



© PEBC, 2020. Tous droits réservés.

Version6.0

Numéro de document: ISMSLID4V6.0

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 PEBC.

# Programme du jour 4

Section  
**21** Surveillance, mesure,  
analyse et évaluation

Section  
**25** Amélioration continue

Section  
**22** Audit interne

Section  
**26** Préparation à l'audit de  
certification

Section  
**23** Revue de direction

Section  
**27** Processus de certification et  
clôture de la formation

Section  
**24** Traitement des problèmes et  
des non-conformités

**PECB**

2

# Section 21

## Surveillance, mesure, analyse et évaluation

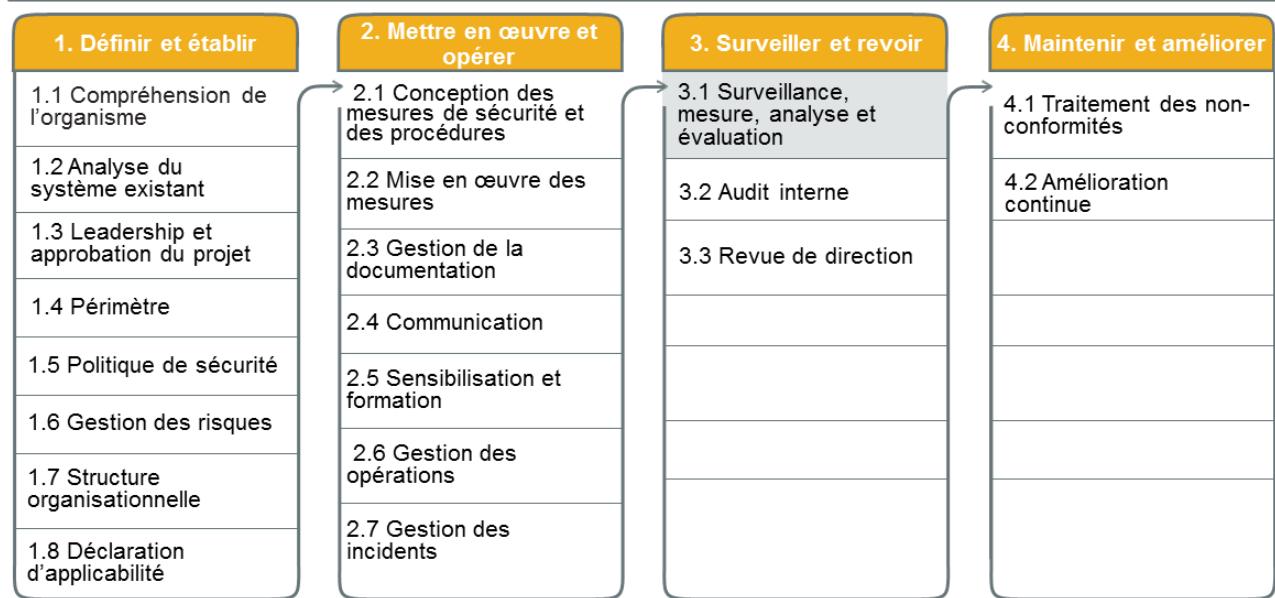
- Déterminer les objectifs de mesure
- Définir ce qui doit être surveillé et mesuré
- Établir des indicateurs de performance du SMSI
- Rendre compte des résultats

PECB

3

La présente section aidera le participant à définir les objectifs de surveillance et de mesure, à déterminer les objectifs de mesure et à renforcer son aptitude à évaluer l'efficacité du SMSI mis en œuvre. De plus, elle aidera le participant à utiliser les connaissances et les compétences acquises pour vérifier dans quelle mesure les exigences du SMSI identifiées ont été respectées.

### 3.1 Surveillance, mesure, analyse et évaluation



PECB

4

# ISO/IEC 27001 Exigences

## ISO/IEC 27001, article 9.1

*L'organisation doit évaluer les performances de sécurité de l'information, ainsi que l'efficacité du système de management de la sécurité de l'information.*

*L'organisation doit déterminer:*

- a) ce qu'il est nécessaire de surveiller et de mesurer, y compris les processus et les mesures de sécurité de l'information;
- b) les méthodes de surveillance, de mesure, d'analyse et d'évaluation, selon le cas, pour assurer la validité des résultats;

*NOTE: Il convient que les méthodes choisies donnent des résultats comparables et reproductibles pour être considérées comme valables.*

- c) quand la surveillance et les mesures doivent être effectuées;
- d) qui doit effectuer la surveillance et les mesures;
- e) quand les résultats de la surveillance et des mesures doivent être analysés et évalués; et
- f) qui doit analyser et évaluer ces résultats.

*L'organisation doit conserver les informations documentées appropriées comme preuves des résultats de la surveillance et des mesures.*

5

Un organisme qui désire se conformer à l'ISO/IEC27001 devrait:

1. Déterminer ce qui doit être mesuré et surveillé
2. Définir les méthodes de surveillance, de mesure, d'analyse et d'évaluation
3. Recueillir les données pour la surveillance, la mesure, l'analyse et l'évaluation
4. Effectuer l'analyse et l'évaluation de la surveillance et des résultats de la mesure

### ***ISO/IEC27003, article 9.1 Surveillance, mesure, analyse et évaluation***

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

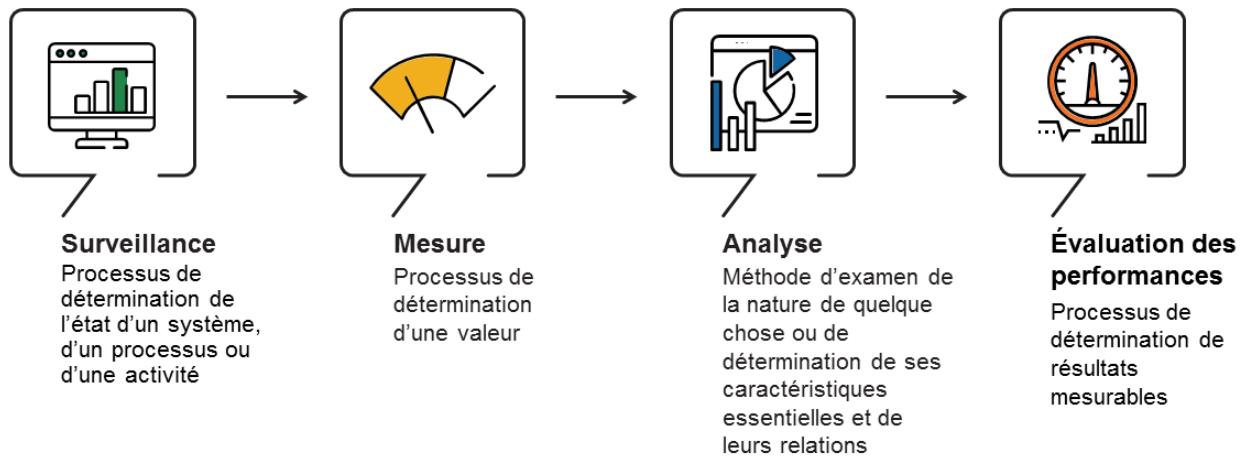
*Il convient d'être prudent lors de la détermination des attributs à mesurer. Il est irréaliste, coûteux et contreproductif de trop mesurer ou de s'intéresser aux mauvais attributs. En plus des coûts de mesure, d'analyse et d'évaluation de trop nombreux attributs, il est possible que les enjeux clés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

*Il existe deux types génériques de mesures:*

**h)*****les mesures de la performance**, qui expriment les résultats prévus en fonction des caractéristiques de l'activité planifiée, telles que le décompte des effectifs, l'accomplissement des étapes ou le degré d'application des mesures de sécurité de l'information; et*

**i)*****les mesures d'efficacité**, qui expriment l'effet que la réalisation des activités planifiées a sur les objectifs de sécurité de l'information de l'organisme.*

# Surveillance, mesure, analyse et évaluation de la performance



PECB

6

La mesure est le processus qui permet de déterminer une valeur. La mesure de la performance peut être définie comme un moyen systématique d'apprécier les objectifs d'un organisme par rapport à ses réalisations réelles. Les mesures de performance sont d'une valeur minime en soi, à moins de les considérer dans le contexte des stratégies et des objectifs de l'organisme.

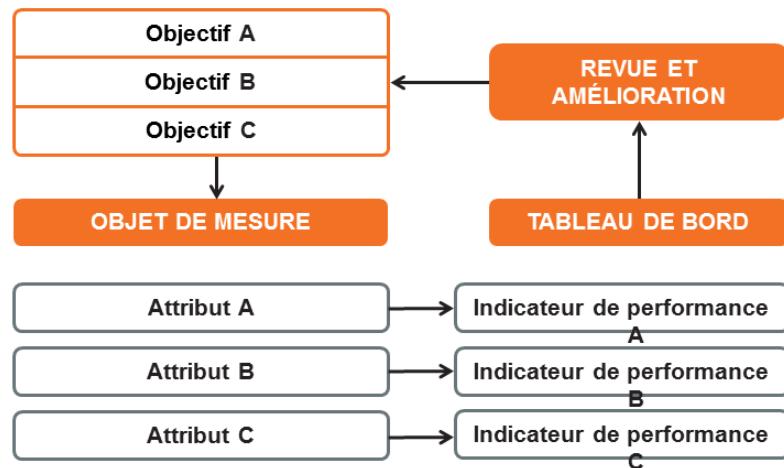
C'est également vrai pour les systèmes de management, qui ne peuvent pas exister en vase clos et doivent contribuer aux objectifs de l'organisation pour être efficaces. Dans ce contexte, la mesure de la performance devrait être une priorité absolue pour les personnes responsables de la mise en œuvre et de la maintenance d'un système de management.

Certains des avantages de la surveillance, de la mesure, de l'analyse et de l'évaluation sont les suivants:

- Mettre en œuvre le mesurage systématique pour assurer la réalisation des processus
- Identifier les écarts sur le SMSI en temps opportun et les traiter en conséquence
- Permettre aux utilisateurs de prendre des décisions concernant les résultats du processus
- Déterminer l'efficacité et l'efficience des processus
- Identifier les possibilités d'amélioration continue

# Surveillance, mesure, analyse et évaluation

Le but principal est l'amélioration du SMSI.



PECB

7

En résumé, le processus de surveillance et de mesure est:

- Identifier les objectifs de mesure
- Sélectionner des objets d'attribut qui peuvent être mesurés
- Créer des indicateurs de performance
- Évaluer les objectifs atteints et améliorer le système de management

**Exemple:**

1. **Objectifs de mesurage:** S'assurer que tous les employés sont sensibilisés aux risques majeurs auxquels l'organisme fait face
2. **Attribut:** L'employé qui a suivi la session de sensibilisation
3. **Indicateur de performance:** % des employés qui ont suivi la session de sensibilisation et qui ont réussi le test

# ISO/IEC 27004

## Lignes directrices pour la mesure de la performance et de l'efficacité d'un SMSI

- La norme traite exclusivement de l'article 9.1 de la norme ISO/IEC 27001.
- Ses principales sections portent sur :
  - ▷ Vue d'ensemble de la mesure de la sécurité de l'information
  - ▷ Responsabilités des gestionnaires
  - ▷ Développement des mesures et du mesurage
  - ▷ Opération de mesurage
  - ▷ Analyse des données et rapport des résultats de mesurage
  - ▷ Évaluation et amélioration du programme de mesure de la sécurité de l'information



PECB

8

### ISO/IEC27004:2009, Introduction

*La présente Norme internationale fournit des lignes directrices sur le développement et l'utilisation de mesures et de mesurage afin d'évaluer l'efficacité d'un système de gestion de la sécurité de l'information (SMSI) et de mesures ou de groupes de mesures mis en œuvre, comme spécifié dans ISO/IEC 27001. Cela comprendrait la politique, la gestion des risques de sécurité de l'information, les objectifs de sécurité, les mesures, les processus et procédures, et soutiendrait le processus de révision, aidant à déterminer si l'un des processus ou des mesures du SMSI doit être modifié ou amélioré. Il est à retenir qu'aucun mesurage des mesures de sécurité ne peut garantir une sécurité totale.*

*La mise en œuvre de cette approche établit un programme de mesurage de la sécurité de l'information. Le programme de mesurage de la sécurité de l'information aidera la direction à identifier et évaluer les processus et les mesures SMSI non conformes et inefficaces et à prioriser les actions associées à l'amélioration ou la modification de ces processus et mesures. Ceci peut également aider l'organisme à démontrer la conformité à ISO/IEC27001 et à offrir des preuves supplémentaires pour les processus de revue de direction et de gestion des risques de la sécurité de l'information.*

*La présente Norme internationale suppose que le point de départ pour l'élaboration des mesures et du mesurage est une solide compréhension des risques de sécurité de l'information auxquels un organisme fait face et que les activités d'évaluation des risques d'un organisme ont été effectuées correctement (c.-à-d. selon ISO/IEC27005), tel que requis par ISO/IEC27001. Le programme de mesurage de la sécurité de l'information encouragera un organisme à fournir de l'information fiable aux parties prenantes pertinentes concernant ses risques à la sécurité de l'information et l'état du SMSI mis en œuvre pour gérer ces risques.*

*Mis en œuvre efficacement, le programme de mesurage de la sécurité de l'information améliorerait la confiance des parties prenantes dans les résultats des mesures et permettrait aux parties prenantes d'utiliser ces mesures pour effectuer des améliorations à la sécurité de l'information et du SMSI. Les résultats accumulés des mesures permettront la comparaison du progrès réalisé pour atteindre les objectifs de sécurité sur une période de temps dans le cadre d'un processus d'amélioration continue du SMSI d'un organisme.*

## 3.1 Surveillance, mesure, analyse et évaluation

### Liste des activités

3.1.1

Déterminer les objectifs de mesure

3.1.2

Définir ce qui doit être surveillé et mesuré

3.1.3

Établir des indicateurs de performance du SMSI

3.1.4

Déterminer la fréquence et la méthode de surveillance et de mesure

3.1.5

Rendre compte des résultats

### 3.1.1 Déterminer les objectifs de mesure

- L'organisme devrait évaluer son système de management et ses procédures afin d'en assurer la pertinence, l'adéquation et l'efficacité continues.
- Il est de bonne pratique de se concentrer sur la surveillance et la mesure des activités liées aux processus critiques qui permettent à l'organisme de réaliser ses objectifs de performance du SMSI.
- Trop de mesures peuvent déformer l'objectif d'une organisation et brouiller l'important.



PECB

10

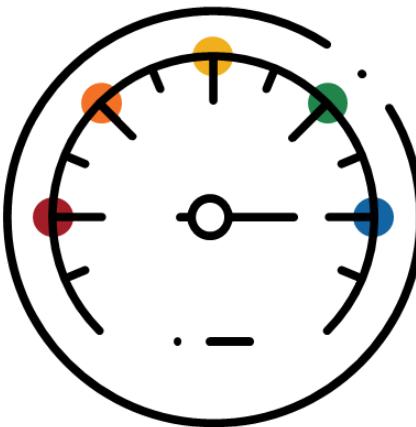
Les mesures de performance choisies seront les vecteurs pour communiquer le succès ou l'échec du système de management. Tout ensemble de mesures de performance doit être soigneusement sélectionné pour assurer qu'il détermine de fait la voie à suivre pour réaliser les objectifs de l'organisme.

Les objectifs de mesure dans le contexte d'un système de management comprennent:

- Évaluer l'efficacité des processus et des procédures mis en place
- Vérifier dans quelle mesure les exigences de la norme ont été respectées
- Faciliter l'amélioration de la performance
- Fournir des éléments d'entrée pour la revue de direction afin de faciliter la prise de décision et de justifier les améliorations nécessaires au système de management

### 3.1.2 Définir ce qui doit être surveillé et mesuré

1. Mesure dans laquelle la politique et les objectifs de l'organisme en matière de sécurité de l'information sont atteints
2. Processus, procédures et fonctions critiques
3. Preuves historiques de performance déficiente du SMSI (p. ex. non-conformité, quasi-accidents, fausses alertes, défaillances, incidents)
4. Conformité aux exigences légales et réglementaires applicables, aux bonnes pratiques de l'industrie et à ses propres politiques et objectifs de sécurité de l'information
5. Données et résultats de surveillance et de mesure pour faciliter l'analyse d'actions correctives et préventives subséquentes



PECB

11

Un petit nombre de mesures de la performance significatives est préférable à une pléthora de mesures non reliées aux objectifs de l'organisme. Plusieurs organismes utilisent la règle SMART (Spécifique, Mesurable, Atteignable, Réaliste, Temporellement défini) quand ils développent leurs mesures de performance.

- **Spécifique:** clair et concentré pour éviter toute méprise
- **Mesurable:** peut être quantifié et comparé aux autres données
- **Atteignable:** réalisable, raisonnable et acceptable dans un contexte de performance particulier
- **Réaliste:** s'inscrit dans la culture de l'organisation et est rentable par rapport aux ressources disponibles
- **Temporellement défini:** réalisable dans les délais impartis

Aucun ensemble de mesures génériques ne saurait être efficace pour tous les organismes et peut même ne pas l'être pour les organismes dans des environnements similaires. L'ensemble final des mesures sera un mélange de contextes opérationnel, législatif et culturel.

Il existe un certain nombre de niveaux des mesures de performance allant de mesures stratégiques de haut niveau à des mesures plus spécifiques au niveau opérationnel ou du programme. Le détail important à retenir est de mesurer les activités qui importent vraiment, et non de gaspiller des ressources et du temps à mesurer des activités simplement parce qu'elles peuvent l'être. En termes d'efficience, un organisme a besoin de mesures significatives qui indiquent ce qui se passe réellement afin qu'il puisse décider de laisser une activité se poursuivre ou d'intervenir pour prendre des actions correctives. En termes d'efficacité, un organisme a besoin de mesures pour comprendre si le système de management est aligné sur les besoins et les objectifs de l'organisme.

### 3.1.3 Établir des indicateurs de performance du SMSI

#### Exemples

- % de fausses alertes par détection d'événement
- Coût moyen d'un incident



Incidents

PECB

- % du personnel ayant reçu une formation et ayant les qualifications
- Nombre d'heures de formation par employé



Formation

- % des systèmes testés pour vulnérabilités dans les 3 derniers mois
- Nombre de jours pour régler les vulnérabilités connues



Vulnérabilités

- % des non-conformités non corrigées dans les délais fixés
- Nombre de jours en moyenne pour régler une non-conformité



Non-conformités

12

Le type et le nombre de mesures de performance dépendent des exigences de l'organisme.

### 3.1.4 Déterminer la fréquence et la méthode de surveillance et de mesure

Comment et quand surveiller et mesurer ?

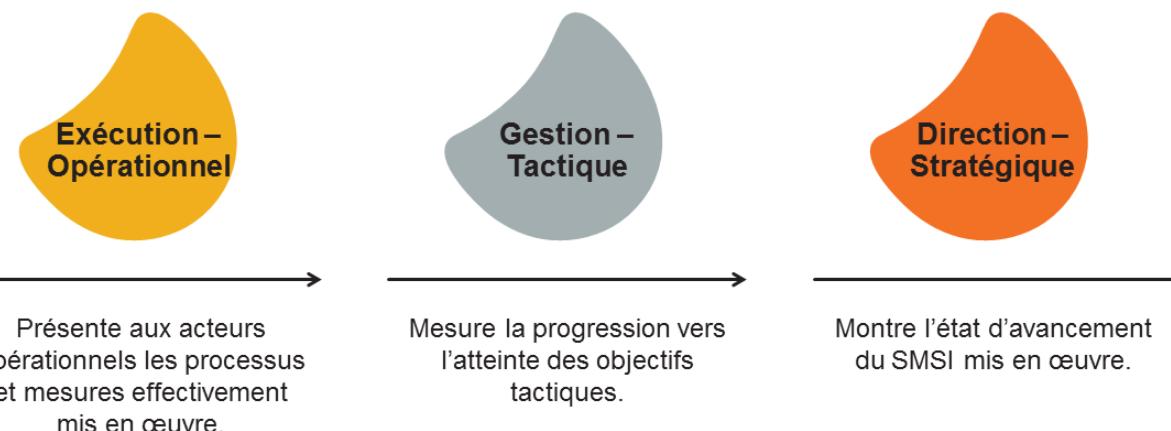
#### Pratiques



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

### 3.1.5 Rendre compte des résultats

#### Exemple de tableau de bord



PECB

14

Il y a plusieurs façons de présenter les résultats de la mesure. Le choix de la méthode dépendra du public ciblé. Les principales méthodes sont:

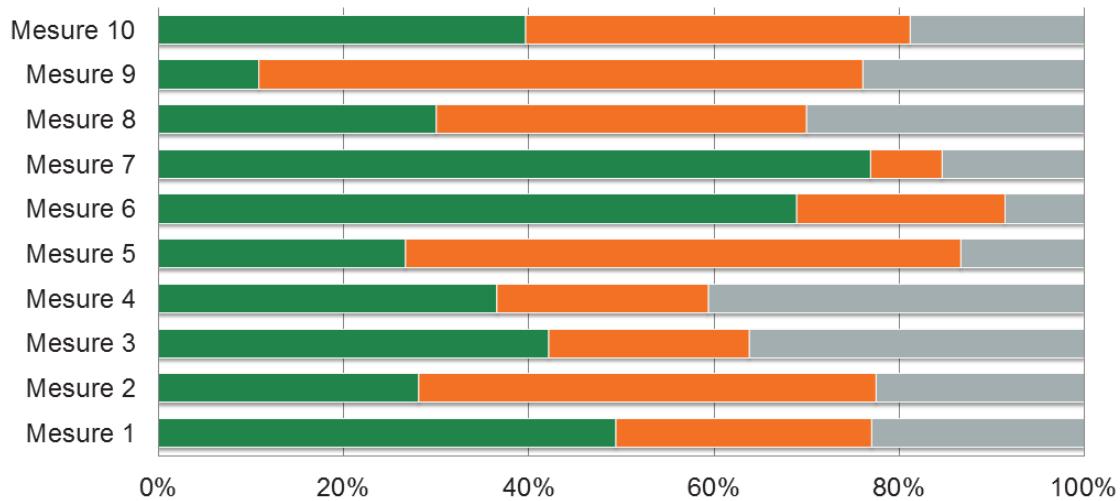
- **Carte de pointage (scorecard) ou tableau de bord stratégique:** Fournit de l'information stratégique en intégrant des indicateurs de haut niveau.
- **Tableaux de bord opérationnels et tactiques:** Moins concentrés sur les objectifs stratégiques et plus liés à l'efficacité des mesures et des processus spécifiques.
- **Rapport:** Simple et statique, p. ex. une liste de mesures pour une période donnée, des rapports croisés plus sophistiqués avec des regroupements imbriqués, des résumés déroulants et un forage ou une liaison dynamique. Le rapport est surtout utile quand l'utilisateur doit regarder des données brutes dans un format facile à lire.
- **Jauge:** Représente des valeurs dynamiques incluant les alertes, les éléments graphiques additionnels et l'étiquetage des paramètres.

