



© PECB, 2020. Tous droits réservés.

Version6.0

Numéro de document: ISMSLID1V6.0

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

Programme de la formation

Jour
1

Introduction à la norme ISO/IEC 27001 et initiation d'un SMSI

Jour
2

Planification de la mise en œuvre d'un SMSI

Jour
3

Mise en œuvre du SMSI

Jour
4

Surveillance, amélioration continue et préparation à l'audit de certification du SMSI

Jour
5

Examen de certification

PECB



2

Jour1: Introduction à la norme ISO/IEC27001 et initiation d'un SMSI

- 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: Initiation de la mise en œuvre du SMSI
- Section6: Compréhension de l'organisme et de son contexte
- Section7: Analyse du système existant

Jour2: Planification de la mise en œuvre d'un SMSI

- Section8: Leadership et approbation du projet
- Section9: Périmètre du SMSI
- Section10: Politique de sécurité de l'information
- Section11: Processus de gestion des risques
- Section12: Structure organisationnelle de la sécurité de l'information
- Section13: Déclaration d'applicabilité et décision de la direction de mettre en œuvre le SMSI

Jour 3: Mise en œuvre du SMSI

- Section 14: Conception des mesures de sécurité et rédaction des politiques spécifiques et des procédures
- Section 15 : Mise en œuvre des mesures de sécurité
- Section 16 : Définition du processus de gestion de documents
- Section 17 : Plan de communication
- Section 18 : Plan de formation et de sensibilisation
- Section 19 : Gestion des opérations
- Section 20 : Gestion des incidents

Page de notes

PECB

3

Jour 4 : Surveillance, amélioration continue et préparation à l'audit de certification du SMSI

- Section 21 : Surveillance, amélioration continue et préparation à l'audit de certification du SMSI
- Section 22 : Audit interne
- Section 23 : Revue de direction
- Section 24 : Traitement des problèmes et des non-conformités
- Section 25 : Amélioration continue
- Section 26 : Préparation à l'audit de certification
- Section 27 : Processus de certification et clôture de la formation

Jour 5 : Examen de certification

References

Normes de référence

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 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/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
- ISO19011:2018, Lignes directrices pour l'audit des systèmes de management

2. Autres normes référencées:

- ISO Guide 73:2009, Management du risque – Vocabulaire
- ISO 9000:2015, Systèmes de management de la qualité – Principes essentiels et vocabulaire
- ISO 9001:2015, Systèmes de management de la qualité – Exigences
- ISO/IEC 17011:2017, Évaluation de la conformité – Exigences pour les organismes d'accréditation procédant à l'accréditation d'organismes d'évaluation de la conformité
- ISO/IEC 17021-1:2015, Évaluation de la conformité – Exigences pour les organismes procédant à l'audit et à la certification des systèmes de management – Partie 1: Exigences
- ISO/IEC 17024:2012, Évaluation de la conformité – Exigences générales pour les organismes de certification procédant à la certification de personnes
- ISO/IEC 27006:2015, Technologies de l'information – Techniques de sécurité – Exigences pour les organismes procédant à l'audit et à la certification des systèmes de management de la sécurité de l'information

- ISO/IEC 27007:2017, Technologies de l'information – Techniques de sécurité – Lignes directrices pour l'audit des systèmes de management de la sécurité de l'information
- ISO/IEC TS27008:2019, Technologies de l'information – Techniques de sécurité – Lignes directrices pour les auditeurs des contrôles de sécurité de l'information
- ISO 31000:2018, Management du risque – Lignes directrices

Liste des acronymes

Liste des acronymes

BS: British Standard

CERT : Computer Emergency Response Team

COBIT: Control Objectives for Information and related Technology

COSO : Committee of Sponsoring Organizations of the Treadway Commission

CSIRT : Computer Security Incident Response Team

EA: European co-operation for Accreditation

EDMS: Electronic Document Management System

FISMA: Federal Information Security Management Act

FPC: Formation professionnelle continue

GAAS : (Generally Accepted Auditing Standards): Normes d'audit généralement admises

GED : Gestion électronique des documents

GLBA: Gramm-Leach-Bliley Act

HIPAA: Health Insurance Portability and Accountability Act

IAF: International Accreditation Forum

IAS: International Accreditation Service

IFAC: International Federation of Accountants

IMS2 : Integrated Implementation Methodology for Management Systems and Standards

IRT: Incident Response Team

ISO: Organisation internationale de normalisation

ITIL: Information Technology Infrastructure Library

LA: Lead Auditor

LI: Lead Implementer

NC: Non-conformité

NIST : National Institute of Standards and Technology

OCDE: Organisation de coopération et de développement économiques

PCI DSS: Payment Card Industry Data Security Standard

PDCA : Planifier-Déployer-Contrôler-Agir

PECB: Professional Evaluation and Certification Board

RFC (Request for Change): Demande de changement

ROI (Return on Investment): Retour sur investissement

ROSI: (Return on Security Investment): Retour sur investissement en sécurité des systèmes d'information

SGC : Système de gestion de contenu

SMCA: Système de management de la continuité d'activité

SMQ : Système de management de la qualité

SMS: Système de management des services

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

SoA: (Statement of applicability): Déclaration d'applicabilité

SOX: Sarbanes–Oxley Act

Section 1

Objectifs et structure de la formation

- Présentation du groupe
- Informations générales
- Objectifs de la formation
- Approche éducative
- Examen et certification
- Qu'est-ce que PECB ?

PECB

6

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.

Activité

PECB

7

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

- Nom
- Fonction actuelle
- Connaissances et expérience relatives à 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 9001, ISO 14001, ISO/IEC 20000, ISO 22301, etc.)
- Objectifs et attentes pour ce cours

Durée de l'activité: 20 minutes

Informations générales



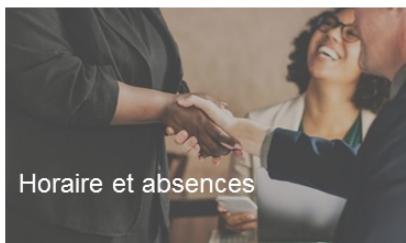
Utilisation des téléphones portables et des appareils d'enregistrement



Sessions interactives et intéressantes



Utilisation de l'ordinateur et accès Internet



Horaire et absences



Repas et pauses



Service à la clientèle

PECB

8

- 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 à tirer le meilleur parti de la formation.

Service à la clientèle

Afin d'assurer la satisfaction du client et l'amélioration continue, le service client de PECB a mis en place un système de tickets d'assistance pour traiter les réclamations et les services offerts à 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).

Si vous avez des suggestions concernant l'amélioration du matériel de formation PECB, nous aimeraisons les connaître. Nous lisons et évaluons les commentaires de nos clients. Vous pouvez le faire directement depuis notre application KATE ou vous pouvez ouvrir un ticket adressé au département de formation depuis le 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 sous la catégorie «Faire une réclamation» depuis le Centre d'aide PECB (www.pecb.com/help).

Objectifs d'apprentissage

Acquisition de connaissances

1

Maîtriser les concepts, les approches, les méthodes et les techniques nécessaires pour la mise en œuvre et le management efficace d'un SMSI

2

Comprendre la corrélation entre ISO/IEC 27001, ISO/IEC 27002 ainsi qu'avec d'autres normes et cadres réglementaires

3

Comprendre le fonctionnement d'un système de management de la sécurité de l'information conformément à la norme ISO/IEC 27001 ainsi que ses principaux processus

4

Savoir interpréter les exigences d'ISO/IEC 27001 dans le contexte spécifique d'un organisme

5

Acquérir une expertise pour accompagner un organisme à planifier, mettre en œuvre, gérer, surveiller et maintenir un SMSI tel que spécifié dans ISO/IEC 27001

PECB

9

La formation est conçue pour aider les participants à acquérir ou à améliorer leurs compétences pour participer à la mise en œuvre d'un système de management de la sécurité informatique (SMSI). D'un point de vue pédagogique, la compétence se compose des 3 éléments suivants:

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

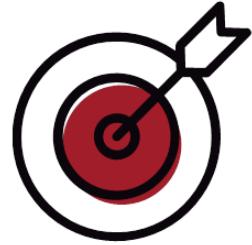
La présente formation fournit une méthodologie complète pour la mise en œuvre du SMSI suivant les exigences d'ISO/IEC27001, et pas seulement une liste des exigences ISO/IEC 27001. Par conséquent, une connaissance générale des concepts de gestion de la sécurité de l'information est nécessaire pour réussir le cours.

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 la formation PECB ISO/IEC 27001 Lead Auditor.

Cette formation porte sur la réalité de la mise en œuvre d'un système de management de la sécurité de l'information. L'étude de cas et les exercices servent à simuler des situations aussi proches que possible de la réalité de terrain.

Objectif principal de la formation

L'objectif principal de cette formation est de s'assurer que, dès la fin de la formation, le candidat a acquis les connaissances et l'expertise nécessaires à la mise en œuvre d'un système de management de la sécurité de l'information (SMSI).



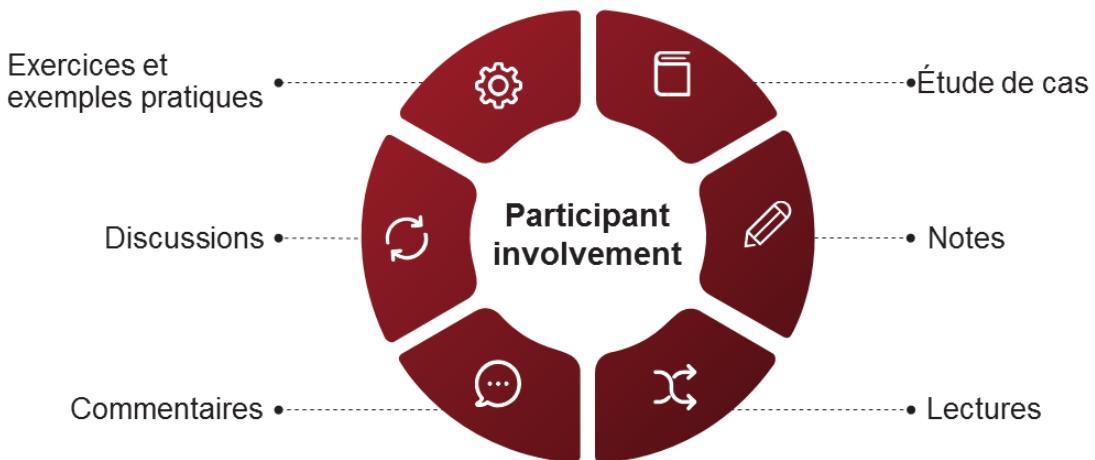
PECB

10

À l'issue de la formation, les participants auront acquis des connaissances et développé des compétences sur **comment** mettre en œuvre et pas seulement sur le **pourquoi** et le **quoi faire** lors de la mise en œuvre d'un SMSI.

Approche éducative

Centrée sur le participant



PECB

11

Ce cours repose principalement sur:

- Des sessions animées par un formateur, où l'interaction par le biais de questions et de suggestions est fortement encouragée
- L'implication des participants à travers divers exercices interactifs, étude de cas, notes, discussions (expériences des participants), 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.

Les exercices sont essentiels à l'acquisition des compétences nécessaires à la mise en œuvre appropriée d'un système de management. Il est donc très important de les faire consciencieusement, considérant que ces exercices aideront les candidats à se préparer à l'examen de certification.

Examen

Domaines de compétence

- 1 Principes et concepts fondamentaux d'un système de management de la sécurité de l'information (SMSI)
- 2 Mesures de sécurité et bonnes pratiques du SMSI basées sur ISO/IEC 27002
- 3 Planification de la mise en œuvre d'un SMSI selon ISO/IEC 27001
- 4 Mise en œuvre d'un SMSI selon ISO/IEC 27001
- 5 Évaluation des performances, surveillance et mesure d'un SMSI selon ISO/IEC 27001
- 6 Amélioration continue d'un SMSI selon ISO/IEC 27001
- 7 Préparation à un audit de certification du SMSI

PECB

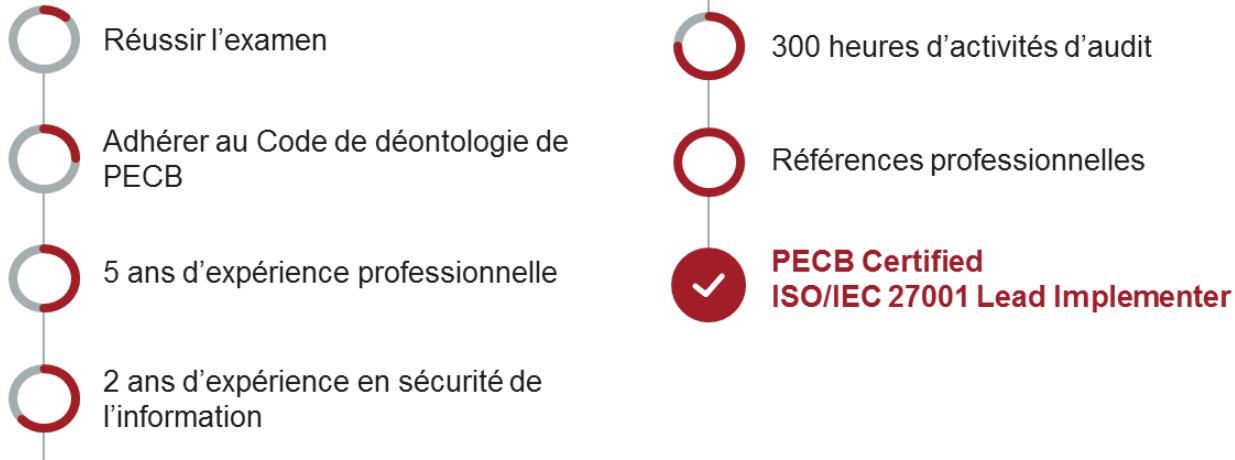
12

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 doit s'assurer que l'élaboration et la pertinence des questions d'examen sont maintenues en fonction des pratiques professionnelles actuelles.

