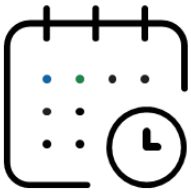
Version6.0

Numéro de document: ISMSFDD1V6.0

Programme de la formation

Jour 1 — Introduction au système de management de la sécurité de l'information (SMSI) et à la norme ISO/IEC 27001

Jour 2 — Système de management de la sécurité de l'information (SMSI) et examen de certification



PECB

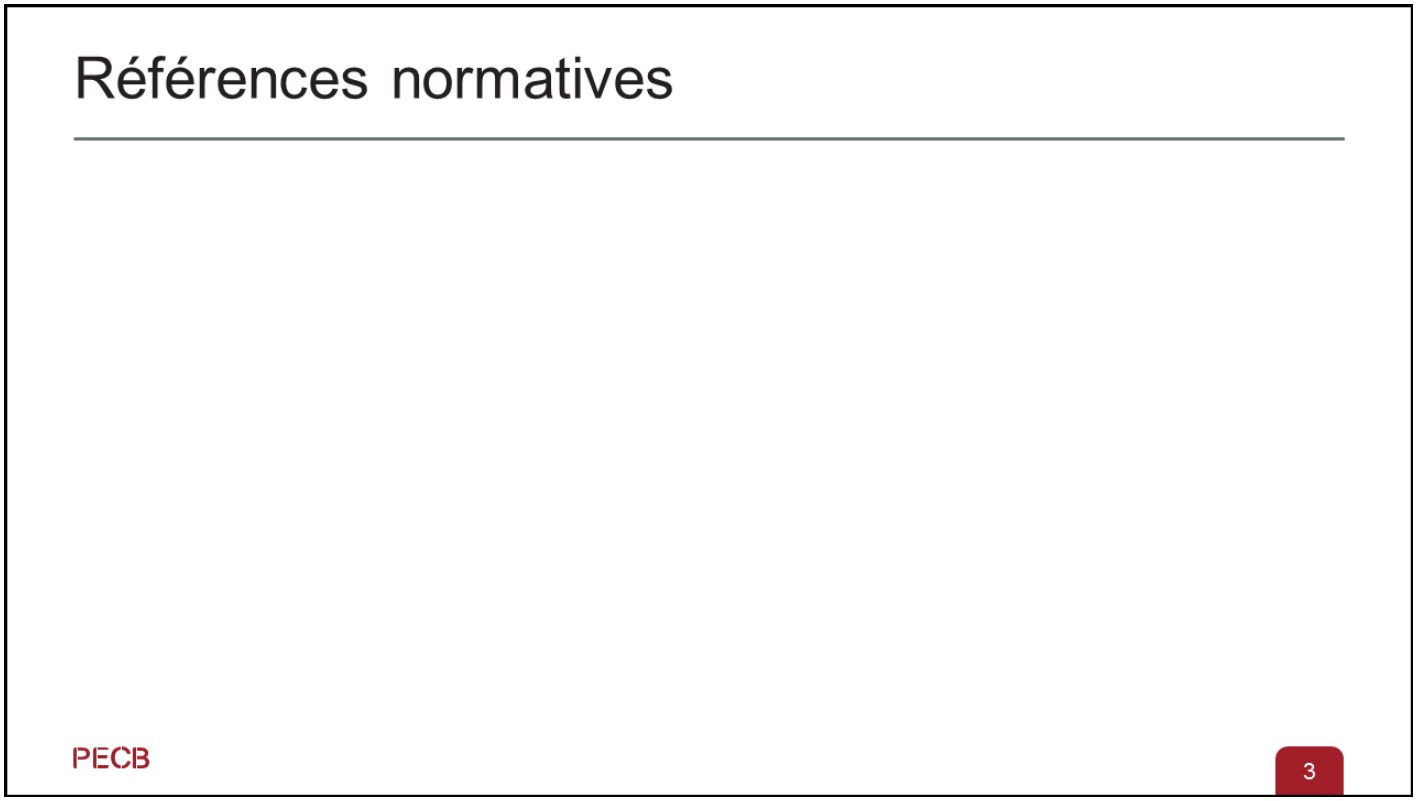
2

Jour 1: Introduction au système de management de la sécurité de l'information (SMSI) et à la norme ISO/IEC 27001

- Section1: Objectifs et structure de la formation
- Section2: Normes et cadres réglementaires
- Section3: Système de management de la sécurité de l'information (SMSI)
- Section4: Concepts et principes fondamentaux de la sécurité de l'information
- Section5: Compréhension de l'organisme et de son contexte
- Section6: Leadership

Jour 2: Système de management de la sécurité de l'information (SMSI) et examen de certification

- Section7: Planification
- Section8: Support
- Section9: Fonctionnement
- Section10: Évaluation des performances
- Section11: Amélioration
- Section12: Mesures et objectifs des mesures
- Section13: Processus de certification et clôture de la formation



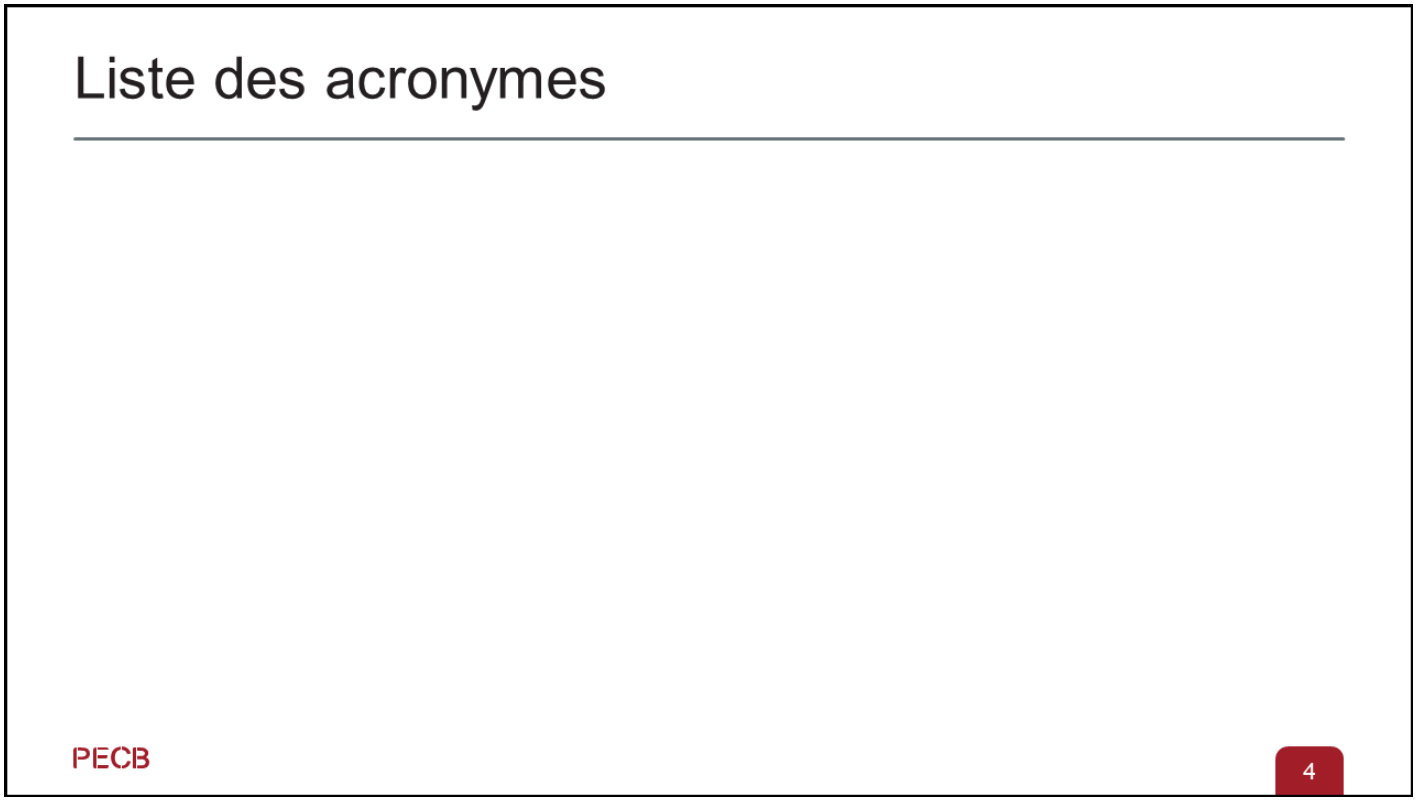
Références normatives

1.Principales normes:

- ISO/IEC 27000:2018, Technologies de l'information –Techniques de sécurité – Systèmes de management de la sécurité de l'information – Vue d'ensemble et vocabulaire
- ISO/IEC 27001:2013, Technologies de l'information – Techniques de sécurité – Systèmes de management de la sécurité de l'information – Exigences
- ISO/IEC 27002:2013, Technologies de l'information – Techniques de sécurité – Code de bonne pratique pour le management de la sécurité de l'information
- ISO/IEC 27003:2017, Technologies de l'information – Techniques de sécurité – Systèmes de management de la sécurité de l'information – Lignes directrices
- ISO/IEC 27005:2018, Technologies de l'information – Techniques de sécurité – Gestion des risques liés à la sécurité de l'information
- ISO 31000:2018, Management du risque – Lignes directrices
- ISO 19011:2018, Lignes directrices pour l'audit des systèmes de management

2.Autres normes référencées:

- Directives ISO/IEC, Partie 1:2019 – Procédures pour les travaux techniques
- NIST SP 500-291, Feuille de route des normes du NIST pour le cloud computing
- ISO 55000:2014, Gestion d'actifs – Aperçu général, principe et terminologie
- ISO/IEC 27021:2017, Technologies de l'information – Techniques de sécurité – Exigences de compétence pour les professionnels de la gestion des systèmes de management de la sécurité
- ISO/TR 31004:2013, Management du risque – Lignes directrices pour l'implémentation de l'ISO 31000
- ISO/Guide 73:2009, Management du risque – Vocabulaire
- ISO 10015:2019, Management de la qualité – Lignes directrices pour la gestion des compétences et le développement des personnes



Liste des acronymes

ANSI : American National Standards Institute

API : (*Application Programming Interface*) Interface de programmation d'applications

CA : Continuité d'activité

CFO : *Chief Financial Officer*

CIO : *Chief Information Officer*

CISO : *Chief Information Security Officer*

CSA : Cloud Security Alliance

CSP : Fournisseurs de services dans le nuage

DoS : Déni de service

GRI : Gestion des ressources d'information

IA : Intelligence artificielle

IAF : Intelligence artificielle forte

IaaS : *Infrastructure as a Service*

IAS : International Accreditation Service

IDS : (*Intrusion Detection System*) Système de détection d'intrusion

ISO : Organisation internationale de normalisation

JS : *Justification Study*

LA : Lead Auditor

LI : Lead Implementer

NSM : Norme de système de management

ONG : Organisation non gouvernementale

PaaS : *Platform as a Service*

PCI DSS: Payment Card Industry Data Security Standard

PDCA : Planifier-Déployer-Contrôler-Agir

PDG : Président-directeur général

PECB : Professional Evaluation and Certification Board

PEST : Politique, Économique, Social et Technologique

PIMS : (*Privacy Information Management System*) Système de management de la protection de la vie privée

RA : Reprise d'activité

RGPD : Règlement général sur la protection des données

RH : Ressources humaines

SaaS : *Software as a Service*

SMI : Système de management intégré

SMSI : Système de management de la sécurité de l'information

STAR : *Security, Trust, and Assurance Registry*

SWOT : (*Strengths, Weaknesses, Opportunities and Threats*) Forces, Faiblesses, Opportunités, Menaces

TC : (*Technical Committees*) Comités techniques

TI : Technologie de l'information

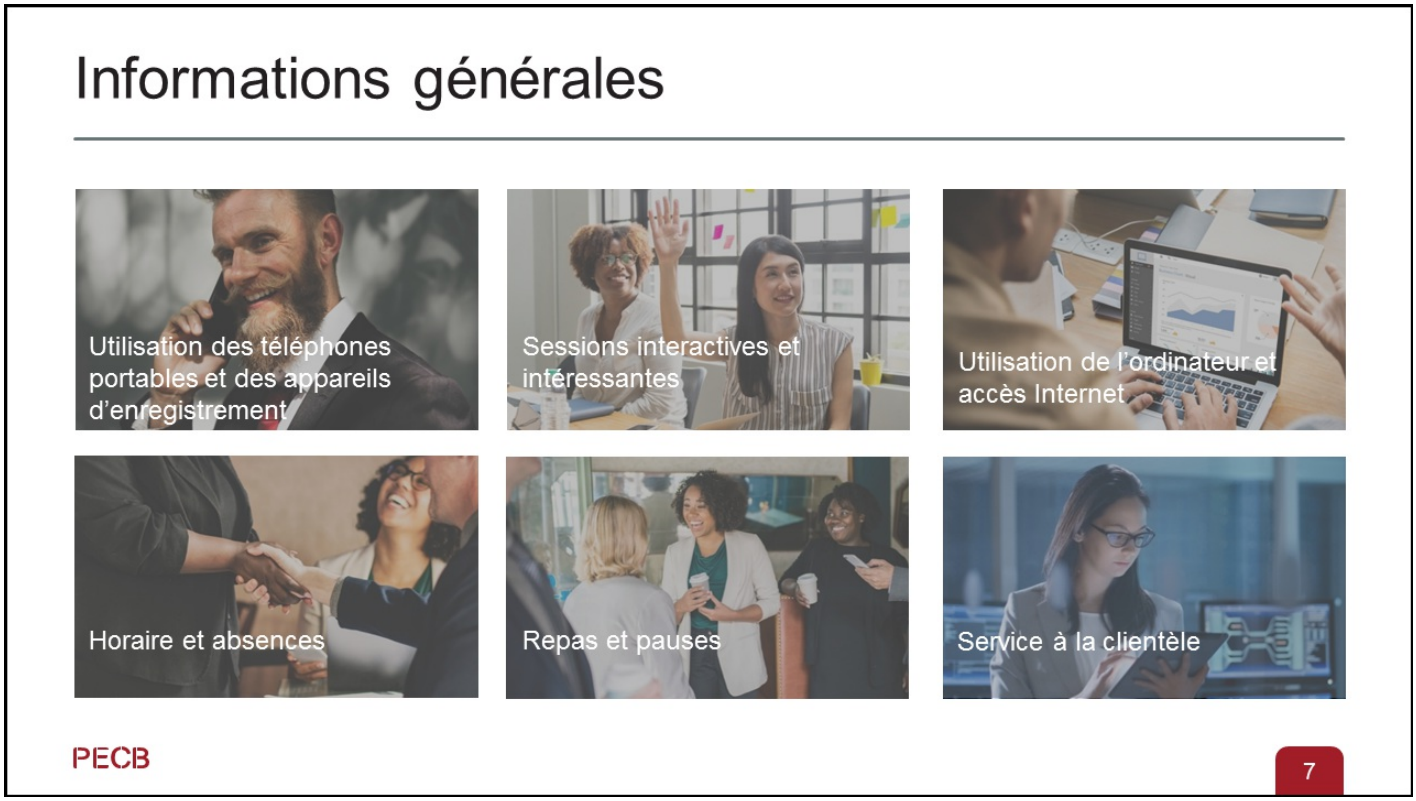
UKAS : United Kingdom Accreditation Service

Cette section fournit des informations qui aideront le participant à acquérir une connaissance globale des objectifs et de la structure de la formation, y compris le processus d'examen et de certification, et davantage d'informations sur PECB.

Afin de briser la glace, tous les participants se présenteront en mentionnant:

- Nom
- Fonction actuelle
- Connaissances et expérience relatives au management de la sécurité de l'information
- Connaissances et expérience avec ISO/IEC 27001 et d'autres normes de la famille 27000 (ISO/IEC 27002, ISO/IEC 27003, ISO/IEC 27004, ISO/IEC 27005, etc.)
- Connaissances et expérience relatives à d'autres systèmes de management (ISO 90001, ISO 14001, ISO/IEC 20000, ISO 22301, etc.) ;
- Attentes en matière de formation

Durée de l'activité: 20 minutes



- Veuillez noter la localisation des issues de secours en cas d'urgence.
- Entente sur l'horaire du cours et les deux pauses. Merci d'être à l'heure.
- Réglez votre téléphone portable en mode silencieux. Si vous devez répondre à un appel, veuillez le faire en dehors de la salle de classe.
- Les appareils d'enregistrement sont interdits, car ils peuvent nuire à la libre discussion.
- Les sessions de formation sont conçues pour encourager chacun à participer et tirer le meilleur parti de la formation.

Service à la clientèle

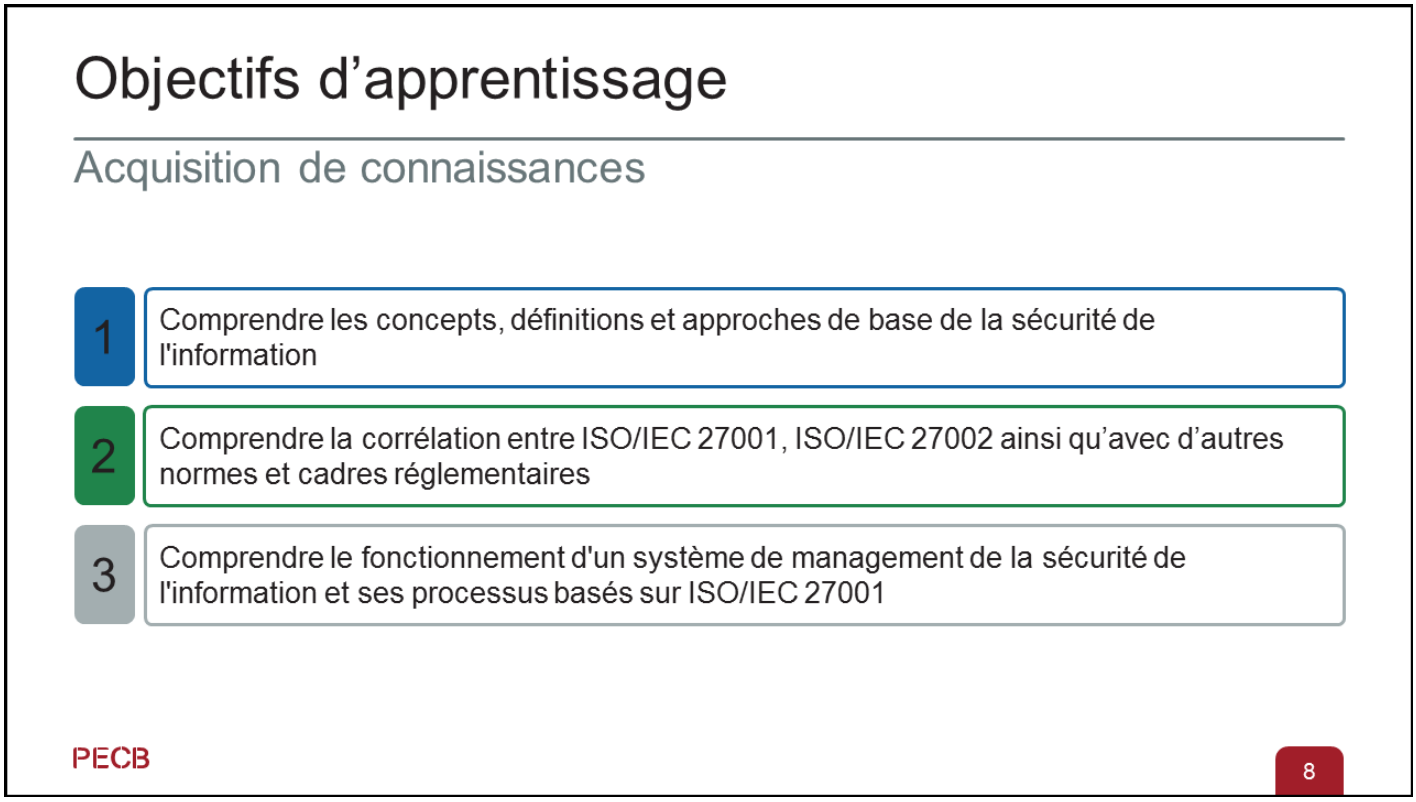
Afin d'assurer la satisfaction du client, le service client de PECB a mis en place un système de tickets d'assistance pour traiter les réclamations de nos clients.

Dans un premier temps, nous vous invitons à discuter de la situation avec le formateur. Si nécessaire, n'hésitez pas à contacter le responsable de l'organisme de formation où vous êtes inscrit. Dans tous les cas, nous restons à votre disposition pour arbitrer tout litige pouvant survenir entre vous et la société de formation.

Pour envoyer vos commentaires, questions ou réclamations, veuillez ouvrir un ticket d'assistance sur le site Web de PECB au Centre d'aide PECB (www.pecb.com/help).

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

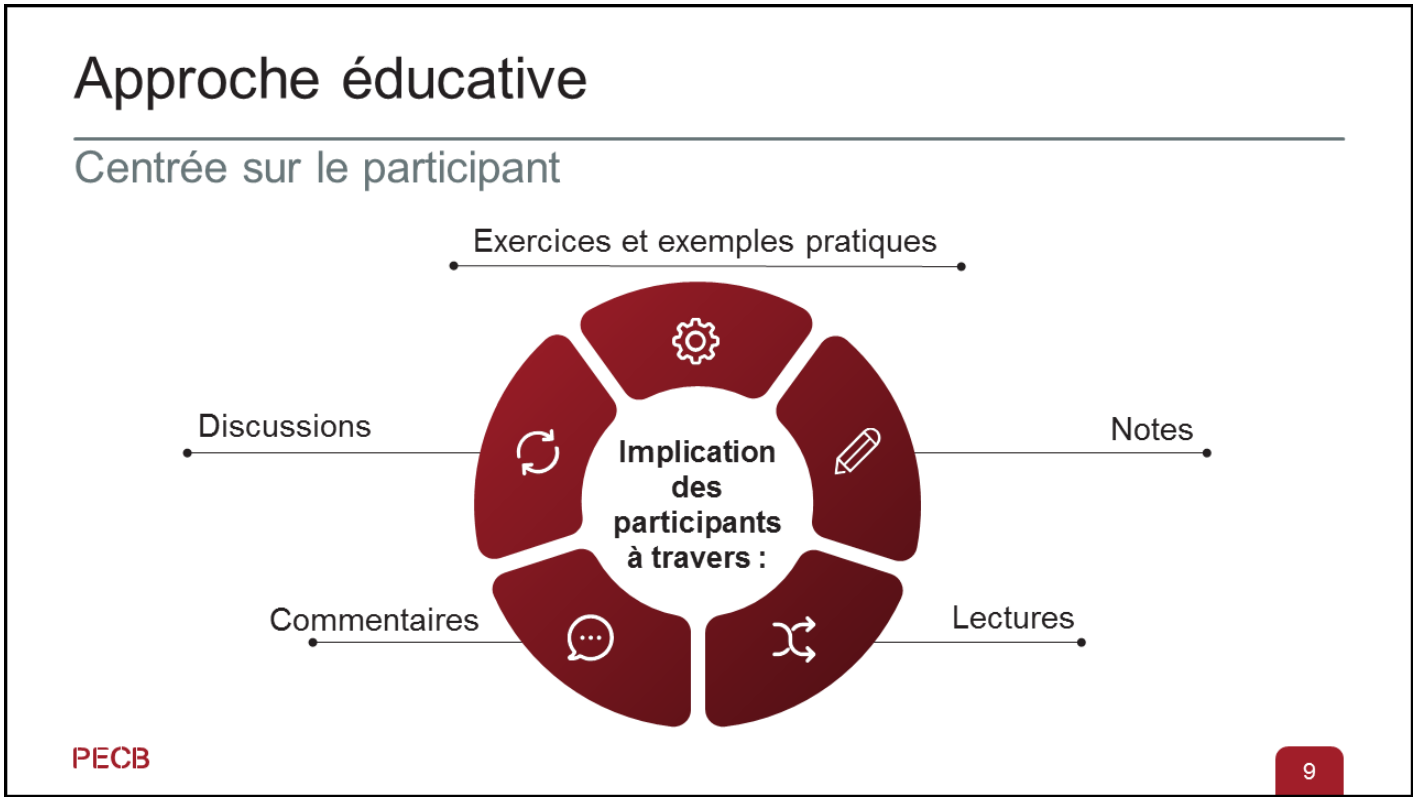
Si vous avez des suggestions concernant l'amélioration du matériel de formation PECB, nous aimerions les connaître. Vous pouvez le faire directement depuis notre application KATE ou vous pouvez ouvrir un ticket adressé au service de formation depuis le Centre d'aide PECB (www.pecb.com/help).



Cette formation est conçue pour aider les participants à comprendre les concepts et principes fondamentaux d'un système de management de la sécurité de l'information (SMSI) basé sur ISO/IEC 27001. D'un point de vue pédagogique, la compétence se compose des 3 éléments suivants:

1. Connaissance
2. Compétence
3. Comportement (attitude)

Pour acquérir les connaissances sur la mise en œuvre d’un SMSI basée sur ISO/IEC 27001 selon une approche de haut niveau et une méthodologie globale, il est recommandé de suivre la formation PECB ISO/IEC 27001 Lead Implementer. Pour acquérir une connaissance plus approfondie d'un processus d'audit du SMSI, y compris les principes d'audit, les techniques et les bonnes pratiques, il est recommandé de suivre le cours de certification de PECB ISO/IEC 27001 Lead Auditor.