**Note:** Un tableau de bord est l'interface utilisateur qui organise et présente l'information d'une façon facile à lire et à comprendre.

- Le tableau de bord n'est que le format de présentation.
- Les indicateurs sont le contenu.

# I. Tableau de bord opérationnel

## Exemple



PECB

15

Les tableaux de bord opérationnels sont utilisés pour surveiller les opérations en temps réel et informer les utilisateurs des écarts. Ils permettent de contrôler les activités opérationnelles et d'assurer que les processus restent dans les limites des objectifs de productivité, de qualité et d'efficience. Ils peuvent aider à l'analyse continue de la performance opérationnelle afin d'éviter les problèmes et les pertes de profit, et dans le même temps de saisir les opportunités, tout en fournissant des données qui permettront d'améliorer le contrôle et l'efficience des processus.

## II. Tableau de bord tactique

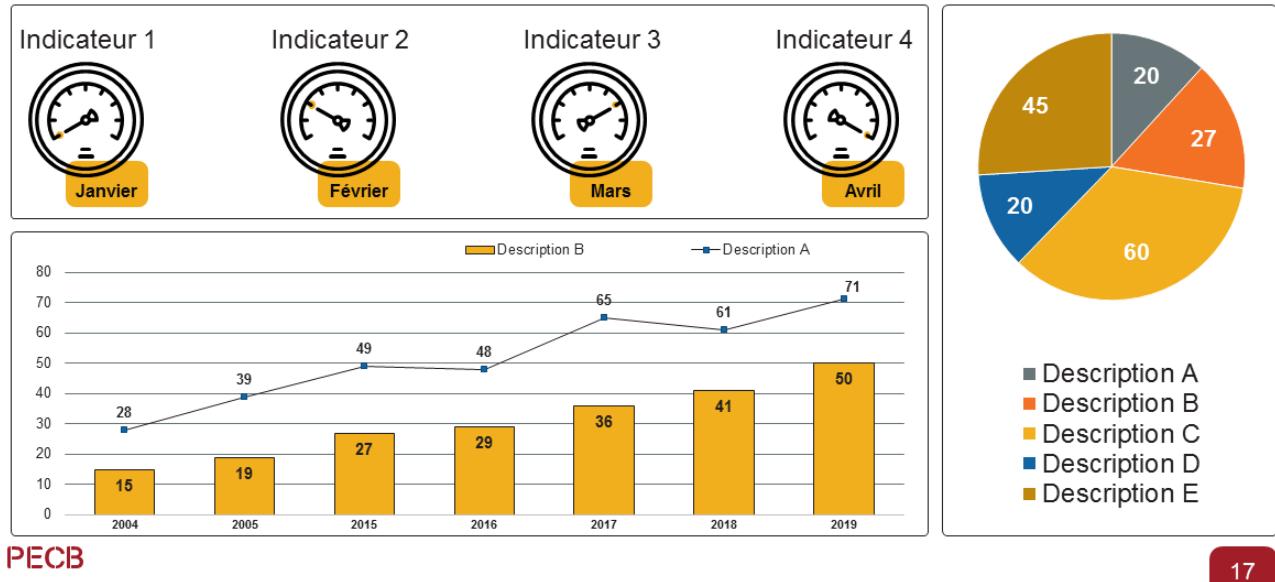
### Exemple

No.	Procédure évaluée	Commentaires sur les forces et faiblesses	Évaluation des procédures								
			1	2	3	4	5	6	7	8	9
1	Procédure de politique de communication									X	
2	Procédure de planification des changements								X		
3	Procédure d'affectation des ressources								X		
4	Procédure de compétence, de sensibilisation et de formation				X						
5	Procédure de maîtrise de l'information documentée										X
6	Procédure de préparation et d'intervention d'urgence								X		
7	Procédure de surveillance et de mesure				X						
8	Procédure d'actions correctives						X				
9	Procédure de revue de direction								X		
10	Procédure d'audits internes									X	
Évaluation globale											
PECB											16

L'évaluation de la conformité des procédures relatives au système de management est un bon exemple du niveau tactique. La diapositive présente les indicateurs de performance sur un tableau de bord.

### III. Tableau de bord stratégique

#### Exemple



Le tableau de bord stratégique soutient les gestionnaires à tous les niveaux d'un organisme et fournit une vue d'ensemble rapide dont les décideurs ont besoin pour surveiller la santé financière de l'entreprise. Le tableau de bord de ce type se concentre sur les mesures de performance et les prévisions de haut niveau.

# Exercice 10

PECB

18



## Exercice 10: Développement d'indicateurs de sécurité de l'information

Pour chacun des articles suivants de la norme ISO/IEC27001, fournissez deux exemples de métriques qui seraient acceptables pour mesurer la conformité à cet article.

### **Exemple: Article 5.1 Leadership et engagement**

- Réunions de revue de direction réalisées périodiquement
- Taux moyen de participation aux revues de direction à ce jour

1. Article 10.1d) Réviser l'efficacité de toute action corrective mise en œuvre
2. Article 5.3 Rôles, responsabilités et autorités au sein de l'organisation
3. Mesure A.8.1.2 Propriété des actifs
4. Mesure A.8.1.4 Restitution des actifs
5. Mesure A.9.3.1 Utilisation d'informations secrètes d'authentification

Durée de l'exercice: 30 minutes

Commentaires: 15 minutes



## Questions ?

PECB

19

# Section 22

## Audit interne

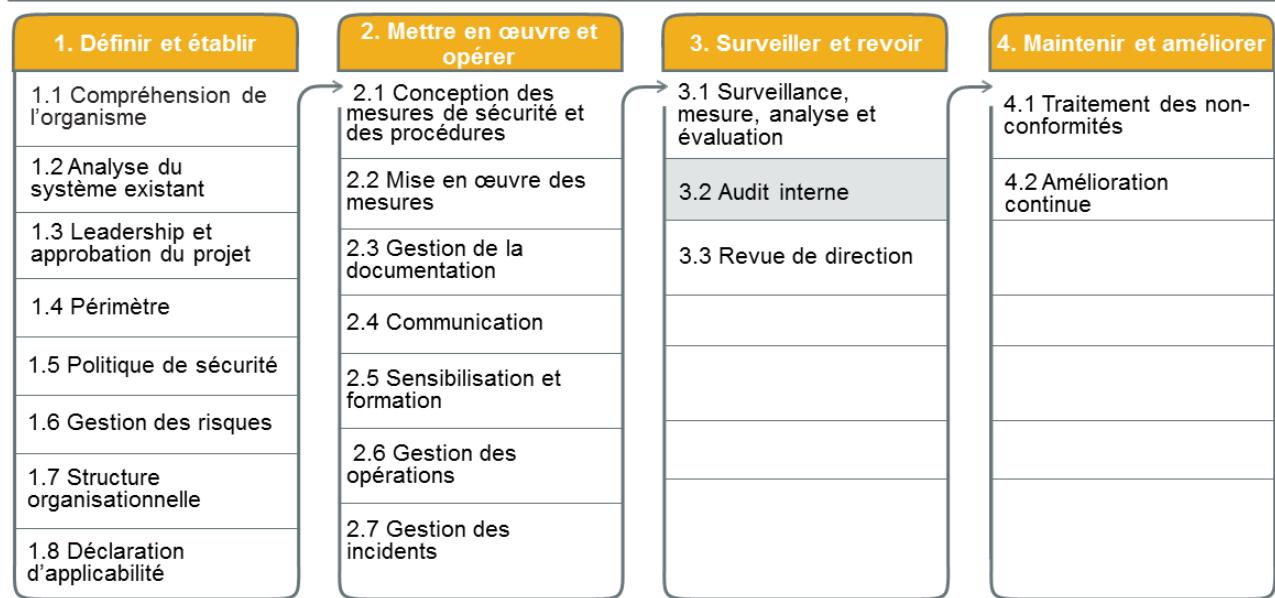
- Définition
- Types d'audits
- Créer un programme d'audit interne
- Nommer un responsable
- Établir l'indépendance, l'objectivité et l'impartialité
- Planifier les activités d'audits
- Réaliser les activités d'audit
- Effectuer le suivi des non-conformités

PECB

20

La présente section aidera le participant à comprendre le rôle d'une fonction d'audit et à identifier les différences entre les audits internes et externes. De plus, le participant sera en mesure de définir les activités de planification de l'audit, puis d'affecter et de gérer les ressources nécessaires pour mener un programme d'audit interne ou externe.

## 3.2 Audit interne



PECB

21

# ISO/IEC 27001 Exigences

## ISO/IEC 27001, article 9.2

L'organisation doit réaliser des audits internes à des intervalles planifiés afin de recueillir des informations permettant de déterminer si le système de management de la sécurité de l'information:

- a) est conforme:
  - 1) aux exigences propres de l'organisation concernant son système de management de la sécurité de l'information; et
  - 2) aux exigences de la présente Norme internationale;
- b) est efficacement mis en œuvre et tenu à jour.

L'organisation doit:

- c) planifier, établir, mettre en œuvre et tenir à jour un ou plusieurs programmes d'audit, couvrant notamment la fréquence, les méthodes, les responsabilités, les exigences de planification et l'élaboration des rapports. Le ou les programmes d'audit doivent tenir compte de l'importance des processus concernés et des résultats des audits précédents;
- d) définir les critères d'audit et le périmètre de chaque audit;
- e) sélectionner des auditeurs et réaliser des audits qui assurent l'objectivité et l'impartialité du processus d'audit;
- f) s'assurer qu'il est rendu compte des résultats des audits à la direction concernée; et
- g) conserver des informations documentées comme preuves de la mise en œuvre du ou des programme(s) d'audit et des résultats d'audit.

PECB

22

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

1. Créer un programme d'audit interne
2. Nommer une personne responsable des activités d'audit interne
3. Établir l'indépendance, l'objectivité et l'impartialité de la fonction d'audit
4. Planifier les activités d'audits
5. Créer des procédures d'audit
6. Réaliser les activités d'audit

## ISO/IEC27003, article 9.2 Audit interne

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

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

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

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

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

# Qu'est-ce qu'un audit ?

## ISO 19011, article 3.1

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

**En bref :** Auditer signifie demander à l'entité auditee ce qu'elle fait et comment elle le fait, afin de vérifier si les pratiques sont conformes aux politiques, procédures et processus de l'organisme.



PECB

23

L'audit est un exercice d'évaluation basé sur des faits. Cette évaluation met en évidence les forces et les faiblesses de l'organisme ou du système audité. Les résultats de l'audit sont communiqués à la direction qui prendra alors les mesures nécessaires et appropriées. Les mêmes principes et techniques de base s'appliquent aux audits de système de management.

- **Audit financier:** Détermine si les pratiques comptables d'un organisme sont conformes aux principes reconnus.
- **Audit administratif:** Détermine l'efficacité des pratiques de management.
- **Audit des systèmes d'information:** Détermine si les actifs d'information sont protégés correctement.
- **Audit de management de la qualité:** Détermine l'efficacité des pratiques de management de la qualité.

# Types d'audits

## Audit de deuxième partie

L'organisme est audité par son client.

**Client**

## Externe

## Audit de deuxième partie

L'organisme audite son fournisseur.

**Fournisseur**

## Audit de tierce partie

L'organisme est audité par un organisme indépendant.

**PECB**

## Interne

## Audit de première partie

L'organisme audite ses propres systèmes.



## Organisme

24

**L'audit interne**, parfois appelé audit de première partie, est une activité indépendante et objective qui donne à un organisme une assurance sur le degré de maîtrise de ses opérations, donne des recommandations pour les améliorer et contribue à créer une valeur ajoutée. Les audits internes sont réalisés par, ou pour le compte de, l'organisme lui-même, pour la revue de direction et les autres besoins internes. L'indépendance de la démarche doit être démontrée par l'absence de responsabilités dans les activités à auditer.

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

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

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

# Différences entre audits internes et externes

## Principales caractéristiques

### Audit interne



Indépendant des activités auditées (pas de l'organisme)



Tient compte de l'efficacité et de l'efficiency du système de management



Rôle de conseil auprès de l'organisme pour l'amélioration continue



Peut être effectué en continu

### Audit externe



Totalement indépendant de l'organisme audité et de ses activités



Ne tient compte que de l'efficacité du système de management



Aucun rôle de conseil auprès de l'organisme (seulement des recommandations générales)



Activité d'audit toujours planifiée dans les délais impartis.

PECB

25

L'audit interne est une activité indépendante, objective et consultative conçue pour actualiser et améliorer le fonctionnement de l'organisme. Il contribue aux objectifs de l'organisme en fournissant une méthodologie systématique et structurée pour évaluer et améliorer l'efficacité du processus de gestion des risques, son contrôle et la prise de décision.

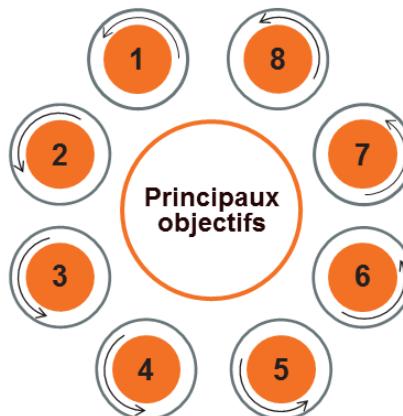
# Principaux services et activités de l'audit interne

Évaluation des objectifs du SMSI

Évaluation de la gouvernance du SMSI

Évaluation de la gestion continue des risques

Évaluation de l'efficacité et de l'efficience des processus et mesures de sécurité



Coordination entre audits interne et externe

Évaluation de l'amélioration continue

Évaluation de la mesure et de la revue du SMSI

Évaluation de l'efficacité et de l'efficience de la gestion du cycle de vie du système de management

PECB

26

Les objectifs de l'audit interne doivent être revus et approuvés par la direction de l'organisme. Dans le contexte d'une certification du système de management, les objectifs de l'audit interne devraient au minimum couvrir l'évaluation des activités liées au système de management. Toutefois, l'audit interne peut couvrir plusieurs autres domaines d'audit: financier, administratif, qualité, etc. La définition des objectifs de l'audit interne peut varier selon la taille de l'organisme, son secteur d'activité ainsi que de sa mission.

Cependant, on inclut habituellement plusieurs des objectifs suivants:

**1. Évaluation des objectifs du système de management:** Évaluer la cohérence entre les objectifs du système de management de l'organisme et la planification des activités afin de valider si l'organisme est en mesure d'atteindre les objectifs qu'il s'est fixés en fonction de ses propres critères

**2. Évaluation de la gouvernance du système de management:** Valider si la direction de l'organisme soutient les activités liées au système de management et si les rôles et responsabilités des parties intéressées sont clairement définis

**3. Évaluation de la gestion continue des risques:** Évaluer si l'organisme a mis en œuvre et maintient une gestion continue des risques. Contrairement à un auditeur externe, un auditeur interne peut participer en tant que partie intéressée à l'identification et à l'appréciation des risques auxquels est confronté son organisme.

**4. Évaluation des processus et mesures dans les opérations:** Évaluer la pertinence, l'efficacité et l'efficience des processus et des mesures de sécurité liés au système de management afin de déterminer s'ils sont alignés avec les exigences normatives, légales, réglementaires et contractuelles ainsi qu'avec les politiques internes de l'organisme

# Page de notes

---

PECB

27

**5. Évaluation de la gestion du cycle de vie du système de management:** Évaluer l'efficacité et l'efficience des processus de gestion du cycle de vie et des mesures de sécurité liées au système de management: planification, préparation, mise en œuvre, opération, surveillance et revue, mise à jour et amélioration du système de management

**6. Évaluation de la mesure et de la revue du système de management:** S'assurer que l'organisme effectue périodiquement une révision de la mesure du système de management pour valider si les objectifs de l'organisme sont atteints

**7. Évaluation de l'amélioration continue:** S'assurer que l'organisme met en œuvre des actions correctives et préventives pour traiter ses non-conformités et améliorer l'efficacité et l'efficience du système de management

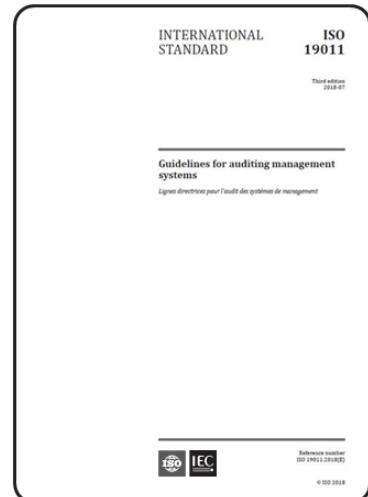
**8. Coordination entre audits interne et externe:** Cordonner les efforts et la planification des activités d'audit interne avec celles des auditeurs externes. L'audit interne a également comme objectif d'assurer que l'organisme effectue un suivi adéquat des rapports d'audit externe et des plans d'action établis et approuvés.

# ISO 19011

## Lignes directrices pour l'audit des systèmes de management

Définitions et lignes directrices liées aux éléments suivants :

- Concepts de systèmes de management de l'audit
- Principales caractéristiques de l'audit et de l'auditeur, et principes de base liés à l'audit
- Éléments clés du processus d'audit
- Aspects clés d'un programme d'audit
- Qualifications des auditeurs



PECB

28

**ISO19011 contient des lignes directrices concernant les méthodes d'audit, mais leur application n'est pas impérative.** Les lignes directrices de cette norme sont prévues pour être flexibles afin de s'adapter facilement à la taille, à la nature, et à la complexité de l'organisme à auditer. La responsabilité d'appliquer correctement ces lignes directrices incombe à chaque auditeur (toujours en accord avec ses propres méthodes de travail).

**Il est à noter que la norme ISO19011 a été élaborée comme ligne directrice pour les audits de systèmes de management.**

### Sommaire de la norme ISO19011:2018

1. Périmètre
2. Références normatives
3. Termes et définitions
4. Principes de l'audit
5. Management d'un programme d'audit
6. Réalisation d'un audit
7. Compétence et évaluation des auditeurs

Annexe A (informative): Lignes directrices supplémentaires destinées aux auditeurs pour la planification et la réalisation des audits

## 3.2 Audit interne

### Liste des activités

**3.2.1** Créer un programme d'audit interne

**3.2.6** Réaliser les activités d'audit

**3.2.2** Nommer un responsable

**3.2.7** Effectuer le suivi des non-conformités

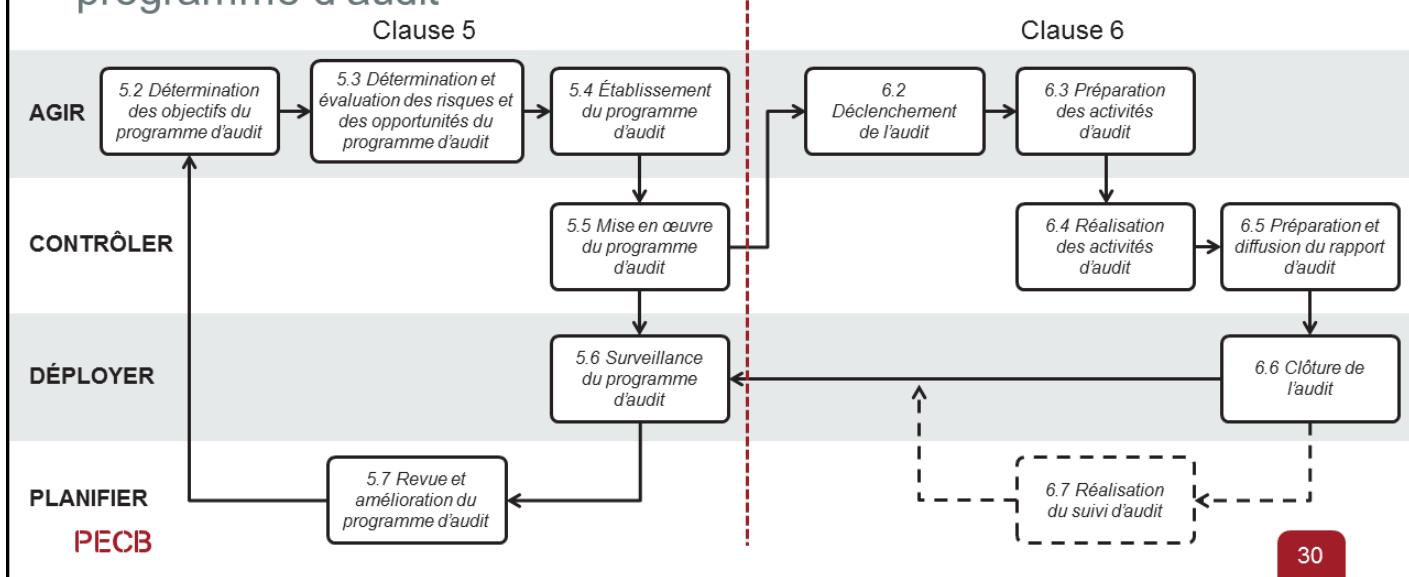
**3.2.3** Établir l'indépendance, l'objectivité et l'impartialité

**3.2.4** Planifier les activités d'audits

**3.2.5** Affecter et gérer les ressources du programme d'audit

### 3.2.1 Créer un programme d'audit interne

ISO 19011, Figure 1 – Logigramme pour le management d'un programme d'audit



30

#### ISO19011, article 3.4 Programme d'audit

*dispositions relatives à un ensemble d'un ou plusieurs audits planifié pour une durée spécifique et dirigé dans un but spécifique*

Le management du programme d'audit devrait respecter le modèle PDCA. Un programme d'audit peut inclure un ou plusieurs audits basés sur la taille, la nature et la complexité de l'organisme à auditer. Ces audits peuvent avoir une variété d'objectifs et peuvent aussi inclure les audits dits «conjoint» et «combinés». Un organisme peut établir plus qu'un programme d'audit.