Tous les domaines de compétence sont couverts par l'examen. Pour lire une description détaillée de chaque domaine de compétences, consultez le Guide de préparation à l'examen sur le site Web de PECB.

PECB Certified ISO/IEC 27001 Lead Implementer

Prérequis à la certification



PECB

13

La réussite de l'examen n'est pas l'unique prérequis à l'obtention de la certification «Certified ISO/IEC 27001Lead Implementer». Cette certification atteste à la fois de la réussite de l'examen et de la validation du dossier d'expérience professionnelle. Malheureusement, après avoir réussi l'examen, certaines personnes prétendent être des Certified ISO/IEC 27001Lead Implementer, sans avoir le niveau d'expérience requis.

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

Un candidat moins expérimenté peut postuler pour la certification «Certified ISO/IEC 27001Implementer» ou «Provisional Implementer».

Note importante: Les frais d'examen et de certification sont inclus avec la formation: Ainsi, le candidat n'aura à débourser aucun supplément pour faire la demande de l'une des certifications suivantes: PECB Certified ISO/IEC 27001 Provisional Implementer, PECB Certified ISO/IEC 27001 Implementer, PECB Certified ISO/IEC 27001Lead Implementer ou PECB Certified ISO/IEC 27001Senior Lead Implementer.

Certification PECB

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



PECB

14

Après la réussite de l'examen, le candidat dispose d'un délai maximal de trois ans pour soumettre sa demande de certification professionnelle.

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. Le certificat est valable pour trois ans. Pour maintenir sa certification, le candidat doit démontrer chaque année qu'il satisfait aux exigences de la certification qui lui a été attribuée et qu'il se conforme au Code de déontologie de PECB. Pour en savoir plus sur la procédure de maintien et de renouvellement des certificats, veuillez consulter le site Web de PECB. Plus de détails seront donnés au cours de la dernière journée de formation.

Pourquoi devenir un Implementer certifié ?

Avantages

-  Se qualifier pour gérer un projet SMSI
-  Obtenir une reconnaissance formelle et indépendante de vos compétences personnelles
-  Gagner un salaire potentiellement plus élevé que les personnes non certifiées

PECB

15

- Une certification internationalement reconnue peut vous aider à **maximiser le potentiel de votre carrière** et à atteindre vos objectifs professionnels.
- Une certification internationale constitue une **reconnaissance officielle** des compétences d'un individu.
- Selon les enquêtes sur les salaires menées au cours des cinq dernières années, les personnes certifiées *Implementer* gagnent un salaire moyen considérablement plus élevé que leurs homologues non certifiés.

Qu'est-ce que PECB ?

PECB propose :

Certification de personnes

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

Example:

PECB Certified
ISO 9001 Lead Auditor



PECB

16

PECB est un organisme de certification des personnes, des systèmes de management et des produits pour un large éventail de normes internationales. 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 TI, 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/IEC17065.

L'objectif de PECB, tel qu'inscrit dans son règlement, est de développer et de promouvoir des normes professionnelles pour la certification et d'administrer des programmes de certification crédibles pour les personnes qui exercent dans des disciplines impliquant la mise en œuvre et l'audit d'un système de management conforme. Cet objectif comprend:

1. Établir les exigences minimales nécessaires pour certifier les professionnels, les organismes et les produits
2. Réviser et vérifier les qualifications des candidats admissibles à une certification professionnelle
3. Élaborer et maintenir des évaluations de certification fiables, valides et à jour
4. Déliver des certificats aux candidats, organismes et produits qualifiés, maintenir à jour et publier un registre des titulaires de certificats 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. Représenter ses membres, le cas échéant, dans les questions d'intérêt commun
8. Promouvoir les avantages de la certification aux employeurs, aux fonctionnaires, aux praticiens dans les domaines connexes et au grand public

Qu'est-ce que PECB ?

PECB propose :

Certification de systèmes de management Un système de management certifié par PECB renforcera la capacité d'un organisme à connaître un succès durable.

Certification de formation (PTCP) Une formation certifiée par PECB démontre que cette formation est fiable et de grande qualité.

Certification des applications (AppCert) Une application certifiée par PECB démontre que ce produit logiciel possède des attributs de fonctionnalité, de convivialité et de sécurité.

Certification des équipes (TeamCert) Une équipe certifiée dans le cadre du programme TeamCert de PECB offre à toutes les parties intéressées l'assurance que cette équipe répond aux exigences d'une performance efficace et réussie.

PECB

17

Certification de systèmes de management

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

Certification de formation:

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

Certification des applications:

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

Certification des équipes:

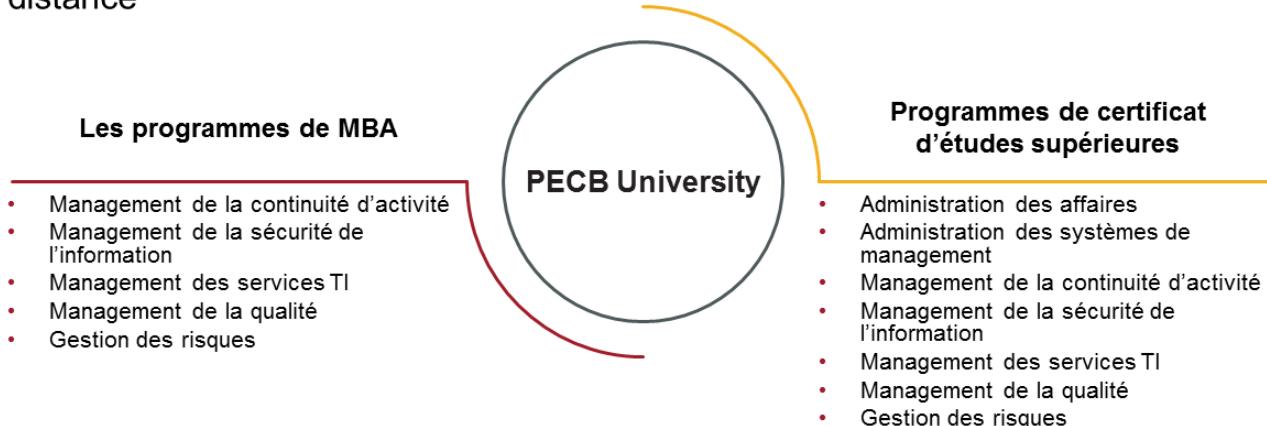
PECB offre des certifications des équipes qui aident les organismes à améliorer l'efficacité et la productivité de leurs équipes. Les équipes cherchant à obtenir la certification feront l'objet d'une évaluation et d'une appréciation afin de vérifier la conformité aux exigences et aux critères.

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

Qu'est-ce que PECB ?

PECB propose :

Des services éducatifs par l'entremise de son université d'apprentissage à distance



PECB

18

L'Université PECB offre en ligne des programmes de MBA et de certificat d'études supérieures en management de la continuité d'activité, de la sécurité de l'information, des services informatiques, de la qualité et du risque.

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

Note importante:

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

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

Organisme de certification de personnes

ISO/IEC 17024

- La norme ISO/IEC 17024 spécifie les critères pour un organisme qui effectue la certification de personnes en relation avec des exigences spécifiques, y compris l'élaboration et le maintien d'un système de certification de personnes.
- PECB est accréditée par l'IAS selon ISO/IEC 17024.



PECB

19

La norme ISO/IEC17024 fournit un cadre complet pour que les organismes de certification tels que PECB puissent fonctionner de manière cohérente et fiable. La fonction première de l'organisme qui procède à la certification de personnes est de réaliser une appréciation indépendante de l'expérience et des compétences d'un candidat applicables au domaine pour lequel la certification est attribuée.

La norme est conçue pour aider les organismes qui procèdent à la certification de personnes à mener des appréciations bien planifiées et structurées en utilisant des critères objectifs de notation afin d'assurer l'impartialité des opérations et de réduire les risques de conflits d'intérêts.

La Norme internationale ISO/IEC17024 traite de la structure et de la gouvernance de l'organisme de certification, des caractéristiques du programme de certification, et des informations qui doivent être mises à la disposition des candidats.

Note importante:

Seul un organisme de certification accrédité selon la norme ISO/IEC17024 assure une reconnaissance internationale. Il est important de valider le statut d'un organisme de certification auprès de l'autorité d'accréditation associée telle qu'IAS, ANSI et UKAS. Pour plus d'informations sur l'accréditation de PECB, veuillez visiter: www.pecb.com/fr/affiliations.



Questions ?

PECB

20

Section 2

Normes et cadres réglementaires

- Structure de l'ISO
- Normes relatives aux systèmes de management
- Systèmes de management intégrés
- Famille ISO 27000
- Avantages d'ISO/IEC 27001

PECB

21

La présente section fournit des informations qui aideront le participant à acquérir des connaissances sur la structure de l'ISO et les normes de systèmes de management, la famille ISO 27000 et les avantages d'ISO/IEC 27001.

Structure de l'ISO

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.
- Plus de 22 000 normes ont été publiées depuis 1947.



PECB

22

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 le résultat d'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.

Normes relatives aux systèmes de management

Les organisations peuvent être certifiées selon les normes principales suivantes :



PECB

23

Depuis 1947, l'ISO a publié plus de 23000 normes internationales. 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 ISO9000 et ISO14000 sont parmi les normes ISO les plus connues. La norme ISO9000 est devenue une référence internationale en matière d'exigences de qualité dans le commerce et les transactions commerciales. La norme ISO14000, pour sa part, est utilisée pour aider les organismes à relever les défis de nature environnementale.

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

Systèmes de management intégrés

Structure commune des normes d'ISO

Exigences	ISO 9001:2015	ISO 14001:2015	ISO/IEC 27001:2013	ISO 22301:2012	ISO 55001:2014
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	7.5	7.5	7.6
Audit interne	9.2	9.2	9.2	9.2	9.2
Revue de direction	9.3	9.3	9.3	9.3	10.3
Amélioration continue	10.3	10.3	10.2	10.2	9.3

PECB

24

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

25

Annexe SL Propositions de normes de systèmes de management

SL.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 SL.

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.