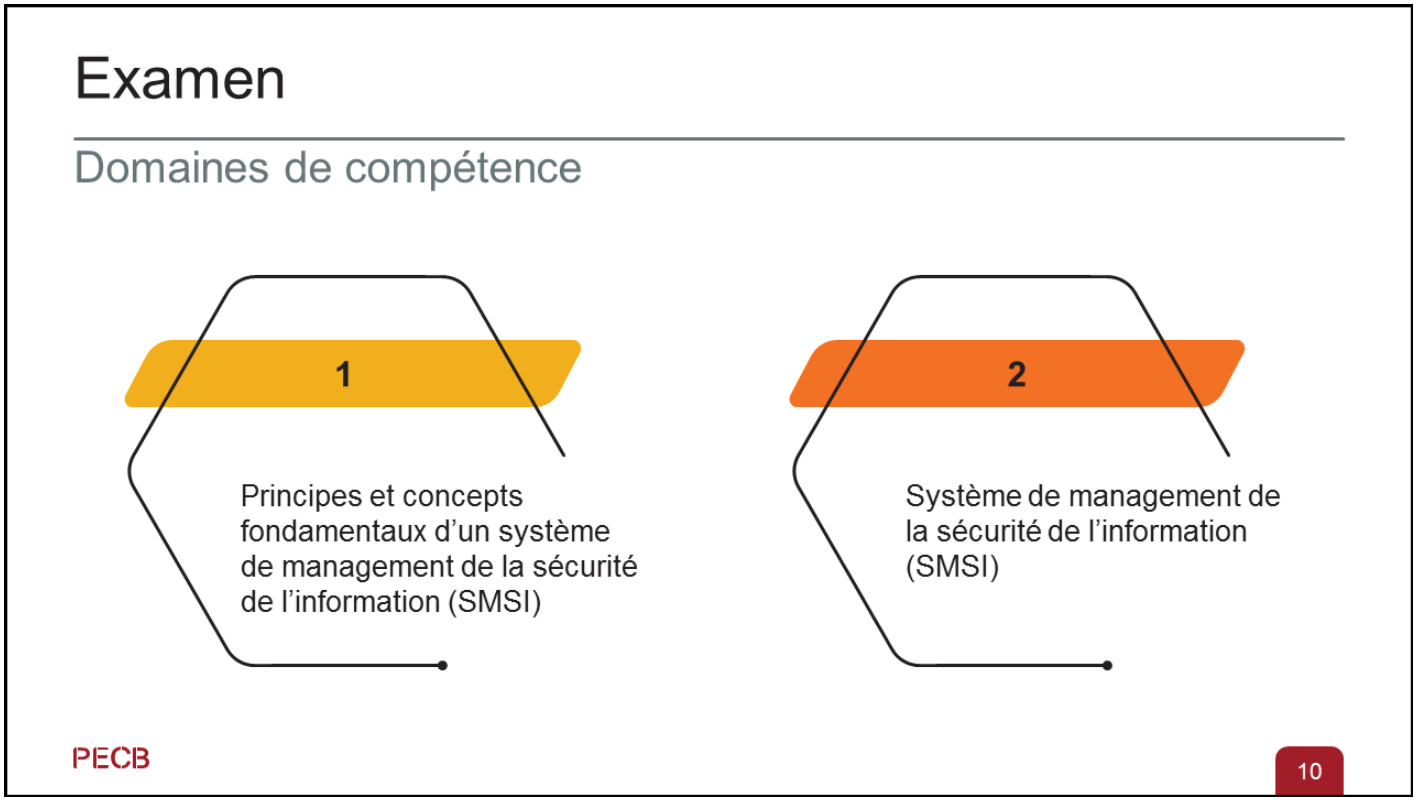


Cette formation repose sur des sessions animées par le formateur, dans lesquelles l'implication des participants est fortement encouragée par le biais d'exercices interactifs, études de cas, discussions (expériences des participants), questions, suggestions, etc.

N'oubliez pas: ce cours est le vôtre ; vous êtes le principal acteur de son succès.

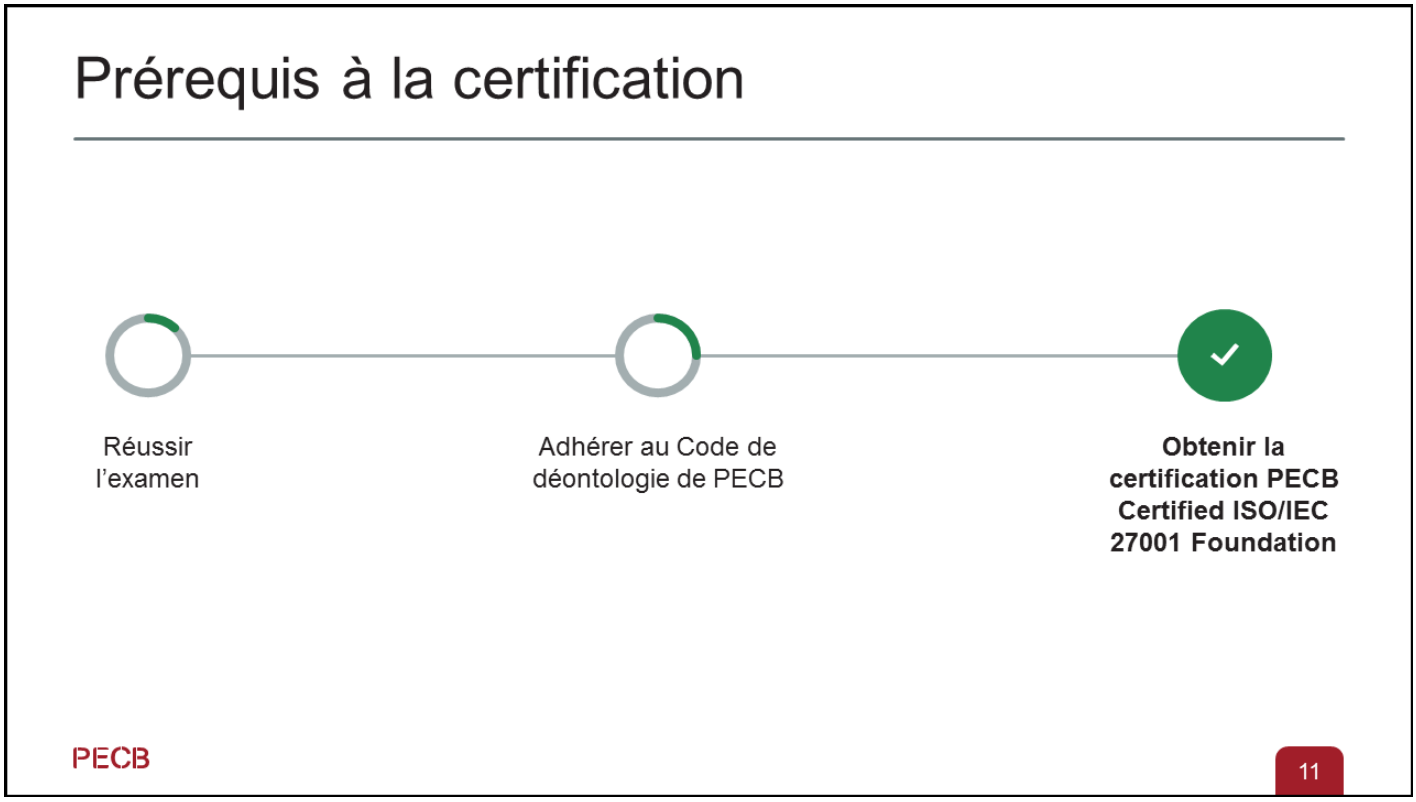
Les participants sont encouragés à prendre des notes complémentaires pendant les sessions de formation, ce qui peut être utile plus tard pendant l'examen.

Il convient de prêter une attention particulière aux exercices et aux quiz, car ils seront utiles pour préparer l'examen de certification.



L'objectif de l'examen de certification est de s'assurer que les candidats maîtrisent les concepts et techniques du SMSI afin d'être en mesure de participer à des projets de SMSI. Le comité d'examen de PECB veille à ce que la pertinence des questions d'examen soit maintenue sur la base de la pratique professionnelle.

Tous les domaines de compétence sont couverts par l'examen.



La réussite de l'examen est l'unique prérequis à l'obtention de la certification «PECB Certified ISO/IEC 27001 Foundation ». Étant donné que la certification professionnelle ISO/IEC 27001 Foundation est un titre d'entrée, il n'est donc pas nécessaire que les candidats aient une expérience professionnelle dans un projet ou un audit de SMSI.

L'ensemble des critères et le processus de certification seront expliqués en détail au cours de la dernière journée de formation.

Note importante: Les frais d'examen et de certification sont inclus avec la formation: Le candidat n'aura pas à payer de frais supplémentaires lors de la demande de certification pour recevoir la certification professionnelle «PECB Certified ISO/IEC 27001 Foundation».

Certification PECB

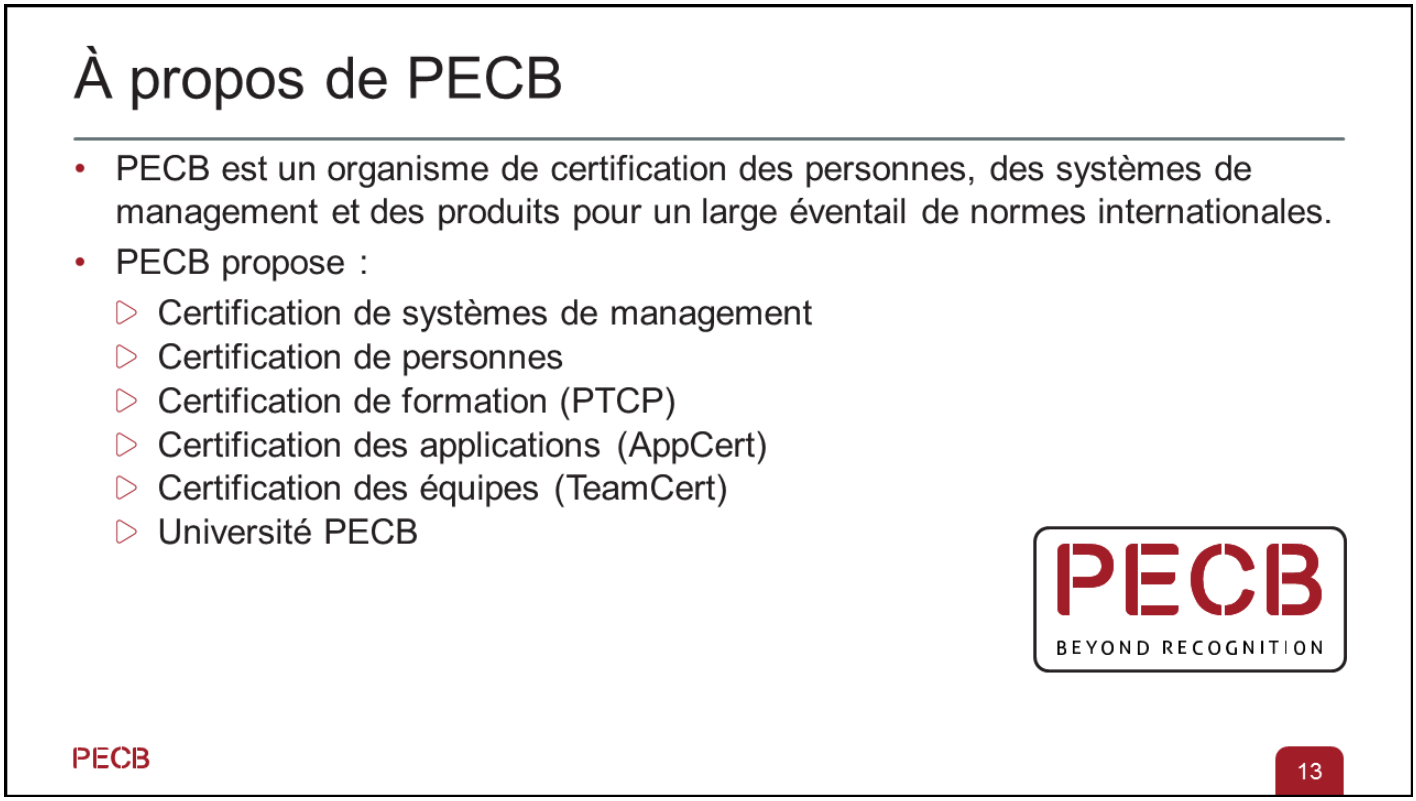
Les candidats ayant satisfait à l'ensemble des prérequis de certification recevront un certificat.

PECB

12

Après avoir réussi l'examen, le candidat dispose d'un délai maximum de trois ans pour demander la certification correspondante.

Une fois sa certification accordée, le candidat recevra un avis de PECB et il pourra télécharger le certificat à partir de son Tableau de bord PECB.



En tant que prestataire mondial de services de formation, d'examen, d'audit et de certification, PECB offre son expertise dans de multiples domaines, notamment la sécurité de l'information, les technologie de l'information, la continuité d'activité, la gestion des services, le management de la qualité, le management du risque, la santé, la sécurité et l'environnement.

Nous aidons les professionnels et les organismes à démontrer engagement et compétence en leur fournissant une formation, une évaluation et une certification de qualité conformément aux exigences de normes reconnues mondialement. Notre mission est de fournir à nos clients des services complets qui inspirent confiance, démontrent une reconnaissance et bénéficient à toute la société.

PECB est accréditée par IAS (*International Accreditation Service*) selon ISO/IEC 17024, ISO/IEC 17021-1 et ISO/IEC 17065.

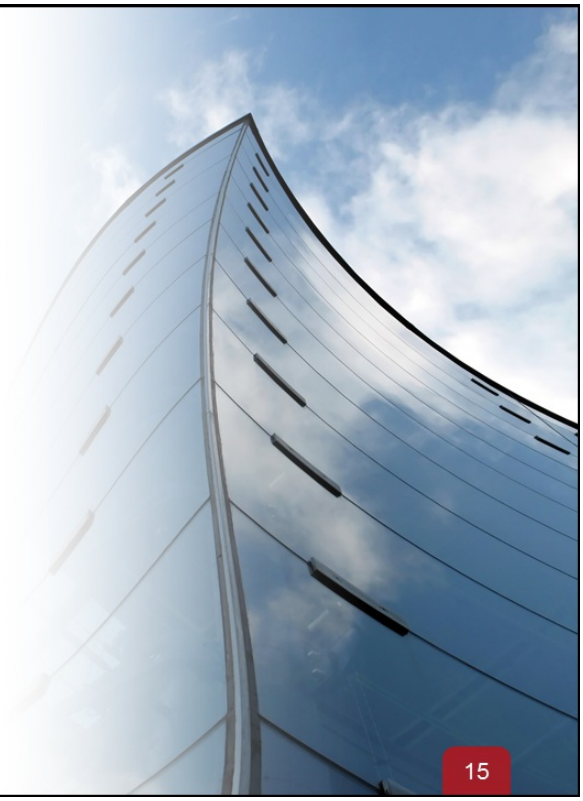
Les principaux objectifs de PECB sont les suivants :

1. Établir les exigences minimales nécessaires pour certifier les professionnels, les organismes et les produits
2. Examiner et vérifier les qualifications des candidats afin de s'assurer qu'ils peuvent prétendre à un certificat PECB
3. Élaborer et maintenir des processus de demande de certificat PECB fiables, valides et actuels
4. Délivrer des certificats aux candidats qualifiés, aux organismes et aux produits ; maintenir à jour et publier un registre des titulaires de certificats PECB valides
5. Établir des exigences pour le renouvellement périodique de la certification et déterminer la conformité à ces exigences
6. S'assurer que les personnes certifiées satisfont aux normes d'éthique et respectent le Code de déontologie de PECB
7. Promouvoir les avantages de la certification aux employeurs, aux fonctionnaires, aux praticiens dans les domaines connexes et au grand public

Section 2

Normes et cadres réglementaires

- Qu'est-ce que l'ISO ?
- La famille de normes ISO/IEC 27000
- Normes et réglementations relatives à la sécurité de l'information
- Avantages d'ISO/IEC 27001



PECB

15

Cette section fournit des informations qui aideront le participant à acquérir des connaissances sur ISO/IEC 27001 et les avantages qu'elle apporte, ainsi que sur d'autres normes et réglementations liées à la sécurité de l'information.

Qu'est-ce que l'ISO ?

- L'ISO est une organisation internationale regroupant des organismes nationaux de normalisation de plus de 160 pays.
- Les résultats finaux des travaux de l'ISO sont publiés en tant que normes internationales.
- L'ISO a publié plus de 22 000 normes depuis 1947.

PECB

16

Principes clés de l'élaboration des normes :

1.Les normes ISO répondent à un besoin du marché.

ISO élabore uniquement des normes pour lesquelles il existe une demande du marché, en réponse à des demandes officielles de secteurs industriels ou des parties prenantes (par ex. des groupes de consommateurs). En général, la demande pour une norme est communiquée aux membres nationaux qui contactent ensuite l'Organisation internationale de normalisation (ISO).

2.Les normes ISO sont élaborées à partir de l'avis d'experts mondiaux.

Les normes ISO sont élaborées par divers comités techniques (TC) composés d'experts du monde entier. Ces experts négocient tous les aspects de la norme, y compris son domaine d'application, ses définitions et son contenu.

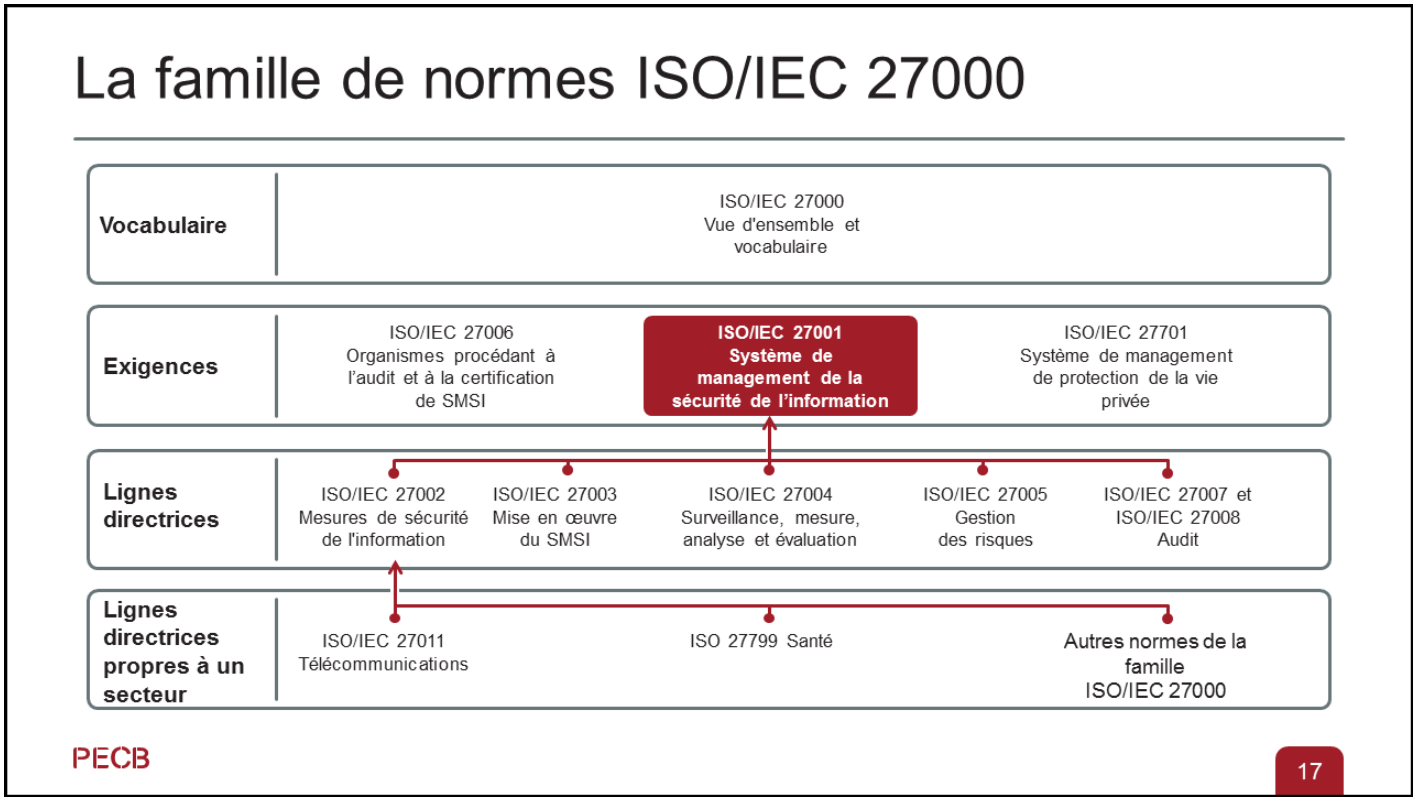
3.Les normes ISO sont élaborées dans le cadre d'un processus multipartite.

Les comités techniques sont composés d'experts de l'industrie concernée, mais aussi d'associations de consommateurs, d'universitaires, d'ONG et de gouvernements.

4.Les normes ISO sont basées sur un consensus.

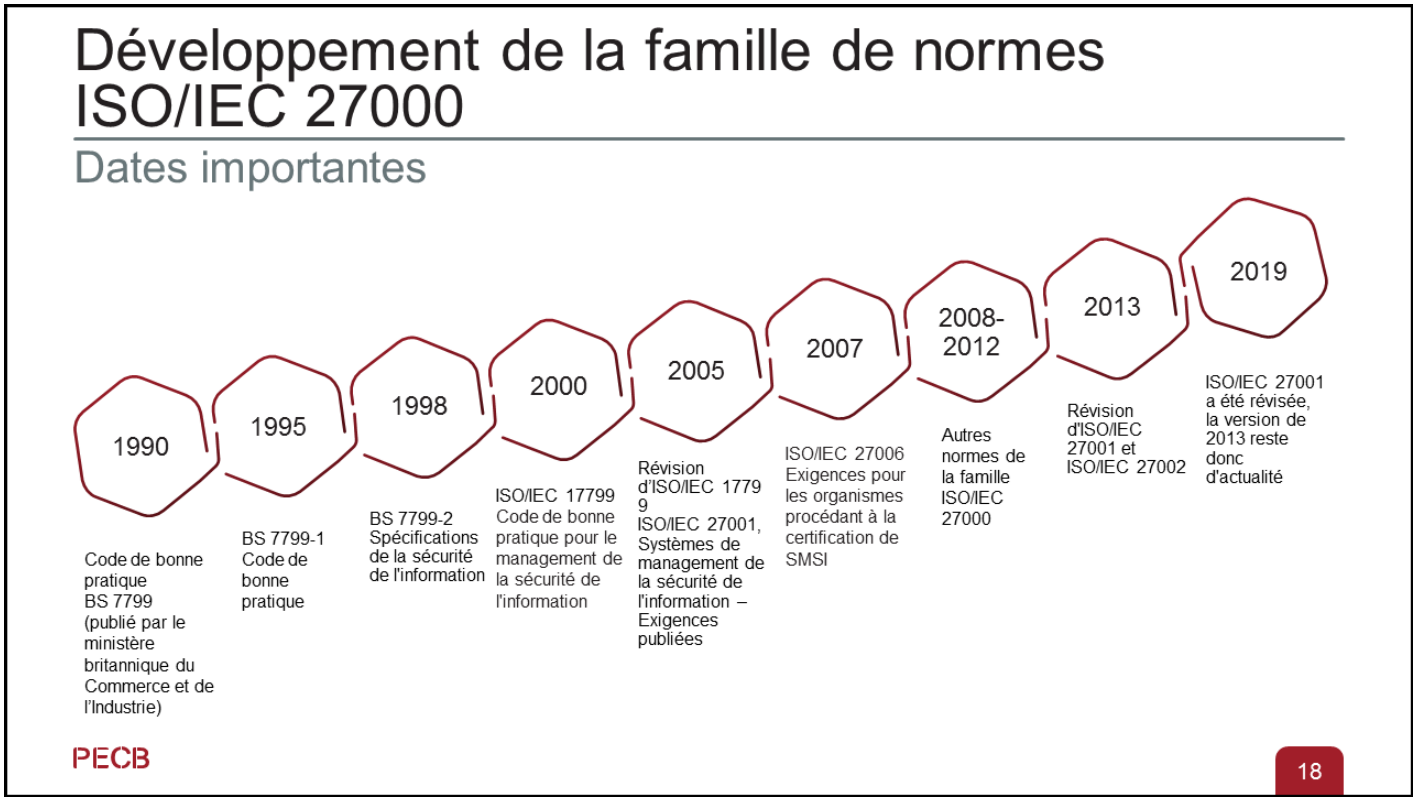
L'élaboration des normes ISO repose sur une approche consensuelle et les commentaires de toutes les parties prenantes sont pris en compte. Tous les pays membres de l'ISO, quelle que soit la taille ou la force de leur économie, sont sur un pied d'égalité en matière d'influence dans l'élaboration de normes.

Pour plus d'informations, veuillez visiter: www.iso.org.



La famille de normes ISO/IEC 27000 est une série de normes de sécurité de l'information. Ces normes sont : :

- **ISO/IEC 27000:** Vue d'ensemble et vocabulaire généralement utilisé dans le domaine de la sécurité de l'information
- **ISO/IEC 27001:** Exigences pour l'établissement, la mise en œuvre, la maintenance et l'amélioration continue d'un SMSI
- **ISO/IEC 27002:** Lignes directrices pour la mise en œuvre des mesures de sécurité de l'information énoncées à l'Annexe A de la norme ISO/IEC27001
- **ISO/IEC 27003:** Lignes directrices pour la mise en œuvre d'un SMSI
- **ISO/IEC 27004:** Lignes directrices sur la surveillance, le mesurage, l'analyse et l'évaluation d'un SMSI
- **ISO/IEC 27005:** Lignes directrices sur la gestion des risques liés à la sécurité de l'information
- **ISO/IEC 27006:** Exigences pour les organismes procédant à l'audit et à la certification des SMSI
- **ISO/IEC 27007**: Lignes directrices pour l'audit des systèmes de management de la sécurité de l'information
- **ISO/IEC TS 27008** : Lignes directrices pour les auditeurs des mesures de sécurité de sécurité de l'information
- **ISO/IEC 27011:** Lignes directrices pour l'utilisation d'ISO/IEC 27002 dans l'industrie des télécommunications
- **ISO/IEC 27031:** Lignes directrices pour la préparation des technologies de la communication et de l'information à la continuité d'activité
- **ISO/IEC 27701:** Exigences et lignes directrices pour l'établissement, la mise en œuvre, la maintenance et l'amélioration continue d'un système de management de l'information sur la vie privée (PIMS) en tant qu'extension des normes ISO/IEC 27001 et ISO/IEC 27002 pour le management de la vie privée
- **ISO 27799:** Lignes directrices pour l'utilisation d'ISO/IEC 27002 en informatique de la santé



L'histoire et le raisonnement derrière l'élaboration des normes de la famille ISO/IEC 27000 :•

- L'industrie a exprimé le besoin de bonnes pratiques et de mesures de sécurité pour soutenir les entreprises et les gouvernements dans la mise en œuvre et l'amélioration de la sécurité de l'information.
- Le Department of Trade and Industry (Royaume-Uni) a constitué un groupe de travail composé de spécialistes de la sécurité de l'information.
- Un «Code de bonne pratique», essentiellement un ensemble de mesures (BS 7799), a été publié. Plusieurs de ces mesures sont reconnaissables dans ISO/IEC 27002.
- Il a été suivi d'une «Spécification de sécurité de l'information» (BS7799-2, précédemment 7799 qui devient 7799-1).
- Ces documents ont finalement été adoptés comme normes ISO, BS7799-2 devenant ISO/IEC 27001 et 7799-1 devenant 27002 (ce qui place logiquement les Exigences en premier et le Code de bonne pratique en deuxième).
- Ils ont ensuite été complétés par les normes ISO/IEC 27003, 27004, 27005 et diverses normes d'interprétation sectorielles.
- Les normes ISO font l'objet d'une révision tous les cinq ans, afin de suivre l'évolution des différentes industries. La dernière révision et confirmation de la norme ISO/IEC 27001 a eu lieu en 2019 ; cette version reste donc d'actualité.

