
- Activités entreprises pour résoudre l'incident et leurs résultats
- Approbation des mesures prises et clôture de l'incident

PECB

147

Il est important de documenter et d'enregistrer tout incident afin de s'assurer que le personnel chargé de traiter l'incident puisse détenir toute l'information nécessaire à sa résolution la plus efficace et rapide possible.

Ces informations serviront d'entrée (intract) pour les actions correctives et de preuves démontrant aux auditeurs (internes et externes) que le SMSI est maintenu. Ceci peut à son tour se répercuter dans les mesures et les métriques.

2.7.7 Mesurer et revoir le processus de gestion des incidents

La performance du processus de gestion des incidents devrait être régulièrement :

- **Mesurée** à l'aide d'indicateurs de performance, comme nous le verrons plus loin dans la formation
- **Réévaluée** afin d'identifier des actions correctives et préventives



PECB

148

Une fois qu'un incident de sécurité de l'information est clos, il est important que les leçons retenues liées au traitement de l'incident de sécurité soient rapidement identifiées et utilisées pour éviter que des incidents similaires se reproduisent. Ces leçons pourraient comprendre:

1. Nouvelles exigences ou des exigences modifiées pour les mesures de sécurité de l'information. Ces mesures pourraient être techniques ou non-techniques (y compris physiques). Selon les «leçons à retenir», les mesures pourraient inclure le besoin pour la mise à jour immédiate du matériel pour l'utiliser lors des sessions de sensibilisation à la sécurité de l'information (pour les utilisateurs et autres membres du personnel), ainsi que la révision et la réécriture de lignes directrices ou de normes de sécurité.
2. Modifications aux processus et procédures de gestion d'incidents de sécurité de l'information, formulaires de rapport et base de données d'événements/incidents de sécurité de l'information.

Au terme de cette activité, il convient de regarder au-delà de ce seul incident de sécurité de l'information et de vérifier les tendances qui pourraient aider à identifier le besoin de changements des mesures de protection.

Page de notes

PECB

149

Identification des améliorations de sécurité

Durant la revue de clôture d'un incident, de nouvelles mesures de sécurité et des modifications aux mesures existantes peuvent être identifiées.

Les recommandations et les exigences relatives aux mesures de protection peuvent ne pas être financièrement réalisables de manière immédiate ; dans de telles circonstances, elles devraient être identifiées comme des objectifs à long terme de l'organisme.

Par exemple, la mise en œuvre d'un coupe-feu plus robuste et sécuritaire peut ne pas être financièrement réalisable à court terme, mais il est nécessaire d'en tenir compte dans les buts à long terme de la sécurité de l'information de l'organisme.

Ces modifications devraient être prises en compte dans l'appréciation des risques, des plans de traitement des risques et de SoA.

Identification du plan d'améliorations

Une fois l'incident résolu, le chef d'équipe du CSIRT ou un candidat doit enquêter sur ce qui s'est passé pour évaluer et donc «quantifier» l'efficacité de la réponse globale aux incidents de sécurité de l'information. Une telle analyse vise à déterminer quelles parties du plan de gestion des incidents liés à la sécurité de l'information ont bien fonctionné et à déterminer où des améliorations s'imposent.

Un aspect important de l'analyse post-incident est de réintroduire de l'information et de la connaissance dans le programme de gestion des incidents de sécurité de l'information. Si l'incident est d'une sévérité élevée, une rencontre avec toutes les parties concernées devrait être planifiée à court terme après la résolution de l'incident, pendant que l'information est encore fraîche en mémoire. Certains facteurs à considérer dans ce type de rencontre incluent:

- Les procédures énoncées dans le plan d'incidents de sécurité de l'information fonctionnent-elles comme prévu?
- Des procédures ou méthodes existantes auraient-elles pu aider à détecter l'incident?
- Des procédures et outils qui auraient pu aider au processus de réponse ont-ils été identifiés?
- Existe-t-il des procédures qui auraient pu aider à restaurer les systèmes d'information à la suite d'un

incident identifié?

- La communication de l'incident à toutes les parties a-t-elle été efficace tout au long des processus de détection, rapport et réponse?

Les résultats de la rencontre devraient être évalués, documentés et toute action convenue devrait être mise à exécution de façon appropriée.

Questions ?

PECB

150

Page de notes

PECB

151

Page de notes

PECB

152