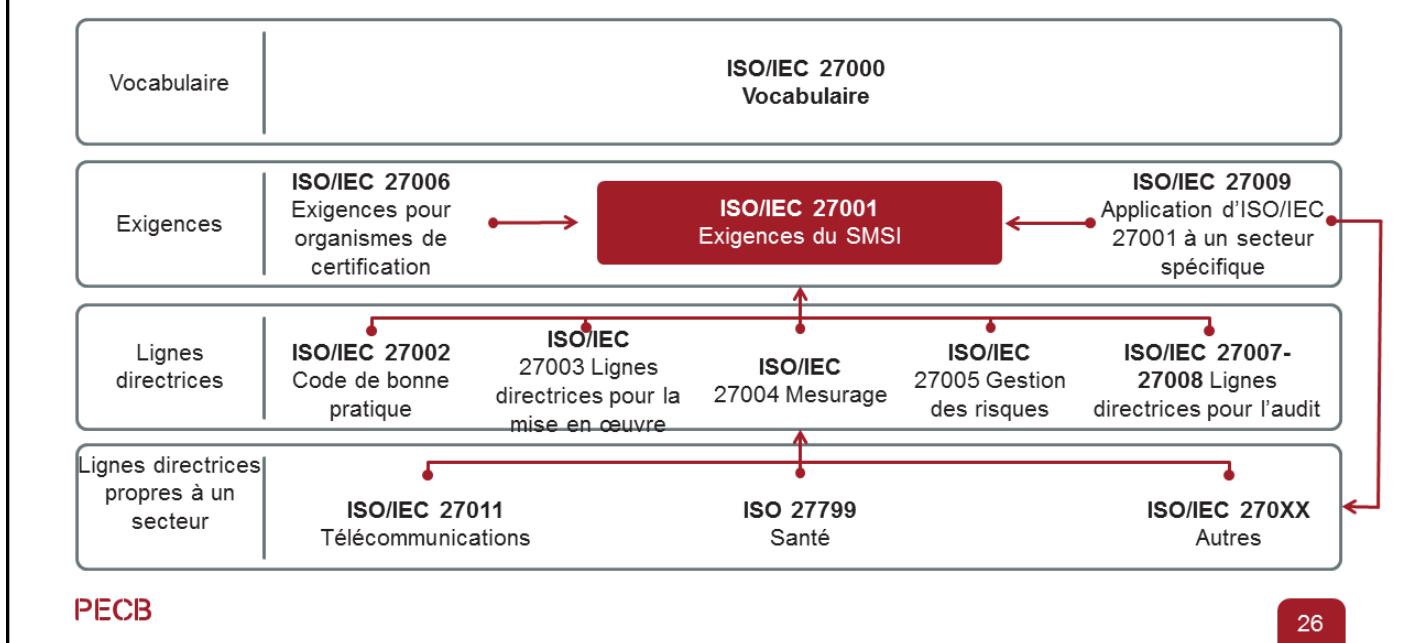
Appendice 1 Questions relatives aux critères de justification

Généralités

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

Famille ISO 27000



PECB

26

La famille de normes ISO27000, qui existe depuis 2005, est dédiée à la sécurité de l'information à travers les systèmes de management de la sécurité de l'information (SMSI). Il existe trois normes «normatives» dans la série, dont la norme ISO/IEC27001 est la seule qui permet à une organisation d'obtenir la certification. Toutes les autres normes sont des lignes directrices.

Les normes de la série27000 sont les suivantes:

- **ISO/IEC27000:** Introduit les concepts de base ainsi que le vocabulaire qui s'applique au développement de systèmes de management de la sécurité de l'information. Un exemplaire gratuit de cette norme peut être téléchargé à partir du site Web de l'ISO.
- **ISO/IEC27001:** Définit les exigences du système de management de la sécurité de l'information (SMSI) et fournit un ensemble de mesures de sécurité de référence dans son Annexe A.
- **ISO/IEC27002 (remplace ISO/IEC17799):** Code de bonne pratique pour le management de la sécurité de l'information Fournit les objectifs et les lignes directrices de mise en œuvre des mesures de sécurité de l'information énoncées à l'Annexe A de la norme ISO/IEC27001. Vise à répondre aux besoins des organismes de tous types et de toutes tailles.
- **ISO/IEC27003:** Lignes directrices pour la mise en œuvre ou la mise en place d'un SMSI
- **ISO/IEC27004:** Lignes directrices pour définir les objectifs de mise en œuvre et les critères d'efficacité de surveillance, mesurage, analyse et évaluation tout au long du processus
- **ISO/IEC27005:** Directives pour la gestion des risques liés à la sécurité de l'information conforme aux concepts, modèles et processus généraux spécifiés dans ISO/IEC27001
- **ISO/IEC 27006 :** Exigences pour les organismes qui auditent et certifient les SMSI
- **ISO/IEC 27007 :** Lignes directrices pour l'audit des systèmes de management de la sécurité de l'information
- **ISO/IEC 27008 :** Lignes directrices pour les auditeurs des contrôles de sécurité de l'information

Page de notes

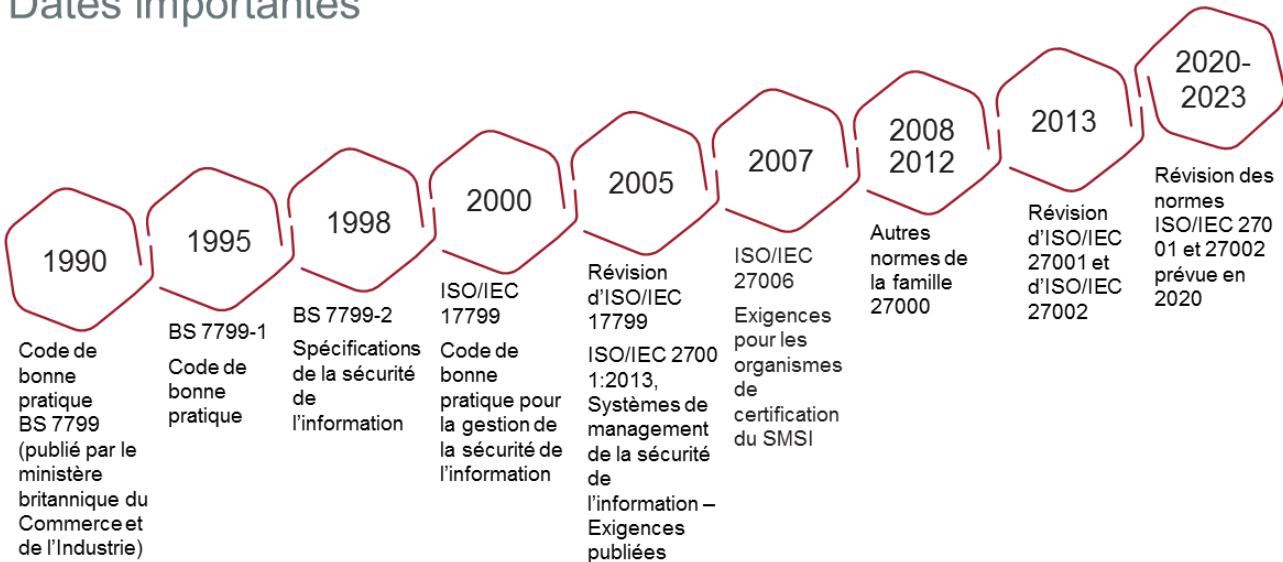
PECB

27

- **ISO/IEC 27009** : Exigences pour les rédacteurs de lignes directrices de mise en œuvre ISO/IEC 27001 spécifiques à un secteur
- **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 27799** : Lignes directrices pour l'utilisation d'ISO/IEC 27002 en informatique de la santé

Développement de la série ISO/IEC 27001

Dates importantes



PECB

28

L'histoire et le raisonnement derrière la famille ISO27000:

- 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 (BS7799), a été publié. Plusieurs de ces mesures sont reconnaissables dans ISO/IEC27002.
- 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/IEC27001 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 documents sont révisés tous les cinq ans, ce qui permet généralement de se conformer à l'évolution de l'industrie. La révision des normes 27001/02 est actuellement en suspens et, une fois lancée, elle devrait prendre trois ans avant d'être publiée.

La norme 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 ».
- Annexe A : 14 articles comportant 35 objectifs de mesure et 114 mesures de sécurité.
- Les organismes peuvent obtenir une certification conformément à cette norme.



PECB

29

ISO/IEC27001:

- Un ensemble d'exigences normatives pour établir, mettre en œuvre, exploiter, surveiller et revoir 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 système de management intégré dans le cadre global du risque associé à l'activité de l'organisme
- Un processus internationalement reconnu, défini et structuré pour gérer la sécurité de l'information
- Une norme internationale qui convient à tous les types d'organisations (entreprises commerciales, agences gouvernementales, organismes à but non lucratif, etc.), de toutes tailles, dans toutes les industries

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.

Page de notes

PECB

30

ISO/IEC 27001, article 0.1 Généralités

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 ».
- Composée de 14 articles, 35 objectifs de mesure et 114 mesures de sécurité.
- Cette norme ne se prête pas à des fins de certification.



PECB

31

ISO/IEC27002:

- ISO/IEC 27002 est un guide de bonne pratique de management de la sécurité de l'information (mesures).
- Cette Norme internationale fournit une liste des objectifs et des mesures de sécurité généralement utilisés dans l'industrie.
- En particulier, les articles 5 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 (articles A.5 à A.18).

ISO/IEC 27002, article 1 Domaine d'application

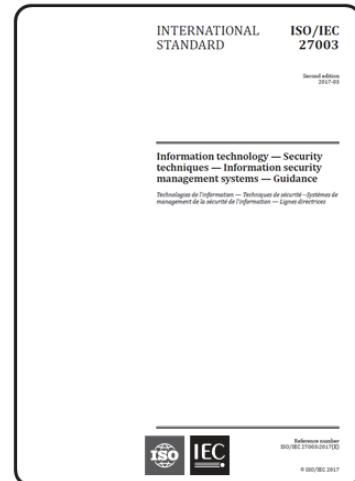
La présente Norme internationale donne des lignes directrices en matière de normes organisationnelles relatives à la sécurité de l'information et des bonnes pratiques de management de la sécurité de l'information, incluant la sélection, la mise en œuvre et la gestion de mesures de sécurité prenant en 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

32

ISO/IEC 27003, article1 Domaine d'application

Le présent document présente des explications et des lignes directrices pour la norme ISO/IEC27001:2013. Il décrit le processus de spécification et de conception du SMSI, du début jusqu'à la production mise en œuvre.

Identifier le problème:

Le but de cette Norme internationale est d'être utilisée par des organisations qui mettent en place un SMSI. Elle s'applique à tous les types d'organisation (ex. entreprises commerciales, agences gouvernementales, organismes à but non lucratif) de toutes les tailles.

La complexité et les risques de chaque organisation sont uniques et les exigences précises de l'organisation dirigeront la mise en œuvre du SMSI. Les plus petites organisations trouveront que les activités notées dans la Norme internationale s'appliquent à leur situation et peuvent être simplifiées.

Les organisations à grande échelle ou complexes pourraient constater qu'une structure ou un système de management à plusieurs niveaux est nécessaire pour gérer les activités de la présente Norme internationale de manière efficace.

Cependant, dans les deux cas, les activités pertinentes peuvent être planifiées en appliquant cette Norme internationale.

Cette Norme internationale donne des recommandations et des explications; elle ne détermine aucune exigence.



Questions ?

PECB

33

Section 3

Système de management de la sécurité de l'information (SMSI)

- Définition d'un SMSI
- Approche processus
- Vue d'ensemble – articles 4 à 10
- Annexe A

PECB

34

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 SMSI

ISO/IEC 27000, article 4.2.1

- *Un SMSI se compose des politiques, procédures, lignes directrices et des ressources et activités associées, gérées collectivement par un organisme dans le but de protéger ses actifs informationnels.*
- *Un SMSI utilise une approche systématique visant à établir, mettre en œuvre, exploiter, surveiller, réexaminer, maintenir et améliorer la sécurité de l'information d'un organisme afin que celui-ci atteigne ses objectifs métier. Cette approche se fonde sur l'appréciation du risque et sur les niveaux d'acceptation du risque définis par l'organisme pour traiter et gérer efficacement les risques.*

PECB

35

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.
La présente norme précise que *l'organisation doit évaluer les performances de sécurité de l'information, ainsi que l'efficacité du système de management de la sécurité de l'information* (ISO/IEC 27001, article 9.1).

Cet article est une composante essentielle d'un système de management, car, sans l'évaluation de l'efficacité des processus et des mesures de sécurité en place, il est impossible de valider si l'organisme a atteint ses objectifs.