ISO/IEC 27001

- Cette norme spécifie les exigences pour la mise en œuvre d'un SMSI (articles 4 à 10).
- Les exigences (articles) sont écrites en utilisant le verbe impératif « doit ».
- Composée de 14 articles, 35 objectifs de mesure et 114 mesures de sécurité.
- Les organismes peuvent obtenir une certification conformément à cette norme.

PECB

19

ISO/IEC 27001:

- Un ensemble d'exigences normatives pour établir, mettre en œuvre, exploiter, surveiller et reviser un système de management de la sécurité de l'information (SMSI)
- Un ensemble d'exigences pour sélectionner les mesures de sécurité adaptées aux besoins de chaque organisme en fonction des bonnes pratiques de l'industrie
- Un processus internationalement reconnu, défini et structuré pour gérer la sécurité de l'information
- Une norme internationale qui convient à tous les types d'organismes, quelle que soit leur taille ou le secteur dans lequel ils opèrent (par exemple, les entreprises commerciales, les agences gouvernementales, les organisations à but non lucratif)

ISO/IEC 27001, article 0.1 Généralités

La présente Norme internationale a été élaborée pour fournir des exigences en vue de l'établissement, de la mise en œuvre, de la tenue à jour et de l'amélioration continue d'un système de management de la sécurité de l'information. L'adoption d'un système de management de la sécurité de l'information relève d'une décision stratégique de l'organisation. L'établissement et la mise en œuvre d'un système de management de la sécurité de l'information d'une organisation tiennent compte des besoins et des objectifs de l'organisation, des exigences de sécurité, des processus organisationnels mis en œuvre, ainsi que de la taille et de la structure de l'organisation. Tous ces facteurs d'influence sont appelés à évoluer dans le temps.

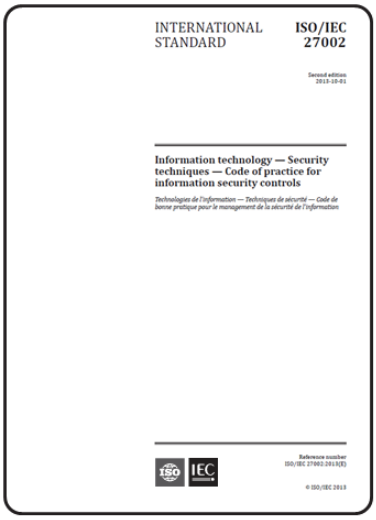
Le système de management de la sécurité de l'information préserve la confidentialité, l'intégrité et la disponibilité de l'information en appliquant un processus de gestion des risques et donne aux parties intéressées l'assurance que les risques sont gérés de manière adéquate.

Il est important que le système de management de la sécurité de l'information fasse partie intégrante des processus et de la structure de management d'ensemble de l'organisation et que la sécurité de l'information soit prise en compte dans la conception des processus, des systèmes d'information et des mesures. Il est prévu qu'un système de management de la sécurité de l'information évolue conformément aux besoins de l'organisation.

La présente Norme internationale peut être utilisée par les parties internes et externes pour évaluer la capacité de l'organisation à répondre à ses propres exigences en matière de sécurité de l'information.

ISO/IEC 27002

- Cette norme présente le code de bonne pratique pour les mesures de sécurité de l'information (outil de référence).
- Les articles sont exprimés par l'expression « il convient que ».
- Cette norme ne se prête pas à des fins de certification.



PECB

20

ISO/IEC 27002:

- ISO/IEC 27002 est un guide des mesures de management de la sécurité de l'information.
- Cette Norme internationale fournit une liste des objectifs et des mesures de sécurité généralement utilisés dans le secteur de la sécurité de l'information.
- En particulier, les articles5 à 18 présentent des lignes directrices détaillées sur les bonnes pratiques à l'appui des mesures de sécurité spécifiées à l'Annexe A de la norme ISO/IEC27001 (articlesA.5 à A.18).

ISO/IEC 27002, article 1 Domaine d'application

La présente Norme internationale donne des lignes directrices en matière de normes organisationnelles relatives à la sécurité de l'information et des bonnes pratiques de management de la sécurité de l'information, incluant la sélection, la mise en œuvre et la gestion de mesures de sécurité prenant en compte le ou les environnement(s) de risques de sécurité de l'information de l'organisation.

La présente Norme internationale est élaborée à l'intention des organisations désireuses

a. *de sélectionner les mesures nécessaires dans le cadre du processus de mise en œuvre d'un système de management de la sécurité de l'information (SMSI) selon l'ISO/CEI 27001;*
b. *de mettre en œuvre des mesures de sécurité de l'information largement reconnues;*
c. *d'élaborer leurs propres lignes directrices de management de la sécurité de l'information.*

ISO/IEC 27003

- Cette norme présente les lignes directrices pour la mise en œuvre d'un système de management de la sécurité de l'information.
- Sert de document de référence à utiliser avec les normes ISO/IEC 27001 et ISO/IEC 27002.
- Elle est composée de 10 articles.
- Cette norme ne se prête pas à des fins de certification.

PECB

21

ISO/IEC 27003, article 1 Domaine d'application

Le présent document présente des explications et des lignes directrices pour la norme ISO/IEC 27001:2013.

ISO/IEC27003:2009, Introduction

Ce document fournit des lignes directrices sur les exigences relatives à un système de management de la sécurité de l'information (SMSI) telles que spécifiées dans ISO/IEC 27001 et fournit des recommandations ("devrait"), des possibilités ("peut") et des autorisations ("peut") à cet égard. Le présent document n'a pas pour objet de fournir des lignes directrices générales sur tous les aspects de la sécurité de l'information.

Les articles 4 à 10 de ce document reflètent la structure d'ISO/IEC 27001:2013.

Ce document n'ajoute aucune nouvelle exigence pour un SMSI et ses termes et définitions connexes. Les organismes devraient se référer à ISO/IEC 27001 et ISO/IEC 27000 pour les exigences et les définitions Les organismes qui mettent en œuvre un SMSI ne sont pas obligés de respecter les lignes directrices de ce document.

PCI DSS (*Payment Card Industry Data Security Standard*)

- La norme de sécurité des données de l'industrie des cartes de paiement (PCI DSS) est un ensemble de normes de sécurité qui unifient les programmes et les politiques de sécurité de l'information en ce qui concerne les informations relatives aux cartes de crédit.
- PCI DSS s'applique à tout organisme qui accepte, transmet ou stocke les données des titulaires de cartes.
- Le PCI Security Standards Council a été fondé en 2006 par American Express, Discover, JCB International, MasterCard et Visa Inc.

PECB

22

PCI DSS se compose de 6 objectifs et de 12 exigences. Ces objectifs sont :

- Construire et maintenir un réseau et des systèmes sécurisés
- Protéger les données des titulaires de carte
- Maintenir un programme de gestion de la vulnérabilité
- Mettre en œuvre des mesures de contrôle d'accès strictes
- Contrôler et tester régulièrement les réseaux
- Maintenir une politique de sécurité de l'information

La cartographie de PCI DSS et ISO/IEC 27001 peut être trouvée ici : https://www.isaca.org/Journal/archives/2016/Volume-1/Documents/Comparison-of-PCI-DSS-and-ISO-IEC-27001-Standards_joa_Eng_0116.pdf

Cloud Security Alliance (CSA)

- La *Cloud Security Alliance* (CSA) est un organisme qui s'est engagé à définir les meilleures pratiques pour garantir un environnement informatique en nuage sécurisé.
- Elle dispose d'un programme d'assurance des fournisseurs de services en nuage à trois niveaux, connu sous le nom de programme STAR (*Security, Trust, and Assurance Registry*) de la CSA. STAR consiste en une auto-évaluation, un audit de tierce partie et un contrôle continu. Son principal objectif est d'aider les clients à évaluer les fournisseurs de services dans le nuage.

PECB

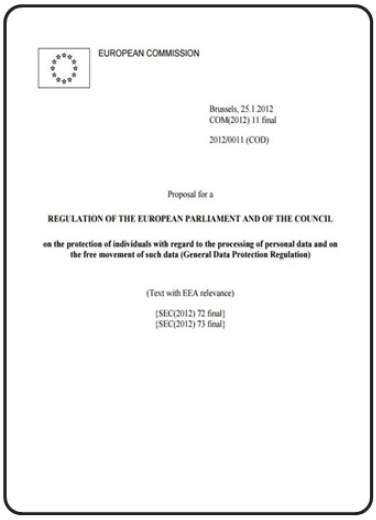
23

La certification CSA STAR est une évaluation indépendante et rigoureuse de la sécurité d'un fournisseur de services dans le nuage. En principe, tout organisme qui se soumet à la certification ISO/IEC 27001 peut simultanément se soumettre à l'évaluation CSA Star et obtenir la certification CSA Star. Les lignes directrices CSA STAR s'appliquent aux fournisseurs de services dans le nuage (CSP) qui relèvent principalement des secteurs ci-dessous :

- Fournisseurs de services dans le nuage
- Centre d'hébergement de données
- Hébergement Web
- Protection de la propriété intellectuelle
- Finances et services de soins de santé

Règlement général sur la protection des données

- Le Règlement général sur la protection des données (RGPD) précise les exigences en matière de protection des personnes physiques à l'égard du traitement et de la libre circulation des données à caractère personnel.
- Le RGPD est disponible sur : https://eur-lex.europa.eu/eli/reg/2016/679/oj


EUROPEAN COMMISSION

Brussels, 25.1.2012
COM(2012) 11 final

2012/0011 (COD)

Proposal for a

REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)

(Text with EEA relevance)

{SEC(2012) 72 final}
{SEC(2012) 73 final}

PECB

24

ISO/IEC 27001 est la principale norme internationale en matière de sécurité de l'information. La mise en œuvre d'ISO/IEC 27001 est acceptée pour couvrir l'article 32 du RGPD. Ainsi, le cadre ISO/IEC 27001 peut être utilisé pour soutenir la conformité avec le RGPD. En outre, ISO/IEC 27001 et le RGPD se recoupent dans de nombreux domaines, tels que la confidentialité, la disponibilité et l'intégrité des données, ainsi que l'appréciation des risques, etc.

La cartographie du RGPD et d'ISO/IEC 27001 peut être trouvée ici : https://www.iso27001security.com/ISO27k_GDPR_mapping_release_1.docx

Exercice 1 : Raisons d’adopter ISO/IEC 27001

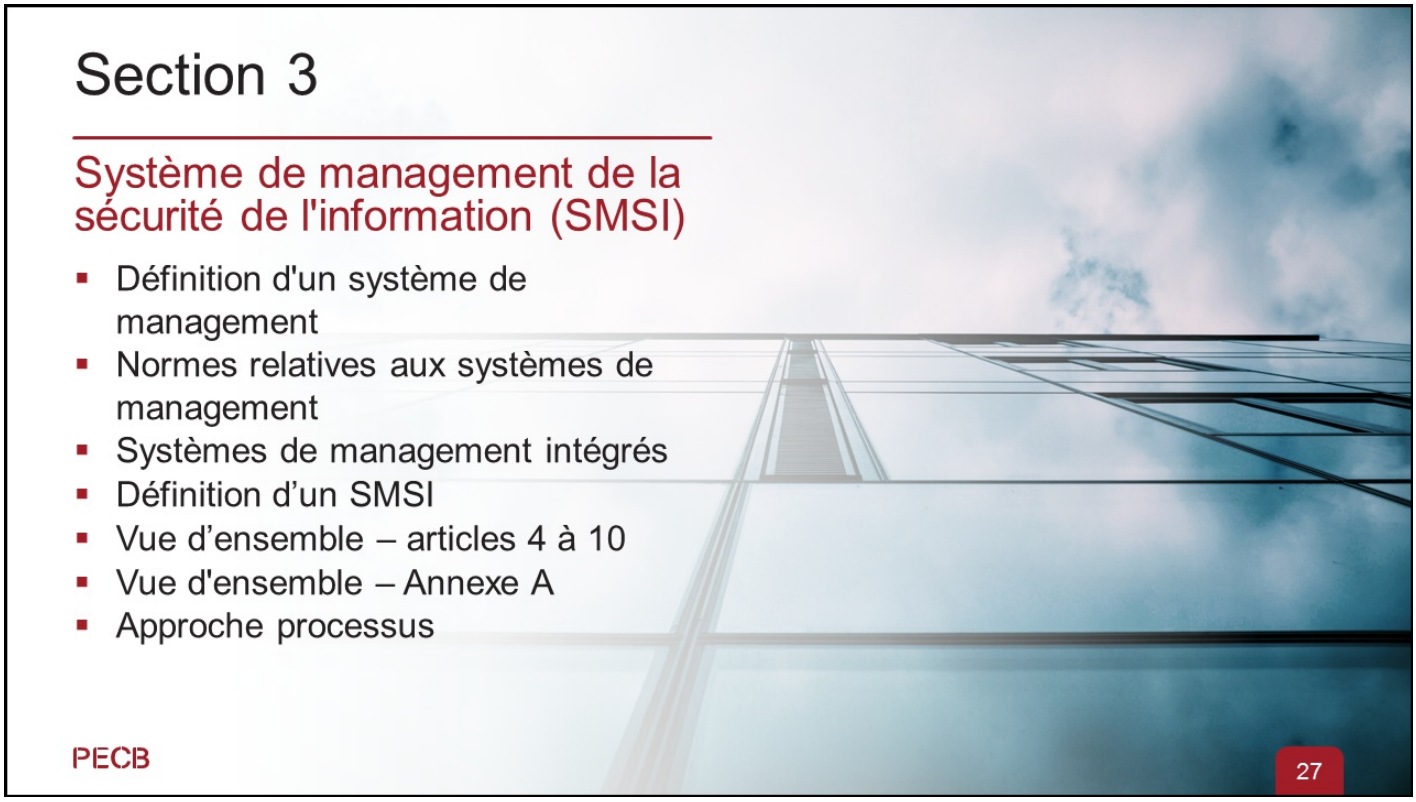
Déterminez les trois avantages les plus significatifs qu'un organisme peut obtenir en adoptant un système de management de la sécurité de l'information (SMSI) basé sur ISO/IEC 27001.

Durée de l’exercice : 15 minutes

Commentaires : 15 minutes

Résumé de la section

- L'Organisation internationale de normalisation (ISO) publie des normes en réponse à une demande du marché. Les normes ISO sont basées sur l'opinion et le consensus d'experts mondiaux et sont élaborées dans le cadre d'un processus multipartite.
- La famille de normes ISO/IEC 27000 comprend des normes pour le management de la sécurité de l'information par la mise en place d'un système de management de la sécurité de l'information (SMSI).
- ISO/IEC 27001 est la principale norme de la famille qui spécifie les exigences d'un SMSI.
- Les avantages de la mise en place d'un SMSI sont multiples : amélioration de la sécurité de l'information, bonne gouvernance, reconnaissance internationale, avantage concurrentiel, revenus supplémentaires, etc.



Cette section fournit des informations qui aideront le participant à acquérir des connaissances sur la définition d'un SMSI, l'approche processus et la structure de la norme ISO/IEC 27001, y compris un aperçu des articles 4 à 10 et de l'Annexe A de cette norme.

Définition d'un système de management

ISO/IEC 27000, article 3.41

- *Ensemble d'éléments corrélés ou en interaction d'un organisme, utilisés pour établir des politiques, des objectifs et des processus de façon à atteindre lesdits objectifs*
- *Note 1 à l'article: Un système de management peut recouvrir une ou plusieurs disciplines.*
- *Note 2 à l'article: Les éléments du système comprennent la structure de l'organisme, les rôles et responsabilités, la planification et les opérations.*
- *Note 3 à l'article: Le domaine d'un système de management peut comprendre l'organisme dans son ensemble, certaines de ses fonctions spécifiques et identifiées, certaines de ses sections spécifiques et identifiées, ou une ou plusieurs fonctions au sein d'un groupe d'organismes.*

PECB

28

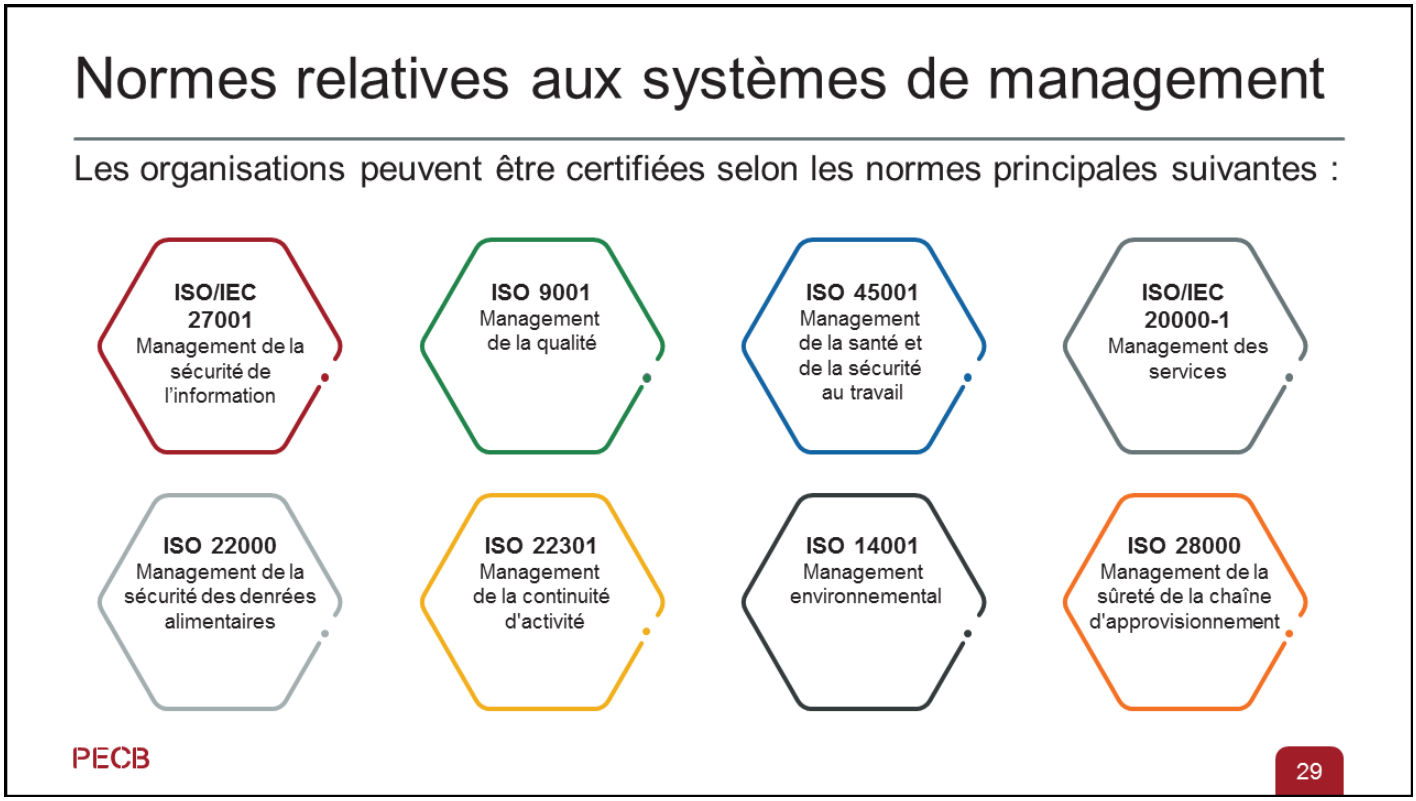
Un système de management est un système permettant à un organisme d'établir des politiques et des objectifs et de les mettre en œuvre par la suite. Le système de management d'un organisme peut inclure différents systèmes de management, comme un système de management de la qualité, de la sécurité de l'information, de l'environnement, etc.

Les organismes utilisent des systèmes de management pour développer leurs politiques et les mettre en application au moyen d'objectifs à l'aide des éléments suivants:

- Une structure organisationnelle
- Des processus systématiques et des ressources associées
- Une méthodologie d'appréciation efficace
- Un processus de révision pour s'assurer que les problèmes soient corrigés adéquatement et que les opportunités d'amélioration soient identifiées et mises en œuvre lorsqu'elles sont justifiées

Note: Ce qui est mis en œuvre doit être contrôlé et mesuré, ce qui est contrôlé et mesuré doit être géré.

ISO/IEC 27001 précise que *l'organisme doit évaluer les performances en matière de sécurité de l'information et l'efficacité du système de management de la sécurité de l'information* (article 9.1). Cet article est une composante essentielle d'un système de management, car il est impossible de valider si l'organisme a atteint ses objectifs sans évaluer l'efficacité des processus et des contrôles.



Les publications de l'ISO vont des activités traditionnelles, telles que l'agriculture et la construction, aux développements les plus récents des technologies de l'information, tels que le codage numérique des signaux audiovisuels pour les applications multimédias.

Les familles ISO 9000 et ISO 14000 sont parmi les normes ISO les plus connues. La norme ISO9001 est devenue une référence internationale en matière d'exigences de qualité. La norme ISO14001, pour sa part, est utilisée pour aider les organismes à relever les défis de nature environnementale. Ces deux normes sont génériques et applicables à tout organisme, quelle que soit la taille ou la complexité des processus.

Pour des informations détaillées sur chaque norme pertinente, veuillez consulter www.pecb.com ou www.iso.org

Systèmes de management intégrés

Structure commune des normes d'ISO

Exigences	ISO 9001:2015	ISO 14001:2015	ISO 55001:2014	ISO 22301:2019	ISO/IEC 27001:2013
Leadership et engagement	5.1	5.1	5.1	5.1	5.1
Politique du système de management	5.2	5.2	5.2	5.2	5.2
Objectifs du système de management	6.2	6.2	6.2	6.2	6.2
Informations documentées	7.5	7.5	7.6	7.5	7.5
Audit interne	9.2	9.2	9.2	9.2	9.2
Revue de direction	9.3	9.3	9.3	9.3	9.3
Amélioration continue	10.3	10.3	10.3	10.2	10.2

PECB

30

Comme les organismes gèrent de plus en plus souvent plusieurs cadres de conformité simultanément, il est recommandé de mettre en œuvre un système de management intégré. Un système de management intégré (SMI) est un système de management qui intègre toutes les composantes d'une entreprise en un seul système cohérent afin de permettre la réalisation de son objectif et de sa mission. Le tableau de la diapositive présente certaines exigences communes à tous les systèmes de management.

Il y a plusieurs bonnes raisons pour l'intégration, notamment:

- Harmoniser et optimiser les pratiques
- Éliminer les conflits de responsabilités et de relations
- Équilibrer des objectifs contradictoires
- Formaliser les systèmes informels
- Réduire la duplication et donc les coûts
- Réduire les risques et augmenter la rentabilité
- Se concentrer sur les objectifs de l'entreprise
- Créer de la cohérence
- Améliorer la communication
- Faciliter la formation et la sensibilisation

Page de notes

PECB

31

Directives ISO/IEC (Partie 1), Annexe L.1 Généralités

Chaque fois qu'est émise une proposition d'élaborer une nouvelle norme de système de management (NSM), y compris une NSM sectorielle, une étude de justification doit être effectuée conformément à l'Appendice 1 à la présente Annexe L.