Un programme d'audit inclut aussi toutes les activités exigées pour planifier et organiser le type et le nombre d'audits ainsi que les mesures pour fournir les ressources afin de les réaliser efficacement dans la période de temps indiquée.

## 3.2.2 Nommer un responsable

### Rôles et responsabilités de l'auditeur interne

- Développer un programme d'audit interne (rôles et responsabilités, procédures, documents de travail, formations des auditeurs, etc.)
- Planifier les activités d'audits
- Gérer les ressources
- Établir des critères de performance et s'assurer que l'audit satisfait à ces critères
- Rédiger des rapports d'audits
- S'assurer que les bonnes pratiques et les procédures sont suivies pendant l'audit
- Mettre en œuvre un programme d'évaluation de l'amélioration continue par un auditeur externe
- Effectuer le suivi des non-conformités et des recommandations des audits antérieurs

PECB

31

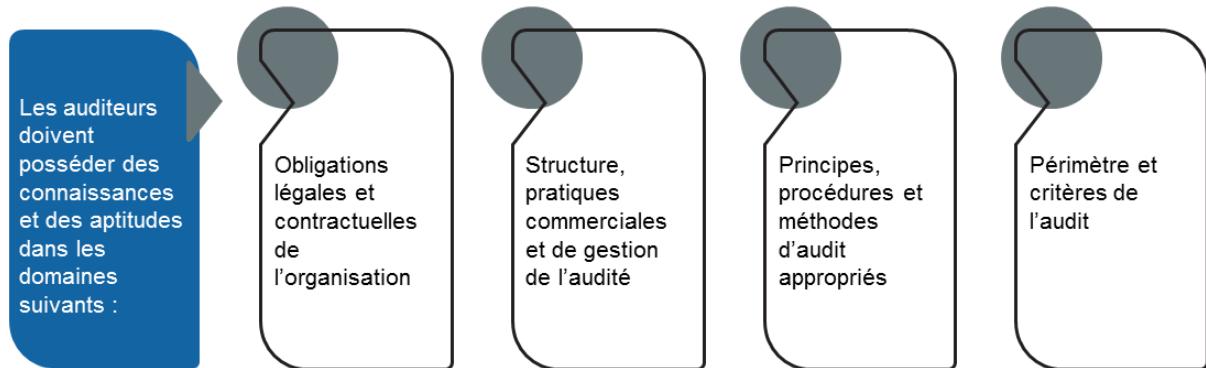
### ***ISO19011, article 5.4.1 Rôles et responsabilités de la ou des personnes responsables du management du programme d'audit***

*Il convient que la ou les personnes responsables du management du programme d'audit:*

- a. établissent l'étendue du programme d'audit en fonction des objectifs pertinents (voir 5.2) et de toute contrainte connue;
- b. déterminent les enjeux externes et internes ainsi que les risques et opportunités susceptibles d'affecter le programme d'audit, et mettent en œuvre les actions pour y faire face, en intégrant ces actions dans toutes les activités d'audit pertinentes, le cas échéant;
- c. s'assurent de la constitution des équipes d'audit et de leur compétence globale pour les activités d'audit, en attribuant les rôles, responsabilités et autorités, et en soutenant le leadership, le cas échéant;
- d. établissent tous les processus pertinents, y compris les processus pour:
  - la coordination et la programmation de tous les audits du programme d'audit;
  - l'établissement des objectifs de l'audit, du (des) champ(s) de l'audit et des critères d'audit, la détermination des méthodes d'audit et la constitution de l'équipe d'audit;
  - l'évaluation des auditeurs;
  - l'établissement des processus de communication externe et interne, le cas échéant;
  - la résolution des différends et le traitement des réclamations;
  - le suivi d'audit, le cas échéant;
  - le compte rendu au client de l'audit et aux parties intéressées pertinentes, le cas échéant;
- e. déterminent et assurent la fourniture de toutes les ressources nécessaires;
- f. s'assurent que les informations documentées appropriées sont préparées et tenues à jour, y compris les enregistrements relatifs au programme d'audit;
- g. surveillent, passent en revue et améliorent le programme d'audit;
- h. communiquent le programme d'audit au client de l'audit et, le cas échéant, aux parties intéressées pertinentes.

*Il convient que la ou les personnes responsables du management du programme d'audit demandent son approbation par le client de l'audit.*

# Connaissances et aptitudes générales



PECB

32

## **ISO19011, article 7.2.3.2 Connaissances et aptitudes générales des auditeurs de systèmes de management**

*Il convient que les auditeurs possèdent des connaissances et des aptitudes dans les domaines suivants:*

a) *Principes, processus et méthodes d'audit: les connaissances et les aptitudes dans ce domaine permettent à l'auditeur de s'assurer que les audits sont réalisés de manière cohérente et systématique.*

*Il convient qu'un auditeur sache:*

- comprendre les types de risques et d'opportunités liés à l'audit et les principes d'une approche par les risques de l'audit;
- planifier et organiser le travail de manière efficace;
- réaliser l'audit dans le temps imparti;
- définir les priorités et se concentrer sur les sujets importants;
- communiquer efficacement, oralement et par écrit (soit personnellement, soit en ayant recours à des interprètes);
- recueillir les informations par des entretiens efficaces, en écoutant, en observant et en passant en revue des informations documentées, y compris des enregistrements et des données;
- comprendre l'adéquation et les conséquences du recours à des techniques d'échantillonnage pour l'audit;
- appréhender et tenir compte des avis des experts techniques;
- auditer un processus du début à la fin, y compris les corrélations avec d'autres processus et des fonctions différentes, le cas échéant;
- vérifier la pertinence et l'exactitude des informations recueillies;
- confirmer le caractère suffisant et adéquat des preuves d'audit pour étayer les constatations et les conclusions d'audit;
- évaluer les facteurs qui peuvent affecter la fiabilité des constatations et des conclusions d'audit;
- documenter les activités d'audit et les constatations d'audit, et préparer des rapports;
- préserver la confidentialité et la sécurité des informations.

# Page de notes

---

PECB

33

## **ISO19011, article 7.2.3.2 Connaissances et aptitudes générales des auditeurs de systèmes de management (suite)**

b) Normes de système de management et autres références: les connaissances et les aptitudes dans ce domaine permettent à l'auditeur de comprendre le champ de l'audit et d'appliquer les critères d'audit et il convient qu'elles couvrent:

- les normes de systèmes de management ou d'autres documents normatifs ou guides/documents connexes utilisés pour la détermination des critères ou méthodes d'audit;
- l'application de normes de systèmes de management par l'audité et d'autres organismes;
- les relations et les interactions entre les processus du ou des systèmes de management;
- la compréhension de l'importance et de la priorité des multiples normes ou références;
- l'application des normes ou références à des situations d'audit différentes.

c) L'organisme et son contexte: les connaissances et les aptitudes dans ce domaine permettent à l'auditeur de comprendre la structure, la finalité et les pratiques de management de l'audité et il convient qu'elles couvrent:

- les besoins et attentes des parties intéressées pertinentes ayant un impact sur le système de management;
- le type d'organisme, sa gouvernance, sa taille, sa structure, ses fonctions et ses relations;
- les concepts généraux d'entreprise et de management, les processus et la terminologie associée, y compris la planification, la budgétisation et la gestion des personnes;
- le contexte culturel et social de l'audité.

d) Exigences légales et réglementaires et autres exigences applicables: les connaissances et les aptitudes dans ce domaine permettent à l'auditeur de connaître et de travailler dans le cadre des exigences qui s'appliquent à l'organisme. Il convient que les connaissances et aptitudes spécifiques au domaine de compétence ou aux activités, processus, produits et services de l'audité couvrent:

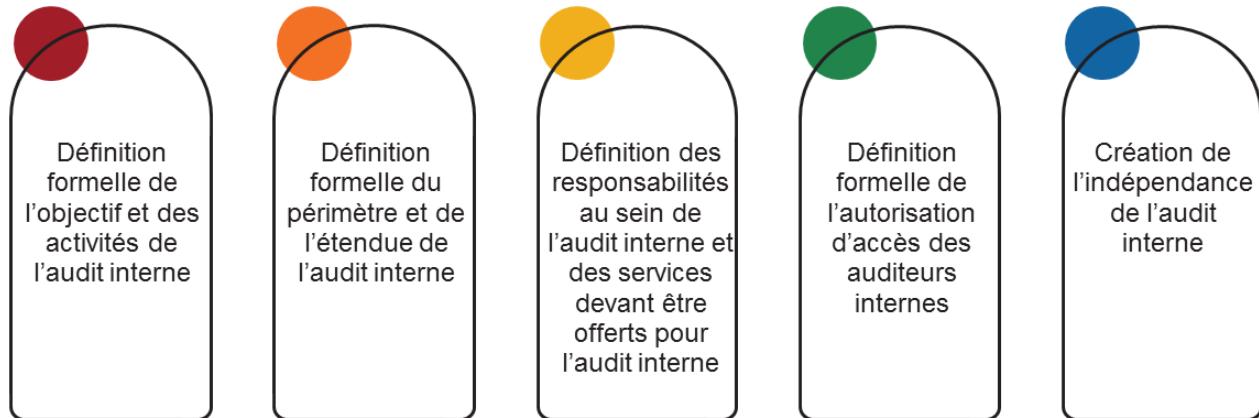
- les exigences légales et réglementaires et les autorités de réglementation associées;
- la terminologie légale de base;
- les contrats et obligations.

**NOTE: La connaissance des exigences légales et réglementaires n'implique pas de compétence juridique et il convient de ne pas traiter l'audit d'un système de management comme un audit de conformité juridique.**

### 3.2.3 Établir l'indépendance, l'objectivité et l'impartialité

#### Charte d'audit

##### Structure de la charte d'audit



PECB

34

La charte d'audit interne est un document officiel qui décrit les activités d'audit interne, les objectifs et les rôles et responsabilités de l'équipe d'audit interne. Elle définit la position de l'audit interne au sein de l'organisation, y compris la nature de la relation hiérarchique de l'auditeur avec la direction; elle autorise l'accès aux documents et dossiers, au personnel et aux propriétés physiques en relation avec les activités; et elle définit le périmètre des activités de l'audit interne. L'approbation finale de la charte d'audit interne devrait être effectuée par la direction.

Afin de garantir l'objectivité et l'impartialité de la fonction d'audit interne, les auditeurs ne doivent pas assumer de rôles opérationnels liés aux systèmes de management. Si une personne a assumé un tel rôle, une période de temps raisonnable (généralement un an) doit s'écouler avant qu'elle puisse occuper le poste d'auditeur interne. Une personne peut cumuler des fonctions d'opération et d'audit seulement si les deux sphères d'activités concernées ne sont pas liées. Dans ce cas, il convient de bien documenter les descriptions de postes afin d'éviter les conflits d'intérêts potentiels et une violation du principe d'indépendance.

**Note importante:** Dans le cas d'un petit organisme, il est souvent préférable d'externaliser la fonction d'audit interne à un tiers. Il est en effet plus facile de démontrer l'indépendance et l'impartialité d'une personne qui n'a aucun lien avec la mise en œuvre et les opérations des systèmes de management.

# Accès et indépendance

## Principes

### Accès aux ressources et collaboration

1

- Pour qu'un audit soit correctement réalisé, les auditeurs internes devraient avoir un accès sans restriction aux bureaux, aux sites et à la documentation. De plus, les auditeurs internes devraient être autorisés à procéder à des entretiens ou à des discussions avec les dirigeants, employés et autres parties de l'organisme.
- Cette nécessité de l'accès doit être documentée (habituellement dans la charte d'audit).

### Indépendance

2

- Les auditeurs internes doivent être indépendants des processus audités et ceci est généralement assuré si les auditeurs se rapportent directement au conseil d'audit de l'organisme plutôt qu'à la direction.
- Cette nécessité d'indépendance devrait être reflétée dans la charte organisationnelle.

PECB

35

Afin de s'assurer qu'un auditeur interne est efficace dans l'accomplissement de son mandat, les entités auditées doivent faire preuve de leur disponibilité et de la collaboration. Dans ce but, les auditeurs ne devraient pas subir, de la part des entités auditées, des limites à leurs interventions ou être sujets à des interférences.

## 3.2.4 Planifier les activités d'audit

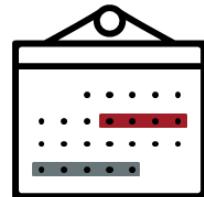
### Planification à court et long terme

#### Planification de haut niveau des activités d'audit sur trois ans

- Cette planification doit tenir compte du fait que l'ensemble du système de management devrait être audité tous les trois ans.

#### Planification annuelle plus détaillée

- Cette planification doit tenir compte du fait que l'auditeur n'est pas obligé d'auditer tous les processus et mesures du système de management chaque année.



36

PECB

La personne officiellement responsable des audits internes est responsable de la planification et de la réalisation des mandats qui lui sont assignés.

# Programme continu d'audit interne

## Avantages

- Détection rapide des anomalies et des non-conformités
- Réduction des tâches manuelles d'audit
- Surveillance et mesure continues
- Évaluation et analyse d'un plus grand nombre de transactions dans les systèmes

## Inconvénients

- Difficultés de mise en œuvre
- Coût élevé de mise en œuvre
- Peut donner une fausse impression de confiance
- Trop d'information peut rendre difficile la détection des anomalies significatives

PECB

37

Dans les organismes qui emploient une équipe d'auditeurs internes à temps plein, il est souhaitable de mettre en œuvre un programme d'audit interne continu.

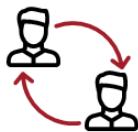
Pour mettre en œuvre un tel programme, plusieurs conditions prévalent:

- Automatisation de haut niveau
- Respect des lignes directrices importantes
- Processus automatisé pour la production rapide d'informations
- Alertes pour la détection de défaillance
- Outils d'audit automatisés
- Rapports automatisés
- Auditeurs SI compétents

## 3.2.5 Affecter et gérer les ressources du programme d'audit



Ressources financières



Ressources humaines



Outils



Politiques et procédures d'audit



Logistique

PECB

38

Une organisation qui met en œuvre un programme d'audit (interne ou externe) doit s'assurer de fournir les ressources nécessaires à son fonctionnement:

1. **Ressources financières** nécessaires pour développer, mettre en œuvre, gérer et améliorer les activités d'audit
2. **Personnel compétent** (auditeurs et experts techniques) pour réaliser les audits
3. **Outils** de travail (ordinateurs, logiciels, etc.)
4. **Politiques et procédures d'audit**
5. **Logistique** (transport, hébergement et autres besoins relatifs à l'audit)

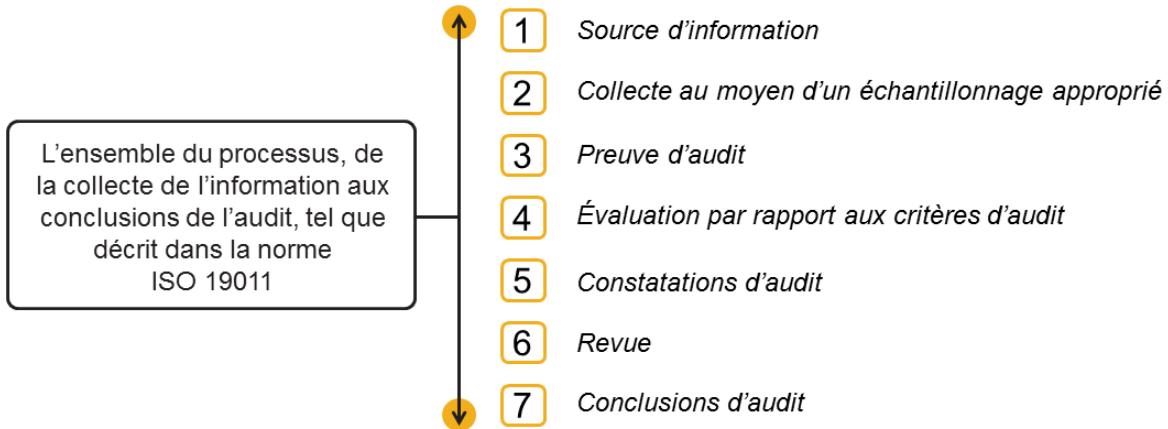
### ***ISO19011, article 5.4.4 Détermination des ressources du programme d'audit***

*Lors de la détermination des ressources nécessaires pour le programme d'audit, il convient que la ou les personnes responsables du management du programme d'audit considèrent:*

- a. *les ressources financières et le temps nécessaires pour développer, mettre en œuvre, manager et améliorer les activités d'audit;*
- b. *les méthodes d'audit;*
- c. *la disponibilité individuelle et globale des auditeurs et des experts techniques possédant les compétences appropriées pour les objectifs particuliers du programme d'audit;*
- d. *l'étendue du programme d'audit et les risques et opportunités associés au programme d'audit;*
- e. *les temps et les coûts de transport, l'hébergement et les autres besoins relatifs à l'audit;*
- f. *l'impact des différents fuseaux horaires;*
- g. *la disponibilité de technologies de l'information et de la communication (par exemple les ressources techniques requises pour mettre en place un audit à distance à l'aide de technologies venant à l'appui d'une collaboration à distance);*
- h. *la disponibilité de tous les outils, technologies et équipements nécessaires;*
- i. *la disponibilité des informations documentées nécessaires, telles que déterminées lors de l'établissement du programme d'audit;*
- j. *les exigences liées à l'installation, y compris les autorisations et équipements de sécurité requis (par exemple vérification des antécédents, équipement de protection individuelle, aptitude à porter une tenue pour salle blanche).*

## 3.2.6 Réaliser les activités d'audit

ISO 19011, article 6.4.7



PECB

39

Pour s'assurer qu'une exigence est satisfaites, l'auditeur doit recueillir les preuves de différentes sources d'information et les évaluer objectivement. La collecte de preuves peut être faite en utilisant des procédures d'audit (méthodes) différentes et l'utilisation d'échantillons est parfois requise.

Après l'évaluation de la preuve d'audit par rapport au critère d'audit, l'auditeur rédige les constatations d'audit. Finalement, après avoir réalisé l'analyse de toutes les constatations d'audit et la revue de la qualité, l'équipe d'audit émet les conclusions d'audit.

### **ISO19011, article 3.9 Preuves d'audit**

*enregistrements, énoncés de faits ou autres informations pertinentes pour les critères d'audit et vérifiables*

### **ISO19011, article 3.10 Constatations d'audit**

*résultats de l'évaluation des preuves d'audit recueillies, par rapport aux critères d'audit*

*Note1 à l'article: Les constatations d'audit indiquent la conformité ou la non-conformité.*

*Note2 à l'article: Les constatations d'audit peuvent conduire à l'identification des opportunités d'amélioration ou à la consignation des bonnes pratiques.*

*Note3 à l'article: En anglais, si les critères d'audit sont choisis parmi les exigences légales ou les exigences réglementaires, la constatation d'audit est qualifiée de « compliance » ou « non-compliance ».*

### **ISO19011, article 3.11 Conclusions d'audit**

*résultat d'un audit, après avoir pris en considération les objectifs de l'audit et toutes les constatations d'audit*

# Réaliser les activités d'audit

**Les procédures d'audit devraient inclure des informations sur comment :**

- 1 Planifier et programmer les audits en tenant compte des risques d'audit
- 2 Gérer la sécurité et la confidentialité de l'information et les risques d'audit
- 3 S'assurer de la compétence des auditeurs et des responsables de l'équipe d'audit
- 4 Sélectionner les équipes d'audit appropriées et leur assigner des rôles et responsabilités
- 5 Réaliser les audits, incluant l'utilisation de méthodes d'échantillonnage appropriées
- 6 Faire le suivi de l'audit, si applicable
- 7 Rapporter le résultat du programme d'audit au client de l'audit
- 8 Maintenir les enregistrements du programme d'audit
- 9 Faire le suivi de l'opération, des risques et de l'efficacité du programme d'audit

Pour les petits organismes, les activités ci-dessus peuvent être couverte par une seule procédure.

**PECB**

40

# Non-conformité

## Définition

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



PECB

41

Les exigences peuvent provenir de plusieurs sources: elles peuvent être spécifiées dans la norme, faire partie d'une exigence interne de l'organisation, provenir d'une loi ou d'un règlement, ou encore être incluses dans un contrat signé avec un client ou partenaire.

Voici des exemples de non-conformités:

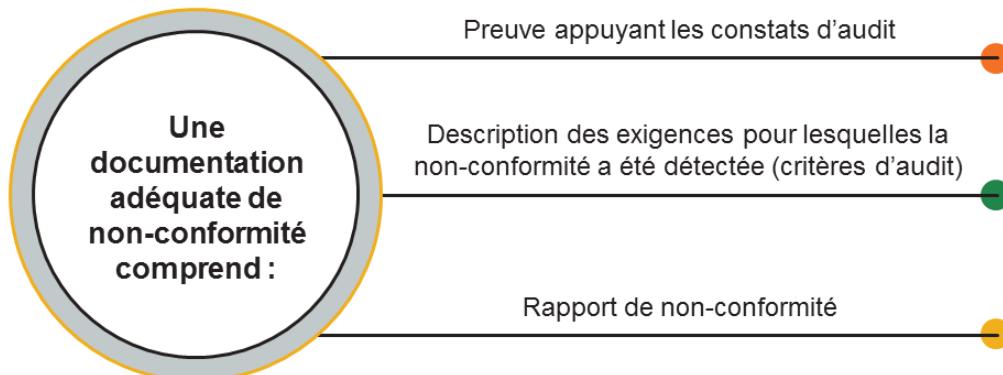
- Documentation pas adéquate
- Mesure de sécurité absente ou ne remplissant pas ses fonctions (conception)
- Mesure de sécurité ne fournissant pas les résultats prévus (efficacité)

### ***ISO9000, article 3.6 Termes relatifs aux exigences***

***3.6.11 Conformité: satisfaction d'une exigence***

***3.6.9 Non-conformité: non-satisfaction d'une exigence***

# Documentation d'une non-conformité



PECB

42

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

Il est à noter que la norme ISO/IEC 27001 contient plusieurs articles qui incluent plus d'une exigence. Il est important que l'auditeur documente les conditions spécifiques de la non-conformité (par exemple, en écrivant le texte exact de l'exigence associée aux critères d'audit).