Page de notes

PECB

36

Définitions liées au concept de « SMSI »

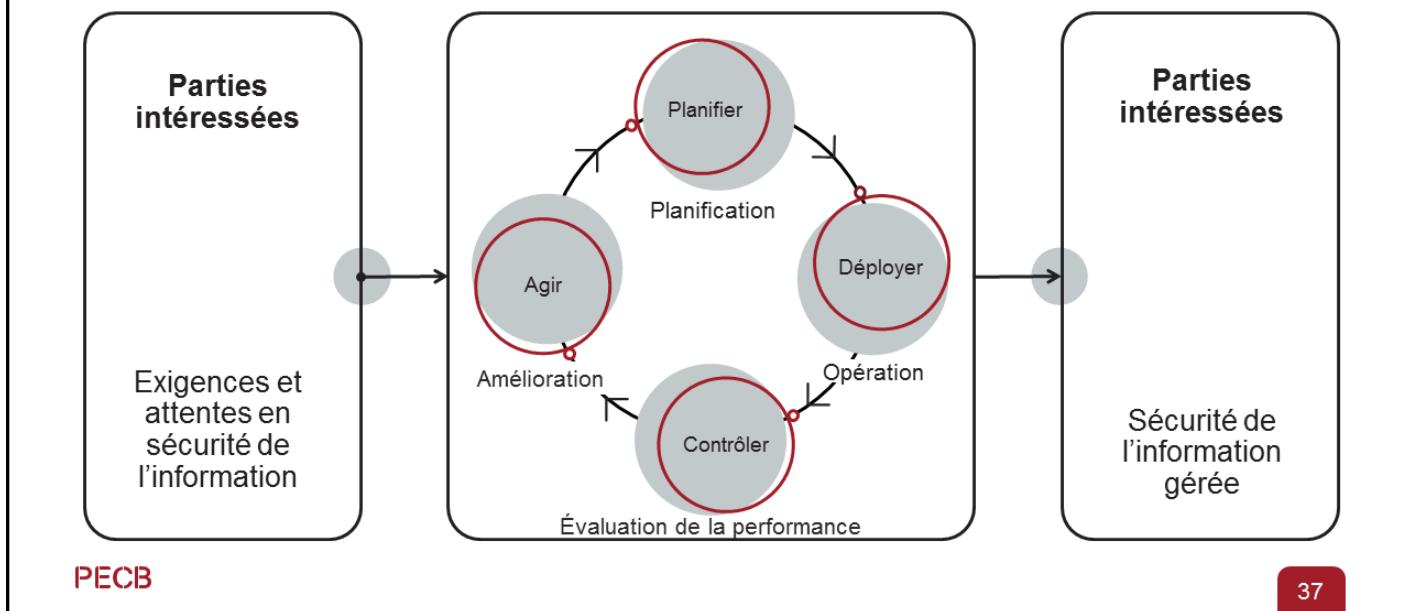
ISO 9000 et ISO/IEC 27000

- **Système** : ensemble d'éléments corrélés ou en interaction (ISO 9000, 3.5.1)
- **Management** : activités coordonnées pour orienter et diriger un organisme (ISO 9000, 3.3.3)
- **Système de management**: 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 (ISO 9000, 3.5.3)
- **Sécurité de l'information** : protection de la confidentialité, de l'intégrité et de la disponibilité de l'information (ISO/IEC 27000, 3.28)

Note de terminologie:

1. Le terme management désigne toutes les activités coordonnées pour orienter et diriger un organisme. Dans ce contexte, le terme management ne désigne pas les personnes. Il se réfère aux activités. ISO 9000 utilise le terme direction pour désigner les personnes..
2. Le système de management d'un organisme peut inclure différents systèmes de management, par exemple un système de management de la qualité (ISO 9001), un système de management de la sécurité de l'information (ISO/IEC 27001), un système de management environnemental (ISO 14001), etc.

Approche processus



37

La présente Norme internationale adopte le modèle de processus «Planifier-Déployer-Contrôler-Agir» (PDCA), ou roue de Deming, qui est appliquée 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.

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.

Contrôler (surveillance et revue du système de management): Évaluer et, le cas échéant, mesurer les performances des processus par rapport à la politique, aux objectifs et à l'expérience pratique et rendre compte des résultats à la direction pour revue.

Agir (maintenance et amélioration du système de management): Entreprendre les actions correctives et préventives sur la base des résultats de l'audit interne et de la revue de direction ou d'autres informations pertinentes, pour une amélioration continue du système.

Audit et approche processus

- L'application de l'approche processus différera d'un organisme à l'autre, selon sa taille, sa complexité et ses activités.
- Les organismes audités trouvent souvent qu'ils ont trop de processus.



PECB

38

On peut définir un processus comme étant un ensemble logique de tâches liées entre elles et exécutées pour atteindre un objectif défini. Un processus est une suite d'activités structurées et mesurées, conçues pour offrir un produit ou un service à un secteur du marché ou un client particulier.

Pour qu'un organisme fonctionne de manière efficace, il doit mettre en œuvre et gérer de nombreux processus corrélés et interactifs. Souvent, l'élément de sortie d'un processus forme directement l'élément d'entrée du processus suivant. L'identification et le management méthodique des processus utilisés dans un organisme, et plus particulièrement les interactions de ces processus, sont appelés « l'approche processus ».

Les mesures de sécurité servent à s'assurer que la conduite des processus d'affaires est effectuée de manière sécurisée en termes d'échanges informationnels. Les processus et les mesures de sécurité sont dépendants des processus d'affaires parce qu'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 d'un organisme. 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

Page de notes

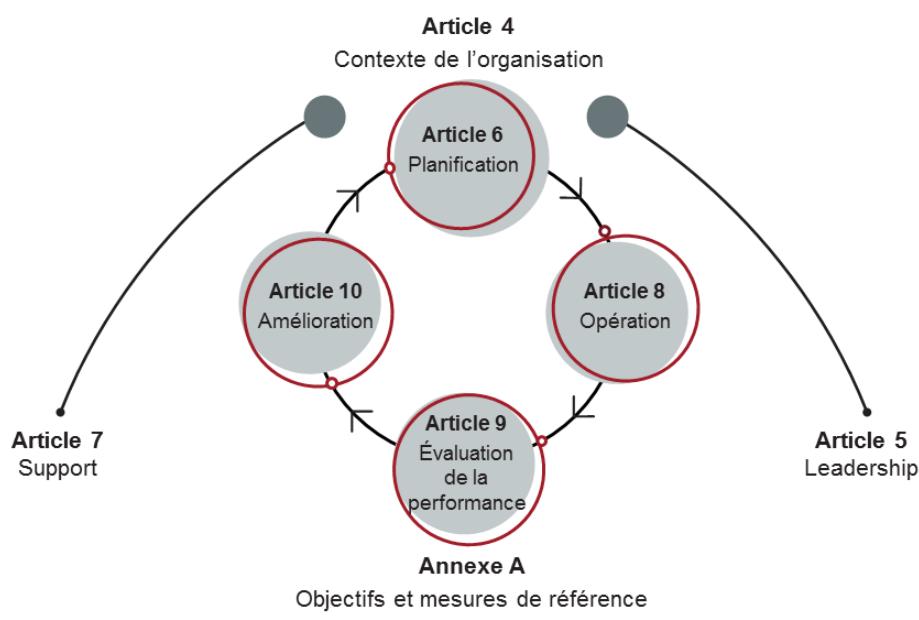
PECB

39

ISO 19011, Annexe A.2 Approche processus pour l'audit

L'utilisation d'une « approche processus » est une exigence pour toutes les normes ISO de système de management, conformément aux Directives ISO/IEC, Partie 1, Annexe SL. Il convient que les auditeurs comprennent qu'auditer un système de management consiste à auditer les processus d'un organisme et leurs interactions par rapport à une ou plusieurs normes de système de management. Des résultats cohérents et prévisibles sont obtenus de manière plus efficace et efficiente lorsque les activités sont comprises et gérées comme des processus corrélés fonctionnant comme un système cohérent.

Structure de la norme ISO/IEC 27001



PECB

40

Toute organisme qui souhaite obtenir la certification ISO/IEC27001 doit se conformer aux exigences énoncées dans les articles 4 à 10 de la présente norme.

Contexte de l'organisation

ISO/IEC 27001, articles 4.1 à 4.4



PECB

41

ISO/IEC27001, article 4.1Compréhension de l'organisation et de son contexte

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.

ISO/IEC27001, article 4.2Compréhension des besoins et des attentes des parties intéressées

L'organisation doit déterminer:

- a. *les parties intéressées qui sont concernées par le système de management de la sécurité de l'information; et*
- b. *les exigences de ces parties intéressées concernant la sécurité de l'information.*

Note: Les exigences des parties intéressées peuvent inclure des exigences légales et réglementaires et des obligations contractuelles.

Page de notes

PECB

42

ISO/IEC 27001, article 4.3 Détermination du domaine d'application du système de management de la sécurité de l'information

Pour établir le domaine d'application du système de management de la sécurité de l'information, l'organisation doit en déterminer les limites et l'applicabilité.

Lorsqu'elle établit ce domaine d'application, l'organisation doit prendre en compte:

- a. *les enjeux externes et internes auxquels il est fait référence en 4.1;*
- b. *les exigences auxquelles il est fait référence en 4.2; et*
- c. *les interfaces et les dépendances existant entre les activités réalisées par l'organisation et celles réalisées par d'autres organisations.*

Le domaine d'application doit être disponible sous forme d'information documentée

ISO/IEC 27001, article 4.4 Système de management de la sécurité de l'information

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

Leadership et engagement de la direction

ISO/IEC 27001, article 5.1

Orientation stratégique	Rendre les ressources disponibles	Communication
<ul style="list-style-type: none">S'assurer que le SMSI est compatible avec l'orientation stratégique de l'organisme.Intégrer les exigences du SMSI dans les processus d'affaires de l'organisme.	<ul style="list-style-type: none">La direction doit déterminer et fournir les ressources nécessaires au SMSI.	<ul style="list-style-type: none">La direction doit communiquer l'importance d'une gestion efficace de la sécurité de l'information et de la conformité aux processus du SMSI

PECB

43

ISO/IEC27001, article 5.1 Leadership et engagement

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

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

Page de notes

PECB

44

ISO/IEC 27021, article 5.2 Compétence : 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

Par son leadership et ses actions, la direction peut créer un environnement au sein duquel tous les acteurs sont totalement impliqués et le système de management peut agir efficacement en synergie avec les objectifs de l'organisme. La direction peut utiliser les principes de gestion d'ISO pour définir son rôle, lequel implique les actions suivantes:

- a. Établir les lignes directrices et les objectifs de l'organisme
- b. Promouvoir les politiques et les objectifs à tous les niveaux de l'organisme pour sensibiliser et augmenter la motivation et l'implication
- c. S'assurer que les exigences des parties intéressées (clients, partenaires, actionnaires, législateurs, etc.) demeurent une priorité à tous les niveaux de l'organisme
- d. Mettre en œuvre les processus et les mesures appropriés pour aider à la conformité aux exigences
- e. Établir, mettre en œuvre et maintenir un système de management efficace et efficient
- f. S'assurer de la disponibilité des ressources nécessaires
- g. S'assurer que les audits internes sont effectués
- 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 système de management

Politique de sécurité de l'information

ISO/IEC 27001, article 5.2

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

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

La politique de sécurité de l'information doit :

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

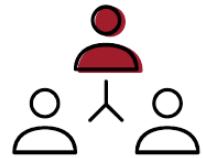
Rôles, responsabilités et autorités au sein de l'organisation

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.*



Planification

ISO/IEC 27001, article 6

Détermination des risques et des opportunités	Sécurité de l'information Appréciation des risques	Traitemen t des risques de la sécurité de l'information	Sécurité de l'information Objectifs
S'assurer que le SMSI puisse atteindre les résultats prévus, prévenir ou réduire les effets non désirés, réaliser l'amélioration continue, planifier les actions pour traiter les risques et saisir les opportunités, mettre en œuvre ces mesures et évaluer leur efficacité.	Établir et maintenir les critères de risques ; s'assurer que la récurrence de l'appréciation des risques produise des résultats cohérents, valides et comparables ; identifier, analyser et évaluer les risques.	Sélectionner les options de traitement des risques, déterminer les mesures à mettre en œuvre, comparer les mesures déterminées, produire la Déclaration d'applicabilité, formuler le plan de traitement des risques, obtenir l'approbation du plan et l'acceptation des risques résiduels	Cohérents avec la politique de SI ; exigences, appréciation des risques et résultats du traitement des risques mesurables et pris en compte ; communiqués et mis à jour. Que va-t-on faire ? Quelles ressources seront nécessaires ? Qui sera responsable ? Quand cela sera-t-il réalisé ? Comment les résultats seront-ils évalués ? etc.

PECB

47

Un organisme qui veut planifier et mettre en œuvre un SMSI doit tenir compte des enjeux mentionnés à l'article 4.1 de la norme ISO/IEC27001 (Compréhension de l'organisation et de son contexte) et des exigences mentionnées à l'article 4.2 (Compréhension des besoins et des attentes des parties intéressées) et déterminer les risques et les opportunités qui doivent être pris en compte.

Support

ISO/IEC 27001, article 7

Ressources	Compétence	Sensibilisation	Communication	Documentation
L'organisme doit déterminer et fournir les ressources nécessaires au SMSI.	L'organisme doit s'assurer d'avoir les personnes compétentes pour exécuter les tâches relatives au SMSI.	Les personnes qui travaillent sous le contrôle de l'organisme seront informées de la politique de SI, de leur rôle dans le SMSI et des exigences de l'organisme.	L'organisme doit établir, mettre en œuvre et maintenir des dispositions pour la communication avec les parties intéressées internes et externes pertinentes.	Le SMSI de l'organisme doit inclure les informations documentées exigées par ISO/IEC 27001 et les enregistrements afin de démontrer l'efficacité du SMSI.