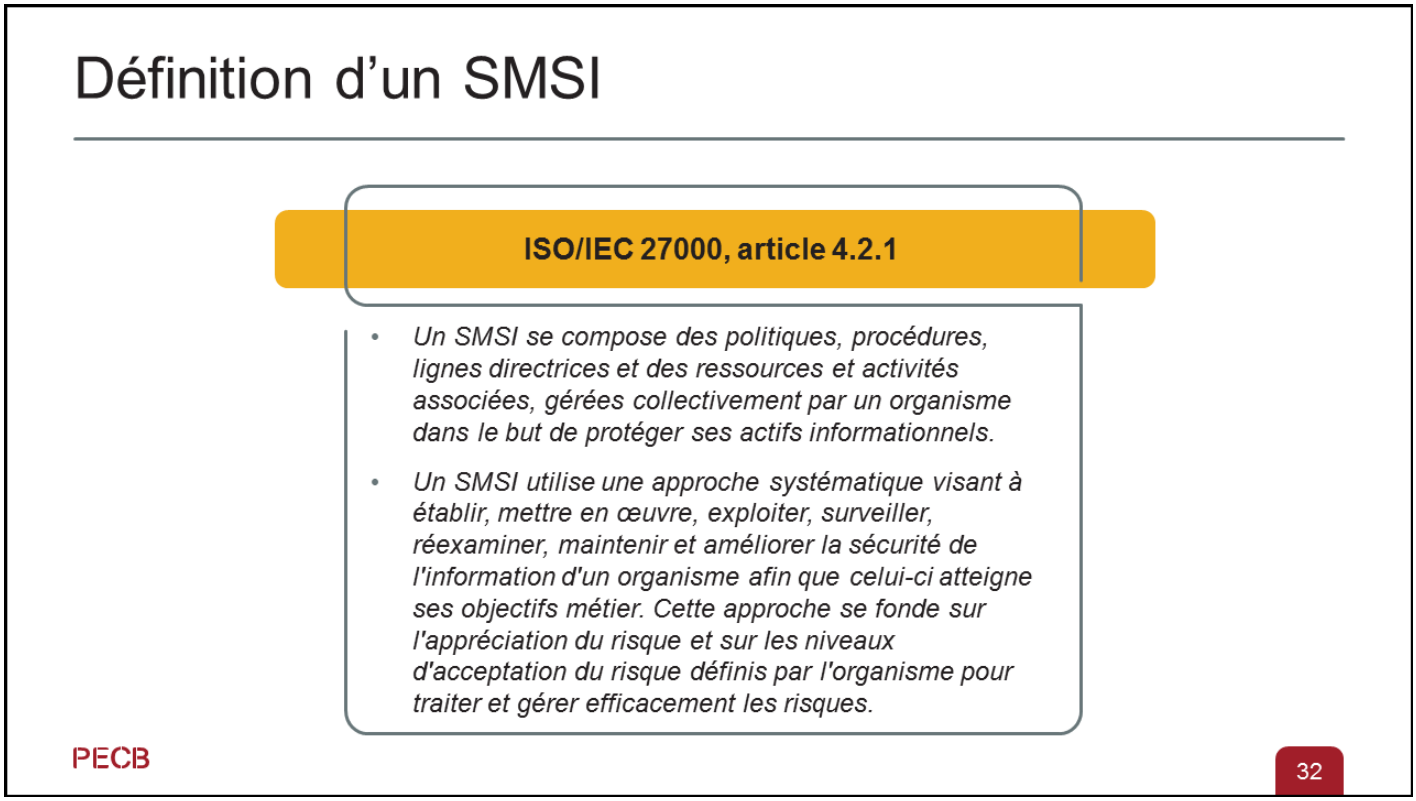
NOTE La révision d'une NSM existante dont l'élaboration a déjà été approuvée, et à condition que le domaine d'application soit confirmé, ne nécessite pas d'étude de justification (sauf s'il n'en a pas été fourni lors de l'élaboration initiale).

Dans la mesure du possible, l'auteur de la proposition s'efforcera d'établir la gamme complète des livrables que comptera la famille de NSM inédite ou révisée, et une étude justificative sera préparée pour chacun de ces livrables.

Directives ISO/IEC (Partie 1), Appendice 1 Questions relatives aux critères de justification

Il convient de tenir dûment compte de chacun des principes généraux et idéalement, que l'auteur de la proposition fournisse, lorsqu'il prépare l'étude de justification, une explication générale de chaque principe, avant de répondre aux questions correspondantes. Les principes auxquels il convient que l'auteur de la proposition de norme de système de management prête dûment attention lorsqu'il prépare l'étude de justification sont les suivants:

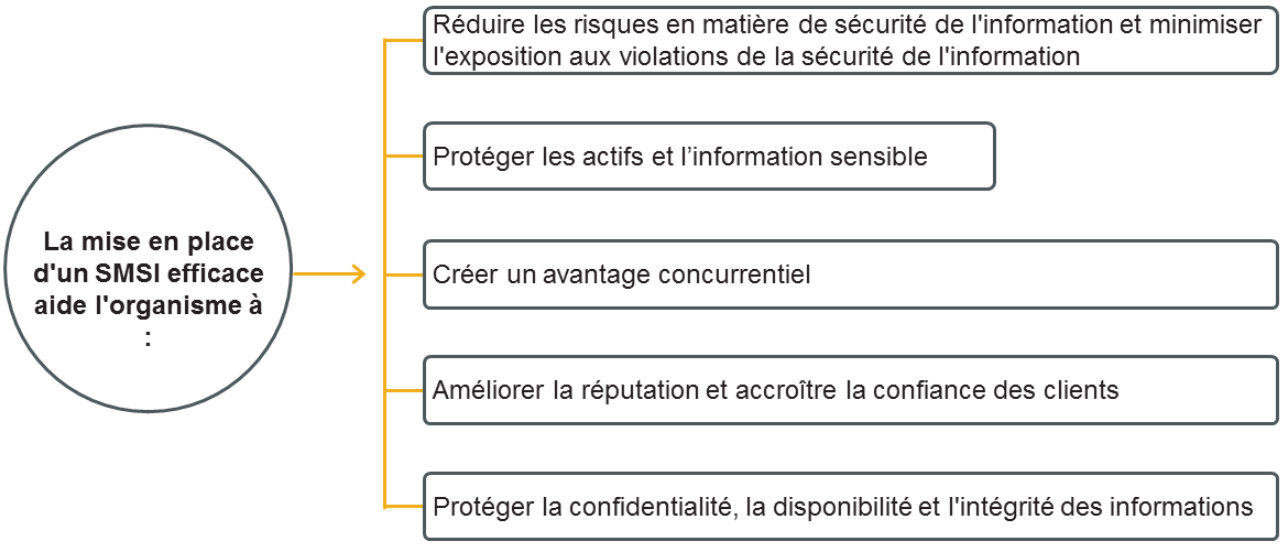
1. *Pertinence pour le marché*
2. *Compatibilité*
3. *Couverture du sujet*
4. *Flexibilité*
5. *Libre échange*
6. *Applicabilité de l'évaluation de conformité*
7. *Exclusions*



ISO/IEC 27000, article 3.28 Sécurité de l'information

protection de la confidentialité, de l'intégrité et de la disponibilité de l'information

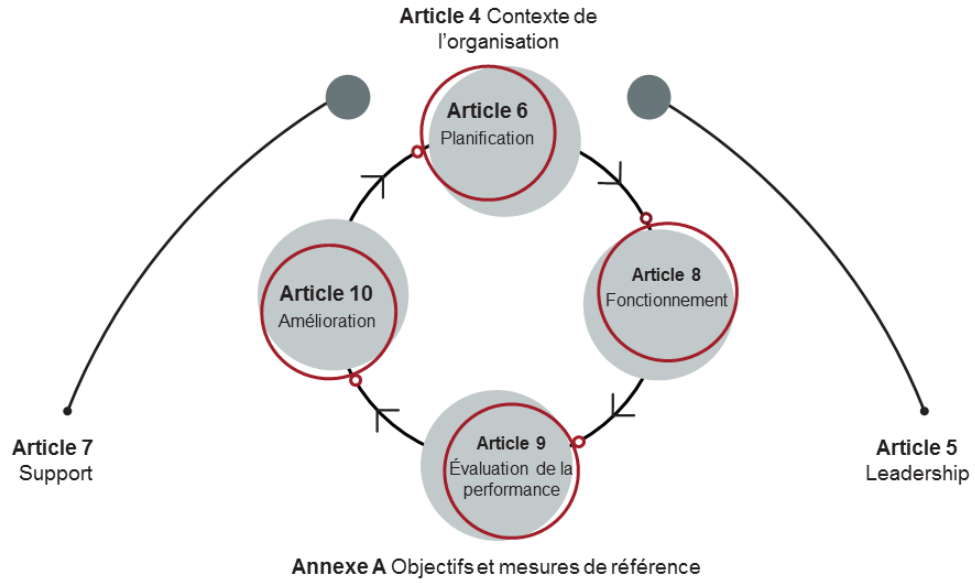
Avantages du SMSI



PECB

33

Structure d'ISO/IEC 27001



PECB

34

Un organisme qui souhaite obtenir la certification ISO/IEC 27001 doit se conformer aux exigences énoncées dans les articles 4 à 10 de la norme.

Contexte de l’organisation

ISO/IEC 27001, article 4

4.1 Compréhension de l’organisme et de son contexte

L'organisme doit déterminer les facteurs externes et internes qui peuvent affecter la réalisation du ou des résultats attendus du SMSI.

4.2 Compréhension des besoins et des attentes des parties intéressées

L'organisme doit déterminer les parties intéressées de la sécurité de l'information et leurs exigences.

4.3 Détermination du domaine d’application du système de management de la sécurité de l’information

L'organisme doit établir le périmètre du SMSI en fixant ses limites et son applicabilité. Le périmètre doit être disponible sous forme d’information documentée.

4.4 Système de management de la sécurité de l’information

L'organisme doit établir, mettre en œuvre, maintenir et améliorer continuellement un système de management de la sécurité de l'information.

PECB

Leadership

ISO/IEC 27001, article 5

5.1 Leadership et engagement	• La direction doit veiller à ce que la politique et les objectifs de sécurité de l'information soient compatibles avec l'orientation stratégique de l'organisme. • La direction doit intégrer les exigences du SMSI dans les processus opérationnels de l'organisme, déterminer les ressources nécessaires au SMSI et communiquer l'importance d'un SMSI efficace.
5.2 Politique	• La direction doit établir une politique de sécurité de l'information qui est communiquée à toutes les parties intéressées et disponible sous forme d'information documentée. • La politique doit être alignée sur la finalité de l'organisme et doit inclure les objectifs de sécurité de l'information, un engagement à remplir les exigences de sécurité de l'information et un engagement d'amélioration continue.
5.3 Rôles, responsabilités et autorités au sein de l'organisation	• La direction doit attribuer les rôles et responsabilités de sécurité de l'information afin de garantir que le SMSI est conforme aux exigences d'ISO/IEC 27001.

Planification

ISO/IEC 27001, article 6

6.1

Actions liées aux risques et opportunités

L'organisme doit établir les risques et les opportunités d'atteindre les résultats escomptés, de prévenir ou de réduire les effets indésirables et de parvenir à une amélioration continue. L'organisme doit également planifier des actions pour faire face aux risques et aux opportunités, mettre en œuvre ces actions et évaluer leur efficacité.

6.1.2

Appréciation des risques de sécurité de l'information

L'organisme doit établir et maintenir des critères de risque, identifier, analyser et évaluer les risques, et s'assurer que le processus d'appréciation des risques génère des résultats cohérents, valables et comparables.

6.1.3

Traitement des risques de sécurité de l'information

L'organisme doit sélectionner les options de traitement des risques, déterminer les mesures nécessaires pour mettre en œuvre les options de traitement des risques, comparer les mesures sélectionnées, produire une déclaration d'applicabilité, formuler un plan de traitement des risques et obtenir l'approbation du plan de traitement des risques.

6.2

Objectifs de sécurité de l'information et plans pour les atteindre

Les objectifs de l'organisme doivent être mesurables et conformes à la politique de sécurité de l'information. Ils doivent également tenir compte des exigences et des résultats de l'appréciation et du traitement des risques. Ces objectifs doivent être communiqués et mis à jour de manière appropriée.

PECB

Support

ISO/IEC 27001, article 7

7.1 Ressources	7.2 Compétence	7.3 Sensibilisation	7.4 Communication	7.5 Informations documentées
L'organisme doit identifier et fournir les ressources nécessaires au projet de SMSI.	L'organisme doit veiller à ce que des personnes compétentes soient affectées aux tâches du SMSI.	L'organisme doit veiller à ce que ses employés soient conscients de la politique de sécurité de l'information, de leur rôle dans le SMSI et des conséquences de non-conformité aux exigences.	L'organisme doit établir des modalités de communication avec les parties intéressées internes et externes pertinentes.	L'organisme doit conserver les informations documentées requises par ISO/IEC 27001 afin de démontrer l'efficacité du SMSI.

Fonctionnement

ISO/IEC 27001, article 8

8.1 Planification et contrôle opérationnels	L'organisme doit planifier, mettre en œuvre et contrôler les processus nécessaires pour se conformer aux exigences de sécurité de l'information. L'organisme doit également mettre en œuvre des plans pour atteindre les objectifs, contrôler les changements prévus et revoir les changements, et contrôler les processus externalisés.
8.2 Appréciation des risques de sécurité de l'information	L'organisme doit procéder à des appréciations des risques de sécurité de l'information à des intervalles planifiés.
8.3 Traitement des risques de sécurité de l'information	L'organisme doit mettre en œuvre le plan de traitement des risques de sécurité de l'information.

PECB

Évaluation des performances

ISO/IEC 27001, article 9

9.1

Surveillance, mesures, analyse et évaluation

L'organisme doit évaluer la performance et l'efficacité du SMSI.

9.2

Audit interne

L'organisme doit effectuer des audits internes à des intervalles planifiés afin de valider l'efficacité du SMSI.

9.3

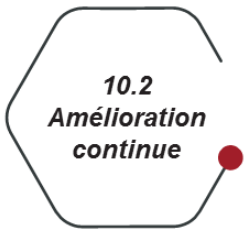
Revue de direction

La direction doit procéder à des revues du SMSI à des intervalles planifiés afin de s'assurer de son adéquation, de sa pertinence et de son efficacité.

Amélioration

ISO/IEC 27001, article 10

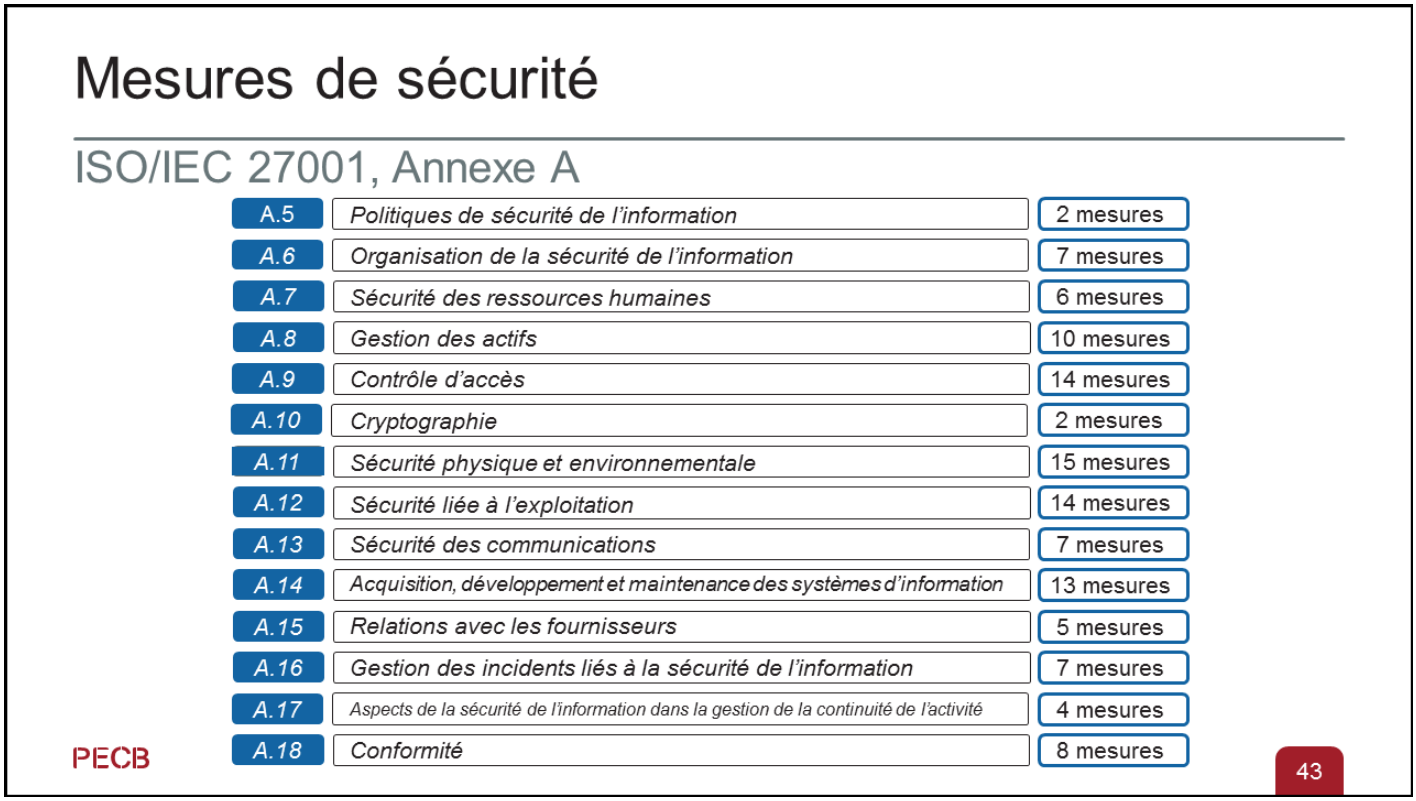
L'organisme doit prendre les mesures appropriées lorsqu'une non-conformité se produit. Il doit évaluer et mettre en œuvre ces actions, examiner leur efficacité et, si nécessaire, apporter des modifications au SMSI.



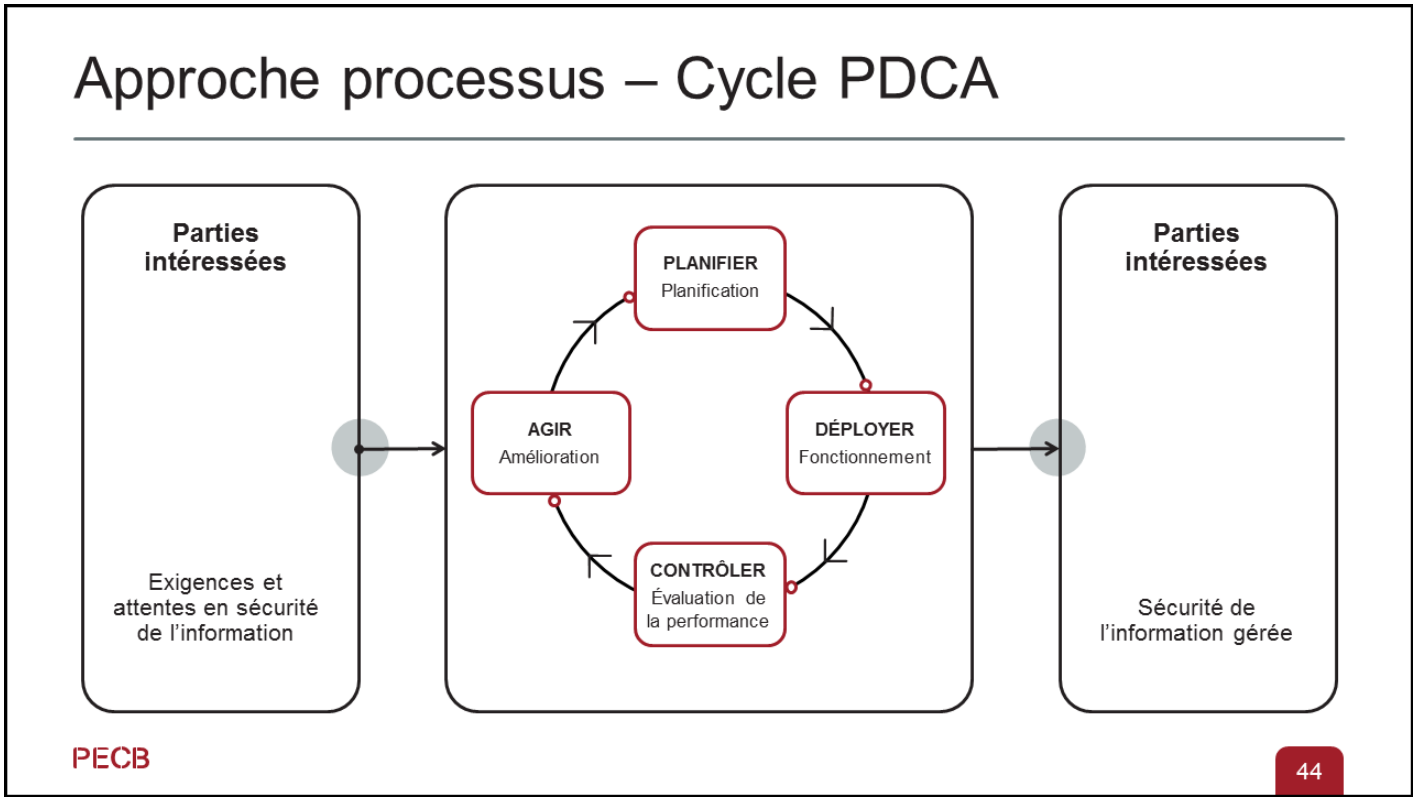
L'organisme doit continuellement améliorer la pertinence, l'adéquation et l'efficacité du système de management de la sécurité de l'information.

Annexe A

- L'annexe A fait partie d'ISO/IEC 27001 et comprend 114 mesures qui doivent être prises en compte pour se conformer à la norme.
- La liste des objectifs et des mesures de sécurité de l'annexe A n'est pas exhaustive. L'organisme peut ajouter des mesures supplémentaires provenant d'autres sources, si nécessaire.
- Si une certaine mesure n'est pas mise en œuvre, l'organisme doit fournir une justification acceptable de son exclusion.



Les objectifs et les mesures de sécurité de l'information énumérés dans l'annexe A (A.5 à A.18) d'ISO/IEC 27001 sont appuyés par les lignes directrices d'ISO/IEC 27002.



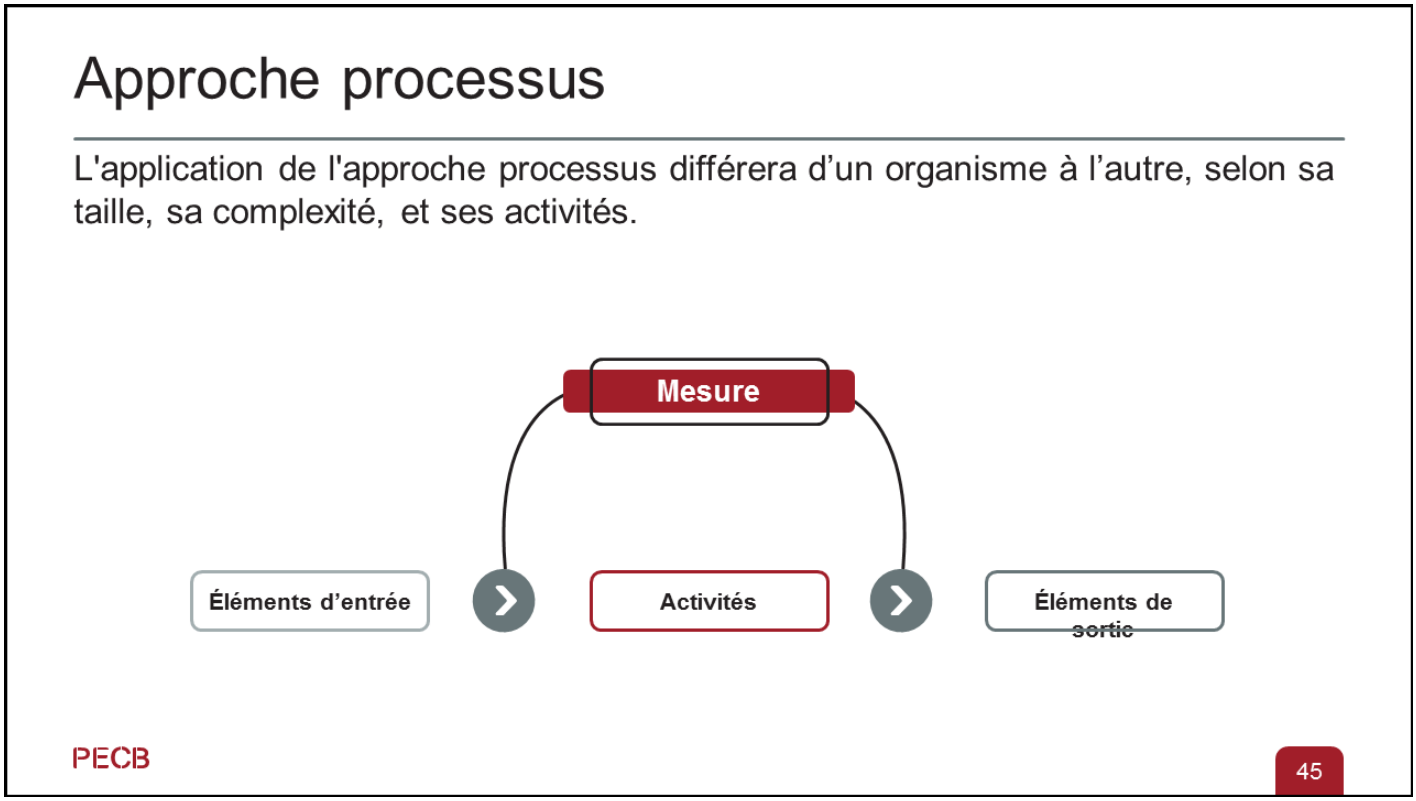
ISO/IEC 27001 adopte le modèle de processus «Planifier-Déployer-Contrôler-Agir» (PDCA), également connu sous le nom de roue de Deming. Le modèle est appliqué à la structure de tous les processus d'un système de management de la sécurité de l'information. La figure illustre la façon dont un système de management utilise comme éléments d'entrée les exigences et les attentes des parties intéressées et comment il produit, par les actions et processus nécessaires, les résultats de sécurité de l'information qui satisfont aux exigences et aux attentes des parties intéressées.

Planifier (établissement du système de management): Établir la politique, les objectifs, les processus et les procédures relatifs à la gestion des risques et à l'amélioration de la sécurité de l'information de manière à fournir des résultats conformes aux politiques et aux objectifs globaux de l'organisme.

Déployer (mise en œuvre et exploitation du système de management): Mettre en œuvre et exploiter la politique, les mesures de sécurité, les processus et les procédures du système de management de la sécurité de l'information.

Contrôler (surveillance et revue du système de management): Évaluer et, le cas échéant, mesurer les performances du processus par rapport à la politique et aux objectifs, et communiquer les résultats à la direction pour revue.