Le rapport de non-conformité devrait:

- Être explicite et lié à une exigence du SMSI
- Être précis et sans équivoque, linguistiquement correct et le plus concis possible

# Rapport de non-conformité

## Exemple

RAPPORT DE NON-CONFORMITÉ		
N° de non-conformité : 3	Client : Thalia Technologies	N° du dossier : 34527
Processus : Gestion des actifs	Numéro de l'article : A.8.1.1	Site : Montréal
<b>Critère d'audit :</b> Tous les actifs doivent être clairement identifiés et un inventaire de tous les actifs importants doit être dressé et géré.		
<b>Description de la non-conformité observée :</b> Sur un échantillon de 25 actifs analysés venant de la liste des actifs, seuls 5 actifs étaient correctement identifiés.		
<b>Recommandation :</b> Établir un inventaire de tous les actifs importants et identifier clairement les actifs en incluant, par exemple, le type, le propriétaire, le format, l'emplacement, les informations relatives à la sauvegarde et à la licence, ainsi que la valeur pour l'organisme.		
Auditeur : John Doe	Reconnaissance du représentant audité : Non-conformité présentée à M. R. Smith et confirmée le 3 juin 2019	Non-conformité
Date : 5 juin 2019		Majeure*
		Mineure*

PECB

43

La partie finale (et la plus importante) de la documentation d'une non-conformité consiste à écrire un rapport de non-conformité. **Le rapport doit préciser le critère d'audit, la description de la non-conformité ainsi que la constatation d'audit. De façon facultative, on peut inclure des recommandations.**

Si ces trois éléments sont bien documentés, l'audité pourra comprendre et reconnaître la non-conformité. Le rapport servira également d'enregistrement utile pour un rapport futur.

Afin d'appuyer la traçabilité et de faciliter le suivi des plans d'action, il est essentiel que les non-conformités soient enregistrées et documentées de manière systématique. Une méthode simple serait d'utiliser un formulaire standard de rapport de non-conformité (*NCR – Nonconformity report*).

## 3.2.7 Effectuer le suivi des non-conformités

### Lignes directrices

Un auditeur interne devrait effectuer le suivi des plans d'action déposés à la suite des non-conformités (issues des audits internes et externes).

L'auditeur interne doit réviser les corrections, identifier les causes et les actions correctives, et vérifier l'efficacité de toutes ces corrections et actions correctives.

Le responsable du SMSI doit informer l'auditeur interne de l'avancement des corrections et des actions correctives.

Les corrections et actions correctives ne doivent pas toutes être mises en œuvre immédiatement.

Note : Selon son expérience et ses connaissances, l'auditeur doit faire preuve de jugement et évaluer si les plans d'action sont appropriés et s'ils permettent de s'attaquer aux causes intrinsèques des non-conformités.

PECB

44

**Un auditeur doit toujours se rappeler qu'il est très peu probable que l'organisme arrive à accomplir toutes les améliorations simultanément.** Chaque amélioration exige l'utilisation de ressources et nécessite du temps pour la mise en œuvre. Les plans d'action peuvent être classés par ordre de priorité par la direction, particulièrement là où des investissements sont nécessaires. Par conséquent, l'auditeur devra chercher à s'assurer que les objectifs d'amélioration sont réalistes en fonction du contexte particulier de l'audité.

Des réponses orales peuvent être reçues par l'auditeur. Dans ce cas, l'auditeur devrait les mettre par écrit par la suite.

L'auditeur doit solliciter ou recevoir une mise à jour périodique de la part de l'audité pour évaluer les progrès qui ont été réalisés. Le suivi des plans d'action est particulièrement important pour les problèmes à haut risque et les actions correctives ayant de longs délais d'exécution.

# Questions ?

PECB

45

# Section 23

## Revue de direction

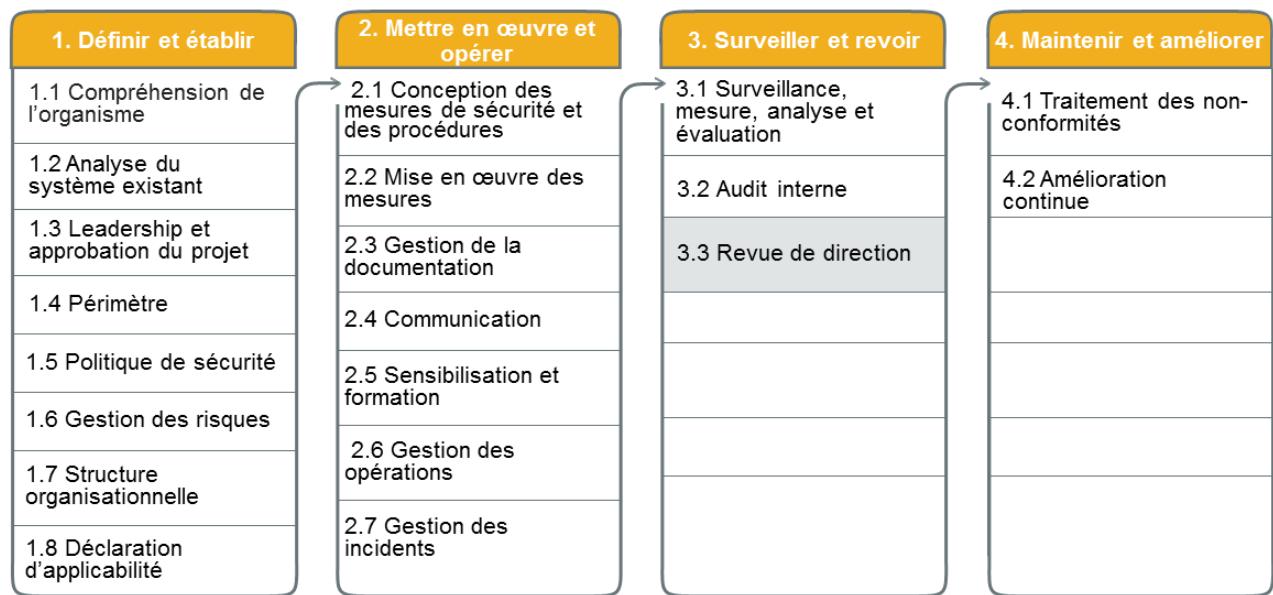
- Préparation d'une revue de direction
- Conduite d'une revue de direction
- Conclusion d'une revue de direction
- Activités de suivi d'une revue de direction

PECB

46

Cette section aidera le participant à acquérir des connaissances sur la façon de préparer et de mener une revue de direction. En outre, le participant sera en mesure de comprendre le processus de clôture et les activités d'un suivi de la revue de direction.

### 3.3 Revue de direction



PECB

47

# ISO/IEC 27001 Exigences

## ISO/IEC 27001, article 9.3

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

La revue de direction doit prendre en compte:

- a) l'état d'avancement des actions décidées à l'issue des revues de direction précédentes;
- b) les modifications des enjeux externes et internes pertinents pour le système de management de la sécurité de l'information;
- c) les retours sur les performances de sécurité de l'information, y compris les tendances concernant:
  - 1) les non-conformités et les actions correctives;
  - 2) les résultats de l'évaluation de la surveillance et des mesures;
  - 3) les résultats d'audit; et
  - 4) la réalisation des objectifs en matière de sécurité de l'information;
- d) les retours d'information des parties intéressées;
- e) les résultats de l'appréciation des risques et l'état d'avancement du plan de traitement des risques; et
- f) les opportunités d'amélioration continue.

Les conclusions de la revue de direction doivent inclure les décisions relatives aux opportunités d'amélioration continue et aux éventuels changements à apporter au système de management de la sécurité de l'information.

L'organisation doit conserver des informations documentées comme preuves des conclusions des revues de direction.

**PECB**

48

Un organisme souhaitant se conformer à la norme ISO/IEC27001 doit au moins effectuer une revue de direction chaque année et conserver les enregistrements.

# Revue de direction

## Définition

Une revue de direction est un examen périodique du système de management effectué par la direction pour analyser sa pertinence, son adéquation et son efficacité continues.

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

## 3.3 Revue de direction

### Liste des activités

3.3.1

Préparer une revue de direction

3.3.2

Mener une revue de direction

3.3.3

Élaborer les résultats de la revue de direction

3.3.4

Faire le suivi d'une revue de direction

### 3.3.1 Préparer une revue de direction

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



PECB

51

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

### 3.3.2 Mener une revue de direction

#### Sujets à mettre à l'ordre du jour

La contribution à une revue de direction devrait inclure des informations sur les sujets suivants :

1. État d'avancement des actions des revues de direction précédentes
2. Modifications des enjeux externes et internes pertinents pour le SMSI
3. Non-conformités et actions correctives
4. Résultats de la surveillance et des mesures
5. Résultats d'audit
6. Réalisation des objectifs de sécurité de l'information
7. Commentaires des parties intéressées
8. Résultats de l'appréciation des risques et l'état du plan de traitement des risques
9. Opportunités d'amélioration continue
10. Revue des actions nouvelles ou en cours

PECB

52

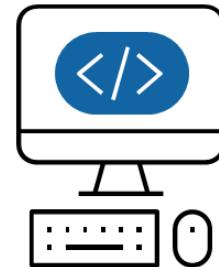
Par souci d'efficacité, la documentation requise pour chacun de ces sujets doit être préparée par le coordonnateur du SMSI. Le rôle de la revue sera de vérifier si les objectifs définis par la direction sont atteints et si le SMSI est conforme à la norme. Pour chaque point, la revue de direction pourra décider d'actions à mettre en place.

### 3.3.3 Élaborer les résultats de la revue de direction

#### Décisions et résolutions

Les résultats de la revue de direction doivent inclure toutes les décisions et actions liées à ce qui suit :

1. Opportunités d'amélioration continue
2. Éventuels changements à apporter au SMSI



### 3.3.4 Faire le suivi d'une revue de direction

---

- Les revues de direction doivent être documentées.
- L'organisme devrait fournir des rapports sur la revue de direction à ceux qui en font partie.
- Le responsable du SMSI et l'équipe d'audit interne ont la responsabilité d'assurer le suivi des plans d'action approuvés par la direction.





## Questions ?

PECB

55

# Section 24

## Traitemen~~t~~ des problèmes et des non-conformités

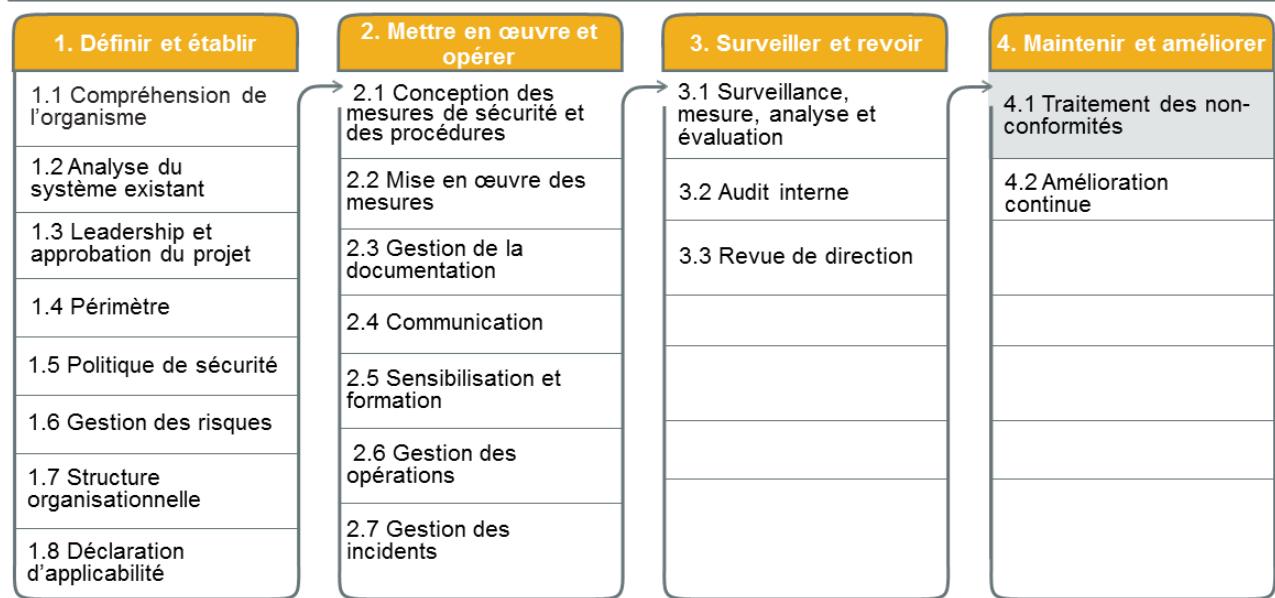
- Processus d'analyse des causes fondamentales
- Outils d'analyse des causes fondamentales
- Procédure d'actions correctives
- Procédure d'actions préventives

PECB

56

Cette section aidera le participant à comprendre l'importance de traiter les problèmes et les non-conformités. En outre, le participant acquerra des connaissances sur les processus et outils d'analyse des causes fondamentales, ainsi que sur les procédures d'actions correctives et préventives.

## 4.1 Traitement des non-conformités



PECB

57

# ISO/IEC 27001 Exigences

## ISO/IEC 27001, article 10.1

*Lorsqu'une non-conformité se produit, l'organisation doit:*

- a) réagir à la non-conformité, et le cas échéant:
    - 1) agir pour la maîtriser et la corriger; et
    - 2) traiter les conséquences;
  - b) évaluer s'il est nécessaire de mener une action pour éliminer les causes de la non-conformité, de sorte qu'elle ne se reproduise plus, ou qu'elle ne se produise pas ailleurs. À cet effet, l'organisation:
    - 1) examine la non-conformité;
    - 2) détermine les causes de non-conformité; et
    - 3) détermine si des non-conformités similaires existent, ou pourraient se produire;
  - c) mettre en œuvre toutes les actions requises;
  - d) réviser l'efficacité de toute action corrective mise en œuvre; et
  - e) modifier, si nécessaire, le système de management de sécurité de l'information.
- Les actions correctives doivent être à la mesure des effets des non-conformités rencontrées.*
- L'organisme doit conserver des informations documentées comme preuves:*
- f) de la nature des non-conformités et de toute action subséquente; et
  - g) des résultats de toute action corrective.

PECB

58

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

1. Définir un processus pour revoir, évaluer et traiter les non-conformités
2. Identifier les non-conformités et réagir avec efficacité

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

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

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

*Les faits suivants peuvent constituer des non-conformités:*

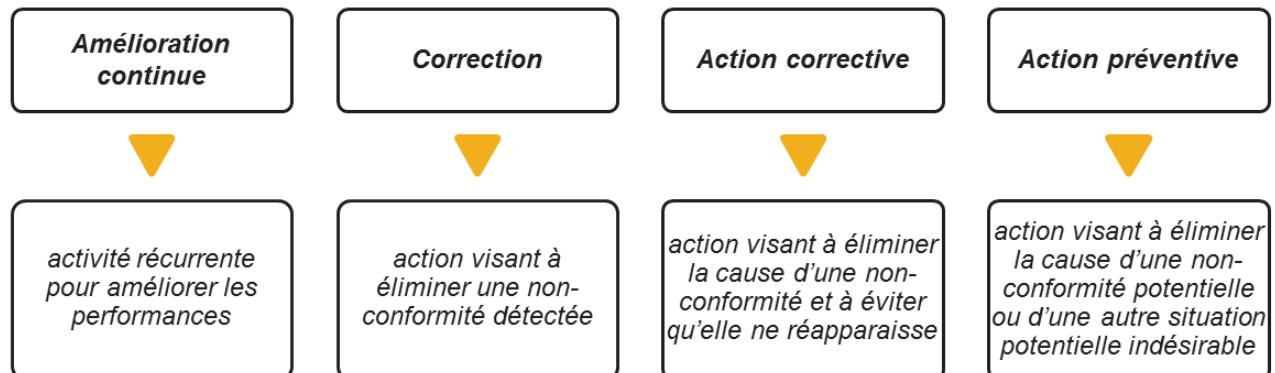
- d. les personnes qui ne se comportent pas comme prévu par les procédures et les politiques;
- e. les fournisseurs qui ne fournissent pas les produits ou les services convenus;
- f. les projets qui ne dispensent pas les résultats escomptés; et
- g. les mesures qui ne fonctionnent pas comme prévu.

*Les non-conformités peuvent être identifiées par:*

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

# Définitions

ISO 9000, article 3.3.2, 3.12.3, 3.12.2 et 3.12.1



PECB

59

## Note de terminologie:

1. Par définition, l'amélioration de la sécurité de l'information est la partie du management de la sécurité de l'information axée sur l'accroissement de la capacité à satisfaire aux exigences de la sécurité de l'information. Ces exigences peuvent être liées à tout aspect tel que l'efficacité, l'efficiency ou la traçabilité.
2. Le processus de définition des objectifs et de recherche d'opportunités d'amélioration est un processus continu utilisant les constatations et les conclusions d'audit, l'analyse des données, les revues de direction et d'autres moyens, et qui mène généralement à des actions correctives ou préventives.
3. Une action préventive est entreprise pour empêcher l'occurrence, alors qu'une action corrective est entreprise afin d'éviter sa réapparition.
4. Une correction peut être menée conjointement avec une action corrective.

## ISO9000, article 3.7.11 Efficacité

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

## ISO9000, article 3.7.10 Efficiency

rapport entre le résultat obtenu et les ressources utilisées

## 4.1 Traitement des non-conformités

### Liste des activités

4.1.1

Élaborer un processus pour résoudre les problèmes et les non-conformités

4.1.2

Déterminer les actions correctives

4.1.3

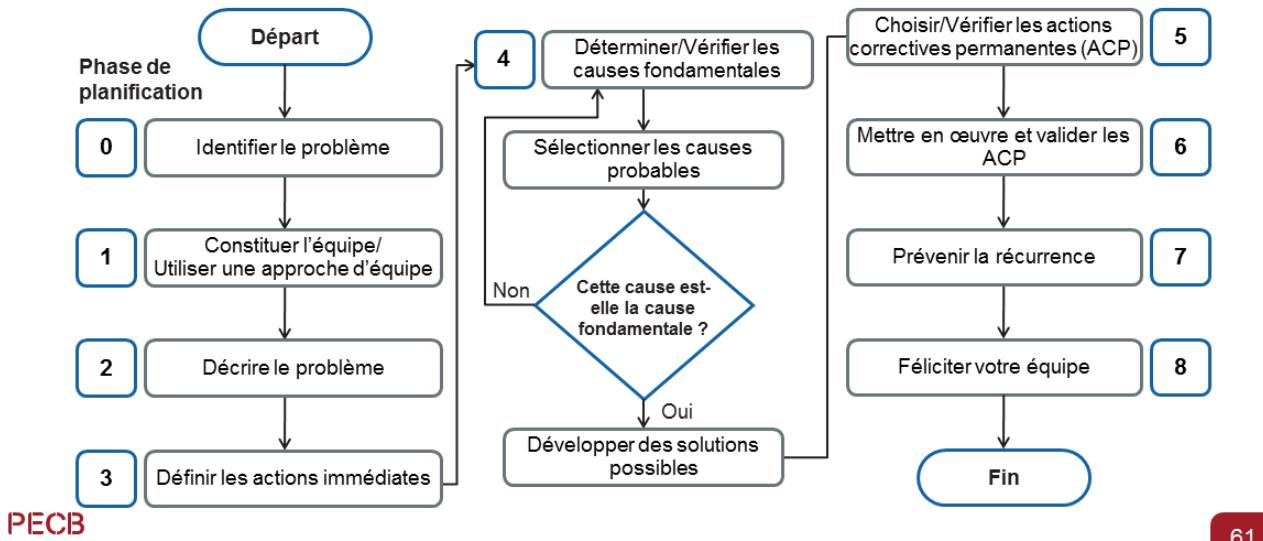
Déterminer les actions préventives

4.1.4

Rédiger le plan d'action

## 4.1.1 Élaborer un processus pour résoudre les problèmes et les non-conformités

Exemple de la méthode de résolution de problèmes en huit disciplines (8D – huit actions à réaliser) :



61

Le 8D est une méthode utilisée pour aborder et résoudre les problèmes et les non-conformités. Son but est d'identifier, de corriger et d'éliminer les problèmes récurrents. Il est utile dans l'amélioration des produits et des processus. Cette méthode établit une action corrective permanente basée sur l'analyse statistique du problème et se concentre sur l'origine du problème en déterminant ses causes fondamentales. À l'origine, la méthode se composait de huit étapes ou disciplines. Par la suite, une étape initiale de planification a été ajoutée.

Les étapes sont les suivantes:

**0.Identifier le problème:** Planifier pour résoudre le problème et déterminer les prérequis.

**1.Constituer l'équipe:** Mettre en place une équipe de personnes possédant une connaissance du produit/processus.

**2.Décrire le problème:** Définir et décrire le problème en le décomposant en éléments mesurables. Le 5W2H (qui, quoi, où, quand, pourquoi, comment et combien – *who, what, where, when, why, how, how many*) peut être utilisé comme outil à cette étape.

**3.Définir les actions immédiates:** Mettre en œuvre et évaluer des actions provisoires: Déterminer et mettre en œuvre des actions de confinement afin de contenir le problème et d'ainsi l'empêcher d'atteindre le client.

# Page de notes

---

PECB

62

**4.Déterminer et vérifier les causes fondamentales (*root causes*) et les points de fuite:** D'abord, identifier et analyser toutes les raisons possibles de l'apparition du problème. En outre, chercher à savoir pourquoi le problème n'a pas été détecté au moment où il s'est produit. Toutes les causes potentielles doivent être vérifiées et prouvées (si requis), et non pas déterminées par un *brainstorming*. Les outils qui peuvent être utilisés pour cartographier l'analyse des causes fondamentales comprennent les cinq pourquoi (5W) ou le diagramme d'Ishikawa.

**5.Choisir et vérifier les actions corrections permanentes (ACP) pour le problème/la non-conformité:** S'assurer que l'action corrective choisie résoudra le problème pour le client au moyen de programmes de préproduction.