PECB

48

ISO/IEC 27001, article 7.1 Ressources

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

ISO/IEC 27001, article 7.2 Compétence

L'organisation doit:

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

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

ISO/IEC 27001, article 7.3 Sensibilisation

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

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

Page de notes

PECB

49

ISO/IEC 27001, article 7.4 Communication

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

- a. *sur quels sujets communiquer;*
- b. *à quels moments communiquer;*
- c. *avec qui communiquer;*
- d. *qui doit communiquer; et*
- e. *les processus par lesquels la communication doit s'effectuer.*

ISO/IEC 27001, article 7.5.1 Généralités

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

- *les informations documentées exigées par la présente Norme internationale; et*
- *les informations documentées que l'organisation juge nécessaires à l'efficacité du système de management de la sécurité de l'information.*

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

- *la taille de l'organisation, ses domaines d'activité et ses processus, produits et services;*
- *la complexité des processus et de leurs interactions; et*
- *la compétence des personnes.*

Information documentée

ISO/IEC 27001, article 7.5

Une procédure doit être établie pour gérer le cycle de vie des documents :



PECB

50

ISO/IEC27001, article 7.5.2 Crédation et mise à jour

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

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

ISO/IEC27001, article 7.5.3 Maîtrise des informations documentées

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

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

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

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

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

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

Planification et contrôle opérationnels

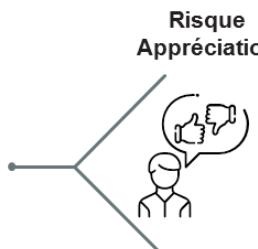
ISO/IEC 27001, article 8.1

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

Appréciation et traitement des risques de sécurité de l'information

ISO/IEC 27001, article 8.2 et 8.3

L'organisation doit réaliser des appréciations des risques de sécurité de l'information à des intervalles planifiés ou quand des changements significatifs sont prévus ou ont lieu, en tenant compte des critères établis en 6.1.2 a).



L'organisation doit mettre en œuvre le plan de traitement des risques de sécurité de l'information.



PECB

52

ISO/IEC27001, article 8.2Appréciation des risques de sécurité de l'information

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

ISO/IEC 27001, article 8.3 Traitement des risques de sécurité de l'information

L'organisation doit conserver des informations documentées sur les résultats du traitement des risques de sécurité de l'information.

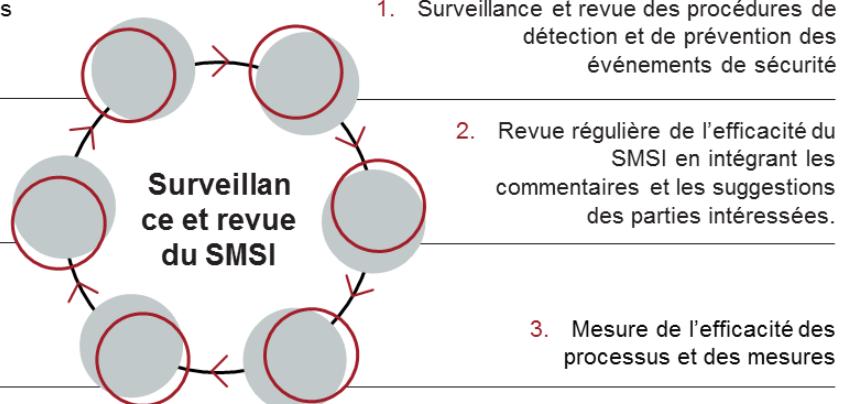
Surveillance et revue du SMSI

ISO/IEC 27001, article 9

6. Revue de direction et mise à jour des plans de sécurité

5. Mener des audits internes

4. Revue de l'appréciation et du traitement des risques



1. Surveillance et revue des procédures de détection et de prévention des événements de sécurité

2. Revue régulière de l'efficacité du SMSI en intégrant les commentaires et les suggestions des parties intéressées.

3. Mesure de l'efficacité des processus et des mesures

PECB

53

ISO/IEC 27001, article 9.1 Surveillance, mesure, analyse et évaluation

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

L'organisation doit déterminer:

- a. ce qu'il est nécessaire de surveiller et de mesurer, y compris les processus et les mesures de sécurité de l'information;
- b. les méthodes de surveillance, de mesurage, d'analyse et d'évaluation, selon le cas, pour assurer la validité des résultats;
 - NOTE: Il convient que les méthodes choisies donnent des résultats comparables et reproductibles pour être considérées comme valables.
- c. quand la surveillance et les mesures doivent être effectuées;
- d. qui doit effectuer la surveillance et les mesures;
- e. quand les résultats de la surveillance et des mesures doivent être analysés et évalués; et
- f. qui doit analyser et évaluer ces résultats.

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

Audit interne du SMSI

ISO/IEC 27001, article 9.2

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

a) est conforme:

- 1) aux exigences propres de l'organisation concernant son système de management de la sécurité de l'information; et
- 2) aux exigences de la présente Norme internationale;

b) est efficacement mis en œuvre et tenu à jour.

L'organisation doit:

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

54

Les audits internes sont utilisés pour estimer le respect des exigences d'une norme sur les systèmes de management. Des activités régulières d'audit interne permettent l'évaluation continue de l'efficacité du système de management et l'identification des opportunités d'amélioration.

L'organisme doit mettre en œuvre un programme d'audit interne pour déterminer si le système de management atteint les objectifs définis de l'organisme, demeure conforme à la norme de même qu'aux autres exigences internes, juridiques, réglementaires et contractuelles et s'il est tenu à jour de manière efficace.

Le programme d'audit doit contenir, au minimum:

1. La définition du critère, du périmètre, de la fréquence, des méthodes et des procédures d'audit
2. La définition des rôles et des responsabilités des auditeurs internes
3. La documentation qui assure l'objectivité et l'impartialité du processus d'audit (exemples: la charte d'audit, le contrat de travail, le code de déontologie des auditeurs internes, etc.)
4. La planification des activités d'audit
5. Les activités de suivi pour auditer les actions prises par l'organisme à la suite de la détection des non-conformités
6. La procédure de conservation en lieu sûr des enregistrements des activités d'audit

Note: La mise en œuvre et le management d'un programme d'audit interne seront expliqués lors du jour4 de la formation.

La revue de direction du SMSI

ISO/IEC 27001, article 9.3

La revue de direction doit prendre en compte:

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

Les conclusions de la revue de direction doivent inclure :

les décisions relatives aux opportunités d'amélioration continue et aux éventuels changements à apporter au système de management de la sécurité de l'information.

PECB

55

Les revues de direction permettent à la direction de l'organisme de revoir périodiquement le niveau de performance (pertinence, adéquation, efficacité et efficiency) du système de management en place. Ces revues permettent à l'organisme de s'adapter ou de recentrer rapidement et efficacement le système de management vers des changements internes ou externes. **Une revue de direction doit être organisée au moins une fois par année.**

Les revues de direction doivent être enregistrées. Il convient que les rapports de ces revues soient distribués à tous les participants à la revue et aux parties intéressées légitimes, dans la mesure définie.

Amélioration du SMSI

ISO/IEC 27001, article 10.1 et 10.2

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

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

- a) réagir à la non-conformité [...];
- b) évaluer s'il est nécessaire de mener une action pour éliminer les causes de la non-conformité, de sorte qu'elle ne se reproduise plus, ou qu'elle ne se produise pas ailleurs. [...];
- c) mettre en œuvre toutes les actions requises;
- d) réviser l'efficacité de toute action corrective mise en œuvre; et
- e) modifier, si nécessaire, le système de management de sécurité de l'information.



56

PECB

ISO/IEC 27001, article 10.1 Non-conformité et actions correctives

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

- a. réagir à la non-conformité, et le cas échéant:
 1. agir pour la maîtriser et la corriger; et
 2. traiter les conséquences;
- b. évaluer s'il est nécessaire de mener une action pour éliminer les causes de la non-conformité, de sorte qu'elle ne se reproduise plus, ou qu'elle ne se produise pas ailleurs. À cet effet, l'organisation:
 1. examine la non-conformité;
 2. détermine les causes de non-conformité; et
 3. détermine si des non-conformités similaires existent, ou pourraient se produire;
- c. mettre en œuvre toutes les actions requises;
- d. réviser l'efficacité de toute action corrective mise en œuvre; et
- e. modifier, si nécessaire, le système de management de sécurité de l'information.

Les actions correctives doivent être à la mesure des effets des non-conformités rencontrées.

L'organisme doit conserver des informations documentées comme preuves:

- f. de la nature des non-conformités et de toute action subséquente; et
- g. des résultats de toute action corrective.

ISO/IEC 27000, article 3.20. Efficacité

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

Annexe A

Objectifs et mesures de sécurité

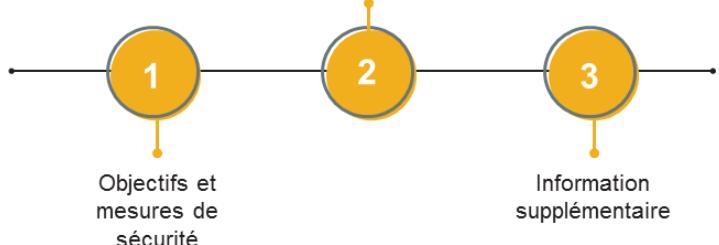
ISO/IEC 27001

Annexe A
(Liste des objectifs et des mesures de sécurité)



ISO/IEC 27002

Recommandations pour la mise en œuvre



Note importante : ISO/IEC 27002 étant un code de pratique, il n'est pas exigible d'observer ses lignes directrices pour obtenir la certification ISO/IEC 27001.

PECB

57

Les objectifs et les mesures de sécurité énumérés dans l'Annexe A (A.5 à A.18) d'ISO/IEC 27001 sont alignés sur les objectifs et les mesures de sécurité énumérés dans les articles 5 à 18 d'ISO/IEC 27002.

Les listes des objectifs et des mesures de sécurité contenus dans l'Annexe A d'ISO/IEC 27001 ne sont pas exhaustives. Un organisme peut choisir des objectifs et des mesures de sécurité supplémentaires ou choisir des mesures d'une source complètement différente.

114 Mesures de sécurité

ISO/IEC 27001, Annexe A

A 5	Politiques de sécurité de l'information	2 mesures
A 6	Organisation de la sécurité de l'information	7 mesures
A 7	Sécurité des ressources humaines	6 mesures
A 8	Gestion des actifs	10 mesures
A 9	Contrôle d'accès	14 mesures
A 10	Cryptographie	2 mesures
A 11	Sécurité physique et environnementale	15 mesures
A 12	Sécurité liée à l'exploitation	14 mesures
A 13	Sécurité des communications	7 mesures
A 14	Acquisition, développement et maintenance des systèmes d'information	13 mesures
A 15	Relations avec les fournisseurs	5 mesures
A 16	Gestion des incidents liés à la sécurité de l'information	7 mesures
A 17	Aspects de la sécurité de l'information dans la gestion de la continuité de l'activité	4 mesures
A 18	Conformité	8 mesures

PECB

58

Les objectifs et les mesures de sécurité énumérés à l'Annexe A (A.5 à A.18) sont étayés par les lignes directrices fournies dans ISO/IEC 27002, articles 5 à 18.

Les listes des objectifs et des mesures de sécurité contenus dans l'Annexe A d'ISO/IEC 27001 ne sont pas exhaustives. Un organisme peut envisager d'inclure des objectifs et des mesures de sécurité supplémentaires si nécessaire (voir article 6.1.3).



Exercice 1

PECB

59

Exercice1: Raisons d'adopter ISO/IEC27001

Veuillez lire la partie suivante de l'étude de cas fournie pour ce cours:

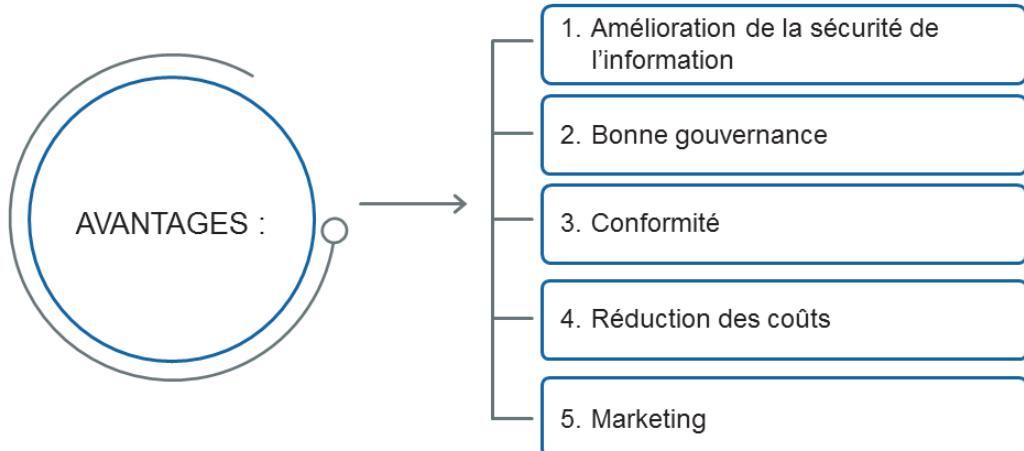
- Introduction et historique

En vous basant sur ces informations, déterminez et expliquez les trois plus grands avantages de la mise en œuvre de la norme ISO/IEC 27001 pour cet organisme et comment on pourrait mesurer ces avantages grâce aux métriques.