Agir (maintenance et amélioration du système de management): Entreprendre des actions correctives et préventives sur la base des résultats de l'audit interne, de la revue de direction ou d'autres informations pertinentes afin d'améliorer continuellement le système de management de la sécurité de l'information

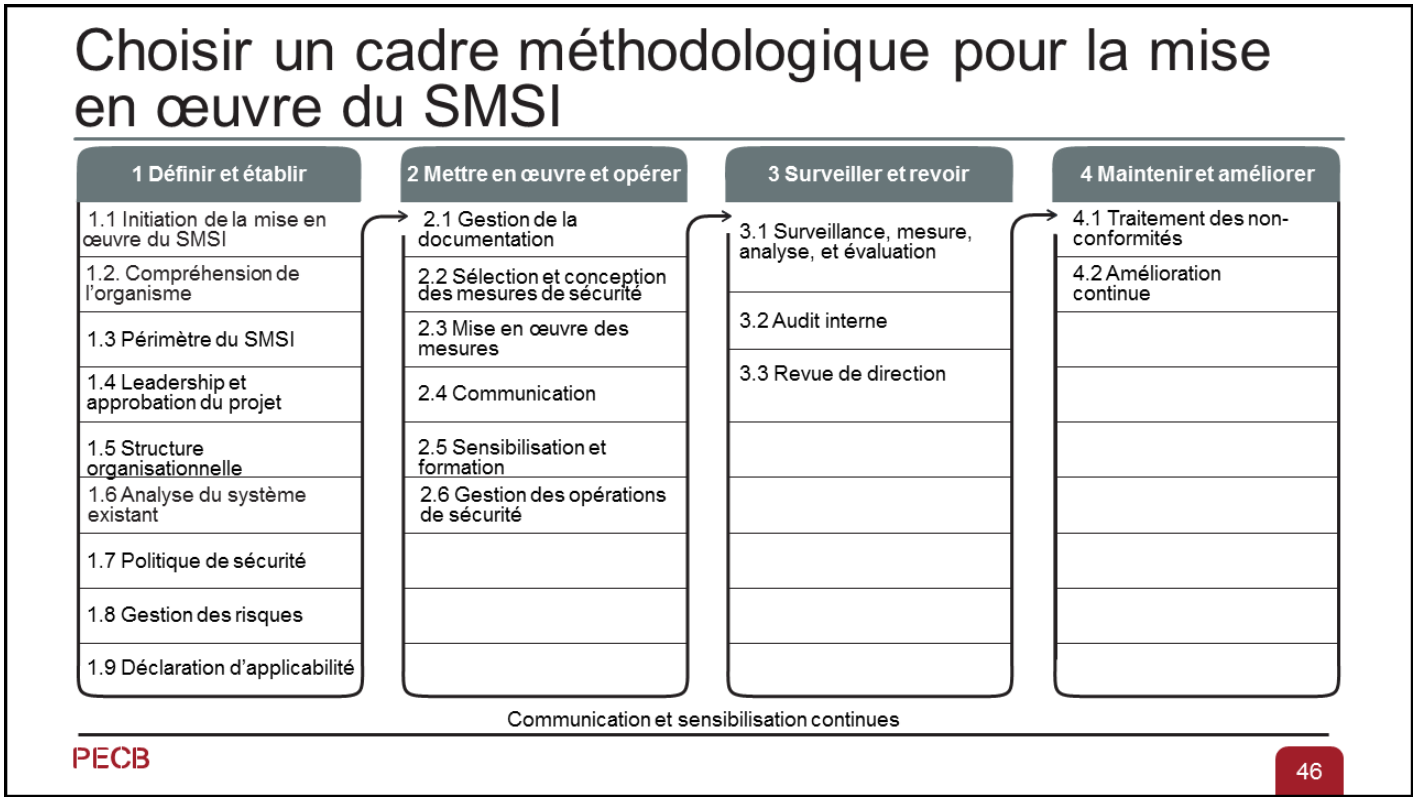


On peut définir un processus comme étant un ensemble de tâches interdépendantes et exécutées pour atteindre un objectif défini. Il s'agit d'une séquence d'activités structurées et mesurées visant à créer un produit ou un service dans un but précis, généralement pour un secteur de marché ou un client particulier.

Pour qu'un organisme fonctionne de manière efficace, il doit mettre en œuvre et gérer de nombreux processus corrélés. Souvent, l'élément de sortie d'un processus forme directement l'élément d'entrée du processus suivant. L'identification et la gestion ordonnée des processus au sein d'un organisme, en particulier les interactions de ces processus, est appelée «l'approche processus».

Les mesures de sécurité servent à s'assurer que les processus d'affaires sont effectués de manière sécurisée en termes de traitement d'informations. Ces processus et mesures de sécurité dépendent des processus d'affaires car ils s'y intègrent. Par exemple, les mesures de sécurité relatives aux ressources humaines devraient s'intégrer aux processus existants de gestion des ressources humaines. Cela permettra aux processus de management des ressources humaines d'être plus fiables en s'assurant que:

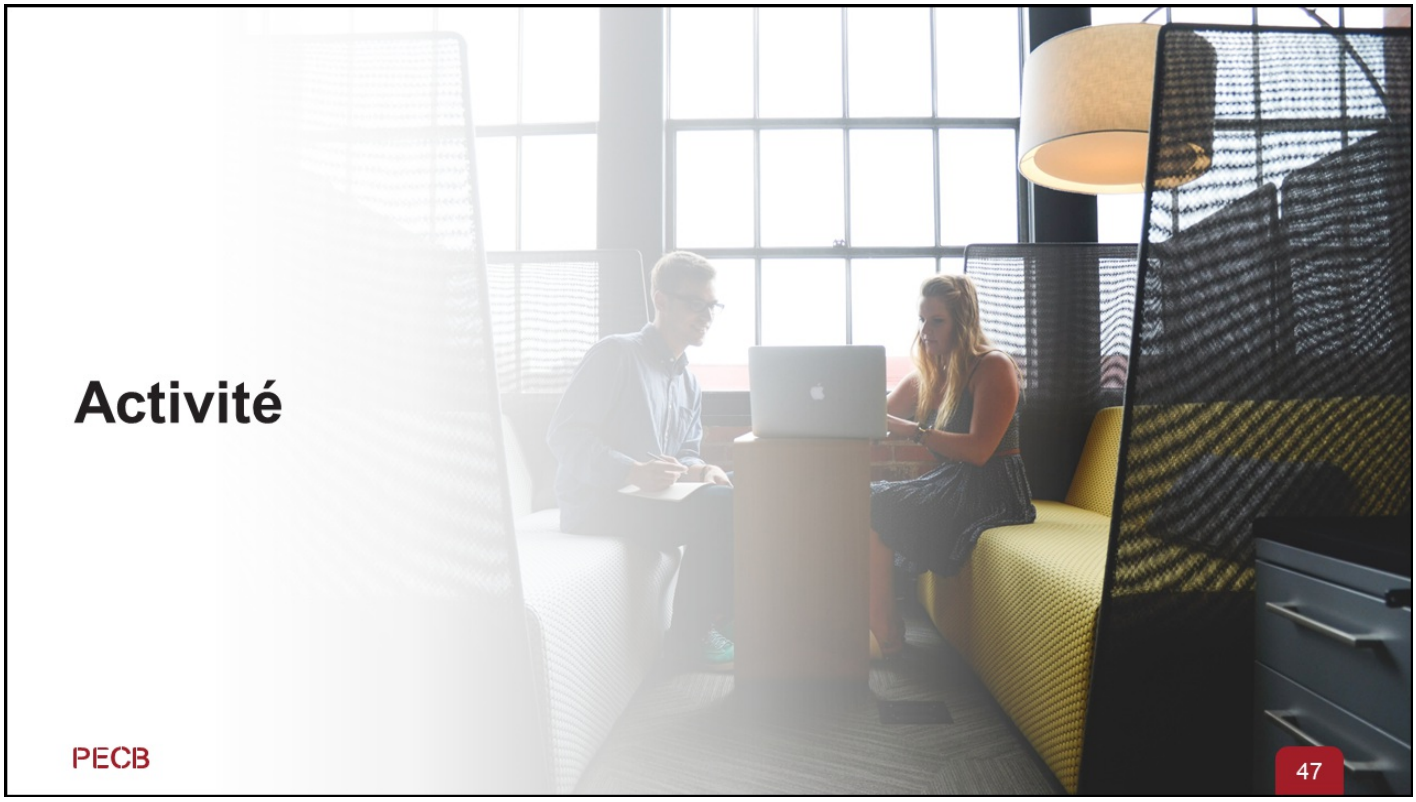
- Les responsabilités de chacun en termes de sécurité de l'information sont clairement définies
- Une vérification des antécédents des postulants est effectuée selon la criticité des informations qu'ils devront traiter
- L'organisme définit un processus disciplinaire formel en cas de brèche de la sécurité de l'information
- L'organisme définit un processus formel de retrait des droits d'accès des utilisateurs lors de la fin de contrat



En suivant une méthodologie structurée et efficace, un organisme s'assure de couvrir les exigences minimales pour la mise en œuvre d'un système de management.

Note importante:

1. La méthodologie présentée dans la diapositive n'est pas destinée à être utilisée de manière stricte ; chaque organisme doit l'adapter à son contexte d'affaires (exigences, taille, périmètre, objectifs, etc.).
2. La séquence des différentes étapes peut être changée (interversion, fusion, etc.). Par exemple, établir la procédure de gestion de la documentation peut être effectuée avant la compréhension de l'organisme.
3. De nombreux processus sont itératifs en raison de la nécessité d'un développement continu tout au long du projet de mise en œuvre (par exemple, la communication et la sensibilisation).



Questions de discussion

1. Comment un système de management peut-il aider un organisme ?
2. Qu'est-ce qu'un système de management de la sécurité de l'information (SMSI) et quels sont ses avantages?
3. Qu'est-ce que l'annexe A d'ISO/IEC 27001 et en quoi consiste-t-elle ?

La présente section fournit des informations qui aideront le participant à acquérir des connaissances sur les principes et concepts fondamentaux de la sécurité de l'information tels que la confidentialité, l'intégrité, la disponibilité, la vulnérabilité, la menace, l'impact, le risque et les mesures de sécurité de l'information, l'intelligence artificielle (IA), et l'informatique en nuage.

Information et actifs

ISO 9000, article 3.8.2 et ISO 55000, article 3.2.1

***Information** : données porteuses de sens*

***Actif** : item, chose ou entité qui a une valeur potentielle ou réelle pour un organisme*

Il existe plusieurs types d'actifs, par exemple :

- Information
- Logiciel, comme un programme d'ordinateur
- Actifs physiques, comme les ordinateurs
- Services
- Personnes et leurs qualifications et compétences
- Actifs intangibles, comme la réputation et l'image

PECB

50

ISO/IEC 27000, article 3.35 Système d'information

ensemble d'applications, services, actifs informationnels ou autres composants permettant de gérer l'information

ISO/IEC 27001, Annexe A.8 définit les objectifs et mesures de sécurité liés à la gestion des actifs.

ISO/IEC 27001, AnnexeA.8.1 Responsabilités relatives aux actifs

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

ISO/IEC 27001, AnnexeA.8.1.1 Inventaire des actifs

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

ISO/IEC 27001, AnnexeA.8.1.2 Propriété des actifs

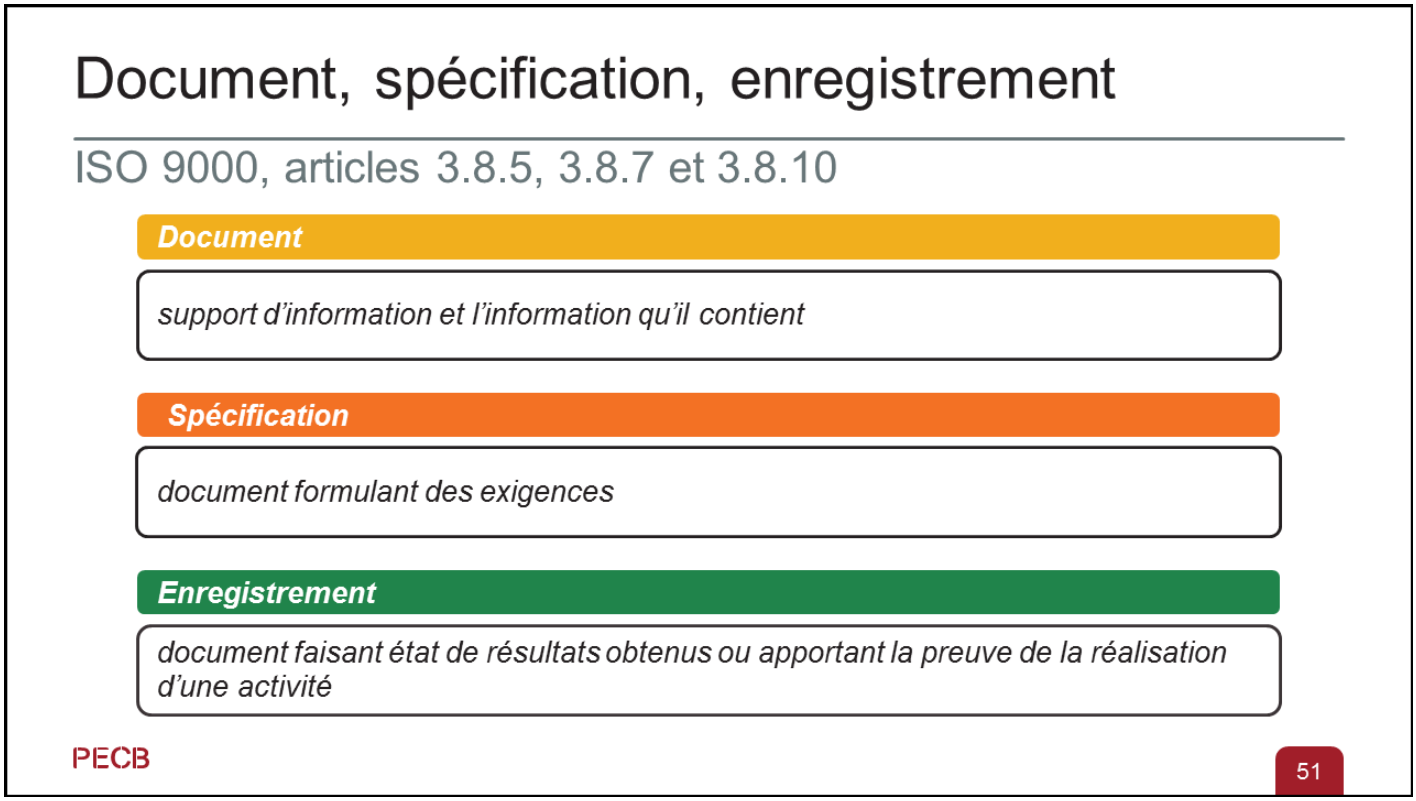
***Mesure :** Les actifs figurant à l'inventaire doivent être attribués à un propriétaire.*

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

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

ISO/IEC 27001, AnnexeA.8.1.4 Restitution des actifs

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



ISO9000, article3.8.5 Document (suite)

EXAMPLE [sic]: Enregistrement, spécification, document de procédure, plan, rapport, norme.

Note1 à l'article: Le support peut être papier, magnétique, électronique ou optique, photographie ou échantillon étalon, ou une combinaison de ceux-ci.

Note2 à l'article: Un ensemble de documents, par exemple spécifications et enregistrements, est couramment appelé « documentation ».

Il est important de faire la différence entre les documents et les enregistrements. Dans les dictionnaires, un enregistrement est un type de document, mais dans la terminologie d'ISO, ce sont des concepts distincts. Un enregistrement est le résultat d'un processus ou d'un contrôle. Par exemple :

1. Une procédure d'audit est un document. La mise en œuvre de cette procédure (c.-à-d. l'exécution d'un audit) génère un rapport d'audit et ces rapports d'audit deviennent des enregistrements.
2. Un processus documenté pour les revues de direction est un document. Ce processus génère des enregistrements tels que les procès-verbaux des revues de direction.
3. Une procédure documentée pour l'amélioration continue est un document. Le formulaire d'une action corrective classée est un enregistrement.

Sécurité de l'information

- La sécurité de l'information détermine quelles informations doivent être protégées, la raison pour laquelle elles doivent l'être, comment les protéger et de quoi il faut les protéger.
- L'objectif de la sécurité de l'information est de réduire les risques et l'impact sur les actifs de l'organisme.
- La sécurité de l'information s'applique à tout type d'information, qu'elle soit numérique, papier, électronique ou verbale.

PECB

52

ISO/IEC27002, article 0.2 Exigences liées à la sécurité de l'information

Une organisation doit impérativement identifier ses exigences en matière de sécurité. Ces exigences proviennent de trois sources principales:

a. *l'appréciation du risque propre à l'organisation, prenant en compte sa stratégie et ses objectifs généraux. L'appréciation du risque permet d'identifier les menaces pesant sur les actifs, d'analyser les vulnérabilités, de mesurer la vraisemblance des attaques et d'en évaluer l'impact potentiel;*
b. *les exigences légales, statutaires, réglementaires et contractuelles auxquelles l'organisation et ses partenaires commerciaux, contractants et prestataires de service, doivent répondre ainsi que leur environnement socioculturel;*
c. *l'ensemble de principes, d'objectifs et d'exigences métier en matière de manipulation, de traitement, de stockage, de communication et d'archivage de l'information que l'organisation s'est constitué pour mener à bien ses activités.*

Il est nécessaire de confronter les ressources mobilisées par la mise en œuvre des mesures avec les dommages susceptibles de résulter de défaillances de la sécurité en l'absence de ces mesures. Les résultats d'une appréciation du risque permettent de définir les actions de gestion appropriées et les priorités en matière de gestion des risques liés à la sécurité de l'information, ainsi que de mettre en œuvre les mesures identifiées destinées à contrer ces risques.

La norme ISO/IEC 27005 fournit des lignes directrices de gestion du risque lié à la sécurité de l'information, y compris des conseils sur l'appréciation du risque, le traitement du risque, l'acceptation du risque, la communication relative au risque, la surveillance du risque et la revue du risque.

Page de notes

PECB 53

Autres définitions liées à la sécurité de l'information :

ISO/IEC27000, article 3.27 Moyens de traitement de l'information

tout système, service ou infrastructure de traitement de l'information, ou le local les abritant

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

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

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

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

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

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

ISO/IEC 27000, article 3.35 Système d'information

ensemble d'applications, services, actifs informationnels ou autres composants permettant de gérer l'information

ISO/IEC 27000, article 3.48 Non-répudiation

capacité à prouver l'occurrence d'un événement ou d'une action donnée(e) et des entités qui en sont à l'origine

ISO/IEC 27000, article 3.55 Fiabilité

propriété relative à un comportement et à des résultats prévus et cohérents

L'Annexe A inclut des objectifs relatifs à la classification de l'information:

ISO/IEC 27001, AnnexeA.8.2 Classification de l'information

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

ISO/IEC 27001, AnnexeA.8.2.1 Classification des informations

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

ISO/IEC 27001, AnnexeA.8.2.2 Marquage des informations

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

ISO/IEC 27001, AnnexeA.8.2.3 Manipulation des actifs

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

Confidentialité

ISO/IEC 27000, article 3.10

Confidentialité

propriété selon laquelle l'information n'est pas diffusée ni divulguée à des personnes, des entités ou des processus non autorisés

La confidentialité exige que seuls les utilisateurs autorisés aient accès aux données sensibles et protégées.

Certaines des pratiques utilisées pour assurer la confidentialité sont les suivantes :

- Processus d'authentification, qui requiert un identifiant et un mot de passe lors du traitement de données confidentielles ;
- Méthodes de sécurité pour assurer l'autorisation du visiteur ;
- Contrôles d'accès qui prévoient des restrictions à l'accès au réseau en fonction des rôles et responsabilités de l'employé.

PECB

54

Exemple:

Les données personnelles d'employés salariés ne doivent être accessibles qu'au personnel autorisé du département des ressources humaines.

Plusieurs types de contrôles d'accès peuvent assurer la confidentialité de l'information. L'authentification est une méthode permettant de contrôler l'accès. Les contrôles d'accès peuvent être :

- Physique (par exemple, serrures sur les portes, classeurs verrouillables, coffres-forts)
- Numérique (par exemple, contrôles d'accès au réseau interne, contrôles d'accès à distance, contrôles d'accès au Web)

Intégrité

ISO/IEC 27000, article 3.36

Intégrité

propriété d'exactitude et de complétude

Intégrité :

- Veille à ce que les informations ne soient pas modifiées lorsqu'elles sont stockées ou en cours de transfert.
- Veille à ce que seules les modifications autorisées soient apportées.
- S'assure que les données sont exactes, authentiques et protégées contre tout accès non autorisé, afin que les utilisateurs puissent se fier à la justesse de l'information lors du traitement.

PECB

55

Intégrité: Les données doivent être complètes et intactes.

Exemple:

Les données comptables doivent être authentiques, complètes et exactes. L'exactitude des informations est assurée en évitant toute modification injustifiée de ces informations.

De nombreux dispositifs manipulant des données, y compris les lecteurs de disques et autres supports ainsi que les systèmes de télécommunications, contiennent des dispositifs de vérification automatique de l'intégrité des données. Les contrôles d'intégrité des données sont essentiels dans les systèmes d'exploitation, les logiciels et les applications. Ils permettent d'éviter la corruption intentionnelle ou involontaire des programmes et des données.

L'intégrité doit être protégée sous trois angles :

- Empêcher un utilisateur autorisé de faire une erreur et de changer les données
- Empêcher un utilisateur non autorisé d'apporter des modifications
- Empêcher tout programme ou application qui interagit directement avec l'information cible d'effectuer des changements non autorisés

Les données précédemment enregistrées doivent rester inchangées pendant le transport des données.

Les données peuvent subir des changements pour plusieurs raisons:

- Érosion du stockage
- Erreurs naturelles ou intentionnelles
- Dommages au système

Disponibilité

ISO/IEC 27000, article 3.7

Disponibilité

propriété d'être accessible et utilisable à la demande par une entité autorisée

La disponibilité de l'information signifie que l'information est accessible :

- comme requis
- quand c'est requis
- là où c'est requis
- pour qui c'est requis

Les responsables de la sécurité de l'information font face à trois défis habituels :

- Déni de service (DoS) à la suite d'attaques intentionnelles (p. ex. lorsqu'un programmeur n'est pas au courant d'un défaut qui pourrait endommager le logiciel en raison d'une entrée spécifique et inattendue)
- Perte des capacités de protection des systèmes d'information en raison de catastrophes naturelles ou d'activités humaines
- Pannes d'équipement

PECB

56

Disponibilité: L'information doit être facilement accessible aux individus qui en ont besoin.

Exemple:

Les données relatives aux clients doivent être accessibles au service du marketing.

En pratique, la disponibilité de l'information exige un système de contrôle comme la sauvegarde des données, la planification de la capacité, les procédures et les critères d'approbation des systèmes, les procédures de gestion des incidents, la gestion des médias amovibles, les procédures de traitement de l'information, l'entretien et le test des équipements, les procédures du concept de la continuité, de même que les procédures pour contrôler l'utilisation des systèmes.

Vulnérabilité

ISO/IEC 27000, article 3.77

Vulnérabilité

faille dans un actif ou dans une mesure de sécurité qui peut être exploitée par une ou plusieurs menaces

- Les vulnérabilités qui n'ont pas de menace correspondante peuvent ne pas nécessiter de mesure, mais doivent être reconnues et surveillées pour détecter les changements.
- Les mesures de sécurité qui fonctionnent mal ou qui sont mal mises en œuvre pourraient devenir des vulnérabilités.

PECB

57

L'appréciation des vulnérabilités peut être compliquée par une perception erronée courante selon laquelle les vulnérabilités sont associées à des caractéristiques négatives. Plusieurs vulnérabilités présentent vraiment des caractéristiques négatives, comme un système d'information où les correctifs (*patchs*) ne sont pas à jour.

Parfois, certaines vulnérabilités peuvent être acceptées au nom des résultats positifs associés au risque que nous prenons. Par exemple, l'achat d'ordinateurs portables au lieu d'ordinateurs de bureau peut augmenter les risques de vol mais aussi améliorer la mobilité des travailleurs.

Les vulnérabilités peuvent être classées en intrinsèques et extrinsèques. Les vulnérabilités intrinsèques sont liées aux caractéristiques de l'actif. Les vulnérabilités extrinsèques, quant à elles, sont les facteurs externes qui peuvent avoir un impact sur l'information.

Exemple:

Un serveur situé dans une zone sujette aux inondations saisonnières est considéré comme une vulnérabilité extrinsèque. L'incapacité d'un serveur à traiter des données est considérée comme une vulnérabilité intrinsèque.

Types de vulnérabilités

ISO/IEC 27005, Annexe D.1

Type	Exemples de vulnérabilités
Matériel informatique	*Maintenance insuffisante/mauvaise installation des supports de stockage*
	Absence de programmes de remplacement périodique
Logiciel	*Tests de logiciel absents ou insuffisants*
	Interface utilisateur compliquée
Réseau	*Voies de communication non protégées*
	Point de défaillance unique
Personnel	*Formation insuffisante à la sécurité*
	Travail non surveillé d'une équipe extérieure ou de l'équipe d'entretien
Site	*Réseau électrique instable*
	Emplacement situé dans une zone sujette aux inondations
Organisme	*Absence de bonne attribution des responsabilités en sécurité de l'information*
	Absence de responsabilités en sécurité de l'information dans les descriptions de postes

PECB

58

L'Annexe D d'ISO/IEC 27005 fournit une typologie pour la classification des vulnérabilités que nous pourrions utiliser, en principe. Cependant, cette liste des vulnérabilités doit être utilisée avec prudence, car elle n'est pas exhaustive. De nouvelles vulnérabilités se produisent régulièrement à cause, entre autres, de l'évolution et des changements dans la technologie.

On devrait utiliser l'annexe D comme guide ou comme rappel pour aider à organiser et à structurer la collecte des données pertinentes sur les vulnérabilités plutôt qu'une liste de contrôles à suivre aveuglément.

Menace

ISO/IEC 27000, article 3.74 et ISO/IEC 27005, article 8.2.3

Menace

cause potentielle d'un incident indésirable, qui peut nuire à un système ou à un organisme

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

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

Il convient d'identifier les sources de menace à la fois accidentelles et délibérées.

PECB

59

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

Une menace peut survenir de l'intérieur ou de l'extérieur de l'organisme. Il convient aussi d'identifier les menaces de manière générique et par type (à titre d'exemples: des actions non autorisées, des dommages physiques, des défaillances techniques) puis, lorsque cela est pertinent, des menaces individuelles particulières peuvent être identifiées au sein d'une classe générique. Cela signifie qu'aucune menace n'est négligée, même une menace imprévue, mais que le volume de travail requis reste limité.

Par définition, une menace est susceptible de nuire à des actifs comme l'information, les processus et les systèmes et, par conséquent, à l'organisme. Les menaces sont associées à l'aspect négatif du risque et, à ce titre, font référence à des événements indésirables.