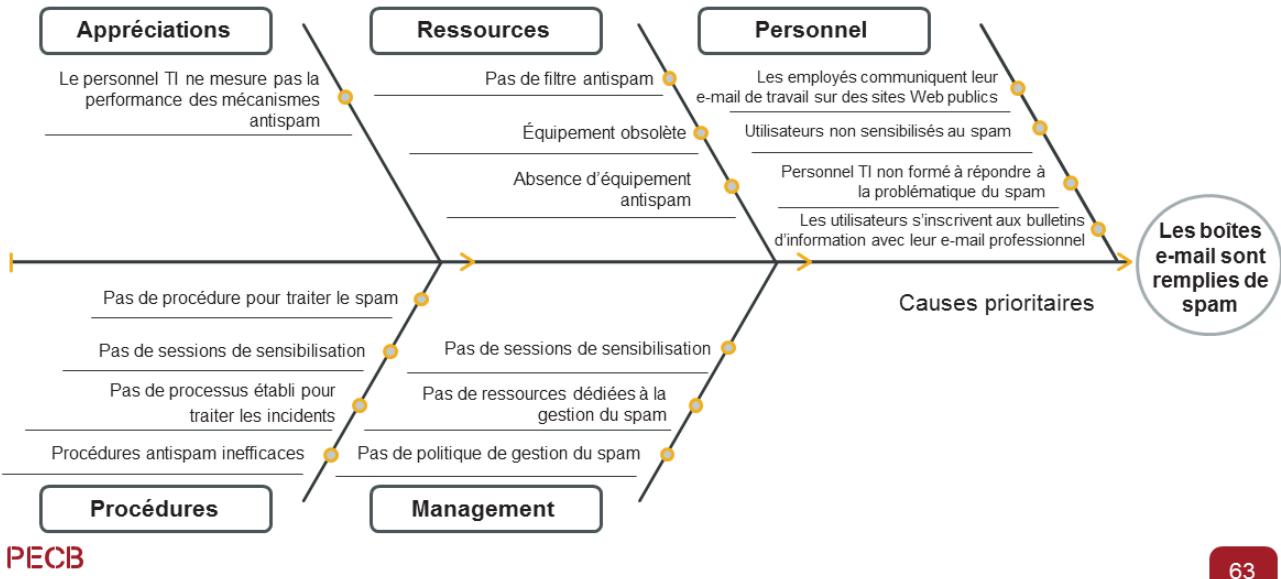
**6.Mettre en œuvre et valider les ACP:** Déterminer et mettre en œuvre les meilleures actions correctives.

**7.Entreprendre des actions préventives:** Afin d'éviter la récurrence des mêmes problèmes ou de problèmes similaires, déployer des actions préventives en modifiant les systèmes de management, les systèmes opérationnels, les pratiques et les procédures.

**8.Féliciter votre équipe:** L'organisme devrait reconnaître les efforts collectifs des membres de l'équipe et les remercier officiellement pour leur travail.

# Outil d'analyse des causes fondamentales

## Diagrammes de causes et effets



63

L'analyse des causes fondamentales est une méthode de résolution des non-conformités basée sur l'identification des causes fondamentales de problèmes ou d'incidents. Cette pratique est basée sur la conviction que les problèmes sont mieux résolus quand nous corigeons ou éliminons les causes fondamentales au lieu de simplement traiter les symptômes immédiats et évidents.

En mettant en place des mesures pour corriger les causes fondamentales, nous réduisons au minimum la probabilité de résurgence de la non-conformité. Mettre en place des mesures qui traitent directement les causes fondamentales est plus efficace que de traiter les symptômes des problèmes. Pour être efficace, l'analyse de la cause fondamentale doit être effectuée systématiquement et les conclusions doivent être soutenues par la preuve. Pour chaque problème analysé, il y a, en général, plus d'une cause fondamentale.

# Poser les bonnes questions

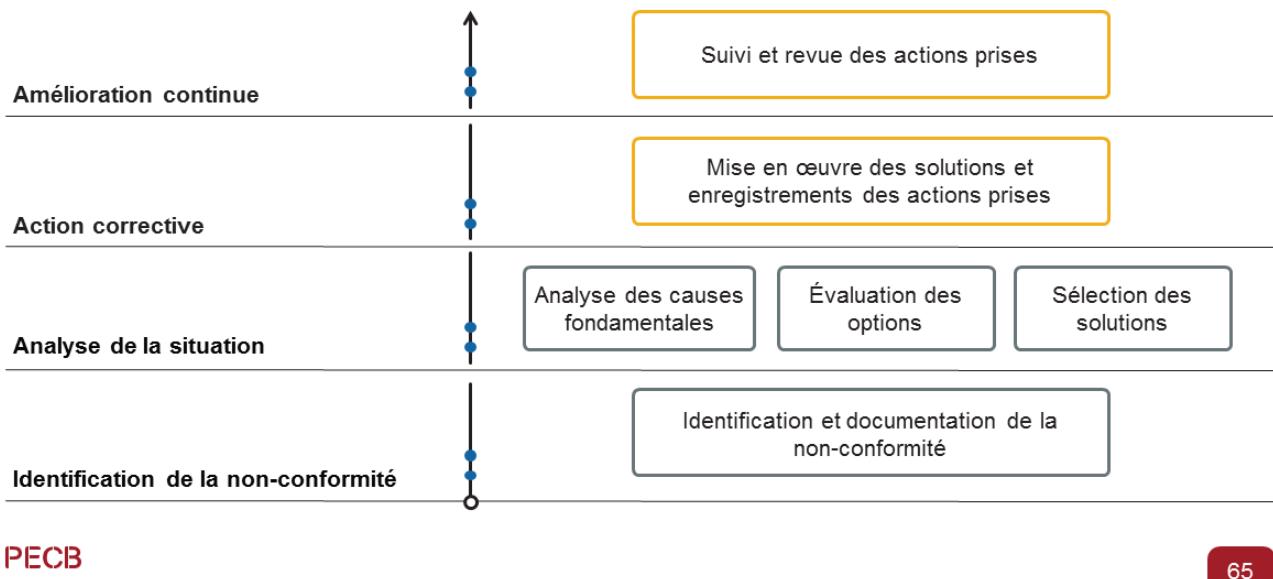
Nécessaire à l'analyse de tout problème

Situation actuelle	Remise en question	Suivi des solutions	Options retenues
Qu'est-ce qui est fait ?	Pourquoi est-ce nécessaire ?	Que pourrait-on faire d'autre ?	Que va-t-on faire ?
Comment est-ce fait ?	Pourquoi de cette façon ?	Comment faire différemment ?	Comment va-t-on le faire ?
Qui l'a fait ?	Pourquoi cette personne ?	Qui d'autre pourrait le faire ?	Qui va le faire ?
Où est-ce fait ?	Pourquoi est-ce fait à cet endroit ?	À quel autre endroit pourrait-on le faire ?	Où va-t-on le faire ?
Quand est-ce fait ?	Pourquoi est-ce fait à ce moment ?	Pourrait-on le faire à un autre moment ?	Quand va-t-on le faire ?

PECB

64

## 4.1.2 Déterminer les actions correctives



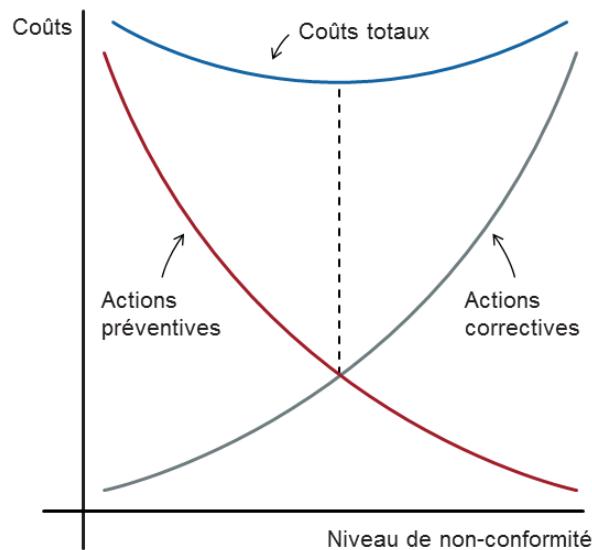
Une action corrective est une action entreprise pour **éliminer définitivement les causes fondamentales** d'une non-conformité ou de tout autre événement indésirable **existant** et pour **empêcher sa récurrence**. Une action corrective est donc un terme qui englobe les réactions à un processus de problème du système, à des incidents de sécurité, à des écarts sur l'atteinte d'objectifs, à des non-conformités, etc.

Le processus d'action corrective devrait inclure:

- Identification de la non-conformité:** L'étape initiale dans le processus est de clairement définir et documenter la non-conformité ainsi que d'analyser ses impacts sur l'organisation.
- Analyse des causes fondamentales:** Détermine la source de la non-conformité et analyse les causes fondamentales.
- Évaluation des options:** On élabore une liste d'actions correctives possibles. À cette étape, si le problème est important ou que sa potentialité de récurrence est élevée, on peut mettre en place des actions correctives temporaires.
- Sélection des solutions:** Une ou plusieurs actions correctives sont sélectionnées pour corriger la situation et les objectifs d'amélioration envisagés sont déterminés. La solution retenue doit corriger le problème et contribuer à éviter que des situations similaires ne se reproduisent.
- Mise en œuvre des actions correctives:** Le plan d'actions correctives qui a été approuvé est mis en œuvre et toutes les actions décrites dans le plan sont documentées.
- Suivi des actions correctives:** On doit vérifier que les nouvelles mesures correctives sont en place et effectives. Le suivi est habituellement effectué, d'une part, par le responsable de projet, et d'autre part, par le service d'audit.
- Revue des actions correctives:** Afin d'effectuer une revue de l'efficacité des actions correctives, on évalue périodiquement si l'organisation a atteint ses objectifs de sécurité à l'aide des actions correctives et si elles demeurent efficaces dans le temps.

## 4.1.3 Déterminer les actions préventives

L'organisme doit déterminer les actions à prendre pour **éliminer les causes potentielles de non-conformité** conformément aux conditions du SMSI.



PECB

66

Une action préventive est toute action entreprise pour **éliminer les causes d'une non-conformité** ou de tout autre événement potentiellement indésirable et pour empêcher leur réalisation future. Une action préventive est lancée pour éviter qu'un problème potentiel ne se produise. Une surveillance et des mesures adéquates doivent être mises en œuvre dans le SMSI pour s'assurer que les problèmes potentiels sont identifiés et éliminés avant qu'ils ne surviennent.

Il est à noter qu'une action visant à prévenir les non-conformités est souvent plus rentable qu'une action corrective. **Un organisme devrait viser l'équilibre coût-efficacité entre la mise en œuvre d'actions correctives et d'actions préventives.**

En établissant un processus continu de gestion des risques, l'organisme est, en général, plus susceptible de détecter un changement dans les facteurs de risque qui la concernent parce que les risques ne sont pas statiques. Les menaces, les vulnérabilités, la probabilité ou les conséquences peuvent changer brusquement. Par conséquent, une surveillance constante est nécessaire pour détecter ces changements et déployer des actions préventives avant qu'un risque ne se produise.

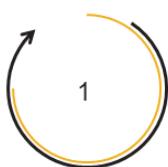
L'organisme peut assurer, par exemple, que les éléments suivants sont surveillés:

- Nouveaux actifs qui ont été inclus dans le SMSI
- Modifications de la valeur des actifs, par exemple, en raison de l'évolution des besoins opérationnels
- Nouvelles menaces (internes ou externes) identifiées qui n'ont pas été évaluées
- Nouvelles vulnérabilités identifiées qui n'ont pas été évaluées
- Vulnérabilités identifiées pour déterminer ceux qui sont exposés à de nouvelles menaces
- Incidents de sécurité

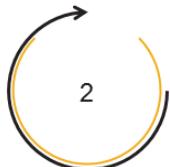
Le processus des actions préventives est similaire au processus des actions correctives: identification d'un problème potentiel, évaluation des solutions, sélection des solutions, mise en œuvre des actions préventives, suivi et révision des actions préventives.

## 4.1.4 Rédiger le plan d'action

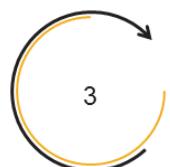
### Plan d'action :



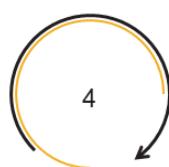
Peut être écrit de façon très sommaire



Doit permettre de corriger la non-conformité



Devrait être basé sur une approche préventive et corrective



Doit inclure une période de réalisation



Doit permettre d'obtenir des résultats vérifiables

PECB

67

Les dates de réalisation doivent être réalistes en fonction des non-conformités observées et des coûts des actions correctives à prendre. Les délais fixés doivent être raisonnables.

# Soumission de plans d'action à la suite d'un audit

- Un plan d'action doit être soumis pour chaque non-conformité et non un plan d'action global pour toutes les non-conformités.
- Chaque plan d'action doit être approuvé par la direction.
- L'auditeur analysera la cause et évaluera si la correction spécifique et les actions correctives prises ou planifiées permettront d'éliminer les non-conformités détectées dans une période de temps définie.



PECB

68

Si, à la suite d'une analyse, la direction décide d'accepter le risque plutôt que de mettre en place des actions correctives, préventives ou d'amélioration, elle doit alors documenter les justifications.

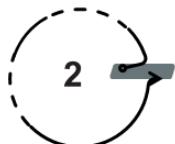
Le plan d'action doit être déposé dans les délais fixés. La plupart des organismes de certification (dans le cas d'un audit de certification) fixent un délai variant de 10 à 60 jours pour le dépôt de plans d'action. **Dans le cas d'une non-réception dans les délais convenus, l'audité ne sera pas recommandé pour la certification.**

# Plans d'action

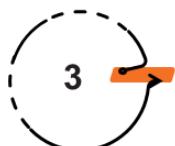
## Exemple



Sur le réseau, pour séparer les données confidentielles des autres bases de données, un nouveau système dédié sera installé afin de gérer les données des comptes clients (2<sup>e</sup> trimestre 2017).



Une nouvelle version de la politique de sécurité doit être éditée afin d'y inclure les mentions légales, réglementaires et les exigences contractuelles (dans un délai de 2 mois).



Les noms des personnes à contacter en cas de désastre doivent être explicitement mentionnés dans le plan de continuité d'activité (immédiatement) et les procédures pour contacter ces personnes doivent être documentées et communiquées.

PECB

69

# Exercice 11

PECB

70

## Exercice11: Plan d'actions correctives

Scientia Online Library a été auditee et plusieurs non-conformités ont été identifiées par l'auditeur. Proposez des actions correctives pour chaque non-conformité et justifiez ces actions.

1. Une non-conformité indique que les seuls enregistrements conservés pour le contrôle d'accès des utilisateurs sont ceux relatifs à l'Active Directory. Les autres enregistrements ne sont pas conservés.
2. Une non-conformité indique le manque de formation et d'expérience de l'auditeur interne. Celui-ci n'a pas identifié plusieurs non-conformités qui auraient pu être facilement détectées. En examinant le CV de l'auditeur interne, on a remarqué qu'il avait plus de 20ans d'expérience en informatique, mais qu'il n'avait jamais suivi un cours d'audit ni jamais effectué d'audit auparavant. Au cours d'un entretien, il a indiqué que cette responsabilité lui avait été confiée parce que personne d'autre ne voulait le faire – il avait bien accueilli ce nouveau défi.
3. Une non-conformité a été soulevée car l'organisme n'a pas traité un incident dans le délai indiqué dans sa politique de gestion des incidents. En effet, la politique de gestion des incidents mentionne explicitement dans ses objectifs que tous les incidents doivent être clôturés dans les cinq jours et que 100% des incidents doivent se clôturer dans les 15jours suivant leur première déclaration. Pour cet incident, un client qui a acheté un livre a déclaré avoir été victime d'une fraude par carte de crédit et voulait un remboursement complet. La personne responsable de la gestion de cet incident est tombée malade le lendemain et n'est revenue au travail que 12jours plus tard. Tant de travail s'était empilé et l'affaire de la fraude par carte de crédit était si complexe que 5jours ont été nécessaires pour que l'employé puisse s'occuper de cette question, enquêter et clore l'incident. Personne d'autre dans l'entreprise ne s'est occupé des incidents en l'absence de l'employé.

# Page de notes

---

PECB

71

4.Une non-conformité a été soulevée parce qu'au cours de l'audit, le site Web de la compagnie a été mis hors service et que la tierce partie responsable de la maintenance du site n'a pas traité ce problème pendant 72heures. Personne dans l'organisme ne semblait savoir quoi faire. Le PDG estime que Scientia Online Library a perdu au moins 35 000\$ de revenus au cours de cette indisponibilité, un montant jugé inacceptable pour l'organisme.

5.Une non-conformité a été soulevée parce que l'auditeur a demandé à un technicien informatique d'effectuer un scan du réseau et plus de 2 000fichiers musicaux ont été découverts. L'organisme n'interdit pas la copie de fichiers musicaux sur son réseau. L'auditeur a remarqué que certains fichiers musicaux étaient conservés dans des dossiers partagés et que certains employés avaient écouté ou copié plusieurs des chansons d'autres employés. L'auditeur a également trouvé des preuves que certaines des chansons ont été téléchargées à partir de sites Web de partage de fichiers. Lors des entrevues avec des employés sur la question, certains ont mentionné qu'ils avaient copié des chansons de leurs CD personnels afin de pouvoir écouter de la musique pendant qu'ils travaillaient. D'autres ont admis qu'ils avaient téléchargé des chansons à partir de sites Web de partage de fichiers, mais qu'ils n'avaient téléchargé que des chansons dont ils possédaient (et payaient) les CD chez eux – « nous sommes conscients de la politique de l'entreprise en matière de respect des droits de propriété intellectuelle et nous ne pourrions en aucun cas écouter de la musique obtenue illégalement ». Ils ont indiqué avoir procédé de la sorte parce qu'ils souhaitaient écouter certaines de leurs chansons favorites qu'ils possédaient par ailleurs à la maison, mais qu'ils ne voulaient pas apporter leurs CD au bureau et les copier sur leur ordinateur.

Durée de l'exercice: 30 minutes

Commentaires: 15 minutes



# Questions ?

PECB

72

# Section 25

## Amélioration continue

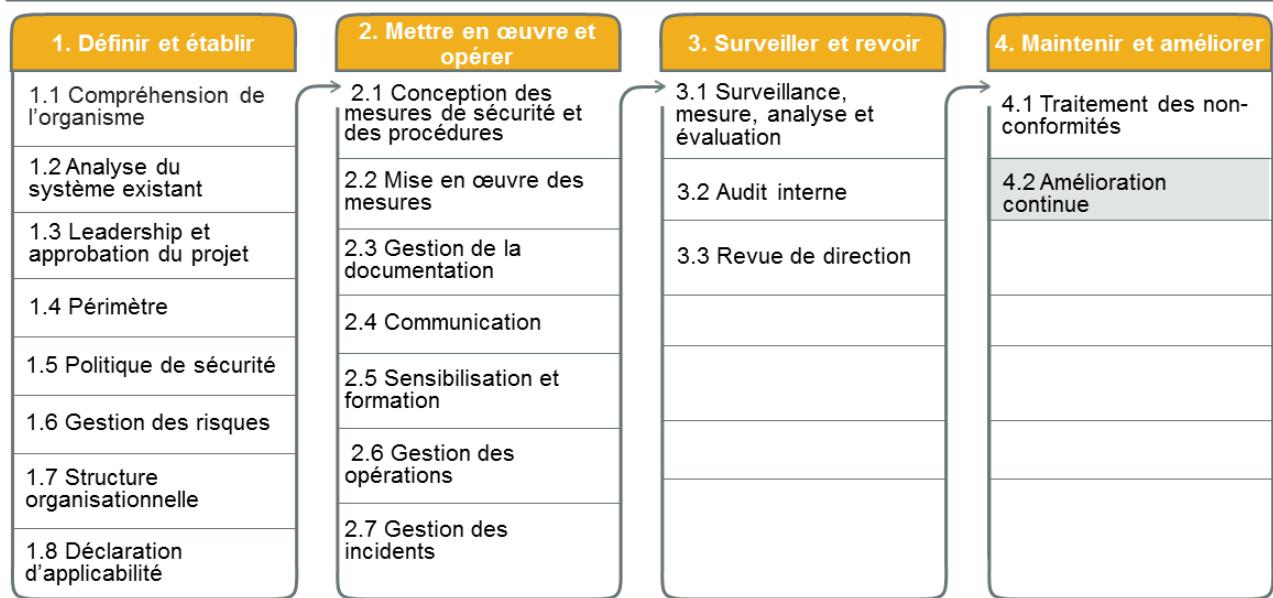
- Processus de surveillance continue des facteurs de changement
- Maintien et amélioration du SMSI
- Mise à jour continue de l'information documentée
- Documenter les améliorations

PECB

73

Cette section fournira de l'information qui aidera le participant à acquérir des connaissances sur l'amélioration continue du système de management de la sécurité de l'information par la surveillance des facteurs de changement, la mise à jour de la documentation et le maintien et l'amélioration du SMSI.

## 4.2 Amélioration continue



PECB

74

# ISO/IEC 27001 Exigences

## ISO/IEC 27001, article 10.2

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



PECB

75

Un organisme souhaitant se conformer à la norme ISO/IEC27001 doit au moins démontrer que des mesures sont prises pour améliorer continuellement l'efficacité du SMSI.

### **ISO/IEC27003, article 10.2 Amélioration continue**

#### **Explication**

*Une approche systématique utilisant une amélioration continue conduira à un SMSI plus efficace, qui améliorera la sécurité de l'information de l'organisme. La gestion du système de la sécurité de l'information oriente les activités opérationnelles de l'organisme afin d'éviter d'être trop réactive, c'est-à-dire que la plupart des ressources sont utilisées pour identifier les problèmes et les résoudre. Le SMSI fonctionne systématiquement grâce à une amélioration continue afin que l'organisation puisse adopter une approche plus proactive. La direction générale peut définir des objectifs pour une amélioration continue, p. ex. par des mesures d'efficacité, des coûts ou de maturité des processus.*

#### **Lignes directrices**

*Il convient que l'amélioration continue du SMSI implique que le SMSI lui-même, ainsi que tous ses éléments, soient évalués en tenant compte des problématiques internes et externes (4.1), des exigences des parties intéressées (4.2) et des résultats de l'évaluation de la performance (article9). Il convient que l'évaluation inclue une analyse de:*

- a. *l'adéquation du SMSI, pour savoir si les problèmes externes et internes, les exigences des parties intéressées, les objectifs de sécurité de l'information établis et les risques identifiés en sécurité de l'information sont correctement traités par la planification et la mise en œuvre du SMSI et les mesures de sécurité de l'information;*
- b. *l'adéquation du SMSI, pour savoir si les processus SMSI et les mesures de sécurité de l'information sont compatibles avec les objectifs, les activités et les processus généraux de l'organisation; et*
- c. *l'efficacité du SMSI, en considérant si les résultats escomptés du SMSI sont atteints, si les exigences des parties intéressées sont respectées, si les risques de sécurité de l'information sont gérés pour atteindre les objectifs de sécurité de l'information, si les non-conformités sont gérées, tandis que les ressources nécessaires pour l'établissement, la mise en œuvre, le maintien et l'amélioration continue du SMSI correspondent à ces résultats.*

# Amélioration continue

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



Les grandes transformations  
se font à petits pas.