Durée de l'exercice: 30 minutes

Commentaires: 15 minutes

Avantages d'ISO/IEC 27001



PECB

60

1. Amélioration de la sécurité de l'information :

- Amélioration générale de l'efficacité de la sécurité de l'information
- Couverture aussi bien des aspects technologiques de sécurité que des autres aspects: sécurité organisationnelle, sécurité physique, etc.
- Revue indépendante du système de management de la sécurité de l'information
- Meilleure sensibilisation à la sécurité de l'information
- Mécanisme de mesure de l'efficacité du système de management de la sécurité de l'information

2. Bonne gouvernance:

- Sensibilisation et responsabilisation du personnel quant à la sécurité de l'information
- Diminution des risques de poursuites judiciaires contre les dirigeants en vertu des principes de due care et de due diligence
- Opportunité d'identifier les faiblesses du SMSI et d'y apporter des corrections
- Augmentation de l'imputabilité de la direction quant à la sécurité de l'information

3. Conformité:

- À d'autres normes ISO
- Aux principes de l'OCDE (Organisation de coopération et de développement économiques)
- À des normes d'industries, par exemple: PCI DSS (Payment Card Industry Data Security Standard), Accord de Bâle II (pour le secteur bancaire)
- Aux lois nationales et régionales en vigueur

4. Réduction des coûts:

- Les décideurs demandent souvent de justifier la rentabilité des projets et exigent des retombées concrètes et mesurables. Un nouveau concept d'évaluation financière a vu le jour et traite spécifiquement du domaine de la sécurité de l'information: Return on Security Investment (ROSI). Le ROSI est un concept dérivé du retour sur investissement (Return on Investment ou ROI). Il peut être interprété comme le gain financier net d'un projet de sécurité en tenant compte de son coût total sur une période donnée.

Page de notes

PECB

61

5. Marketing:

- Différenciation, procurant à l'organisation un avantage concurrentiel
- Satisfaction des exigences du client et des autres parties intéressées
- Consolidation de la confiance de la clientèle, des fournisseurs et des partenaires de l'organisation



Questions ?

PECB

62

Section 4

Concepts et principes fondamentaux de la sécurité de l'information

- Information et actif
- Sécurité de l'information
- Confidentialité, intégrité et disponibilité
- Vulnérabilité, menace et impact
- Risque lié à la sécurité de l'information
- Objectifs et mesures de sécurité
- Classification des mesures de sécurité

PECB

63

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.

Information et actif

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

64

ISO/IEC27000, 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/IEC27001, AnnexeA.8 Gestion des actifs

A.8.1 Responsabilités relatives aux actifs

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

A.8.1.1 Inventaire des actifs

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.

A.8.1.2 Propriété des actifs

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

A.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.

A.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.

Document – Spécification – Enregistrement

ISO 9000, articles 3.8.5, 3.8.7 et 3.8.10

Document

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

Spécification

document formulant des exigences

Enregistrement

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

PECB

65

ISO9000, article 3.8.5 Document

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 le monde 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.
- En protégeant l'organisme contre les menaces et les vulnérabilités, la sécurité de l'information réduit les risques et l'impact sur ses actifs.



PECB

66

ISO/IEC27002, article 0.2Exigences 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,*
- d. *de stockage, de communication et d'archivage de l'information que l'organisation s'est constitué*
- e. *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/IEC27005 fournit des lignes directrices de gestion du risque lié à la sécurité de l'information, y compris des conseils sur l'appreciation du risque, le traitement du risque, l'acceptation du risque, la communication relative au risque, la surveillance du risque et la revue du risque.

Sécurité de l'information

ISO/IEC 27000, article 3.28

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

Note : En outre, d'autres propriétés, telles que l'authenticité, l'imputabilité, la non-répudiation et la fiabilité peuvent également être concernées [mais se résument finalement à C-I-D].



PECB

67

D'autres définitions d'ISO/IEC27000:

ISO/IEC27000, article 3.6 Authenticité

Propriété selon laquelle une entité est ce qu'elle revendique être

ISO/IEC27000, article 3.23 Gouvernance de la sécurité de l'information

Système par lequel un organisme conduit et supervise les activités liées à la sécurité de l'information

ISO/IEC27000, article 3.26 Besoin d'information

Information nécessaire pour gérer les objectifs, les buts, les risques et les problèmes

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 3.29 Continuité de la sécurité de l'information

Processus et procédures visant à assurer la continuité des opérations liées à la sécurité de l'information

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

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

ISO/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

Page de notes

PECB

68

ISO/IEC27000, article 3.34 Communauté de partage d'informations

Groupe d'organismes qui s'accordent pour partager des informations

Note1 à l'article: Un organisme peut être un individu.

ISO/IEC27000, article 3.35 Système d'information

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

ISO/IEC27000, 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/IEC27000, article 3.55 Fiabilité

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

Sécurité de l'information

Couvre tout type d'information :

- Imprimée ou manuscrite
- Enregistrement (en utilisant un support technique)
- Transmise par e-mail ou électroniquement
- Incluse sur un site Web
- Montrée sur vidéos d'entreprise
- Mentionnée durant une conversation



PECB

69

ISO/IEC 27001 est une norme de sécurité de l'information. **Cela signifie qu'elle s'applique à la protection de l'information, quels que soient son type et sa forme, qu'il s'agisse d'une communication humaine numérique, papier, électronique ou verbale.**

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 conforme à son importance pour l'organisation.

A.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.

A.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.

A.8.2.3 Manipulation des actifs

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

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



PECB

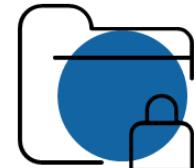
70

Confidentialité: S'assurer que l'information n'est accessible qu'aux individus autorisés.

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

Confidentialité

- 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 permettent aux utilisateurs de rester dans les limites de leur rôle.



PECB

71

Plusieurs types de contrôles d'accès peuvent assurer la confidentialité de l'information. Le chiffrement représente un exemple d'un tel contrôle d'accès. Il peut être utilisé pour protéger la confidentialité de l'information. Les contrôles d'accès peuvent être appliqués à différents aspects d'un système de management de la sécurité de l'information:

- Aspect physique (par exemple, verrous sur les portes, cabinets de classeurs qui se verrouillent, coffrets de sûreté, etc.)
- Aspect logique (par exemple, contrôles d'accès à l'information)

Intégrité

ISO/IEC 27000, article 3.36

Intégrité : propriété d'exactitude et de complétude



PECB

72

Intégrité: Les données doivent être complètes et intactes.

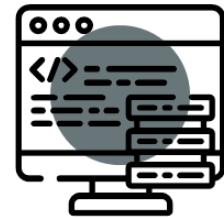
Par exemple: Les données comptables doivent être authentiques (complètes et exactes). L'exactitude des informations est assurée en évitant toute modification injustifiée de ces informations.

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.

Des contrôles d'intégrité doivent être inclus dans les procédures. Ils contribuent à réduire le risque d'erreur, de vol et de fraude. Les contrôles de validation des données, la formation des utilisateurs ainsi que certaines mesures opérationnelles en sont de bons exemples.

Intégrité

- Veiller à ce que les informations ne soient pas modifiées lorsqu'elles sont stockées ou en cours de transfert
- S'assurer que seules les modifications autorisées sont apportées
- S'assurer 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

73

L'intégrité doit être analysée sous trois angles:

- Empêcher un utilisateur ayant l'autorisation de modification de faire une erreur et de changer les données
- Empêcher un utilisateur sans autorisation de modification 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.

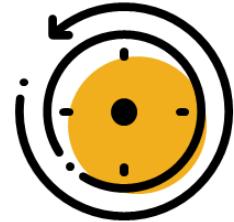
Les données peuvent subir des changements pour plusieurs raisons:

- 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



PECB

74

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

Par exemple, les données relatives aux clients doivent être accessibles au service du marketing.

Disponibilité

La disponibilité de l'information est cruciale pour la sécurité de l'information moderne.

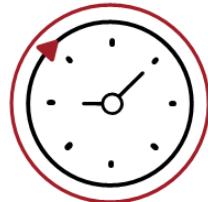
C'est l'information qui est accessible :

- 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 ; par exemple, 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



75

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 définit la vulnérabilité comme suit : *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 qui ne sont pas mises en œuvre correctement ou qui fonctionnent mal pourraient devenir des vulnérabilités.



PECB

76

L'évaluation de la vulnérabilité peut être compliquée par une perception erronée courante selon laquelle les faiblesses ou les lacunes sont toujours associées à des caractéristiques négatives. Plusieurs vulnérabilités sont vraiment des caractéristiques négatives, comme dans un système d'information où les correctifs (*patches*) ne sont pas à jour.

Nous pouvons accepter certaines vulnérabilités en raison des résultats positifs associés au risque que nous prenons. Par exemple, l'achat d'ordinateurs portables peut être un bon exemple par opposition aux ordinateurs de bureau; ils améliorent la mobilité des travailleurs mais augmentent les risques de vol.

Les vulnérabilités peuvent être divisées en deux groupes (intrinsèque et extrinsèque). 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'actif.

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
Logiciels	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

77

L'Annexe D d'ISO/IEC27005 fournit une typologie pour la classification des vulnérabilités que nous pourrions utiliser, en principe. Cependant, cette liste des vulnérabilités devrait être utilisée avec prudence. Cette liste n'est pas exhaustive, car de nouvelles vulnérabilités se produisent régulièrement à cause, entre autres, de l'évolution et des changements dans la technologie.

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

Menaces

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

78

ISO/IEC 27005, article 8.2.3 (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'organisation. Les menaces sont associées à l'aspect négatif du risque et, à ce titre, font référence à des événements indésirables.

Dans les entretiens, il convient qu'un langage simple soit utilisé pour faciliter la discussion sur les menaces. Par exemple, on peut demander aux parties intéressées pour quels événements elles souhaitent préserver les ressources de l'organisation et de fournir à cette fin une liste d'exemples.

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

79

L'Annexe C d'ISO/IEC27005 fournit une typologie pour la classification des menaces. On doit utiliser la liste des menaces avec prudence. Cette liste n'est pas complète et ne peut se prétendre exhaustive, puisque de nouvelles menaces apparaissent régulièrement en raison, entre autres, de l'évolution des technologies et des capacités d'évolution des sources de menaces.

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 : 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

80

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.

Notez que la mise en œuvre incorrecte, la mauvaise utilisation ou la défaillance d'une mesure pourrait, en soi, représenter une menace. Une mesure peut être efficace ou non selon l'environnement dans lequel elle opère. D'un autre côté, une menace qui n'est pas en lien avec une vulnérabilité ne peut pas représenter un risque.

Impact

Exemples d'impacts sur la disponibilité

- Dégradation de la performance
- Interruption du service
- Indisponibilité du service
- Interruption des opérations

Exemples d'impacts sur la confidentialité

- Atteinte à la vie privée des utilisateurs ou des clients
- Atteinte à la vie privée des employés
- Fuite d'information confidentielle

Exemples d'impacts sur l'intégrité

- Changement accidentel
- Changement délibéré
- Résultats incorrects
- Résultats incomplets
- Perte de données

PECB

81

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. Perte d'efficience ou d'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

- *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.*
- *Un risque est souvent exprimé en termes de combinaison des conséquences d'un événement (incluant des changements de circonstances) et de sa « vraisemblance ».*
- *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.*



82

ISO/IEC27000, 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/IEC27000, 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 [...].*

ISO/IEC27000, 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/IEC27000, 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.*

Page de notes

PECB

83

ISO/IEC27000, article 3.64 Appréciation du risque: ensemble du processus d'identification du risque, d'analyse du risque et d'évaluation du risque

ISO/IEC27000, 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/IEC27000, 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

Note 1 à l'article: L'évaluation du risque aide à la prise de décision relative au traitement du risque.

ISO/IEC27000, article 3.68 Identification des risques : processus de recherche, de reconnaissance et de description des risques

Note 1 à l'article: L'identification du risque comprend l'identification des sources de risque, des événements, de leurs causes et de leurs conséquences potentielles.

Note 2 à l'article: Identification du risque.

ISO/IEC27000, article 3.69 Gestion des risques: activités coordonnées visant à diriger et contrôler un organisme vis-à-vis du risque

ISO/IEC27000, 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

Note 1 à l'article : L'ISO/IEC 27005 emploie le terme « processus » pour décrire le management du risque dans sa globalité.