Types de menaces

ISO/IEC 27005, Annexe C

Type	Menaces
Dommage physique	Incendie
	Dégât des eaux
Catastrophes naturelles	Phénomène volcanique
	Inondation
Perte de services essentiels	Panne du système de climatisation ou d'alimentation en eau
	Perte de la source d'alimentation en électricité
Perturbation due à des rayonnements	Rayonnements électromagnétiques
	Rayonnements thermiques
Compromission d'informations	Piégeage de matériel
	Vol de supports ou de documents
Défaillances techniques	Panne de matériel
	Dysfonctionnement du logiciel
Actions non autorisées	Utilisation non autorisée du matériel
	Corruption de données
Compromission des fonctions	Erreur d'utilisation
	Abus de droits

PECB

60

L'Annexe C d'ISO/IEC 27005 fournit une typologie pour la classification des menaces. Comme la liste des vulnérabilités, la liste des menaces n'est pas exhaustive. De nouvelles menaces apparaissent régulièrement en raison des tendances technologiques et de l'évolution des capacités des agents de menace.

On doit utiliser l'Annexe C comme guide ou comme liste de contrôle pour aider à organiser et à structurer la collecte et le tri des données pertinentes sur les menaces plutôt que comme liste de contrôle à suivre aveuglément.

Relation entre vulnérabilité et menace

Exemples

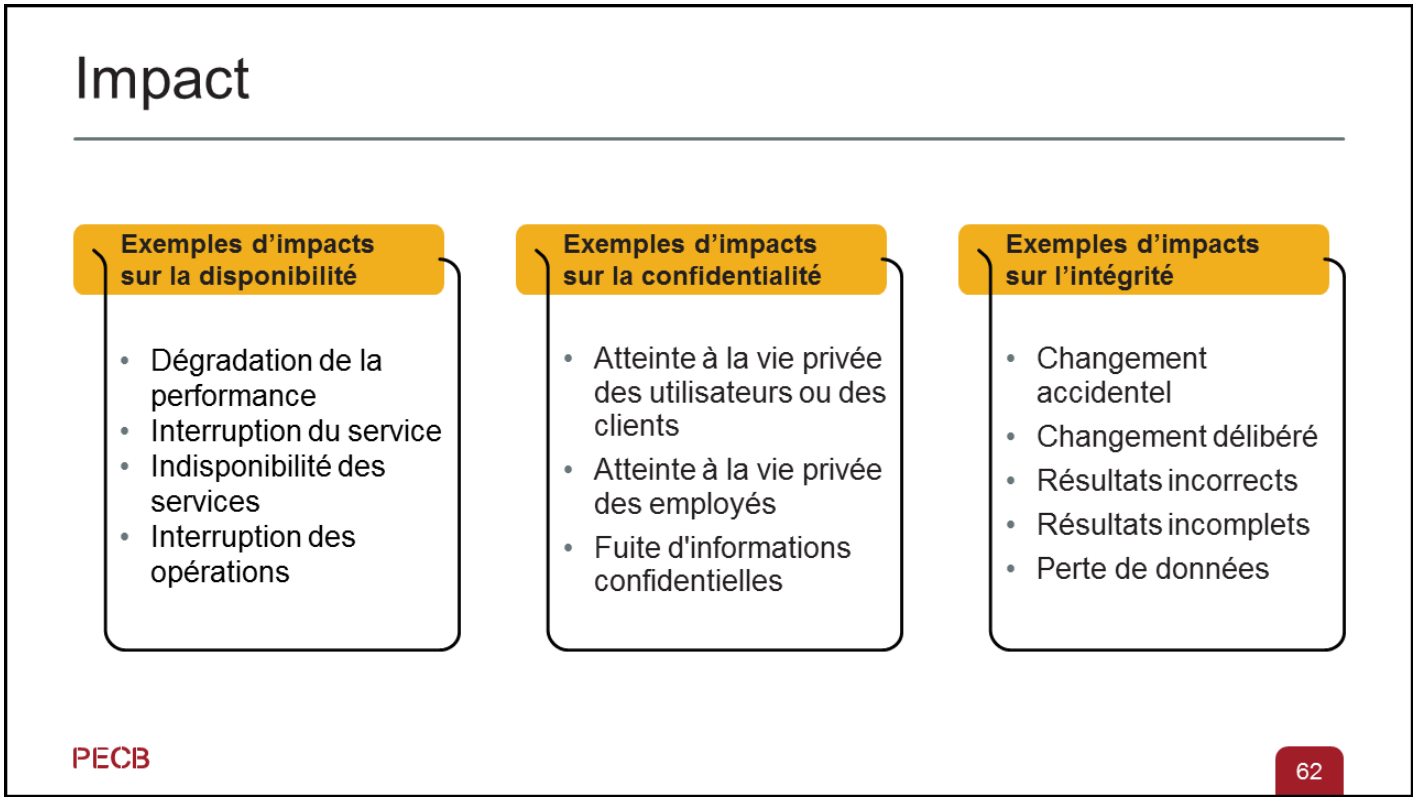
Vulnérabilités	Menaces
Entrepôt non protégé et sans surveillance	Vol
Procédures compliquées de traitement des données	Erreur d'entrée des données par le personnel
Pas de séparation des tâches	Fraude, utilisation non autorisée d'un système
Données non chiffrées	Vol de données
Utilisation de logiciels piratés	Poursuite judiciaire, virus
Pas de revue des droits d'accès	Accès non autorisé par des personnes qui ont quitté l'organisme
Pas de procédures de sauvegarde	Perte d'information

PECB

61

En soi, la présence d'une vulnérabilité ne produit pas de dommage ; une menace doit exister pour l'exploiter. Une vulnérabilité qui ne correspond pas à une menace ne requiert pas d'installer une mesure de sécurité, mais elle doit être identifiée et surveillée en cas de changements.

La mise en œuvre incorrecte, la mauvaise utilisation ou la défaillance d'une mesure pourrait, en soi, représenter une menace.



Voici une liste de plusieurs impacts potentiels (voir ISO/IEC 27005, AnnexeB.2) qui peuvent affecter la disponibilité, l'intégrité, la confidentialité ou une combinaison de celles-ci:

1. Pertes financières
2. Pertes d'actifs ou de leur valeur
3. Perte de clients et fournisseurs
4. Procédures et peines judiciaires
5. Perte d'avantage concurrentiel
6. Perte d'avantage technologique
7. Baisse de l'efficience ou de l'efficacité
8. Atteinte à la vie privée des utilisateurs ou des clients
9. Interruption du service
10. Incapacité à fournir le service
11. Perte d'image de marque ou de réputation
12. Interruption des opérations
13. Perturbation des opérations des tiers (fournisseurs, clients, etc.)
14. Incapacité de remplir les obligations légales
15. Incapacité de remplir les obligations contractuelles
16. Mise en danger de la sécurité du personnel ou des utilisateurs

Risque lié à la sécurité de l'information

ISO/IEC 27000, article 3.61

- *Note 4 à l'article: Un risque est souvent exprimé en termes de combinaison des conséquences d'un événement (incluant des changements de circonstances) et de sa « vraisemblance ».*
- *Note 5 à l'article: Dans le contexte des systèmes de management de la sécurité de l'information, les risques liés à la sécurité de l'information peuvent être exprimés comme l'effet de l'incertitude sur les objectifs de sécurité de l'information.*
- *Note 6 à l'article: Le risque lié à la sécurité de l'information est associé à la possibilité que des menaces exploitent les vulnérabilités d'un actif ou d'un groupe d'actifs informationnels et nuisent donc à un organisme.*

PECB

63

ISO/IEC 27000, article 3.57 Risque résiduel

risque subsistant après le traitement du risque

Note1 à l'article: Un risque résiduel peut inclure un risque non identifié.

Note2 à l'article: Un risque résiduel peut également être appelé «risque conservé».

ISO/IEC 27000, article 3.61 Risque

effet de l'incertitude sur les objectifs

Note1 à l'article: Un effet est un écart, positif ou négatif, par rapport à une attente.

Note2 à l'article: L'incertitude est l'état, même partiel, de défaut d'information concernant la compréhension ou la connaissance d'un événement, de ses conséquences ou de sa vraisemblance.

Note3 à l'article: Un risque est souvent caractérisé en référence à des «événements» potentiels et des «conséquences» potentielles, ou à une combinaison des deux.

ISO/IEC 27000, article 3.62 Acceptation du risque

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

Note1 à l'article: L'acceptation du risque peut avoir lieu sans traitement du risque ou lors du processus de traitement du risque.

Note2 à l'article: Les risques acceptés font l'objet d'une surveillance et d'une revue.

ISO/IEC 27000, article 3.63 Analyse du risque

processus mis en œuvre pour comprendre la nature d'un risque et pour déterminer le niveau de risque

Note1 à l'article: L'analyse du risque fournit la base de l'évaluation du risque et des décisions relatives au traitement du risque.

Note2 à l’article: L'analyse du risque inclut l'estimation du risque.

ISO/IEC 27000, article 3.64 Appréciation du risque

ensemble du processus d'identification du risque, d'analyse du risque et d'évaluation du risque

Page de notes

PECB

64

ISO/IEC 27000, article 3.66 Critères de risque

termes de référence vis-à-vis desquels l'importance d'un risque est évaluée

Note1 à l'article: Les critères de risque sont fondés sur les objectifs de l'organisme et sur le contexte externe et le contexte interne.

Note2 à l'article: Les critères de risque peuvent être issus de normes, de lois, de politiques et d'autres exigences.

ISO/IEC 27000, article 3.67 Évaluation du risque

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

Note1 à l'article: L'évaluation du risque aide à la prise de décision relative au traitement du risque

ISO/IEC 27000, article 3.68 Identification des risques

processus de recherche, de reconnaissance et de description des risques

Note1 à l'article: L'identification du risque comprend l'identification des sources de risque, des événements, de leurs causes et de leurs conséquences potentielles.

Note2 à l'article: L'identification du risque peut faire appel à des données historiques, des analyses théoriques et des avis d'experts et autres personnes compétentes, et tenir compte des besoins des parties prenantes.

ISO/IEC 27000, article 3.69 Gestion des risques

activités coordonnées visant à diriger et contrôler un organisme vis-à-vis du risque

ISO/IEC 27000, article 3.70 Processus de management du risque

application systématique de politiques, procédures et pratiques de management aux activités de communication, de concertation, d'établissement du contexte, ainsi qu'aux activités d'identification, d'analyse, d'évaluation, de traitement, de surveillance et de revue des risques

Note1 à l'article: L'ISO/IEC 27005 emploie le terme « processus » pour décrire le management du risque dans sa globalité. Les éléments qui composent le processus de management du risque sont appelés « activités ».

ISO/IEC 27000, article 3.71 Propriétaire du risque

personne ou entité ayant la responsabilité du risque et ayant autorité pour le gérer

ISO/IEC 27000, article 3.72 Traitement du risque

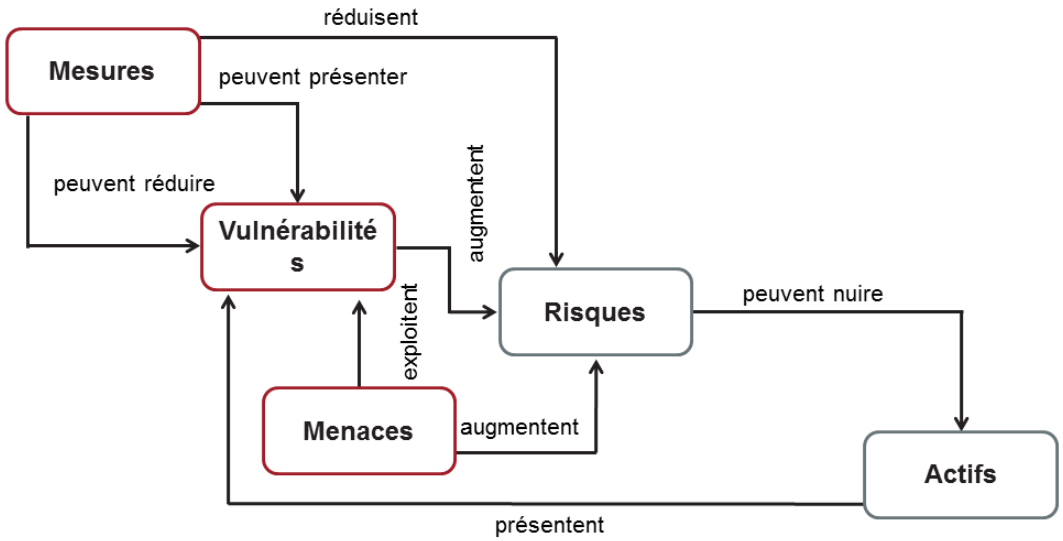
processus destiné à modifier un risque

Note1 à l'article: Le traitement des risques peut inclure:

- *un refus du risque en décidant de ne pas démarrer ni poursuivre l'activité porteuse du risque;*
- *la prise ou l'augmentation d'un risque afin de saisir une opportunité,*
- *l'élimination de la source de risque;*
- *une modification de la vraisemblance;*
- *une modification des conséquences;*
- *un partage du risque avec une ou plusieurs autres parties (incluant des contrats et un financement du risque);*
- *un maintien du risque fondé sur un choix argumenté.*

Relations entre les éléments de sécurité de l'information

Vue d'ensemble



PECB

65

1. Les actifs et les mesures peuvent présenter des vulnérabilités qui pourraient être exploitées par des menaces.
2. La combinaison des menaces et des vulnérabilités peut augmenter l'effet potentiel du risque.
3. Les mesures de sécurité permettent de réduire les vulnérabilités. Un organisme a peu d'options pour agir contre les menaces. Par exemple, les mesures de sécurité peuvent être mises en œuvre pour protéger contre les intrusions du système, mais il est impossible pour un organisme de réduire le nombre de pirates sur Internet.

Note: Les descripteurs de relations sont valables pour les deux composantes auxquelles ils s'interconnectent – ils ne sont pas destinés à être lus comme une «histoire» de bout en bout ou à travers une séquence de composantes et de relations.

Intelligence artificielle (IA)

- Le dictionnaire anglais Oxford définit l'intelligence artificielle (IA) comme « la théorie et le développement de systèmes informatiques capables d'exécuter des tâches nécessitant habituellement l'intelligence humaine, telles que la perception visuelle, la reconnaissance vocale, la prise de décision et la traduction entre langages ».
- L'interconnectivité et les transferts de données rapides rendus possibles par l'utilisation de la 5G permettront aux applications d'IA de faire partie intégrante de nos vies.
- Applications communes de l'IA :
  - Banque
  - Marketing
  - Santé
  - Véhicules autonomes

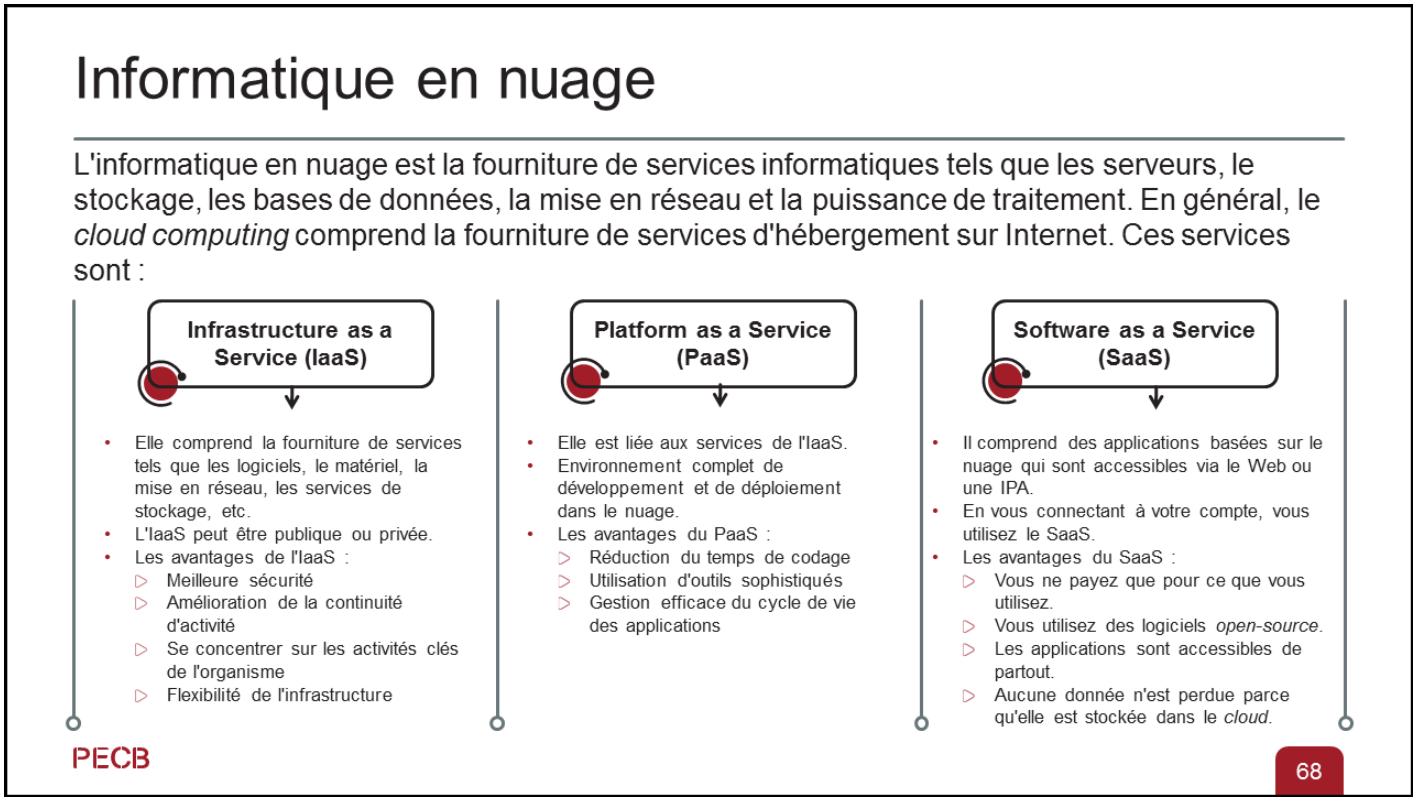
Intelligence artificielle

IA faible et forte

- L'IA faible est également connue sous le nom d'IA étroite.
- L'IA faible se concentre sur une tâche spécifique et surpasse les humains lorsqu'elle effectue des tâches techniques et automatisées. Cependant, lorsqu'une IA faible doit effectuer une tâche qu'elle ne reconnaît pas, elle ne sera pas en mesure de la mener à bien à moins d'être spécifiquement programmée pour le faire.
- L'avantage d'une IA faible est l'automatisation des tâches.
- Parmi les exemples d'IA faible, citons Siri d'Apple, Alexa, AlphaGo, etc.

- L'IA forte est également connue sous le nom d'intelligence artificielle générale (*artificial general intelligence*).
- L'IAF a la capacité de comprendre de nouveaux problèmes et d'en déduire des solutions basées sur des connaissances préalables.
- L'avantage d'une IA forte est la résolution des problèmes.
- Les exemples d'IA forte comprennent l'IA qui peut communiquer en langage naturel, utiliser la pensée critique, etc.

PECB



NIST SP 500-291, chapitre 3

L'informatique en nuage est un modèle permettant un accès réseau omniprésent, pratique et à la demande à un ensemble partagé de ressources informatiques configurables (p. ex. réseaux, serveurs, stockage, applications et services) qui peuvent être rapidement approvisionnées et libérées avec un minimum d'efforts de gestion ou d'interaction avec le fournisseur de services.

Les services d'informatique en nuage fonctionnent différemment selon le fournisseur, mais ils servent tous le même objectif. De nombreux fournisseurs proposent un tableau de bord convivial basé sur un navigateur permettant à tous les professionnels des TI de gérer facilement leurs comptes.

Parmi les avantages de l'informatique en nuage, on peut citer :

- **Réduction des coûts:** L'informatique en nuage réduit le coût nécessaire à la gestion et à la maintenance du système de réseau.
- **Flexibilité :** Le système en nuage donne aux employés une plus grande flexibilité en leur donnant la possibilité d'accéder aux données où qu'ils se trouvent.
- **Sécurité :** L'infonuagique promeut la sécurité de l'information, car les données sont acccessibles quoi qu'il arrive à la machine.
- **Productivité :** L'informatique en nuage supprime de nombreuses tâches telles que la correction des logiciels, le racking and stacking, la configuration du matériel, etc., permettant aux équipes informatiques de consacrer du temps à la réalisation d'objectifs commerciaux plus importants.
- **Fiabilité :** En cas d'incident, si le plan de continuité d'activité de l'organisme comprend des services de sécurité dans le nuage, les données ne seront très probablement pas perdues. Au contraire, elles seront sécurisées dans un endroit sûr.

Note: L'interface de programmation d'application (IPA) permet à différentes applications de communiquer entre elles.

Quiz 1 : Concepts et principes fondamentaux de la sécurité de l'information

1. **En quoi consiste la sécurité de l'information ?**
   A. La protection de la confidentialité, de l'intégrité et de la disponibilité des données physiques uniquement
   B. La protection de la confidentialité, de l'intégrité et de la disponibilité des données confidentielles uniquement
   C. La protection de la confidentialité, de l'intégrité et de la disponibilité de tous les types de données
2. **Lequel des éléments suivants garantit que les informations ne sont pas mises à disposition ou divulguées à des utilisateurs non autorisés ?**
   A. Confidentialité
   B. Intégrité
   C. Disponibilité
3. **Parmi la liste ci-dessous, quels sont les exemples de contrôles d'accès ?**
   A. L'authentification numérique dans les réseaux internes
   B. Coffres-forts, serrures sur les portes et classeurs
   C. Toutes ces réponses
4. **Quelle propriété de la sécurité de l'information garantit que les informations ne sont pas modifiées lorsqu'elles sont stockées ou en transit ?**
   A. Confidentialité
   B. Intégrité
   C. Disponibilité
5. **Quelle attaque n'affecte pas l'intégrité des informations ?**
   A. Déni de service (DoS)
   B. Violation de données
   C. Violation du réseau

6.Parmi les éléments suivants, lequel est défini comme la faiblesse d'un actif ou d'un contrôle qui peut être exploité par une ou plusieurs menaces ?

A. Risque
B. Vulnérabilité
C. Menace

7.Dans quelle catégorie de vulnérabilité se situe le réseau électrique instable ?

A. Vulnérabilité du matériel
B. Vulnérabilité du réseau
C. Vulnérabilité du site

8.Quel type de menace est la perte d'alimentation en électricité ?

A. Perte de services essentiels
B. Perte des services de réseau
C. Perte d'informations causée par des événements naturels

9.Quel type de menace regroupe le vol, la fraude et le sabotage ?

A. Menaces sur les systèmes de services
B. Menaces liées au facteur humain
C. Menaces environnementales

10.Comment un organisme peut-il empêcher la perte de ses informations ?

A. En cryptant les données
B. En sécurisant le réseau
C. En mettant en place des procédures de sauvegarde

Résumé de la section

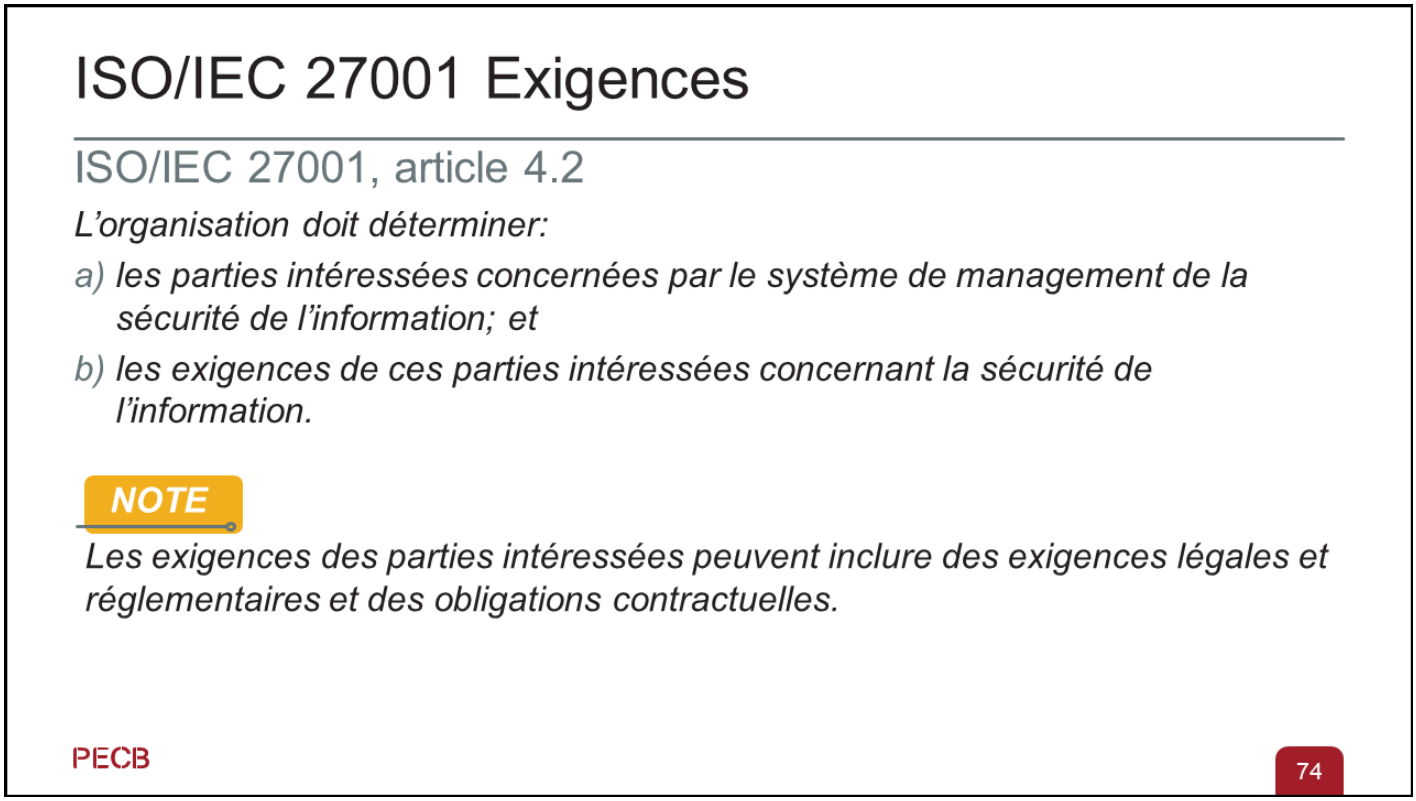
- ISO/IEC 27000 définit la sécurité de l'information comme étant la «protection de la confidentialité, de l'intégrité et de la disponibilité de l'information».
- La confidentialité assure que seuls les utilisateurs autorisés ont accès aux données sensibles et confidentielles.
- L'intégrité assure que les informations ne sont pas modifiées lorsqu'elles sont stockées ou en transit.
- La disponibilité assure que l'information est accessible comme il se doit, quand il se doit, où il se doit et à qui il se doit.
- ISO/IEC 27000 définit la vulnérabilité comme une «faille dans un actif ou dans une mesure de sécurité qui peut être exploitée par une ou plusieurs menaces».
- ISO/IEC 27000 définit la menace comme la «cause potentielle d'un incident indésirable, qui peut nuire à un système ou à un organisme».
- Le risque est exprimé en termes de combinaison des conséquences d'un événement et de la probabilité d'occurrence associée.
- Les applications les plus courantes de l'IA comprennent l'IA dans les domaines bancaires, du marketing, de la santé et des véhicules autonomes.
- Les services d'informatique en nuage comprennent l'infrastructure en tant que service (IaaS), la plate-forme en tant que service (PaaS) et le logiciel en tant que service (SaaS).