PECB

76

L'accent est mis sur l'amélioration continue par l'établissement d'objectifs de performance organisationnelle, de la mesure, de la revue et de la modification subséquente des processus, des systèmes, des ressources, de la compétence et des aptitudes.

Cela peut être indiqué par l'existence d'objectifs explicites par rapport auxquels la performance de l'organisation et de chaque gestionnaire est mesurée. La performance de l'organisme peut être publiée et communiquée. Normalement, il y aura au moins une revue annuelle de la performance puis une révision des processus et la fixation d'objectifs de performance révisés pour la période suivante.

## 4.2 Amélioration continue

### Liste des activités

**4.2.1**

Définir les facteurs de changements à surveiller

**4.2.2**

Maintenir et améliorer le SMSI

**4.2.3**

Assurer la mise à jour continue des informations documentées

**4.2.4**

Documenter les améliorations

## 4.2.1 Définir les facteurs de changements à surveiller

Facteurs de changement du SMSI à surveiller			
Changements organisationnels	Changements dans les technologies	Changements externes	Changements au SMSI
<ul style="list-style-type: none"><li>• Mission</li><li>• Objectifs d'activité</li><li>• Budget et ressources</li><li>• Nouveaux produits et services</li><li>• Changement dans le personnel</li></ul>	<ul style="list-style-type: none"><li>• Matériel informatique</li><li>• Logiciels</li><li>• Procédures TI</li><li>• Processus TI</li></ul>	<ul style="list-style-type: none"><li>• Lois et règlements</li><li>• Préoccupations et exigences des clients et des fournisseurs</li><li>• Fournisseurs</li><li>• Changements d'environnement (ex. : nouveaux concurrents)</li></ul>	<ul style="list-style-type: none"><li>• Politique SMSI</li><li>• Scénarios de nouveau risque</li><li>• Changements des procédures</li><li>• Résultats de tests et d'exercices</li><li>• Résultats d'audit</li></ul>

PECB

78

Pour être efficace, le système de gestion devrait refléter avec précision les exigences, procédures, structure organisationnelle et politiques de l'entreprise. Durant la phase d'amélioration continue, les processus et les procédures subissent de fréquents changements à cause des besoins croissants de l'activité, des améliorations de la technologie ou des nouvelles politiques internes ou externes. Il est donc essentiel que le système de management soit revu et amélioré régulièrement dans le cadre du processus de gestion du changement de l'organisme afin de s'assurer que les nouvelles informations sont documentées et que les mesures de sécurité sont révisées si nécessaire.

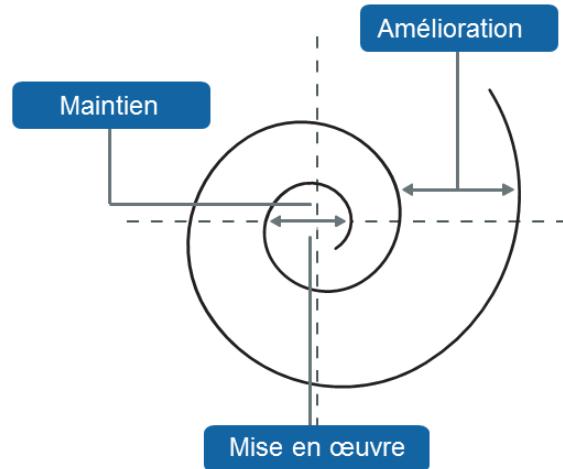
Règle générale, le plan devrait être révisé pour assurer son exactitude et son exhaustivité, et ce, à une fréquence définie par l'organisme ou chaque fois que des changements touchent un élément du plan. Certains éléments, tels que les listes de contacts, nécessiteront des revues plus fréquentes.

Alors que toutes les stratégies devraient être revues de manière continue, la fréquence à laquelle la stratégie du SMSI de l'organisme doit être revue dépend de la nature, de la taille et de la complexité de l'organisme, de son profil de risque métier et de l'environnement dans lequel il opère. Les bonnes pratiques indiquent qu'une revue de la stratégie de l'organisme devrait être faite au moins tous les 12 mois, sauf dans les cas suivants:

- Il s'agit du développement et de la documentation initiale de la stratégie.
- Il y a un changement significatif dans la technologie clé ou dans les télécommunications, y compris les systèmes et les réseaux.
- Le rythme des changements affectant l'activité de l'entreprise est particulièrement agressif.

## 4.2.2 Maintenir et améliorer le SMSI

- Le SMSI doit être maintenu et mis à jour périodiquement.
- Les responsables respectifs de la sécurité de l'information devraient être informés de toute mesure qu'il a été convenu de prendre pour améliorer les processus afin qu'aucun risque ou élément de risque ne soit négligé ou sous-estimé avant que les changements soient mis en œuvre.



## 4.2.3 Assurer la mise à jour continue des informations documentées

### Changement continu

#### Documentation du SMSI

- Politique de sécurité de l'information
- Objectifs, cibles et plans d'action
- Analyse des risques
- Stratégie
- Programmes de sensibilisation
- Programmes de formation
- Plans de gestion d'incident
- Continuité d'activité et plans de reprise
- Contrôle de l'information documentée

#### Facteurs de changement

- Évolution organisationnelle
- Nouveaux règlements
- Changements dans le périmètre d'activité
- Incidents
- Opération défectiveuse
- Pannes
- Rapports de gestion des risques
- Résultats de tests
- Audits internes
- Audits externes

Réviser et adapter

PECB

80

La documentation du SMSI est la pierre angulaire d'un système de management. En cas de crise, il est important d'avoir une documentation complète et à jour pour permettre aux acteurs impliqués dans une urgence de suivre une liste d'actions plutôt que d'avoir à décider en improvisant ou par intuition.

Le maintien adéquat de l'information documentée n'élimine en aucun cas les décisions spontanées puisqu'il ne faut pas s'attendre à ce qu'elle soit entièrement à jour. Il prépare simplement les principaux acteurs à agir lorsque la situation l'exige, en donnant des conseils et en évitant autant d'erreurs que possible.

Le SMSI est un système dynamique et le changement continu est impératif.

**En conséquence, l'information documentée doit être adaptée à chaque fois que se produit un changement.**

# Les avantages de l'amélioration continue

## Changement continu

### Avantages

#### Efficacité accrue

L'amélioration continue permet d'accroître la productivité, puisque les changements peuvent conduire à des résultats positifs à long terme.

#### Collaboration au sein de l'équipe

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

#### Satisfaction accrue de la clientèle

Tout en recherchant activement des moyens d'améliorer leur système de management, les organismes augmentent indirectement la valeur et la qualité des produits et services qu'ils offrent.

#### Réduction des erreurs

Tout en cherchant activement des moyens d'améliorer le système de management, les organismes réduisent indirectement le nombre d'erreurs.

PECB

81

## 4.2.4 Documenter les améliorations

Habituellement par la procédure de gestion du changement

Enregistrement des changements			
Page n°	Commentaire	Date du changement	Signature

PECB

82

Le coordonnateur du SMSI devrait enregistrer les modifications apportées au plan à l'aide d'un enregistrement des changements, qui indique le numéro de page, un commentaire et la date de la modification. L'enregistrement des changements, illustré dans le tableau, devrait être intégré dans les différents documents inclus dans le SMSI.



## Questions ?

PECB

83

# Section 26

## Préparation à l'audit de certification

- Sélection de l'organisme de certification
- Préparation à l'audit de certification
- Étape 1 de l'audit
- Étape 2 de l'audit
- Suivi d'audit
- Décision de certification

PECB

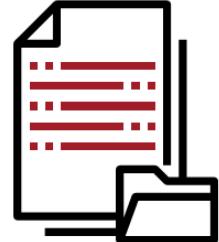
84

La présente section fournit des informations qui aideront le participant à acquérir des connaissances sur les audits de certification, à choisir l'organisme de certification, à se préparer à l'audit et à effectuer les étapes 1 et 2 de l'audit. De plus, le participant acquerra des connaissances sur le suivi d'audit et la décision de certification.

# ISO/IEC 27001 Exigences

## ISO/IEC 27001, article 1

*Les exigences fixées dans la présente Norme internationale sont génériques et prévues pour s'appliquer à toute organisation, quels que soient son type, sa taille et sa nature. Il n'est pas admis qu'une organisation s'affranchisse de l'une des exigences spécifiées aux Articles 4 à 10 lorsqu'elle revendique la conformité à la présente Norme internationale.*



PECB

85

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

1. Se conformer à l'ensemble des articles 4 à 10 ainsi qu'à l'ensemble des mesures de sécurité applicables.
2. Avoir un SMSI en application depuis plus de trois mois.

# Organisme de certification

## ISO/IEC 17021-1

- **Organisme de certification** : organisme tiers qui évalue la conformité des systèmes de management
- **Certification** : procédure par laquelle un tiers atteste par écrit qu'un produit, un processus ou un service est conforme aux critères spécifiés



PECB

86

### ISO/IEC17021-1, article1 Domaine d'application

La présente partie de l'ISO/IEC 17021 spécifie les principes et les exigences relatifs à la compétence, à la cohérence et à l'impartialité des organismes procédant à l'audit et à la certification de tous les types de systèmes de management.

Les organismes de certification conformes à la présente partie de l'ISO/IEC17021 ne sont pas tenus de proposer tous les types de certification de système de management.

La certification de systèmes de management est une activité d'évaluation de la conformité par tierce partie (voir l'ISO/IEC17000:2004, 5.5) et les organismes exerçant cette activité sont par conséquent des organismes d'évaluation de la conformité par tierce partie.

Note1: Les exemples de systèmes de management incluent les systèmes de management environnemental, les systèmes de management de la qualité, les systèmes de management de la sécurité de l'information.

Note2: Dans la présente partie de l'ISO/IEC 17021, la certification de systèmes de management est désignée « certification » et les organismes d'évaluation de la conformité par tierce partie sont désignés « organismes de certification ».

Note3: Un organisme de certification peut être gouvernemental ou non gouvernemental, avec ou sans pouvoir réglementaire.

Note4: La présente partie de l'ISO/IEC17021 peut être utilisée comme référentiel pour l'accréditation, l'évaluation par des pairs ou d'autres processus d'audit.

# Page de notes

---

PECB

87

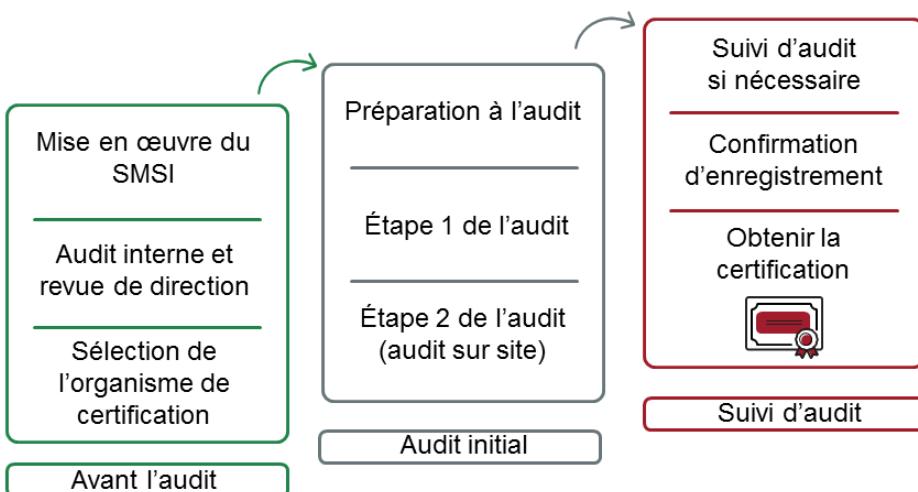
## ***ISO/IEC17021-1 Introduction***

*La certification d'un système de management assure par une démonstration indépendante que le système de management de l'organisme:*

- a. *est conforme aux exigences spécifiées;*
- b. *est capable de réaliser de manière fiable la politique et les objectifs qu'il a déclarés;*
- c. *est mis en œuvre de manière efficace.*

*La certification comprend l'audit du système de management d'un organisme. La manière d'attester la conformité à une norme spécifique du système de management ou à d'autres exigences normatives prend généralement la forme d'un document de certification ou d'un certificat.*

# Processus de certification



**Note :**

Après l'obtention de la certification, un audit de surveillance sera mené afin d'assurer l'amélioration continue.

**PECB**

88

Obtenir une certification pour l'organisme:

1. Mettre en œuvre le SMSI
2. Réaliser un audit interne et une revue de direction
3. Sélectionner l'organisme de certification
4. Préparer l'audit de certification
5. Préparer l'étape1 de l'audit
6. Préparer l'étape2 de l'audit (audit sur site)
7. Effectuer le suivi d'audit
8. Confirmer l'enregistrement
9. Obtenir la certification ISO/IEC27001

**Note importante:** L'amélioration continue peut être décrite comme un processus continu visant à améliorer les procédures, les processus et les produits ou services de l'organisme en général.

L'audit de surveillance est une activité qui est effectuée une fois par an (ou plus) en fonction des besoins de l'organisme afin de maintenir la confiance que le système de management de l'organisme respecte les exigences du système de management qui le concerne (norme).

# Page de notes

---

PECB

89

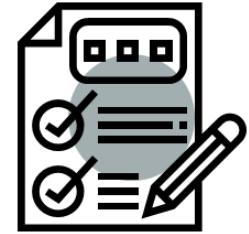
1. **Sélection de l'organisme de certification (registraire):** Chaque entreprise peut choisir l'organisme de certification (registraire) de son choix.
2. **Pré-audit (facultatif):** Un organisme peut choisir de faire un pré-audit pour mesurer l'écart entre son système de management actuel et les exigences de la norme.
3. **Étape1 de l'audit:** Le but de l'étape1 est de vérifier si le système de management est conçu de manière à répondre aux exigences de la norme et des objectifs de l'organisme. Il est recommandé qu'au moins une partie de l'étape1 se déroule sur le site de l'audité.
4. **Étape2 de l'audit (audit sur site):** L'étape2 de l'audit a pour objectif de vérifier si le système de management déclaré est conforme à toutes les exigences de la norme, s'il est effectivement en œuvre dans l'organisme et s'il est en mesure de permettre à l'organisme d'atteindre ses objectifs. L'étape2 a lieu dans les locaux de l'entité auditee où le système de management est effectivement mis en œuvre.
5. **Suivi d'audit:** Si des non-conformités sont détectées, l'auditeur effectuera une visite de suivi pour valider uniquement les plans d'action associés à ces non-conformités (ce qui dure généralement jusqu'à une journée).
6. **Confirmation d'enregistrement:** Si l'organisme est conforme aux exigences de la norme, l'organisme de certification confirme l'enregistrement et publie le certificat.

**Note:** Notez que les termes «organisme» et «entité auditee» ont été utilisés de façon interchangeable dans cette diapositive.

# Avant l'audit

---

- Avant d'être audité, un SMSI doit être en application depuis un certain temps.
- Habituellement, le délai minimal demandé est de 3 mois.
- Au minimum, un audit interne doit avoir été effectué ainsi qu'une revue de direction.



# 1. Sélection de l'organisme de certification

## Principaux critères

**1**

Notoriété et crédibilité

**4**

Possibilité d'audit combiné

**2**

Présence géographique

**5**

Qualification et expérience de l'équipe d'audit

**3**

Références dans votre secteur

**6**

Prix

PECB

91

Voici les principaux critères de sélection d'un organisme de certification:

- Notoriété et crédibilité:** La valeur de la certification repose sur la notoriété et la crédibilité de l'organisme de certification qui l'émet. Il est donc nécessaire de choisir un organisme de certification crédible et respecté.
- Présence géographique:** Il est conseillé de s'assurer que l'organisme de certification opère dans votre région (lieu) ou que les membres de l'équipe d'audit parlent la langue locale (connaissent les coutumes locales).
- Références dans votre secteur:** Si votre industrie a des exigences réglementaires spécifiques, il est fortement souhaitable de choisir un organisme de certification qui possède déjà des clients dans votre secteur d'activités.
- Possibilité d'un audit combiné:** Si vous envisagez de certifier selon plusieurs normes (par exemple ISO9001 ou 14001), vous voudrez peut-être vous assurer que l'organisme de certification peut effectuer des audits combinés.
- Qualification et expérience de l'équipe d'audit:** Il est de bonne pratique de prendre contact avec l'auditeur principal de l'organisme de certification pour s'assurer de la compétence de l'équipe d'audit.
- Prix:** Les prix varient légèrement entre les organismes de certification. Il est conseillé de comparer plusieurs offres, étant donné que le nombre de jours proposé pour la certification peut varier et influence directement les coûts d'audit.

# Page de notes

---

PECB

92

Vous trouverez ci-dessous une liste des autorités d'accréditation de plusieurs pays (voir la liste complète sur le site Web de l'IAF: [www.iaf.nu](http://www.iaf.nu)):

**Argentine** : Organismo Argentino de Acreditación (OAA), [www.oaa.org.ar](http://www.oaa.org.ar)

**Australie et Nouvelle Zélande** : Joint Accreditation System of Australia and New Zealand (JAS-ANZ), [www.jas-anz.org](http://www.jas-anz.org)

**Autriche**: Federal Ministry for Digital and Economic Affairs (BMDW), [www.en.bmdw.gv.at](http://www.en.bmdw.gv.at)

**Belgique**: Belgian Accreditation Body (BELAC), [www.belac.fgov.be](http://www.belac.fgov.be)

**Brésil**: General Coordination for Accreditation (CGCRE), [www.inmetro.gov.br](http://www.inmetro.gov.br)

**Canada**: Conseil canadien des normes (SCC), [www.scc.ca/fr](http://www.scc.ca/fr)

**Chili**: Instituto Nacional de Normalización (INN), [www.inn.cl](http://www.inn.cl)

**Chine**: China National Accreditation Service for Conformity Assessment (CNAS), [www.cnas.org.cn/english](http://www.cnas.org.cn/english)

**Égypte** : Egyptian Accreditation Council (EGAC), [www.egac.gov.eg](http://www.egac.gov.eg)

**Finlande**: Finnish Accreditation Service (FINAS), [www.finias.fi](http://www.finias.fi)

**France**: Comité français d'accréditation (COFRAC), [www.cofrac.fr](http://www.cofrac.fr)

**Allemagne**: Deutsche Akkreditierungsstelle GmbH (DAkkS), [www.dakks.de](http://www.dakks.de)

**Hong Kong, Chine** : Hong Kong Accreditation Service (HKAS), [www.itc.gov.hk/hkas](http://www.itc.gov.hk/hkas)

**Inde**: National Accreditation Board for Certification Bodies (NABCB), [www.nabcb.qci.org.in](http://www.nabcb.qci.org.in)

**Iran** : National Accreditation Center of Iran (NACI), [www.naci.ir](http://www.naci.ir)

**Irlande**: Irish National Accreditation Board (INAB), [www.inab.ie](http://www.inab.ie)

**Japon:** International Accreditation Japan (IAJapan), [www.nite.go.jp/en/iajapan](http://www.nite.go.jp/en/iajapan)

**Corée:** Korea Accreditation Board (KAB), [www.kab.or.kr](http://www.kab.or.kr)

**Malaisie:** Standards Malaysia (DSM), [www.jsm.gov.my](http://www.jsm.gov.my)

**Mexique:** Entidad Mexicana de Acreditación (EMA), [www.ema.org.mx](http://www.ema.org.mx)

**Pays-Bas:** Dutch Accreditation Council (Raad voor Accreditatie) (RvA), [www.rva.nl](http://www.rva.nl)

**Norvège:** Norwegian Accreditation (NA), [www.akkreditert.no](http://www.akkreditert.no)

**Pakistan :** Pakistan National Accreditation Council (PNAC), [www.pnac.org.pk](http://www.pnac.org.pk)

**Philippines:** Philippine Accreditation Office (PAB), [www.dti.gov.ph/pab](http://www.dti.gov.ph/pab)

**Portugal:** Instituto Português de Acreditação (IPAC), [www.ipac.pt](http://www.ipac.pt)

**Espagne:** Entidad Nacional de Acreditación (ENAC), [www.enac.es](http://www.enac.es)

**Roumanie:** Romanian Accreditation Association (RENAR), [www.renar.ro/en](http://www.renar.ro/en)

**Russie:** Scientific Technical Centre on Industrial Safety (STC-IS), [www.oaontc.ru/en/](http://www.oaontc.ru/en/)

**Singapour:** Singapore Accreditation Council (SAC), [www.sac-accreditation.gov.sg](http://www.sac-accreditation.gov.sg)

**Slovénie:** Slovenska akreditacija (SA), [www.slo-akreditacija.si](http://www.slo-akreditacija.si)

**Afrique du Sud:** South African National Accreditation System (SANAS), [www.sanas.co.za](http://www.sanas.co.za)

**Suède:** Swedish Board for Accreditation and Conformity Assessment (SWEDAC), [www.swedac.se/?lang=en](http://www.swedac.se/?lang=en)

**Suisse:** Service d'accréditation Suisse (SAS), [www.sas.ch](http://www.sas.ch)

**Taiwan:** Taiwan Accreditation Foundation (TAF), [www.taftw.org.tw](http://www.taftw.org.tw)

**Thaïlande:** National Standardization Council of Thailand (NSC), [www.tisi.go.th](http://www.tisi.go.th)

**Tunisie:** Conseil National d'Accréditation (TUNAC), [www.tunac.tn](http://www.tunac.tn)

**Turquie:** Turkish Accreditation Agency (TURKAK:), [www.turkak.org.tr](http://www.turkak.org.tr)

**Émirats arabes unis:** Emirates International Accreditation Centre (EIAC), [www.eiac.gov.ae](http://www.eiac.gov.ae)

**Royaume-Uni:** United Kingdom Accreditation Service (UKAS), [www.ukas.com](http://www.ukas.com)

**États-Unis:** ANSI National Accreditation Board (ANAB), [www.anab.org](http://www.anab.org)

**États-Unis:** American National Standards Institute (ANSI), [www.ansi.org](http://www.ansi.org)

**États-Unis:** International Accreditation Services (IAS), [www.iasonline.org](http://www.iasonline.org)

**Uruguay:** Organismo Uruguayo de Acreditación (OUA), [www.organismouruguayodeacreditacion.org](http://www.organismouruguayodeacreditacion.org)

**Vietnam:** Bureau of Accreditation (BoA), [www.boa.gov.vn](http://www.boa.gov.vn)

# Modèle : Combien de temps devrait durer un audit ?

ISO/IEC 27006, tableau B.1 – Tableau des délais d'audit (extrait)

Nombre d'employés	Temps d'audit (jour/personne) ISO 9001	Temps d'audit (jour/personne) ISO/IEC 27001
1 à 10	1,5-2	5
11 à 15	2,5	6
16 à 25	3	7
26 à 45	4	8,5
46 à 65	5	10
66 à 85	6	11
86 à 125	7	12
126 à 175	8	13
176 à 275	9	14

PECB

93

L'équipe d'audit doit disposer de suffisamment de temps pourachever l'audit. Le temps disponible pour réaliser un audit peut varier en fonction de ce qui suit:

- Périmètre du système de management
- Complexité des processus du système de management
- Champ d'activité de l'audité
- Complexité et diversité des technologies utilisées
- Nombre de sites à auditer
- Audits précédents chez l'audité
- Accords relatifs à des services externalisés
- Règlements, lois et ententes contractuelles

# Modèle : Combien de temps devrait durer un audit ?

ISO/IEC 27006, tableau B.1 – Tableau des délais d'audit (extrait)

Nombre d'employés	Temps d'audit (jour/personne) ISO 9001	Temps d'audit (jour/personne) ISO/IEC 27001
276 à 425	10	15
426 à 625	11	16,5
626 à 875	12	17,5
876 à 1175	13	18,5
1176 à 1550	14	19,5
1551 à 2025	15	21
2026 à 2675	16	22
2676 à 3450	17	23
3451 à 4350	18	24

PECB

94

# Refus d'un auditeur

- L'audité peut demander le remplacement de membres de l'équipe d'audit pour des motifs valables.
- L'équipe d'audit peut se retirer si elle estime que les raisons invoquées ne sont pas valables.