ISO/IEC27000, article 3.71 Propriétaire du risque: personne ou entité ayant la responsabilité du risque et ayant autorité pour le gérer

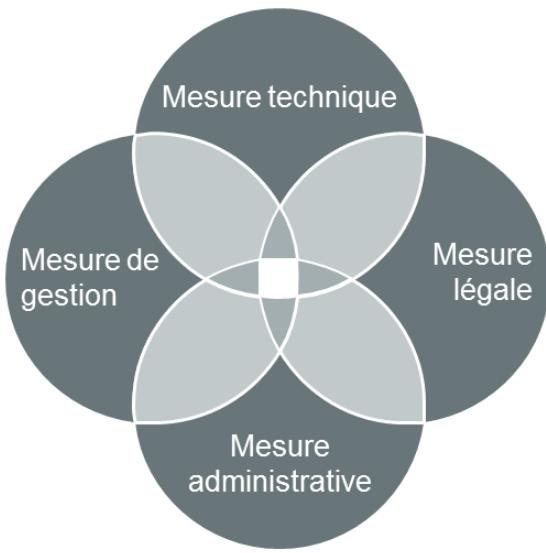
ISO/IEC27000, article 3.72 Traitement du risqué : processus destiné à modifier un risque

processus destiné à modifier un risque : 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.

Objectifs et mesures de sécurité

ISO/IEC 27000, articles 3.14 et 3.15



PECB

Mesure

- mesure qui modifie un risque
- Les mesures de sécurité comprennent tous les processus, politiques, dispositifs, pratiques ou autres actions qui modifient un risque.

Objectif d'une mesure de sécurité

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

84

Les mesures de sécurité de l'information comprennent tout processus, politique, procédure, ligne directrice, pratique ou structure organisationnelle, qui peuvent être de nature administrative, technique, de gestion ou légale, qui modifient les risques liés à la sécurité de l'information. Synonymes de mesure de sécurité: mesure, contre-mesure, dispositif de sécurité, etc.

1. **Mesure technique:** Mesure liée à l'utilisation de mesures techniques ou technologiques comme les pare-feu, les systèmes d'alarme, les caméras de surveillance, les systèmes de détection d'intrusion (IDS), etc.
2. **Mesure administrative:** Mesure liée à la structure organisationnelle comme la séparation des tâches, la rotation des postes, les descriptions de tâches, les processus d'approbation, etc.
3. **Mesure managériale:** Mesure liée à la gestion du personnel, incluant la formation et le coaching des employés, les revues de direction et les audits.
4. **Mesure légale:** Mesure liée aux applications d'une législation, aux exigences réglementaires ou aux obligations contractuelles.

Note:

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

Lien entre les objectifs et les mesures de sécurité

ISO/IEC 27001, Annexe A

Objectifs de sécurité

- S'assurer que l'information bénéficie d'un niveau de protection approprié conforme à son importance pour l'organisation (A.8.2)
- Assurer l'exploitation correcte et sécurisée des moyens de traitement de l'information (A.12.1)
- Limiter l'accès à l'information et aux moyens de traitement de l'information (A.9.1)

Mesures de sécurité

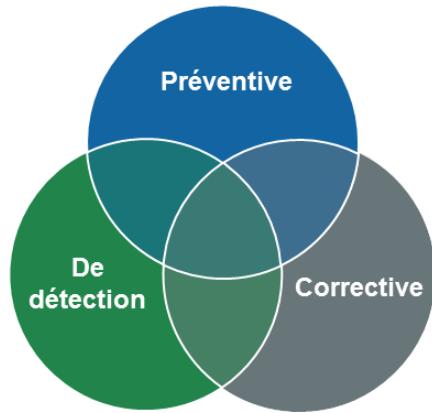
- Classification des informations (A.8.2.1)
 - Marquage des informations (A.8.2.2)
 - Manipulation des actifs (A.8.2.3)
-
- Procédures d'exploitation documentées (A.12.1.1)
 - Gestion des changements (A.12.1.2)
 - Dimensionnement (A.12.1.3)
 - Séparation des environnements de développement, de test et d'exploitation (A.12.1.4)
-
- Politique de contrôle d'accès (A.9.1.1)
 - Accès aux réseaux et aux services réseau (A.9.1.2)

PECB

85

Mesures

Classification des mesures de sécurité



Mesures préventives

Décourager ou prévenir l'apparition des problèmes

Mesures de détection

Rechercher, détecter et identifier les problèmes

Mesures correctives

Résoudre les problèmes détectés et en prévenir la récurrence

PECB

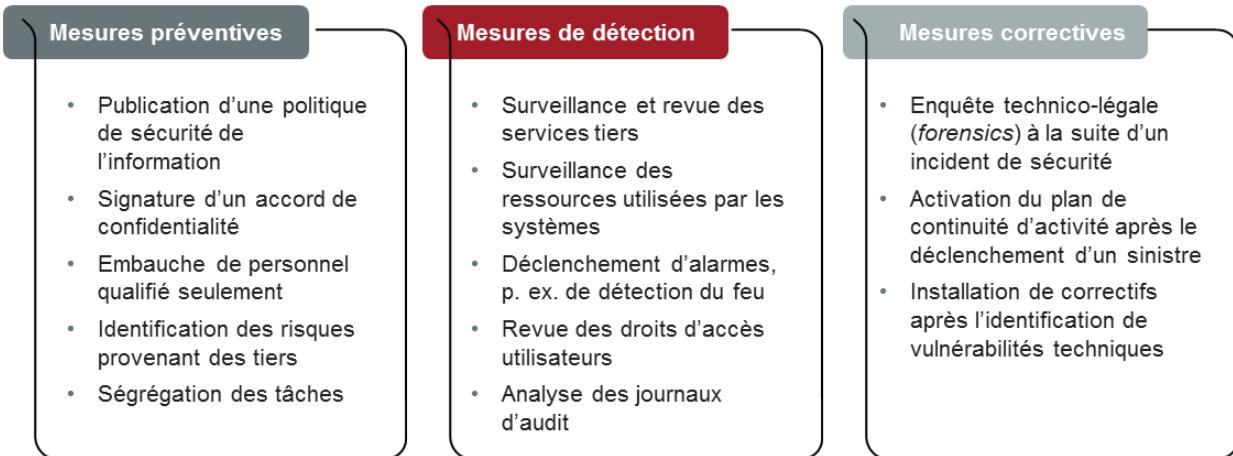
86

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

Note importante: Ces différents types de mesures sont liés entre eux. Par exemple, l'établissement d'une solution antivirus est une mesure préventive pour protéger l'information contre les programmes malveillants. En même temps, elle constitue une mesure de détection quand elle détecte un virus potentiel. Elle offre également une mesure corrective quand un dossier «suspect» est mis en quarantaine ou éradiqué.

Classification des mesures de sécurité

Exemples



PECB

87

1. Mesures préventives

But: Décourager ou prévenir l'apparition de problèmes

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

Exemples

- Séparer le développement des équipements, des essais et de l'exploitation
- Limiter l'accès aux systèmes en dehors des heures de bureau
- Sécuriser les bureaux, les salles et l'équipement
- Utiliser des procédures clairement définies (pour éviter les erreurs)
- Utiliser la cryptographie
- Utiliser un logiciel de contrôle d'accès qui permet uniquement au personnel autorisé d'accéder aux fichiers sensibles

Page de notes

PECB

88

2. Mesures de détection

But : Rechercher et identifier les problèmes et les incidents

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

Exemples

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

3. Mesures correctives

But : Résoudre les problèmes découverts et en prévenir la récurrence

- Minimiser l'impact d'une menace
- Remédier aux problèmes découverts par les mesures de détection
- Identifier les causes du problème
- Corriger les erreurs résultant d'un problème
- Modifier le système de traitement pour réduire au minimum la présence de problèmes futurs

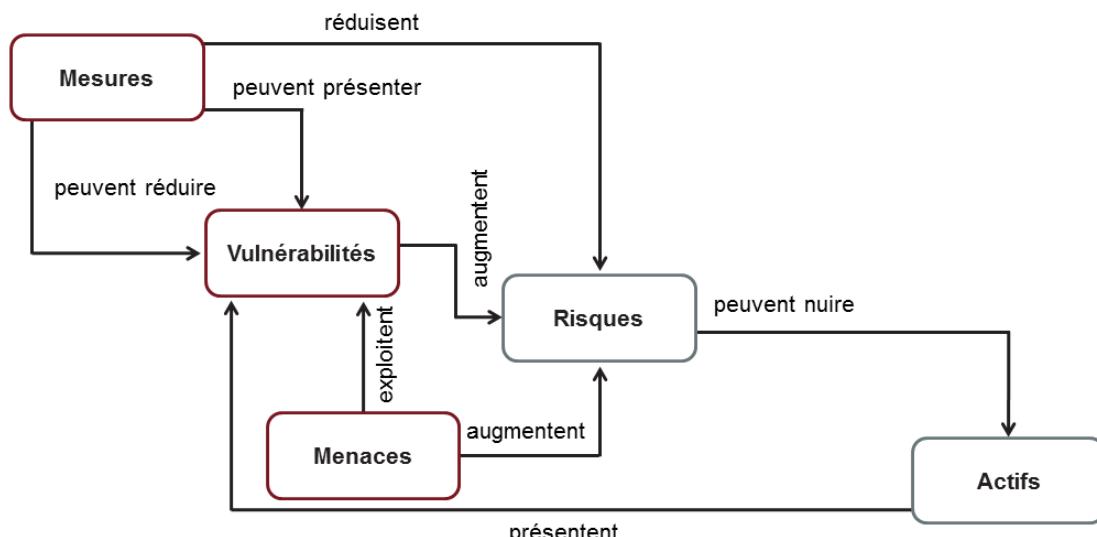
Exemples

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

- Déconnecter automatiquement les sessions inactives
- Installer des correctifs après l'identification de vulnérabilités techniques

Relations entre les éléments de sécurité de l'information

Vue d'ensemble



PECB

89

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 difficile 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.

Exercice 2

PECB

90

Exercice2: Classification des mesures de sécurité

Pour chacune des cinq mesures suivantes, indiquez si elle est utilisée comme mesure préventive, corrective et/ou de détection; précisez si la mesure est une mesure administrative, technique, managériale ou légale. Justifiez votre réponse.

Exemple: L'installation d'une clôture autour du site de l'organisme.

C'est une mesure préventive qui aidera à sécuriser le site de l'organisme contre l'accès physique non autorisé. L'installation d'une clôture métallique est une mesure technique qui implique une installation matérielle.

1. Attribution des responsabilités en matière de sécurité de l'information à chaque membre de l'organisme
2. Mise en place d'un système d'alarme incendie
3. Cryptage des communications électroniques
4. Enquête sur un incident de sécurité
5. Identification de la législation applicable

Durée de l'exercice: 20 minutes

Commentaires: 15 minutes

Questions ?

PECB

91

Section 5

Initiation de la mise en œuvre du SMSI

- Définir l'approche de mise en œuvre du SMSI
- Approches de mise en œuvre proposées
- Application des approches de mise en œuvre proposées
- Choisir un cadre méthodologique pour gérer la mise en œuvre d'un SMSI
- Approche et méthodologie
- Alignement sur les bonnes pratiques

PECB

92



Cette section fournira de l'information qui aidera le participant à acquérir des connaissances sur le processus de recherche d'une approche pour réussir la mise en œuvre du SMSI.

Gestion de projet – Définitions

Définitions ISO 9000 relatives à la gestion de projet

ISO 9000, article 3.4.2 Projet

processus unique qui consiste en un ensemble d'activités coordonnées et maîtrisées comportant des dates de début et de fin, entrepris dans le but d'atteindre un objectif conforme à des exigences spécifiques, incluant les contraintes de délais, de coûts et de ressources

ISO 9000, article 3.3.11 Activité

Smallest identified object of work in a project

ISO 9000, article 3.3.12 Management de projet

Planning, organizing, monitoring, controlling and reporting of all aspects of a project, and the motivation of all those involved in it to achieve the project objectives

PECB

93

Note de terminologie:

1. Les projets sont temporaires en ce sens qu'ils ont un début et une fin définis dans le temps.
2. Un projet individuel peut faire partie d'une structure de projet plus vaste.
3. La complexité des interactions entre les activités d'un projet n'est pas nécessairement liée à la taille du projet.
4. Il convient de faire la distinction entre la gestion du projet SMSI et la gestion des opérations du SMSI. La gestion d'un projet SMSI fait référence à la mise en œuvre d'un SMSI. La gestion des opérations du SMSI, quant à elle, fait référence à la gestion et à l'entretien quotidiens du SMSI.

Note importante: La présente formation vise à expliquer la méthodologie de mise en œuvre du SMSI, et non la gestion des opérations quotidiennes du SMSI.