Cette section explique l'importance de comprendre le contexte d'un organisme, y compris les objectifs du SMSI et la définition préliminaire de son périmètre, l'environnement interne et externe, les parties intéressées et les exigences opérationnelles.

ISO/IEC 27001 Exigences

ISO/IEC 27001, article 4.1

L'organisation doit déterminer les enjeux externes et internes pertinents compte tenu de sa mission et qui influent sur sa capacité à obtenir le(s) résultat(s) attendu(s) de son système de management de la sécurité de l'information.



Définitions reliées au concept de l'organisme

ISO9000, article3.2.1 Organisme

personne ou groupe de personnes ayant un rôle avec les responsabilités, l'autorité et les relations lui permettant d'atteindre ses objectifs

ISO9000, article3.5.2 Infrastructure

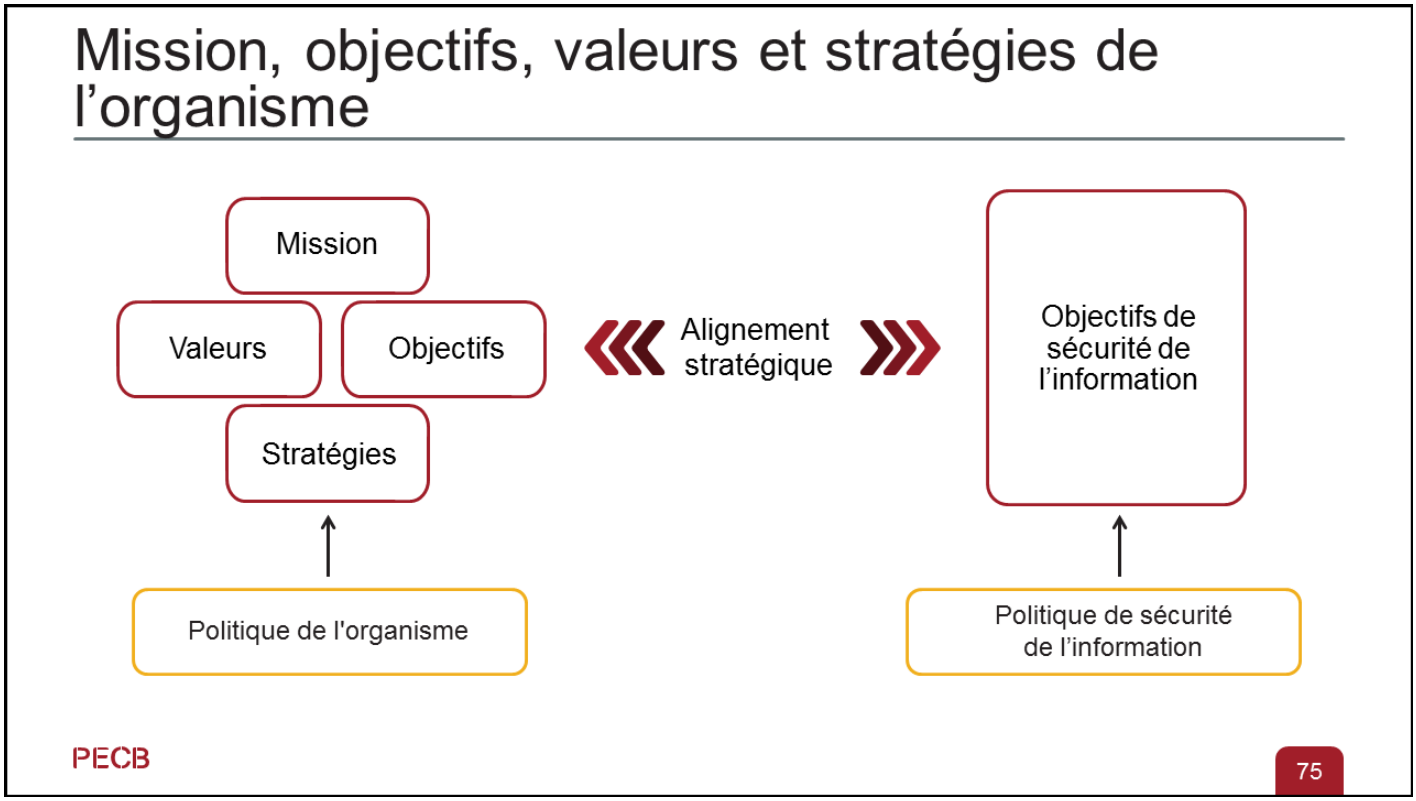
système des installations, équipements et services nécessaires au fonctionnement d'un organisme

ISO9000, article3.6.4 Exigence

besoin ou attente formulé, généralement implicite ou obligatoire

Note de terminologie:

1. Un organisme est un ensemble structuré et habituellement enregistré auprès d'une instance gouvernementale. Cela peut être, par exemple: une compagnie, une institution, une œuvre de bienfaisance, une association ou une combinaison de ceux-ci. Une organisation peut être publique ou privée.
2. Cela dit, l'utilisation du terme «organisation» dans ISO/IEC 27001 peut faire référence à une composante d'une entité enregistrée ou officiellement établie, c'est-à-dire un département, une entité commerciale ou un emplacement géographique spécifique (par exemple un centre informatique, mais non les bureaux administratifs distincts d'une organisation).
3. «Infrastructure» peut être utilisée comme un synonyme d'«actif en support» tel que défini par ISO/IEC 27005.
4. Ne pas confondre l'utilisation du terme «exigence» dans le contexte des spécifications édictées dans une norme et «exigences de l'organisme». Les exigences de l'organisme peuvent provenir de différentes parties intéressées. Elles peuvent être explicites (définies par contrat, par convention, par règlement) ou implicites (non documentées).



Il est nécessaire d'obtenir une vue d'ensemble de l'organisme afin de comprendre les défis en matière de sécurité de l'information auxquels il est confronté et le risque inhérent à ce segment de marché. Cela implique de comprendre la mission, les stratégies, l'objectif principal et les valeurs de l'organisme.

Mission: La mission est ce qui justifie et définit l'existence de l'organisme. Elle sert de point de référence pour que tout le monde sache où va l'organisme.

Valeurs: Les valeurs sont les convictions fondamentales et durables qui sont partagées par les membres d'un organisme et qui influencent le comportement des individus.

Objectifs : Les objectifs sont le résultat que l'organisme veut atteindre.

Stratégies: La stratégie consiste en une séquence définie d'actions visant à atteindre un ou plusieurs objectifs.

L'organisme doit s'assurer que les objectifs stratégiques de sécurité de l'information et la mission de l'organisme sont bien alignés.

Objectifs du SMSI

Les objectifs du SMSI sont nécessaires à la détermination du périmètre et devront être validés au plus haut niveau de l'organisme. Par exemple :

- Assurer la conformité aux exigences légales, réglementaires et contractuelles
- Faire preuve de diligence raisonnable
- Inspirer confiance aux parties intéressées
- Protéger les actifs essentiels de l'organisme
- Assurer la sécurité des informations en suivant les bonnes pratiques
- Améliorer la réponse aux incidents de sécurité de l'information
- Réduire les coûts liés aux incidents de sécurité de l'information
- Faciliter la continuité d'activité

PECB

76

ISO/IEC 27001, article 6.2 Objectifs de sécurité de l'information et plans pour les atteindre

L'organisation doit établir, aux fonctions et niveaux concernés, des objectifs de sécurité de l'information.

Les objectifs de sécurité de l'information doivent:

a. *être cohérents avec la politique de sécurité de l'information;*
b. *être mesurables (si possible);*
c. *tenir compte des exigences applicables à la sécurité de l'information, et des résultats de l'appréciation et du traitement des risques;*
d. *être communiqués; et*
e. *être mis à jour quand cela est approprié.*

L'organisation doit conserver des informations documentées sur les objectifs liés à la sécurité de l'information.

Lorsqu'elle planifie la façon d'atteindre ses objectifs de sécurité de l'information, l'organisation doit déterminer:

f.ce qui sera fait;
g.les ressources qui seront nécessaires;
h.qui sera responsable;
i.les échéances; et
j.la façon dont les résultats seront évalués.

Détermination du périmètre préliminaire

ISO/IEC 27003, article 4.3

L'organisme détermine les limites et l'applicabilité du SMSI pour établir son domaine d'application.

Les facteurs suivants peuvent influer sur la détermination du domaine d'application :

a) les enjeux externes et internes auxquels il est fait référence en 4.1;
b) les parties intéressées et leurs exigences qui sont déterminées conformément à ISO/IEC 27001:2013, 4,2;
c) l'état de préparation des activités commerciales à inclure dans la couverture du SMSI;
d) toutes les fonctions de soutien, c.-à-d. les fonctions qui sont nécessaires pour soutenir ces activités commerciales (p. ex. la gestion des ressources humaines, les services de TI et les applications logicielles, la gestion des installations des immeubles, des zones physiques, des services essentiels et des services publics); et
e) toutes les fonctions qui sont externalisées, soit à d'autres parties de l'organisme, soit à des fournisseurs indépendants.

PECB

77

Pour établir le périmètre d'un SMSI, un organisme doit déterminer le périmètre préliminaire, le périmètre affiné et le périmètre final, puis l'approuver.

Environnement interne et externe

Avis pratique

- Étant donné qu'ISO/IEC 27001 n'offre aucune approche pratique pour analyser le contexte d'un organisme, l'organisme est libre de choisir les outils qu'il juge les plus appropriées.
- Plusieurs méthodologies existent pour comprendre le fonctionnement d'un organisme.
- L'important est d'identifier les caractéristiques des facteurs internes et externes qui influenceront le système de management de la sécurité de l'information : mission, principales activités, parties intéressées, etc.

PECB

78

Il existe plusieurs modèles qui ont été développés pour analyser et comprendre le contexte stratégique d'un organisme. Il faut noter que cette étape ne doit pas devenir un projet en soi. Dans la plupart des organismes, des études ont été menées en interne ou auprès d'autres organismes sur leur positionnement stratégique. Il convient simplement de recueillir ces études, de les analyser et d'interviewer quelques acteurs clés pour s'assurer d'une bonne compréhension de l'organisme.

Parmi les modèles fréquemment utilisés figurent l'analyse SWOT (Strengths, Weaknesses, Opportunities, and Threats), l'analyse PEST (Political, Economic, Social, and Technological) et l'analyse des cinq forces de Porter.

Environnement interne et externe

Structure organisationnelle et acteurs principaux

Comprendre les structures et les acteurs principaux de l'organisme liés au périmètre au plan :

- Stratégique (Qui définit les orientations stratégiques ?)
- Du pilotage (Qui coordonne et gère les opérations ?)
- Opérationnel (Qui est impliqué dans les activités de production et de soutien ?)

PECB

79

Dans l'analyse de l'environnement interne, il est nécessaire d'identifier les structures regroupant les différents acteurs et les relations entre eux (hiérarchiques et fonctionnelles). Il s'agit notamment de la séparation des tâches, des responsabilités et des pouvoirs au sein de l'organisme. Il convient également d'identifier les fonctions externalisées aux sous-traitants.

L'organigramme est un excellent outil à utiliser pour comprendre l'environnement interne. Il représente, à l'aide d'un schéma, la structure de l'organisme. Cette représentation met en évidence les liens de subordination et de délégation d'autorité, mais aussi les dépendances. Même si le graphique montre qu'il n'existe pas d'autorité formelle, les flux d'informations peuvent être déduits de ces liens.

Principaux processus et activités

Actifs

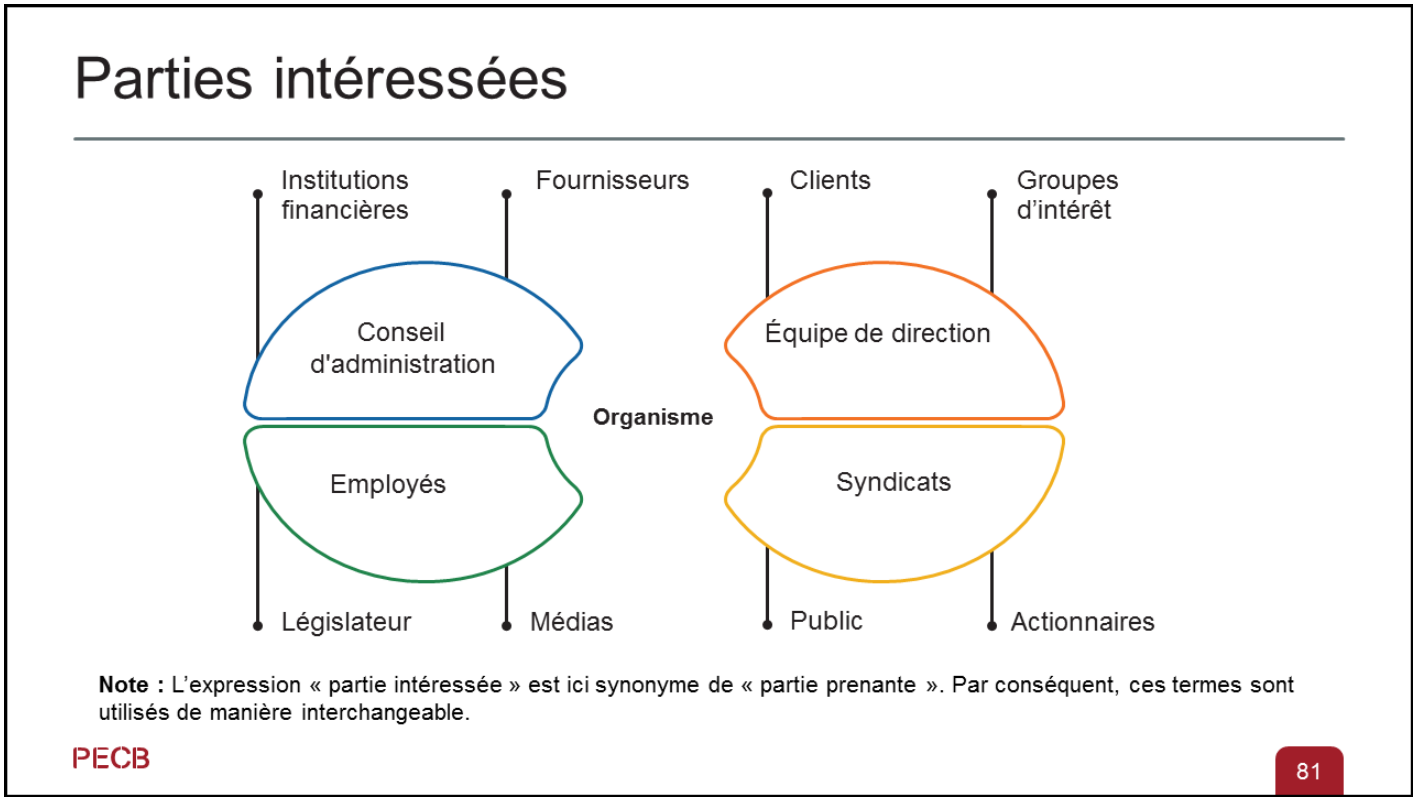
Quels sont les principaux actifs de l'organisme ?

Activités de l'organisme

Quels sont les biens et les services produits par l'organisme ?

Processus opérationnels

Quels sont les principaux processus qui permettent à l'organisme de réaliser sa mission ?



Définitions

ISO 9000, article 3.2.3 Partie intéressée

Partie prenante

personne ou organisme qui peut soit influer sur une décision ou une activité, soit être influencée ou s'estimer influencée par une décision ou une activité

Exemple : Clients, propriétaires, personnel d'un organisme, prestataires, établissements financiers, autorités réglementaires, syndicats, partenaires ou société qui peut inclure des concurrents ou des groupes de pression d'opposition.

Note1 à l'article: Il s'agit de l'un des termes communs et définitions de base pour les normes de systèmes de management de l'ISO, donnés dans l'Annexe SL du Supplément ISO consolidé aux Directives ISO/IEC, Partie 1. La définition initiale a été modifiée par l'ajout de l'Exemple.

ISO 9000, article 3.2.4 Client

personne ou organisme qui est susceptible de recevoir ou qui reçoit un produit ou un service destiné à, ou demandé par, cette personne ou cet organisme

Exemple : Consommateur, utilisateur final, détaillant, destinataire d'un produit ou service issu d'un processus interne, bénéficiaire et acheteur.

Note1 à l'article: Le client peut être interne ou externe à l'organisme.

ISO 9000, article 3.2.5. Prestataire

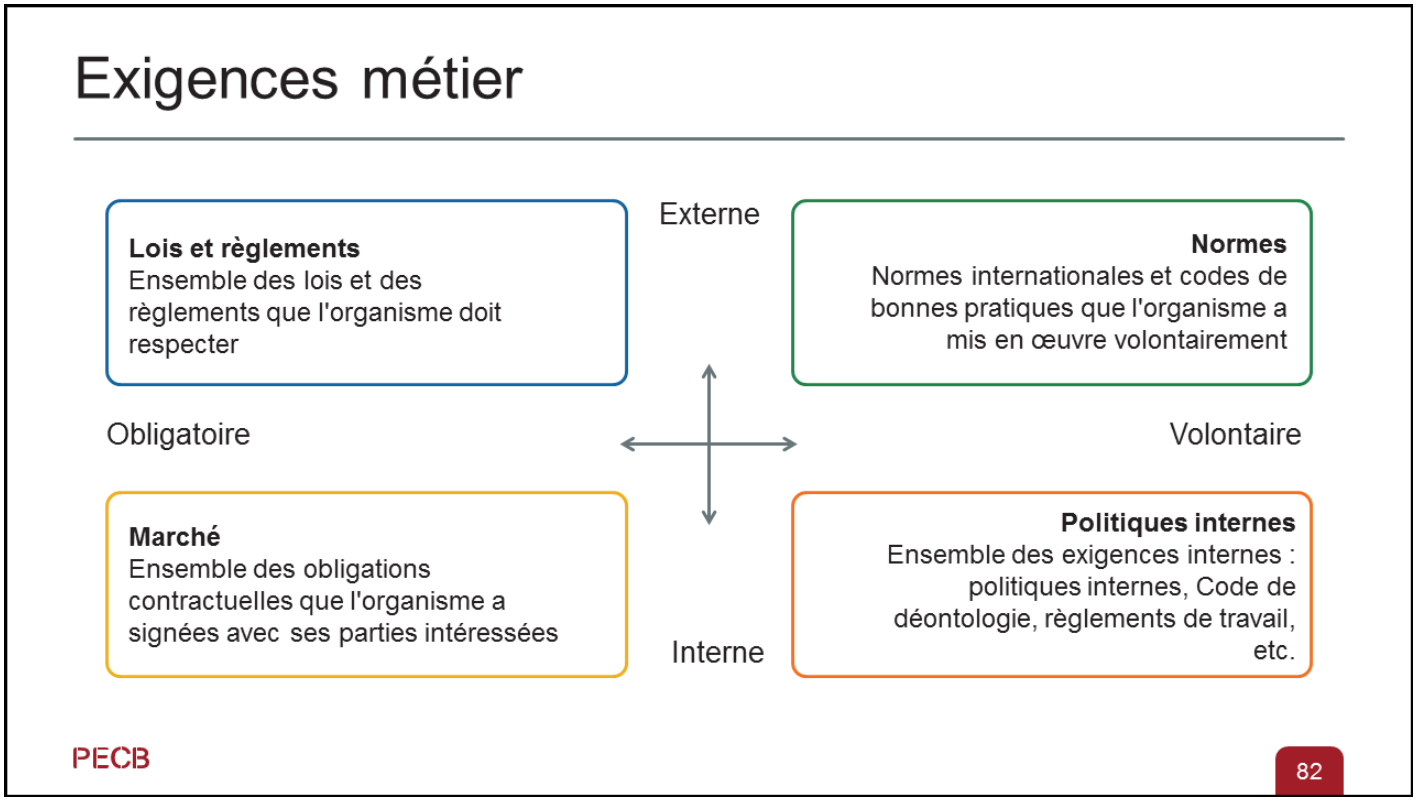
Fournisseur

organisme qui procure un produit ou un service

Exemple : Producteur, distributeur, détaillant ou marchand d'un produit ou d'un service.

Note1 à l'article: Un prestataire peut être interne ou externe à l'organisme.

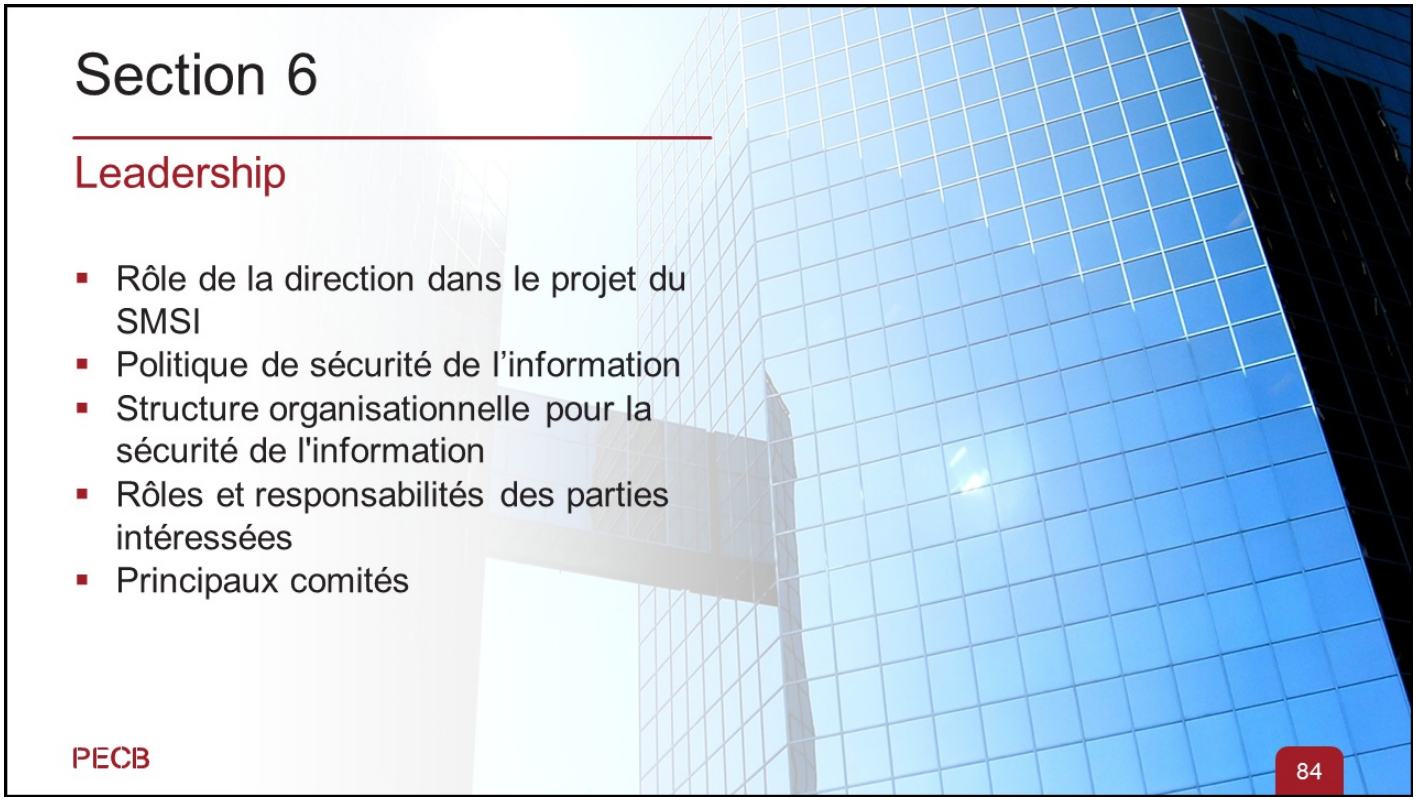
Note2 à l'article: Dans une situation contractuelle, le prestataire peut être appelé « contractant ».



L'organisme doit tenir compte des exigences commerciales, légales ou réglementaires, de même que des obligations contractuelles avec différentes parties intéressées. Pour y parvenir, il est important d'identifier et de prendre en compte l'ensemble des exigences de l'organisme qui pourraient influencer les orientations de mise en œuvre du SMSI. Enfin, ces exigences doivent être incluses dans le processus d'appréciation des risques dans le cadre duquel le risque de non-conformité est analysé.

Résumé de la section

- Le SMSI devrait être bien aligné sur la mission, les objectifs et les stratégies commerciales de l'organisme.
- Les objectifs du SMSI sont essentiels pour déterminer le périmètre.
- L'important est d'identifier les caractéristiques des facteurs internes et externes qui influenceront le système de management de la sécurité de l'information : mission, principales activités, parties intéressées, etc.



Cette section fournit des informations sur la politique de sécurité de l'information, les rôles et responsabilités des parties intéressées et des principaux comités, et la structure organisationnelle de la sécurité de l'information.