## Exemple de motifs valables :

- Auditeur en situation de conflit d'intérêts (réel ou potentiel)
- Auditeur ayant précédemment fait preuve de comportement contraire à la déontologie
- Auditeur qui n'a pas l'habilitation de sécurité requise par l'audité



PECB

95

On peut toujours demander le remplacement de membres de l'équipe d'audit pour des motifs valables. En contrepartie, l'équipe d'audit peut se désister si elle juge que les motifs évoqués ne le sont pas.

Un motif évident serait qu'un auditeur ait précédemment fait preuve d'une conduite non professionnelle. D'autres exemples de motifs valables sont les situations de conflit d'intérêts réel (p. ex. un membre de l'équipe d'audit ayant été employé il y a peu de temps dans l'organisme qu'il doit auditer) ou perçu (p. ex. l'auditeur à travaillé chez l'un des principaux concurrents de l'entreprise qu'il doit auditer).

Dans certaines industries (militaire, énergie nucléaire, service de renseignement, etc.), un audité peut demander que chaque membre de l'équipe d'audit possède une habilitation de sécurité ou qu'il soit soumis à une vérification de ses antécédents avant d'être admis sur le site.

Il est recommandé de communiquer ces motifs au responsable de l'équipe d'audit et aux responsables du programme d'audit avant de prendre une décision concernant le remplacement d'un membre de l'équipe d'audit.

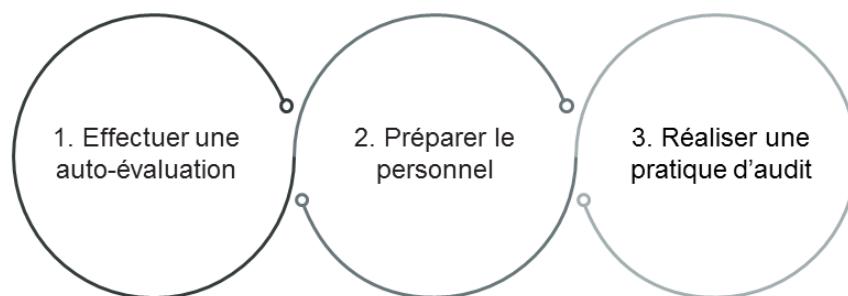
### **ISO/IEC 17021-1, article 9.2.3.5 Communication concernant les membres de l'équipe d'audit**

*L'organisme de certification doit fournir le nom et, lorsque cela est demandé, les informations nécessaires concernant chacun des membres de l'équipe d'audit au client dans un délai suffisant pour permettre à ce dernier de formuler une objection à la désignation d'un membre particulier de l'équipe d'audit et ainsi permettre à l'organisme de certification de reformer l'équipe en réponse à toute objection valide.*

## 2. Préparation à l'audit de certification

### Recommandations

#### Préparation à l'audit de certification



PECB

96

Avant que l'équipe d'audit externe vienne auditer l'organisme, il est recommandé de se préparer:

1. **Effectuer une auto-évaluation** – Examiner les exigences des articles 4 à 10 et répondre aux questions suivantes:
  - Le processus est-il bien défini?
  - Les responsabilités ont-elles été définies?
  - L'information documentée est-elle maintenue?
  - Le processus est-il efficace pour obtenir les résultats requis?
2. **Préparer le personnel** – Préparer les employés pour l'audit:
  - Organiser des sessions de formation
  - Réaliser des entretiens d'entraînement
  - Préparer des fiches d'information
  - Examiner l'information documentée
3. **Réaliser une pratique d'audit** – Embaucher un auditeur externe pour effectuer une pratique d'audit. Il devra:
  - Examiner l'information documentée
  - Préparer le personnel
  - Conseiller la direction concernant l'audit
  - Accompagner l'organisme lors de l'audit

### 3. Étape 1 de l'audit

1

#### Visite du site

- Évaluation des bureaux/locaux du client et des conditions spécifiques du site
- Réunion avec le personnel de l'audité
- Observation des technologies utilisées
- Observation générale des opérations du SMSI

2

#### Entretiens avec les acteurs clés

- Validation du périmètre ainsi que des contraintes légales, réglementaires et contractuelles applicables
- Validation de la réalisation d'audits internes et de la revue de direction
- Préparation de l'étape 2 de l'audit

3

#### Revue de l'information documentée

- Compréhension du fonctionnement du système de management
- Évaluation de la conception du système de management ainsi que des processus et mesures de sécurité reliés
- Revue de l'information documentée afin de valider que les audits internes et les revues de direction ont été effectués.

**Note :** La revue de l'information documentée est la principale activité de l'étape 1.

PECB

97

**Durant l'étape1 de l'audit, l'auditeur ne cherche pas à vérifier l'efficacité du système de management en place, mais plutôt à vérifier la conception du système de management.** Lors de l'étape2 (audit sur site), l'auditeur mesurera l'efficacité du système de management afin de valider si les processus documentés existent, sont efficaces et conformes aux processus déclarés.

L'étape1 de l'audit a lieu idéalement 2 à 4 semaines avant l'étape2 (audit sur site).

Elle est généralement réalisée peu de temps avant le début de l'étape2. Ceci est fait afin d'éviter des changements substantiels du système de management entre les deux étapes de l'audit. Il convient toutefois que les étapes1 et 2 soient suffisamment distancées pour permettre la préparation du plan d'audit sur site. Habituellement, 30% du temps total de l'audit est consacré à l'étape1.

Dans certaines circonstances, elle peut être combinée avec l'étape2 de l'audit (ou exécutée distance), de façon à ne pas compromettre l'efficacité de l'audit. C'est souvent le cas quand les membres de l'équipe doivent se déplacer sur de longues distances pour réaliser l'audit.

Il est à noter que, même si un accord de confidentialité est signé, **un audité est en droit d'exiger que la consultation des documents se déroule sur site et qu'aucun document ne soit transporté à l'extérieur.**

## 4. Étape 2 de l'audit

Étape 2 de l'audit (visite sur site) :

Évaluer si le système de management déclaré :

- Est conforme à toutes les exigences de la norme

- Est effectivement mis en œuvre au sein de l'organisme

- Permet à l'organisme d'atteindre ses objectifs de sécurité

PECB

98

### **ISO/IEC 17021-1, article 9.3.1.3 Étape 2**

*L'objet de l'étape 2 est d'évaluer la mise en œuvre et l'efficacité du système de management du client. L'étape 2 doit se dérouler sur le ou les sites du client. Elle doit comprendre au minimum l'audit des éléments suivants:*

- a. *les informations et les preuves relatives à la conformité à toutes les exigences de la norme relative au système de management ou d'autres documents normatifs applicables;*
- b. *la surveillance, le mesurage, le compte rendu et la revue des performances par rapport aux objectifs de performance clé et aux cibles (en cohérence avec les attentes de la norme de système de management ou de tout autre document normatif applicable);*
- c. *l'aptitude du système de management du client et ses performances concernant la satisfaction des exigences légales, réglementaires et contractuelles applicables;*
- d. *la maîtrise opérationnelle des processus du client;*
- e. *les audits internes et la revue de direction;*
- f. *les responsabilités de la direction vis-à-vis des politiques de l'organisme client.*

# Recommandation de certification

En conclusion de l'audit, l'auditeur doit émettre l'une des quatre recommandations suivantes relatives à la certification :

1. Recommandation pour la certification
2. Recommandation sous condition – appliquer les plans d'actions correctives sans visite préalable
3. Recommandation sous condition – appliquer les plans d'actions correctives avec une visite préalable
4. Recommandation défavorable



**1. Recommandation pour la certification:** L'auditeur a une assurance raisonnable que l'audité est conforme aux exigences de la norme. Aucune non-conformité n'a été observée durant l'audit.

**2. et 3. Recommandation pour la certification sous condition du dépôt d'un plan d'action de mesures correctives:** L'auditeur a une assurance raisonnable que l'audité est conforme aux exigences de la norme, mais un certain nombre de non-conformités mineures ont été constatées. On demande à l'audité de déposer un plan d'actions correctives pour chaque non-conformité mineure dans un court délai. Si le plan d'action est accepté, l'audité pourra être certifié. Dans certains cas, l'auditeur peut exiger une nouvelle visite du site avant d'émettre la recommandation de certification. Dans la situation où il n'y a pas de visite préalable exigée, une vérification des mesures correctives incluses dans le plan d'action sera validée lors des audits de surveillance.

**4. Recommandation défavorable:** L'auditeur recommande de ne pas émettre de certificat de conformité à l'audité. Un nouvel audit complet ou partiel est recommandé. Si une ou plusieurs non-conformités majeures sont signalées, l'auditeur devrait émettre une recommandation défavorable. Notez qu'il n'y a pas de déclaration publique des organismes qui ont reçu une recommandation défavorable. Seuls les organismes certifiés font l'objet d'une déclaration publique (sauf exception).

**Il est à noter que les auditeurs n'émettent qu'une recommandation de certification. La décision finale de certification est prise par le comité de certification de l'organisme de certification.**

## 5. Suivi d'audit

- Selon les conclusions de l'audit, l'auditeur peut réaliser un suivi d'audit avant que l'organisme ne soit recommandé à la certification.
- Au cours du suivi, l'efficacité de toutes les corrections et actions correctives prises est évaluée.

Une non-conformité majeure implique habituellement un suivi d'audit.

PECB

100

Partie intégrante du processus d'audit, les activités de suivi doivent être planifiées au même titre que les autres étapes nécessaires à l'exécution d'un audit.

L'objectif du suivi d'audit est de valider les plans d'action soumis par l'audité et les mesures correctives mises en œuvre. Si des non-conformités majeures sont relevées, l'organisme doit les résoudre avant d'être recommandé pour la certification.

Un suivi d'audit est habituellement réalisé 4 à 12 semaines après l'audit initial, car on doit laisser le temps à l'organisme de répondre au rapport d'audit et de mettre en œuvre les actions correctives. Souvent, le suivi d'audit ne dure qu'une journée.

### ***ISO19011, article 6.7 Réalisation du suivi d'audit***

*Les conclusions de l'audit peuvent mentionner, selon les objectifs de l'audit, la nécessité de corrections ou d'actions correctives, ou des opportunités d'amélioration. Ces actions sont généralement décidées et réalisées par l'audité dans des délais convenus. Le cas échéant, il convient que l'audité informe la ou les personnes responsables du management du programme d'audit et/ou l'équipe d'audit de l'état d'avancement de ces actions.*

*Il convient de vérifier l'achèvement et l'efficacité des actions entreprises. Cette vérification peut faire partie intégrante d'un audit ultérieur. Il convient de communiquer les résultats à la personne responsable du management du programme d'audit ainsi qu'au client de l'audit pour la revue de direction.*

## 6. Décision de certification

Une évaluation des résultats et des conclusions de l'audit

L'organisme de certification doit prendre la décision de certification en se fondant sur :

Toute autre information pertinente (par exemple information publique, commentaires du client sur le rapport d'audit)

Les auditeurs ayant réalisé l'audit ne participent jamais à la décision de certification

PECB

101

### **ISO/IEC 17021-1, article 9.5.1.1**

*L'organisme de certification doit assurer que les personnes ou les comités qui prennent les décisions d'octroi ou de refus de la certification, d'extension ou de réduction du périmètre de la certification, de suspension ou de rétablissement de la certification, de retrait ou de renouvellement de la certification, sont différents de celles ou ceux ayant réalisé les audits. La ou les personnes chargées de décider de la certification doivent avoir les compétences appropriées.*

### **ISO/IEC 17021-1, article 9.5.3.1**

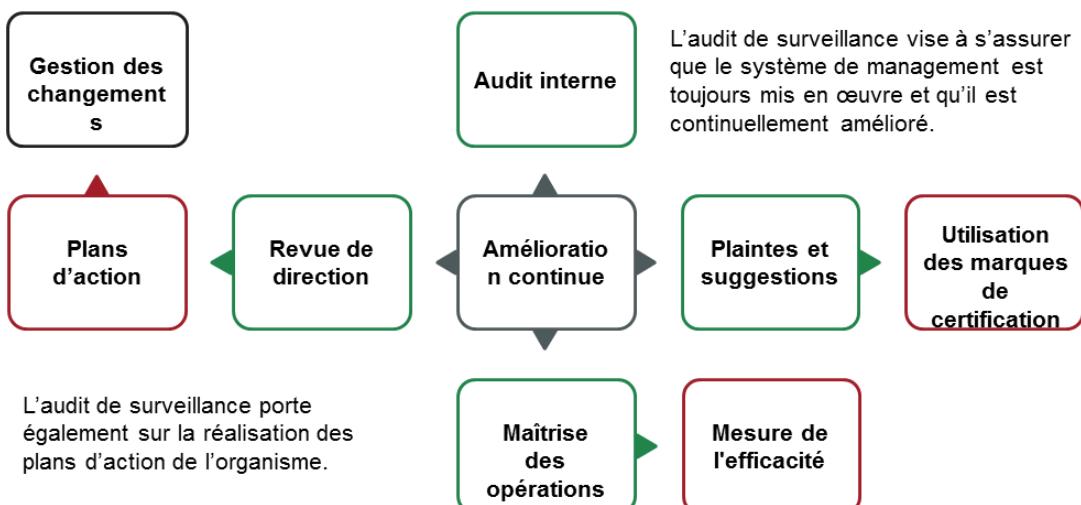
*Les informations fournies par l'équipe d'audit à l'organisme de certification pour lui permettre de prendre une décision doivent, au minimum, comprendre les éléments suivants:*

- a. *le rapport d'audit;*
- b. *les observations relatives aux non-conformités et, le cas échéant, les corrections et actions correctives entreprises par l'organisme client;*
- c. *la confirmation des informations fournies à l'organisme de certification et utilisées pour la revue de la demande;*
- d. *la confirmation que les objectifs de l'audit ont été atteints;*
- e. *une recommandation relative à la décision de délivrer ou non la certification, accompagnée de toutes réserves ou observations.*

### **ISO/IEC 17021-1, article 9.5.3.2**

*Si l'organisme de certification n'est pas en mesure de vérifier la mise en œuvre des corrections et actions correctives pour toute non-conformité majeure dans un délai de 6 mois à compte du dernier jour de l'étape 2, l'organisme de certification doit recommencer l'étape 2 avant de recommander la certification.*

# Éléments à auditer lors d'un audit de surveillance



PECB

102

## ISO/IEC 17021-1, article 9.6.2.2 Audit de surveillance

Les audits de surveillance sont des audits sur site qui ne sont pas nécessairement des audits du système complet et qui doivent donc être planifiés en même temps que les autres activités de surveillance de manière que l'organisme de certification puisse garder confiance dans le système de management certifié du client et dans sa capacité à rester conforme aux exigences de la certification dans l'intervalle entre deux audits de renouvellement de la certification.

Chaque surveillance selon la norme de système de management applicable doit porter sur les éléments suivants:

- a. les audits internes et la revue de direction;
- b. la revue des actions entreprises vis-à-vis des non-conformités identifiées au cours de l'audit précédent;
- c. le traitement des plaintes;
- d. l'efficacité du système de management par rapport à la réalisation des objectifs du client certifié et des résultats escomptés du(des) système(s) de management pertinent(s);
- e. l'état d'avancement des activités planifiées visant à l'amélioration continue;
- f. la maîtrise opérationnelle continue;
- g. la revue de toute modification apportée;
- h. l'utilisation des marques et/ou toute autre référence à la certification.

# Renouvellement de la certification

## ISO/IEC 17021-1, article 9.6.3.1.1

- *Le but de l'audit de renouvellement est de confirmer le maintien de la conformité et de l'efficacité du système de management dans son ensemble ainsi que sa pertinence et son applicabilité en permanence au regard du périmètre de la certification.*
- *Un audit de renouvellement de la certification doit être planifié et effectué en vue d'évaluer le maintien de la conformité à toutes les exigences de la norme relative au système de management ou de tout autre document normatif applicable.*
- *Ceci doit être planifié et effectué en temps opportun pour organiser le renouvellement avant la date d'expiration du certificat.*

PECB

103

## ISO/IEC 17021-1, article 9.6.3.1.2

*L'activité de renouvellement de la certification doit comprendre la revue des rapports d'audit de surveillance précédents et doit tenir compte des performances du système de management pendant le cycle de certification le plus récent.*

## ISO/IEC 17021-1, article 9.6.3.1.3

*Lorsque des modifications significatives sont apportées au système de management, à l'organisme client ou au contexte dans lequel le système de management opère (par exemple modifications de la législation), l'activité correspondant à un audit de renouvellement de la certification peut nécessiter une étape 1.*

*NOTE: Ces modifications peuvent intervenir à tout moment au cours du cycle de certification et il peut être nécessaire que l'organisme de certification réalise un audit spécial (voir 9.6.4) qui peut être ou non un audit en deux étapes.*

## ISO/IEC 17021-1, article 9.6.3.2.1

*L'audit de renouvellement de la certification doit comporter un audit sur site, qui traite des points suivants:*

- a. *l'efficacité du système de management dans sa totalité, à la lumière des changements internes et externes ainsi que sa pertinence et son applicabilité en permanence au regard du périmètre de la certification;*
- b. *la preuve de l'engagement à maintenir l'efficacité et l'amélioration du système de management afin d'augmenter les performances globales;*
- c. *l'efficacité du système de management par rapport à la réalisation des objectifs du client certifié et des résultats escomptés du(des) système(s) de management pertinent(s).*

# Utilisation des marques déposées de l'ISO

- Un organisme certifié est autorisé à afficher publiquement sa certification et à s'en servir à des fins publicitaires.
- La certification ne peut pas être affichée directement sur un produit ou d'une façon qui laisserait à penser que le produit est certifié.
- L'organisme de certification fournit à l'audité un logo pouvant être utilisé à des fins de marketing.



PECB

104

## ISO/IEC 17021-1, article 8.3.1

*Un organisme de certification doit disposer de règles régissant toute marque de certification de système relative aux systèmes de management qu'il autorise des clients certifiés à utiliser. Ces règles doivent, entre autres, garantir la traçabilité vers l'organisme de certification. Il ne doit y avoir aucune ambiguïté dans la marque ou le texte d'accompagnement en ce qui concerne l'objet de la certification et l'organisme qui a accordé la certification. Cette marque ne doit pas être utilisée sur un produit ni un emballage de produit ni de toute autre manière pouvant être interprétée comme une indication de la conformité dudit produit.*

*NOTE: L'ISO/IEC 17030 fournit les informations supplémentaires relatives à l'utilisation des marques de tierces parties..*

## ISO/IEC 17021-1, article 8.3.1

*Un organisme de certification ne doit pas autoriser l'apposition de ses marques par les clients certifiés sur les rapports de laboratoire d'essai, sur les rapports d'étalonnage ou d'inspection ou sur les certificats.*

# Questions ?

PECB

105

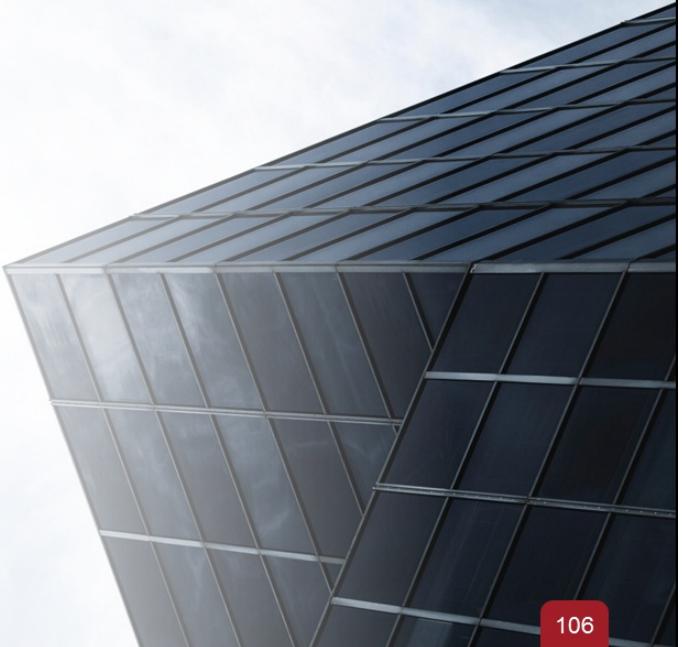
## Section 27

### Processus de certification et clôture de la formation

- Compétences du Lead Implementer
- Schéma de certification PECB ISO/IEC 27001
- Processus de certification PECB
- Autres formations et certifications PECB

PECB

106



Cette section fournira des informations qui aideront le participant à acquérir des connaissances sur les compétences et l'évaluation du *Lead Implementer*, ainsi que sur les procédures de certification de PECB.

# Compétences du Lead Implementer

Le Lead Implementer doit faire preuve de compétences pour :

- Planifier un projet de mise en œuvre d'un SM (y compris l'utilisation efficace des ressources)
- Présenter l'équipe de projet aux clients
- Gérer et conseiller les membres de l'équipe de projet
- Prévenir et résoudre des conflits
- Préparer, défendre et expliquer l'avancement du projet MS aux parties intéressées



107

# Qualification du Lead Implementer par secteur d'industrie

## Exigences

- Un Lead Implementer est qualifié par secteur d'industrie.
- Les codes du système de qualification utilisés sont :
  - ▷ EAC (utilisé par UKAS au Royaume-Uni)
  - ▷ NACE (utilisé par la Communauté européenne)
  - ▷ NAICS (utilisé aux États-Unis)
- Le Lead Implementer doit pouvoir démontrer sa connaissance du secteur d'industrie pour lequel il est qualifié :
  - ▷ Lois et règlements spécifiques
  - ▷ Enjeux et risques liés à l'industrie
  - ▷ Processus organisationnels
  - ▷ Terminologie
  - ▷ Technologies fréquemment utilisées

**Note :** Au cours du processus de demande de certification PECB, le candidat doit déclarer les secteurs d'industrie dans lesquels il a acquis une expérience professionnelle.

PECB

108

Le journal de projet d'un Lead Implementer devrait contenir la liste de tous les mandats effectués en incluant:

1. Expérience (nombre de jours) pour la mise en œuvre des projets (sur place et hors site)
2. Nombre de personnes ayant participé au projet de mise en œuvre
3. Rôles et responsabilités du Lead Implementer dans les projets de mise en œuvre
4. Normes qu'il a mises en œuvre
5. Nom et coordonnées du client
6. Nom de l'organisme, coordonnées et secteur d'activité où le projet a été mis en œuvre.
7. Nom et coordonnées du chef de l'équipe de projet

# Qualifications et connaissance du SMSI

---

1. Comprendre l'application d'un SMSI dans le contexte d'ISO/IEC 27001
2. Comprendre le processus de la sécurité de l'information et la relation entre les différentes composantes du SMSI



PECB

109

# Programme de certification PECB ISO/IEC 27001

## Résumé des exigences

Examen	Certification professionnelle	Expérience professionnelle	Expérience d'audit SMSI	Expérience de projet SMSI
ISO/IEC 27001 Foundation	ISO/IEC 27001 Foundation	-----	-----	-----
ISO/IEC 27001 Lead Auditor	ISO/IEC 27001 Provisional Auditor	-----	-----	-----
	ISO/IEC 27001 Auditor	2 ans (1 en sécurité de l'information)	200 heures	-----
	ISO/IEC 27001 Lead Auditor	5 ans (2 en sécurité de l'information)	300 heures	-----
	ISO/IEC 27001 Senior Lead Auditor	10 ans (7 en sécurité de l'information)	1000 heures	-----
ISO/IEC 27001 Lead Implementer	ISO/IEC 27001 Provisional Implementer	-----	-----	-----
	ISO/IEC 27001 Implementer	2 ans (1 en sécurité de l'information)	-----	200 heures
	ISO/IEC 27001 Lead Implementer	5 ans (2 en sécurité de l'information)	-----	300 heures
	ISO/IEC 27001 Senior Lead Implementer	10 ans (7 en sécurité de l'information)	-----	1000 heures
ISO/IEC 27001 LI+LA (4 examens Foundation supplémentaires)	ISO/IEC 27001 Master	15 ans (10 en sécurité de l'information)	700 heures	700 heures

PECB

110

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

Les principales certifications d'auditeur:

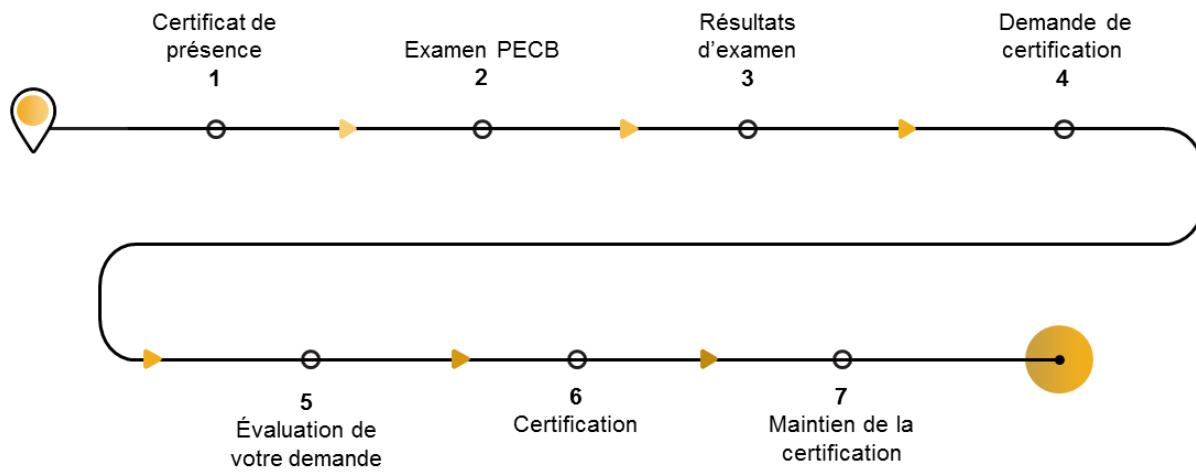
1. La certification « **Certified Provisional Auditor** » reconnaît que la personne possède les connaissances de base en audit et peut intégrer une équipe d'audit en tant que membre.
2. La certification « **Certified Auditor** » reconnaît que la personne possède les connaissances nécessaires pour participer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

Les principales certifications d'Implementer:

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

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

# Processus de certification PECB



PECB

111

**Cette certification atteste à la fois la réussite de l'examen et la validation du dossier d'expérience professionnelle.** Malheureusement, après avoir réussi l'examen, de nombreuses personnes se déclarent ISO/IEC 27001 Lead Implementer sans avoir le niveau d'expérience requis.

**Note importante:** Les frais d'examen et de certification sont inclus avec la formation: Le candidat n'aura donc pas à payer de frais supplémentaires lorsqu'il présente une demande de certification et qu'il reçoit l'une des certifications professionnelles: PECB Certified ISO/IEC 27001 Provisional Implementer, PECB Certified ISO/IEC 27001 Implementer, PECB Certified ISO/IEC 27001 Lead Implementer ou PECB Certified ISO/IEC 27001 Senior Lead Implementer.

# 1. Certificat de présence

Unités de formation professionnelle continue (FPC)



PECB

112

Après avoir assisté à la formation et soumis le **Formulaire d'évaluation** de la formation, un certificat de présence sera généré dans votre tableau de bord **monPECB**, sous l'onglet **Mes formations**. Le certificat de participations est valable pour 31unités de FPC.

## 2. Examen PECB

### Préparation à l'examen

- L'examen de certification a pour objectif de s'assurer que les candidats comprennent et maîtrisent la mise en œuvre et la gestion d'un système de management de la sécurité de l'information basé sur ISO/IEC 27001.
- L'examen est disponible en plusieurs langues.
- Pour plus d'informations sur le processus d'examen, veuillez visiter [Politiques et règlement relatifs l'examen](#).



PECB

113

L'objectif de l'examen de certification est de s'assurer que les candidats maîtrisent tous les concepts et techniques nécessaires liés au SMSI afin qu'ils puissent participer à des projets de mise en œuvre.

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

L'examen est disponible en plusieurs langues. Pour passer l'examen dans une langue particulière, veuillez demander au formateur, ou nous contacter en envoyant un e-mail à [examination@pecb.com](mailto:examination@pecb.com).

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

### 3. Résultats d'examen

Il y a deux résultats possibles :



- Vous recevezz par e-mail un numéro d'examen pour faire une demande de certification.
- Ce numéro d'examen est important pour faire votre demande de certification PECB.
- Vous pouvez reprendre l'examen gratuitement dans les douze mois suivant l'examen initial.
- Veuillez contacter le prestataire de la formation pour déterminer la date de reprise de l'examen.

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

PECB

114

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

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

Si le candidat échoue à l'examen, une explication lui sera fournie sur les domaines dans lesquels il n'a pas démontré les compétences requises. Le candidat dispose de douze (12) mois pour reprendre l'examen. Pour ce faire, le candidat doit communiquer avec le responsable de l'organisme de formation. Le candidat peut reprendre l'examen gratuitement. Toutefois, des frais administratifs d'examen pourraient s'appliquer.

## 4. Demande de certification

### Processus général

- Après avoir réussi l'examen, vous pouvez faire la demande en ligne pour obtenir votre certification PECB au [www.pecb.com](http://www.pecb.com).
- Dans votre demande, vous devrez fournir les informations suivantes :



Vos coordonnées



Votre expérience professionnelle et de projet



Au moins deux références

PECB

115

Après avoir réussi l'examen, le candidat dispose d'un délai maximum de trois ans pour soumettre un dossier professionnel afin d'obtenir une des certifications liées au programme de certification ISO/IEC27001. Un candidat peut postuler pour plus d'une certification liée au programme de certification ISO/IEC27001 (p. ex. Lead Implementer, Lead Auditor, Master) en même temps s'il répond à toutes les exigences.

Lors de votre demande, vous devrez fournir les informations suivantes:

#### 1. Vos coordonnées

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

#### 2. Votre expérience professionnelle et de projet

- Vous devez fournir un CV pour présenter votre expérience. L'expérience professionnelle peut être toute activité démontrant que vous possédez des compétences et des connaissances générales sur le fonctionnement d'un organisme.
- Pour l'expérience de projet, veuillez vous assurer d'indiquer le nombre d'heures effectuées.
- Aucune équivalence n'est accordée pour l'expérience professionnelle. Les diplômes d'études ne remplacent pas l'expérience de travail réelle.

#### 3. Au moins deux références

- Les références doivent être fournies par des personnes qui peuvent confirmer votre expérience (collègues, partenaires, superviseurs, etc.). Il est important que ces personnes vous connaissent suffisamment pour attester vos qualifications.
- Votre demande sera évaluée une fois que les références auront été soumises.

# Demande de certification

## Dossier d'expérience professionnelle

### Expérience de mise en œuvre valide

- Mise en œuvre interne
- Mise en œuvre externe ou consultation
- Mise en œuvre partielle

### Activités de mise en œuvre du SMSI

- Rédaction d'une étude de faisabilité de la mise en œuvre du SMSI
- Gestion d'un projet de mise en œuvre du SMSI
- Mise en œuvre du SMSI
- Gestion de l'information documentée
- Mise en œuvre des métriques
- Mise en œuvre des actions correctives et préventives
- Organisation d'une revue de direction
- Gestion de la performance du SMSI
- Gestion d'une équipe SMSI

PECB

116

Par exemple, un consultant qui a effectué une appréciation des risques chez un client afin de l'accompagner à la mise en œuvre de son cadre de conformité sera considéré comme ayant une expérience pertinente.

## 5. Évaluation de votre candidature

Une fois votre candidature soumise, PECB en fera l'évaluation.

Vos références seront contactées afin de valider :

- Votre expérience de travail
- Votre attitude personnelle et professionnelle

Votre candidature ne sera pas évaluée tant qu'au moins deux références n'auront pas répondu.



Vous pouvez vérifier si vos références ont répondu dans votre tableau de bord **monPECB** sous l'onglet **Mes certifications**.

PECB

117

Vos références seront contactées pour remplir un court questionnaire visant à attester votre expérience et évaluer vos qualités personnelles (selon 13aptitudes de comportement professionnel définies par ISO19011).

Vous pouvez vérifier si vos références ont répondu sur votre compte de membre de PECB sous l'onglet **Mes certifications**. Si leurs réponses tardent, vous devriez les relancer pour vous assurer qu'ils aient reçu la demande de référence.

Dans le cas où PECB serait incapable de communiquer avec une de vos références ou qu'ils n'aient pas répondu au questionnaire, il vous sera demandé de fournir d'autres références.

## 6. Certification

- Une fois votre demande approuvée, PECB délivrera un certificat professionnel en format PDF qui peut être téléchargé à partir de votre compte PECB.
- Ce certificat comporte un numéro de certification qu'il est possible de valider sur le site de PECB [www.pecb.com](http://www.pecb.com) sous l'onglet Valider un certificat.
- Seules les personnes dûment certifiées peuvent utiliser le titre « PECB Certified ISO/IEC 27001 Lead Implementer ».
- Il est également possible d'utiliser les titres suivants :
  - ▷ PECB Certified ISO/IEC 27001 LI
  - ▷ PECB ISO/IEC 27001 Lead Implementer
  - ▷ PECB ISO/IEC 27001 LI



PECB

118

Lorsque le candidat est certifié, il reçoit un avis du système et peut télécharger le certificat à partir de son compte PECB. Le certificat est valable pour trois ans. Au-delà de cette période, la certification sera renouvelée si le demandeur remplit les conditions pour maintenir sa certification.

## 7. Maintien de la certification

### Maintien et amélioration continue des compétences

Qualification	Exigences annuelles		Total sur 3 ans
	Expérience/Éducation		Expérience/Éducation
<i>Foundation et Provisional</i>	0	Aucune	Aucune
<i>Implementer</i>	20	Heures d'expérience de travail de mise en œuvre, consultation, formation, études privées, coaching, participation à des séminaires et conférences ou à d'autres activités pertinentes	60 heures
<i>Auditor, Assessor</i>	20	Heures d'expérience de travail d'audit ou évaluation, de formation, études privées, coaching, participation à des séminaires et conférences ou à d'autres activités pertinentes	60 heures
<i>Lead Implementer</i>	30	Heures d'expérience de travail de mise en œuvre, consultation, formation, études privées, coaching, participation à des séminaires et conférences ou à d'autres activités pertinentes	90 heures

PECB

119

Afin de conserver un certificat, le candidat devrait démontrer suffisamment d'heures d'activités de formation professionnelle continue liées au programme de certification. En fonction de la certification, ces activités devraient couvrir l'audit, la mise en œuvre ou les activités de projets, l'autoformation, les formations, études, séminaires, conférences, publications, etc. Pour plus d'informations, veuillez consulter le tableau ci-dessus.

#### Activités de formation professionnelle et maintien de la certification

- PECB exige un minimum de 90heures d'activités par période de 3ans pour le maintien d'une certification «Lead Auditor» ou «Lead Implementer» (60 heures pour «Auditor» ou «Implementer», 180heures pour «Senior Lead Auditor» ou «Senior Lead Implementer», 270heures pour la certification de «Master»).
- La soumission des activités de formation professionnelle continue devrait être réalisée annuellement, en particulier 30heures par année pour le maintien d'une certification « Lead Auditor » ou « Lead Implementer », 20heures pour le maintien d'une certification « Auditor » ou « Implementer », 60heures pour le maintien de la certification «Senior Lead Auditor» ou «Senior Lead Implementer» et 90heures pour le maintien de la certification « Master ».

#### Frais annuels de maintenance (FAM)

- Un membre sera facturé pour les FAM selon la date d'échéance du certificat.
- Le coût annuel des FAM est de:
  - 200\$ par certification pour le titre Master
  - 100\$ par certification pour tous les autres titres de compétence

**Note importante:** Aucune activité n'est nécessaire pour maintenir les certifications suivantes: «Foundation», «Provisional Implementer» et «Provisional Auditor».

# Maintien de la certification

## Maintien et amélioration continue des compétences

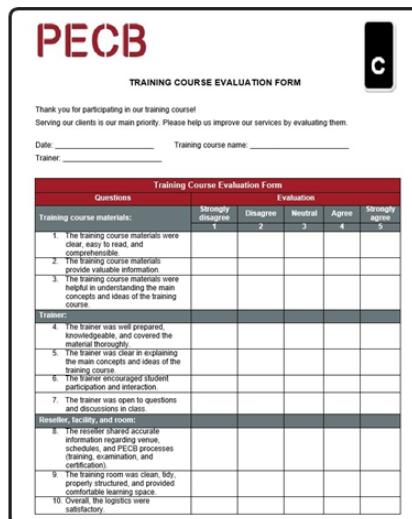
Qualification	Exigences annuelles		Total sur 3 ans
	Expérience/Éducation		Expérience/Éducation
<b>Lead Auditor, Lead Assessor</b>	30	Heures d'expérience de travail d'audit ou évaluation, de formation, études privées, coaching, participation à des séminaires et conférences ou à d'autres activités pertinentes	90 heures
<b>Senior Lead Implementer</b>	60	Heures d'expérience de travail de mise en œuvre, consultation, formation, études privées, coaching, participation à des séminaires et conférences ou à d'autres activités pertinentes	180 heures
<b>Senior Lead Auditor</b>	60	Heures d'expérience de travail d'audit ou évaluation, de formation, études privées, coaching, participation à des séminaires et conférences ou à d'autres activités pertinentes	180 heures
<b>Master</b>	90	Heures de mise en œuvre, gestion ou audit, de formation, études privées, coaching, participation à des séminaires et conférences ou à d'autres activités pertinentes	270 heures

PECB

120

# Évaluation de la formation

## Formulaire d'évaluation de la formation



The image shows a 'TRAINING COURSE EVALUATION FORM' from PECB. The form is titled 'PECB' at the top left. It includes fields for 'Date', 'Training course name', and 'Trainer'. Below these, there is a table titled 'Training Course Evaluation Form' with two columns: 'Questions' and 'Evaluation'. The 'Evaluation' column has five rows labeled 'Strongly disagree', 'Disagree', 'Neutral', 'Agree', and 'Strongly agree'. There are two sections of questions: 'Training course materials' and 'Trainer'. Both sections have 10 numbered statements for evaluation.

Questions	Evaluation	
Training course materials:	Strongly disagree 1 2 3 4 5 Disagree Neutral Agree Strongly agree	
1. The training course materials were clear, easy to read, and contained valuable information. 2. The training course materials provide valuable information. 3. The training course materials were helpful in understanding the main concepts and ideas of the training course.		
Trainer:	4. The trainer was well prepared, knowledgeable, and covered the material thoroughly. 5. The trainer did a good job explaining the main concepts and ideas of the training course. 6. The trainer encouraged student participation and interaction. 7. The trainer was open to questions and discussions in class.	
Respective room and place:	8. The room was clean, tidy, properly structured, and provided comfortable learning space. 9. Overall, the logistics were satisfactory.	

PECB

121

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

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

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

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

Après avoir participé à cette formation, les participants recevront par e-mail un Certificat de présence valide pour 31 crédits de FPC (Formation professionnelle continue).

# Autres formations et certifications PECB

## Développement de carrière de consultant



PECB

122

- Principes et concepts fondamentaux d'un système de management de la sécurité de l'information (SMSI)
  - Concepts et principes fondamentaux de l'audit
  - Préparer un audit ISO/IEC 27001
  - Réaliser un audit ISO/IEC 27001
  - Clore un audit ISO/IEC 27001
  - Gérer un programme d'audit ISO/IEC 27001
- 
- Classification des actifs
  - Identification et analyse des risques
  - Approches quantitative et qualitative
  - Traitement des risques
  - Gestion du risque résiduel
  - Gouvernance et gestion des risques
  - Connaissance des méthodes compatibles (CRAMM, OCTAVE, etc.)

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

La formation ISO/IEC 27001Lead Auditor permet aux participants de développer l'expertise nécessaire à la réalisation d'un audit de système de management de la sécurité de l'information (SMSI) en appliquant des principes, procédures et techniques largement reconnus en audit. Au cours de cette formation, le participant acquerra les connaissances et les compétences nécessaires pour planifier et réaliser des audits internes et externes conformément au processus de certification selon ISO19011 et ISO/IEC17021-1. Sur la base d'exercices pratiques, les participants seront en mesure de maîtriser les techniques d'audit et de devenir compétents pour gérer un programme d'audit et une équipe d'audit.

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

La formation ISO/IEC 27005Certified Risk Manager permet de maîtriser les éléments fondamentaux relatifs à la gestion des risques liés à la sécurité de l'information: planification d'un programme de gestion des risques, analyse, appréciation, traitement des risques, communication et surveillance des risques. Par des lectures, des exercices basés sur des cas réels, des discussions et des démonstrations avec des outils de modélisation des risques, le participant sera en mesure de réaliser une évaluation optimale des risques et de gérer les risques dans le temps par la connaissance de leur cycle de vie. Il est à noter que cette formation s'inscrit parfaitement dans le cadre d'un processus de mise en œuvre de la norme ISO/IEC 27001.

# Questions ?

PECB

123

## Suivez-nous sur les médias sociaux

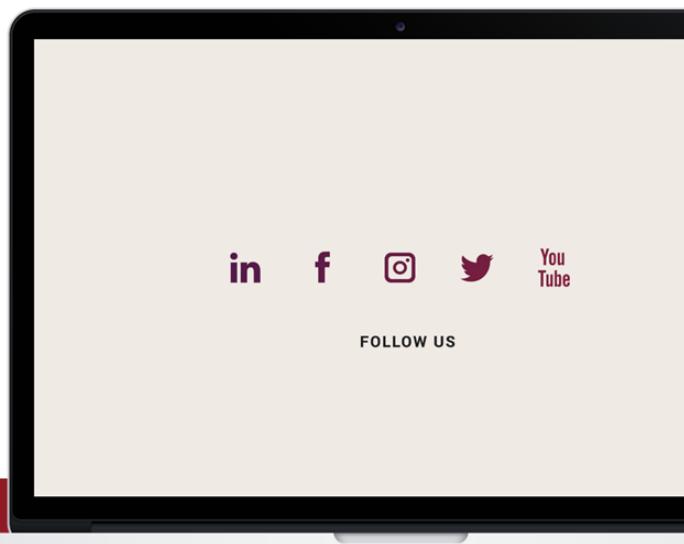
[www.pecb.com/facebook](http://www.pecb.com/facebook)

[www.pecb.com/linkedin](http://www.pecb.com/linkedin)

[www.pecb.com/twitter](http://www.pecb.com/twitter)

[www.pecb.com/youtube](http://www.pecb.com/youtube)

[www.instagram.com/pecb.official](http://www.instagram.com/pecb.official)



PECB

# Page de notes

---

PECB

125

# Page de notes

---

PECB

126



PECB

MERCI