ISO/IEC 27001 Exigences

ISO/IEC 27001, article 5.1

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

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

Leadership et compétence

ISO/IEC 27021, article 5.2

ISO/IEC 27001:2013 article/sous-article (le cas échéant)	5 Leadership
Résultats escomptés:	*Diriger, motiver et encourager le personnel à l'échelle de l'organisme à assurer la sécurité de l'information*
Connaissances requises	*— Théories du leadership* *— Techniques de négociation*
Compétences requises	*— Définir et orienter la sécurité de l'information à l'échelle de l'organisme* *— Fournir des lignes directrices, fixer des objectifs et stimuler le progrès au sein de la fonction de sécurité de l'information, de l'équipe et de l'organisme* *— Respecter les engagements* *— Déployer les responsabilités et les autorités aux différents niveaux de l'organisme*

PECB

86

La direction de l'organisation devrait créer un environnement au sein duquel tous les acteurs sont totalement impliqués et dans lequel le SMSI peut agir efficacement en synergie avec les objectifs de l'organisme.

Le rôle de la direction de l'organisme dans la sécurité de l'information implique :

a. Établir les lignes directrices et les objectifs
b. Promouvoir les politiques et les objectifs à tous les niveaux de l'organisme pour augmenter la sensibilisation, la motivation et l'implication
c. S'assurer que les exigences des parties intéressées (clients, partenaires, actionnaires, législateurs, etc.) demeurent une priorité
d. Mettre en œuvre les processus et les mesures appropriés pour faciliter la conformité aux exigences
e. Établir, mettre en œuvre et maintenir un SMSI efficient et efficace
f. Affecter les ressources nécessaires au SMSI
g. S'assurer que des audits internes du SMSI sont réalisés
h. Réaliser la revue de direction au moins une fois l'an
i. Décider des actions concernant la politique et les objectifs
j. Décider des actions visant à améliorer le SMSI

Engagement de la direction

L'engagement de la direction au projet de SMSI peut apporter plusieurs avantages :

- Meilleure connaissance des lois, règlements, obligations contractuelles et normes applicables à la sécurité de l'information
- Allocation optimale des ressources dévolues à la sécurité de l'information
- Identification et protection des actifs critiques
- Surveillance et revue des processus de sécurité de l'information

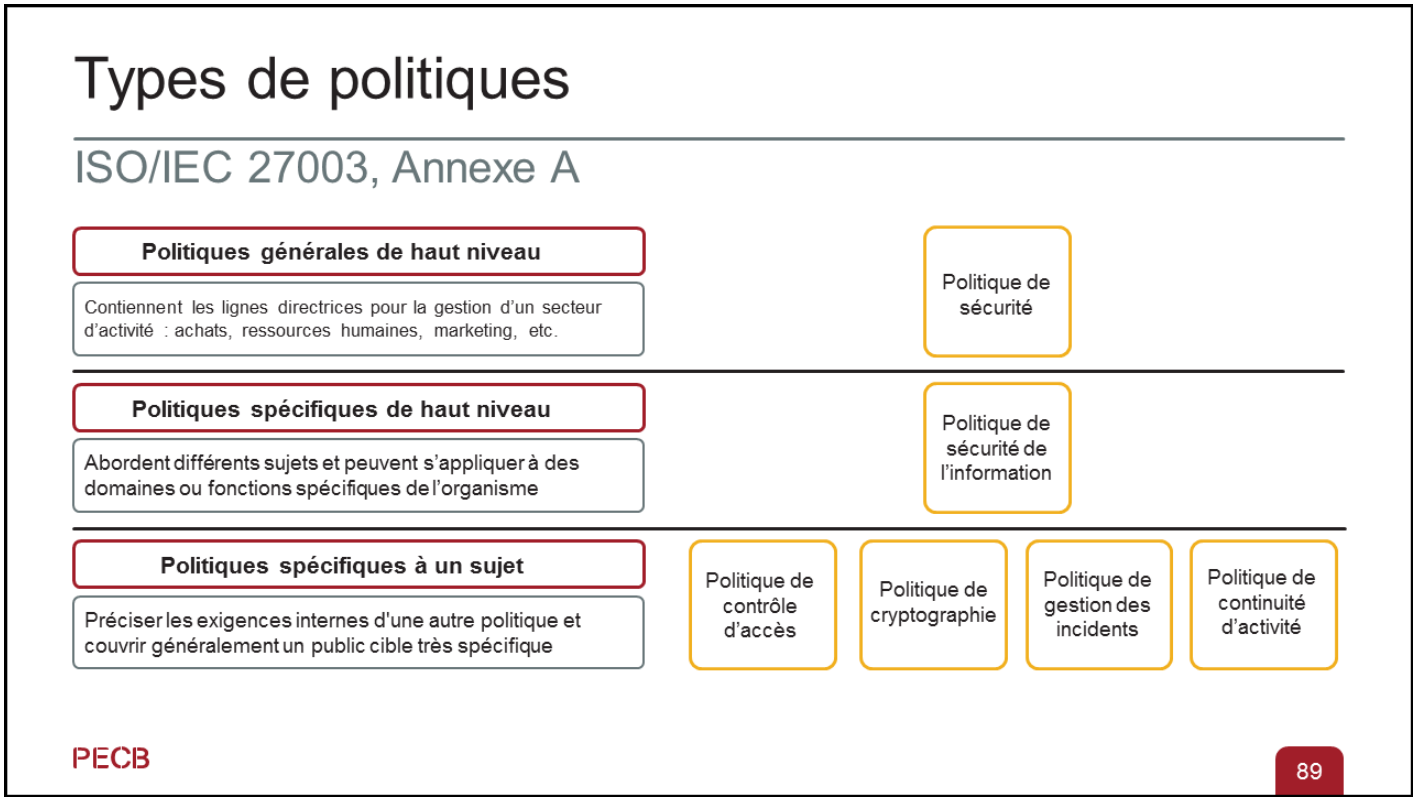
PECB

87

Les déclarations de soutien et d'autorisation de la direction doivent être formellement documentées.

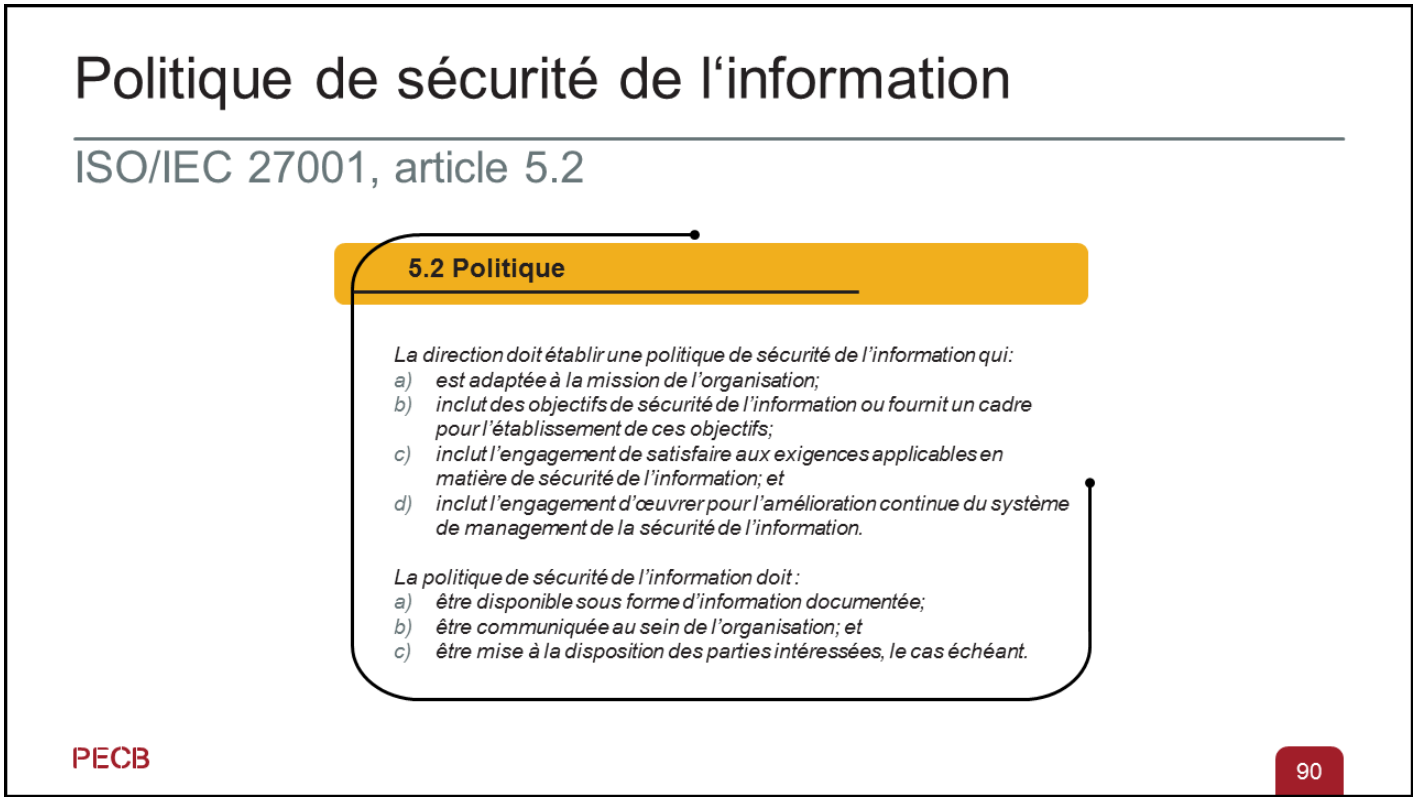
Rôle de la direction dans le projet du SMSI

Objectif	Aligner le SMSI sur les objectifs et la stratégie de l'entreprise
Missions	1. Établir les objectifs et la stratégie du SMSI 2. Valider les rôles et responsabilités des parties prenantes clés du projet 3. Valider les politiques 4. Approuver les critères d'acceptation des risques 5. Approuver le plan de traitement des risques 6. Fournir des ressources adéquates pour la mise en œuvre et la maintenance du SMSI.
Membres	Direction générale (PDG, CIO, VP Finance, etc.)
Fréquence des réunions	Plusieurs réunions correspondant aux jalons importants du projet : rapport de l'analyse de risque, plan de traitement des risques, Déclaration d'applicabilité, revue de direction, etc.



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

1. **Les politiques générales de haut niveau** définissent un cadre général dans lequel la sécurité de l'information sera assurée et les objectifs généraux visant à assurer la continuité de l'activité et à limiter ou prévenir les dommages potentiels aux actifs de l'organisation à un niveau acceptable et, à ce titre, à limiter les conséquences potentielles des incidents de sécurité.
2. **Les politiques spécifiques de haut niveau** définissent un sous-ensemble de règles et de pratiques encore assez générales, mais qui sont relatives à un domaine précis. Elles sont subordonnées aux politiques générales de haut niveau, le plus souvent.
    - **Note:** Ces deux types de politiques sont habituellement soumises à un processus de revue en raison de leur nature sensible par rapport à la stratégie fonctionnelle de l'organisme qu'elles sont censées soutenir.
3. **Les politiques spécifiques à un sujet** sont des politiques qui soutiennent la politique de sécurité de l'information. Elles déterminent la manière de procéder afin d'assurer la sécurité de l'information dans des domaines d'application spécifiques. À titre d'exemples, on peut citer les politiques suivantes : politique de contrôle d'accès, politique d'utilisation de l'internet, politique de cryptographie, etc.
    - **Note :** Certaines de ces politiques spécifiques à un sujet sont indépendantes, tandis que d'autres sont rattachées à et dépendent d'une autre politique. Par exemple, un organisme peut avoir une politique de sécurité (générale) qui est complétée par une politique (spécifique à un sujet) sur la sécurité physique et une autre sur la sécurité de l'information. À son tour, la politique de sécurité de l'information peut être la référence pour la publication de politiques spécifiques telles que la politique sur le contrôle d'accès.



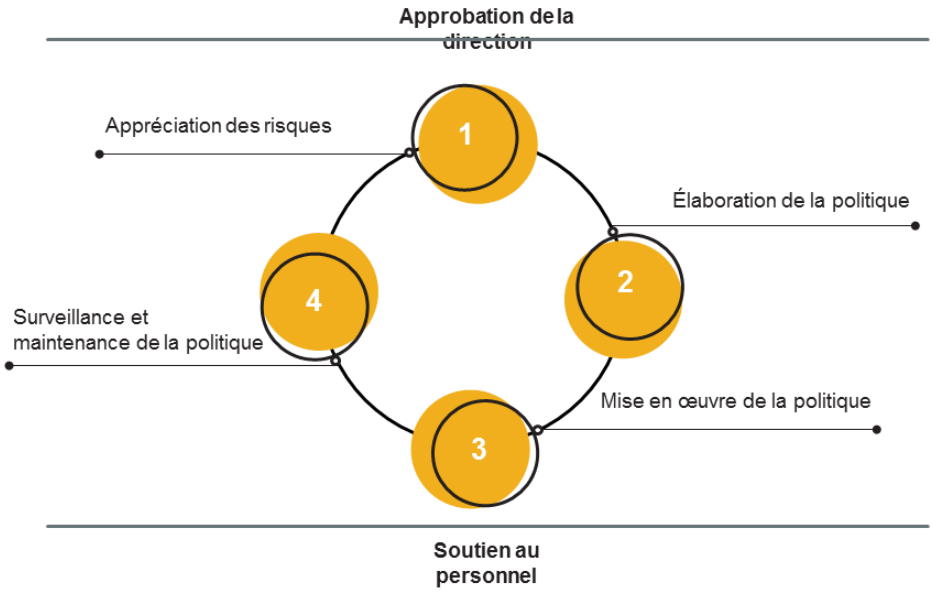
ISO/IEC 27003, article 5.2 Politique

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

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

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

Cycle de vie de l'élaboration de la politique de sécurité de l'information



PECB

91

Le cycle de vie de l'élaboration de la politique est un processus itératif. Il comprend généralement quatre phases: l'appréciation des risques, l'élaboration de la politique, la mise en œuvre de la politique, et le suivi et la maintenance de la politique. L'approbation de la direction et le soutien du personnel sont nécessaires tout au long du cycle de vie.

Il est de la responsabilité de la direction d'approuver les politiques et de les communiquer aux parties intéressées.

ISO/IEC 27001 Exigences

ISO/IEC 27001, article 5.3

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

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

a) *s'assurer que le système de management de la sécurité de l'information est conforme aux exigences de la présente Norme internationale; et*

b) *rendre compte à la direction des performances du système de management de la sécurité de l'information.*

NOTE

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

PECB

92

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

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

g)*propriétaires d'informations;*

h)*propriétaires de processus;*

i)*propriétaires d'actifs (par exemple, les propriétaires d'application ou d'infrastructure);*

j)*propriétaires de risques;*

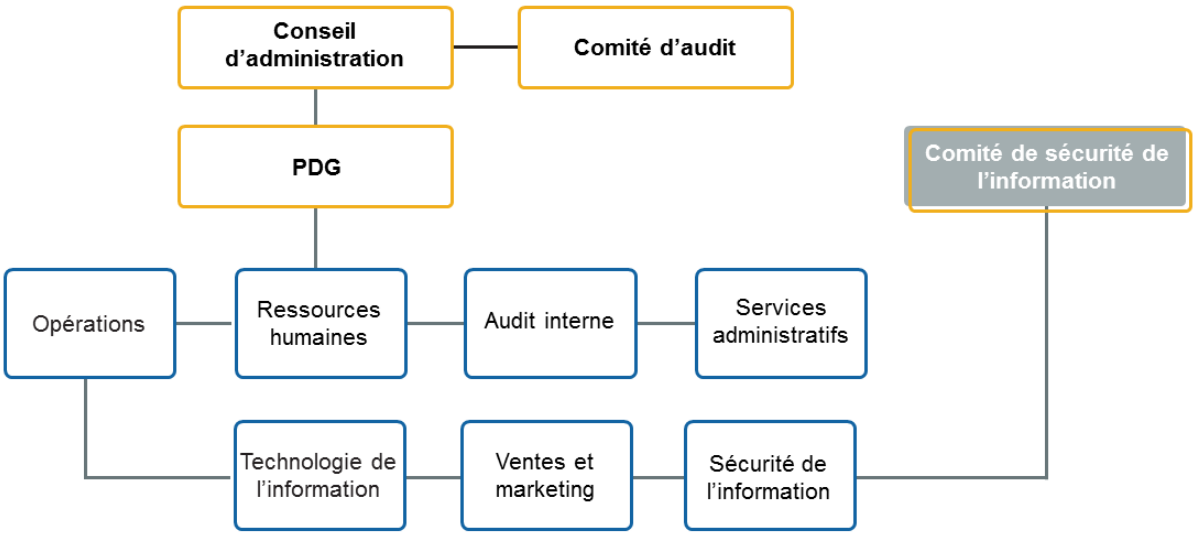
k)*fonctions de coordination de la sécurité de l'information ou de responsable (ce rôle particulier est normalement un rôle de support dans le SMSI);*

l)*gestionnaires de projet;*

m)*gestionnaires hiérarchiques; et*

n)*utilisateurs d'informations.*

Structure organisationnelle pour la sécurité de l'information



PECB

93

L'un des éléments les plus importants pour définir le management de la sécurité de l'information et sa gouvernance est de placer le responsable de la sécurité de l'information (CISO) dans la hiérarchie de l'organisme.

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

Rôles et responsabilités des parties intéressées

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

PECB

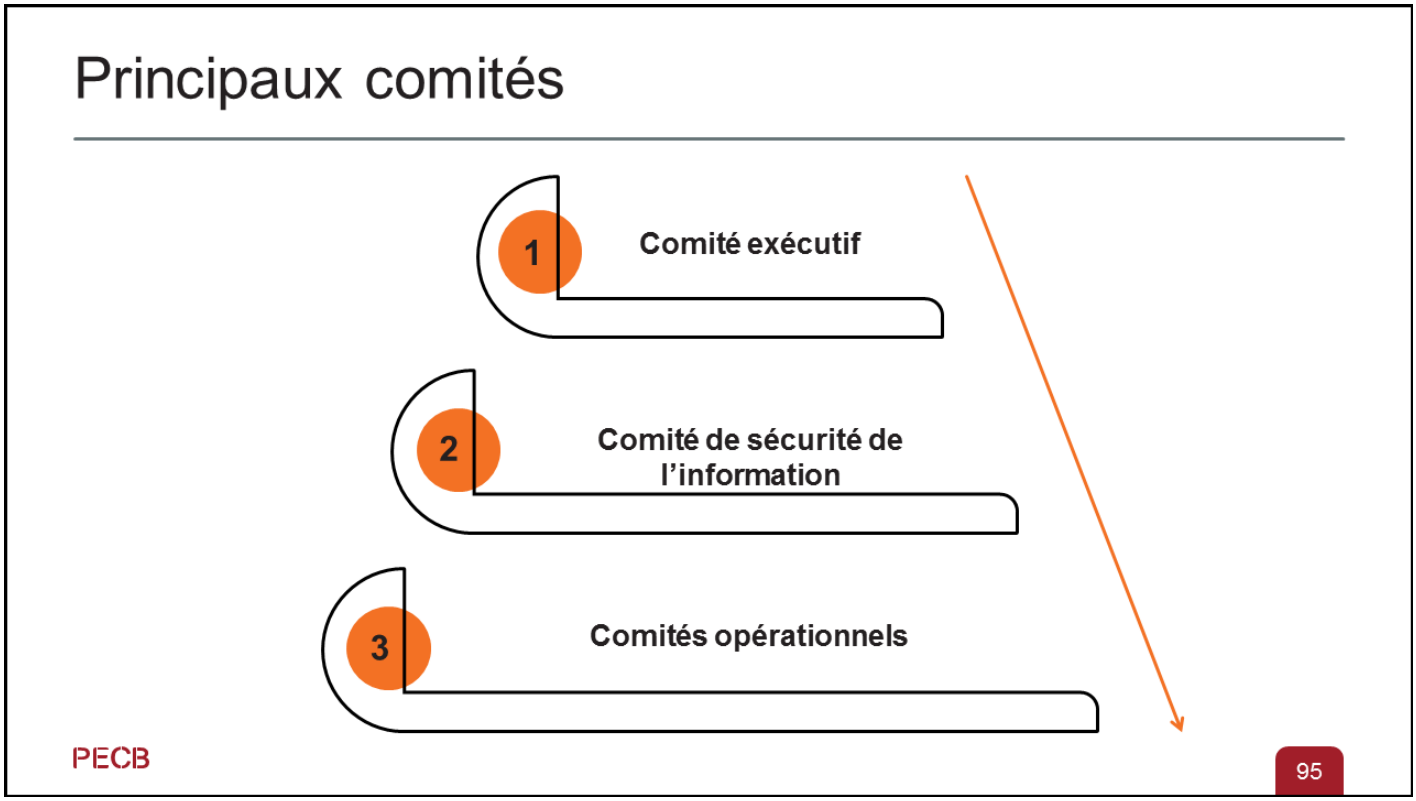
94

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

Le responsable d'une tâche peut déléguer des tâches, mais pas des responsabilités.

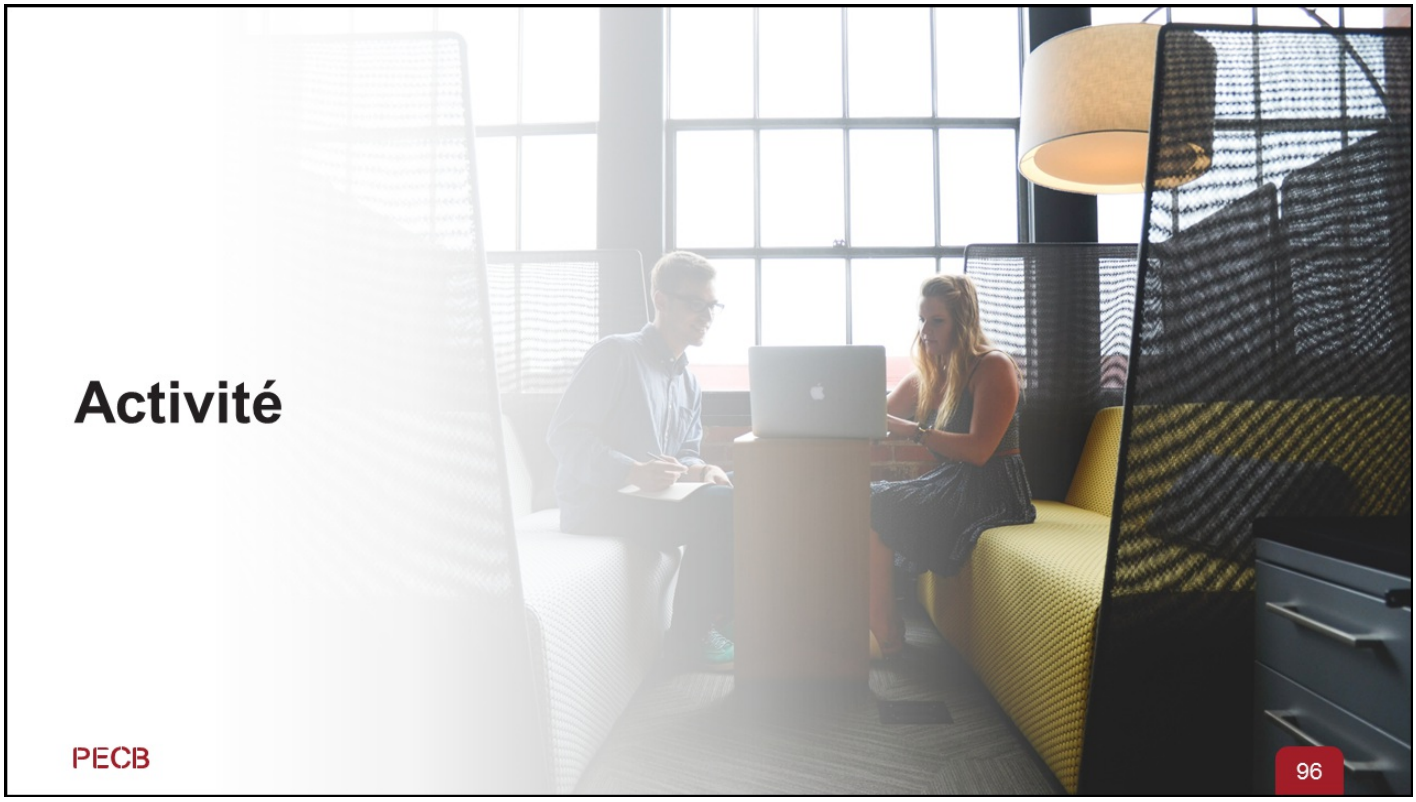
Dans le cas de la gestion d'un actif, un propriétaire peut assigner un «gardien» qui, par délégation assurera la sécurité des actifs sous sa responsabilité. Sa tâche consistera donc à :

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



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

- Le comité exécutif assure les orientations, le contrôle, la validation, la prise de décision et l'arbitrage pour le SMSI.
- Le comité de sécurité de l'information assure le bon déroulement des opérations du SMSI et des mesures de sécurité de l'information.
- Les comités opérationnels assurent l'efficacité des actions correctives visant à combler les écarts dans le SMSI



Questions de discussion

1. Comment la direction d'un organisme peut-elle faire preuve de leadership et d'engagement pour le SMSI ?
2. Que définit une politique spécifique de haut niveau ?
3. Quelles sont les phases du cycle de vie de l'élaboration de la politique de sécurité de l'information ?
4. Quel est le rôle du responsable de la sécurité de l'information ?

Page de notes

PECB

98

Résumé du jour 1

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

- Définition du SMSI et avantages qu'il apporte aux organismes
- Vue d'ensemble des principaux articles et de l'annexe A d'ISO/IEC 27001
- Concepts et principes fondamentaux de la sécurité de l'information
- Confidentialité, intégrité et disponibilité des informations
- Vulnérabilité, menace, impact, et leur relation
- Risques de sécurité de l'information
- Intelligence artificielle et informatique en nuage (cloud computing)
- Mission, objectifs, valeurs et stratégies de l’organisme
- Approbation par la direction du projet SMSI
- Rôles et responsabilités des parties intéressées et des comités
- Politique de sécurité de l’information

Page de notes

Page de notes