Définir l'approche de mise en œuvre du SMSI

Sélection de l'approche de mise en œuvre du SMSI basée sur :



PECB

94

Un organisme qui souhaite se conformer à ISO/IEC27001 peut considérer plusieurs approches basées sur:

- **La vitesse de la mise en œuvre**
- **Le niveau de maturité ciblé des processus ou des mesures**
- **Les attentes et le périmètre d'application**

Il est raisonnable de prévoir une période de 6 à 12mois pour le projet, de la conception jusqu'à l'achèvement du premier cycle d'audits et au suivi du système.

Selon un sondage (*ISO/IEC 27001 Global Survey 2008, Certification Europe*) mené auprès de 312entreprises certifiées ISO/IEC27001, 60% d'entre elles déclarent avoir eu besoin de moins de 12mois pour la mise en œuvre du SMSI proposé et 20% d'entre elles ont eu besoin de moins de 6mois. Il est important de signaler que toutes les entreprises qui ont mis moins de 6mois pour mettre en œuvre un SMSI avaient déjà un autre système de management en place dans l'organisme.

Dans le cas des PME, le sondage révèle que, pour un projet SMSI qui dure de 6 à 12mois, il y a 3 à 4personnes travaillant à temps partiel (effort de 35 à 60jours par personne). Pour les grandes entreprises, le temps d'achèvement moyen est de 12 à 18mois, deux personnes en moyenne contribuant à temps plein au projet (en plus de nombreux collaborateurs de temps à autre). Cette moyenne doit s'appliquer à tout type d'organisme déjà raisonnablement sécurisé.

Lorsqu'un périmètre limité pour le SMSI est considéré au début du projet, par exemple, l'approche «IT Governance fast track» (approche destinée à atteindre l'objectif très rapidement dans un contexte d'affaires donné), une organisation de taille moyenne peut espérer compléter de tels projets en 4 à 7mois.

Approches de mise en œuvre proposées

Types



PECB

95

Normalement, les approches de mise en œuvre d'un SMSI proposées sont séquentielles. Le plan de projet de l'organisation est finalisé avant la mise en place d'un projet dédié au SMSI. De même, les phases de surveillance et d'amélioration ne sont activées qu'une fois que l'emplacement des composants du système a été identifié. Dans chaque phase, les processus ou mesures du SMSI peuvent être mis en œuvre de façon séquentielle (par exemple, la politique antivirus est développée et approuvée avant que les procédures et les instructions de travail relatives à la gestion de cette mesure soient effectivement rédigées et mises en place).

L'un des inconvénients importants de cette approche est qu'elle est laborieuse et exige beaucoup de ressources, que ce soit pour planifier, approuver ou mettre en œuvre le système petit à petit. Cette approche élimine également l'intérêt immédiat du système de management à contrôler puisqu'il devra attendre que toutes les pièces du puzzle soient assemblées avant que l'on puisse constater un effet positif direct au sein de l'organisation. Cette approche présente aussi l'inconvénient «d'épuiser» les participants pendant le processus de mise en œuvre, constituant un risque majeur d'abandon en cours de projet.

L'approche proposée dans ce cours tente de contourner cette difficulté en proposant une philosophie axée sur cinq principes directeurs permettant d'initier un tel système dans un délai raisonnable pour l'organisme:

1. **Approche commerciale** – Intégration du SMSI dans le contexte des activités commerciales à l'échelle de l'organisation.
2. **Approche par systèmes** – Mise en œuvre globale des processus du SMSI, et non en isolant certains processus.
3. **Approche systématique** – Application des meilleures pratiques en matière de management de projet telles qu'ISO10006.
4. **Approche intégrée** – Intégration ou harmonisation du SMSI avec d'autres systèmes de management ou exigences établis au sein de l'organisation.
5. **Approche itérative** – Mise en œuvre rapide du SMSI en respectant les exigences minimales de la norme et en procédant ensuite à une amélioration continue.

Application de l'approche de mise en œuvre proposée

Recommandations

1. Éviter l'intégration de nouvelles technologies
2. Intégrer le SMSI dans les processus existants
3. Appliquer les principes de l'amélioration continue
4. Impliquer les parties intéressées de l'organisme
5. Obtenir le soutien de la direction
6. Identifier et nommer formellement un responsable du projet SMSI



PECB

96

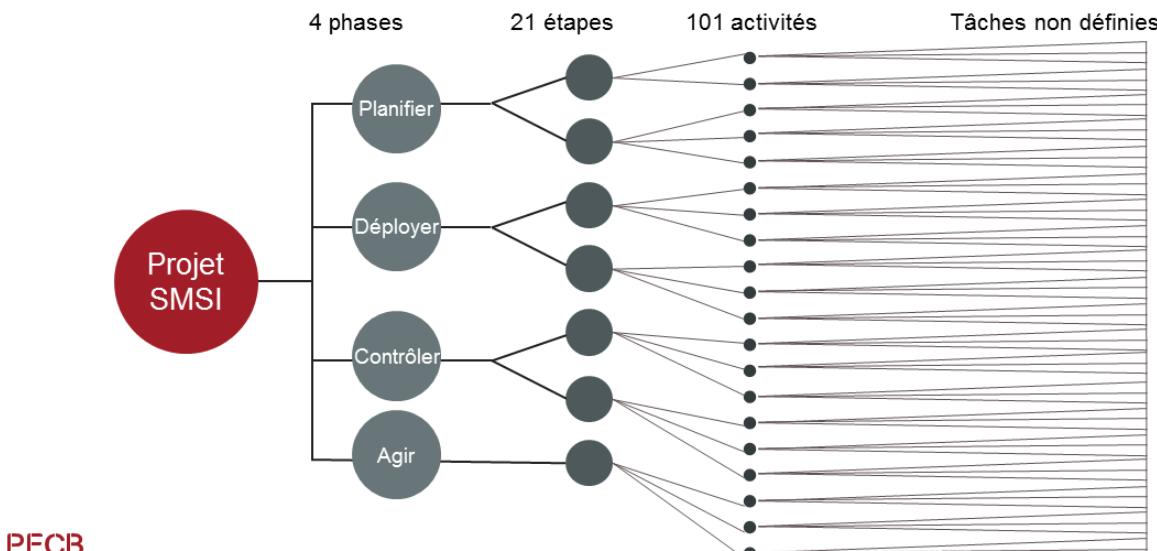
Voici quelques recommandations pour appliquer convenablement les approches de mise en œuvre proposées dans la pratique:

1. **Éviter l'intégration de nouvelles technologies** – Concevoir le système initial avec les technologies déjà en place dans l'organisme. La plupart des organismes ont déjà mis en place les technologies nécessaires pour mettre en œuvre un SMSI. L'optimisation du SMSI avec des technologies plus efficaces pourra se faire en mode d'amélioration continue par la suite.
2. **Intégrer le SMSI dans les processus existants** – Utiliser les processus personnalisés existants et ajuster ces processus en fonction des exigences du cadre SMSI. Éviter de créer des processus qui ne collent pas à la réalité de l'organisme.
3. **Appliquer les principes de l'amélioration continue** – Appliquer les principes d'amélioration continue en tenant compte des suggestions d'amélioration recommandées par toutes les parties intéressées du projet. Des objectifs à petite échelle devraient être envisagés dès le départ et une amélioration progressive doit être fixée pour le long terme.
4. **Impliquer les parties intéressées de l'organisme** – Définir les rôles et les responsabilités de toutes les parties intéressées au projet dès le début du processus de mise en œuvre, s'assurer de leur implication-motivation, analyser leurs relations et les maintenir dans le système une fois qu'il est initié.
5. **Obtenir le soutien de la direction** – S'assurer que la direction comprend et appuie le projet. Ce sont eux qui fourniront les ressources et les autres moyens nécessaires à la réussite de la mise en œuvre du système de management. Ils procéderont également à des revues régulières du système de management au fil du temps afin d'en assurer le succès continu.
6. **Identifier et nommer officiellement un gestionnaire de projet SMSI** – Identifier et nommer une personne qui sera responsable de la mise en œuvre du projet. Celui-ci ne sera pas forcément le responsable du SMSI dans sa forme achevée, mais sera garant de la bonne marche des opérations d'implantation, de leur calendrier et de leur support (budget, approbations, etc.)

Note importante: Il n'est pas nécessaire de mettre en œuvre des systèmes de management dans le but de traiter des questions complexes. La plupart du temps, le sens commun et la gestion de projets dicteront la conduite à adopter.

Méthodologie de mise en œuvre intégrée des systèmes de management et des normes (IMS2)

Méthodologie PECB pour la mise en œuvre du SMSI



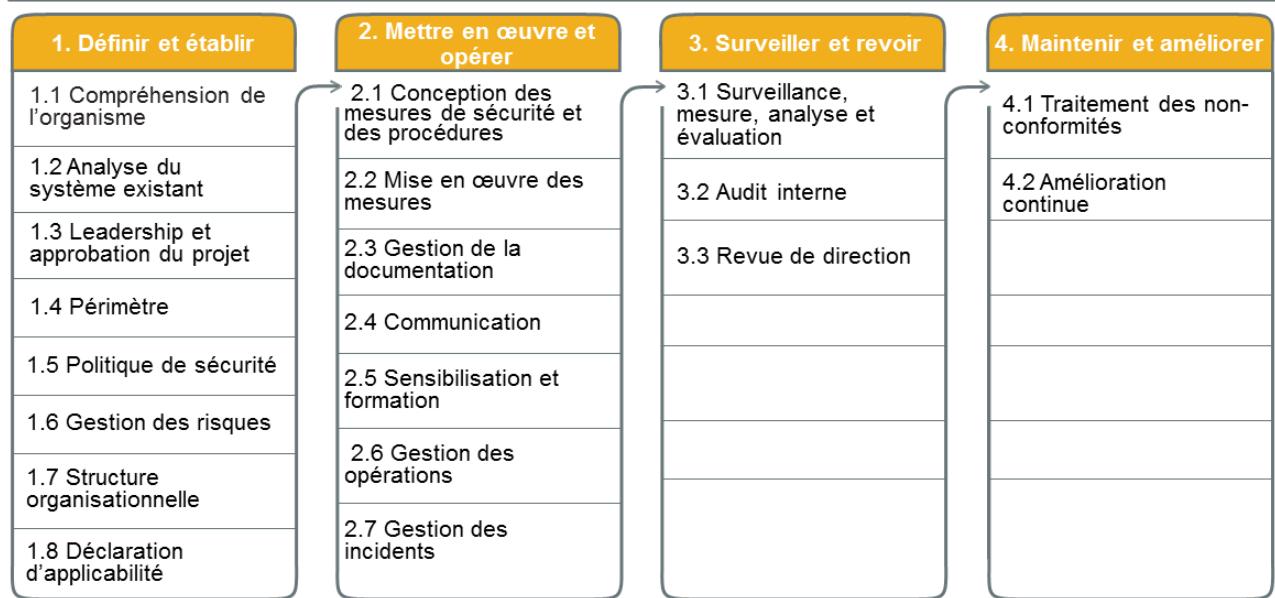
97

PECB a développé une méthodologie pour mettre en œuvre un système de management. Cette méthodologie est appelée «Méthodologie de mise en œuvre intégrée des systèmes de management et des normes (IMS2)» et est basée sur les bonnes pratiques. Elle s'appuie aussi sur les lignes directrices des normes ISO et satisfait aux exigences d'ISO/IEC27001.

IMS2 est basée sur le cycle PDCA divisé en quatre phases: Planifier, Déployer, Contrôler et Agir. À leur tour, ces phases sont divisées en étapes, les étapes en activités, les activités en tâches, etc. Au cours de la formation, les étapes et les activités seront présentées dans l'ordre chronologique du déroulement d'un projet de mise en œuvre.

Les tâches ne seront pas détaillées parce qu'elles sont spécifiques à chaque projet et dépendent du contexte de l'organisme. Par exemple, les activités 1.4.2 (Établir l'équipe de projet SMSI) impliqueront une série de tâches telles que la description des postes, l'entrevue des candidats, la signature d'un contrat, etc.

Choisir un cadre méthodologique pour gérer la mise en œuvre d'un SMSI



PECB

98

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.

Notes importantes:

1. Peu importe la méthodologie utilisée, l'organisme doit l'adapter à son contexte particulier (exigences, taille de l'organisme, périmètre, objectifs, etc.) et non l'appliquer de façon rigide.
2. La séquence des différentes étapes peut être changée (interversion, fusion, etc.). Par exemple, la mise en œuvre de la procédure de gestion de la documentation peut être effectuée avant la compréhension de l'organisation.
3. De nombreux processus sont itératifs en raison de la nécessité d'un développement progressif tout au long du projet de mise en œuvre, par exemple, la communication et la formation.

Approche et méthodologie

Basée sur les meilleures pratiques



ISO 10006
Lignes directrices pour
le management de la
qualité dans les projets



PMBOK
Guide PMBOK (*Project
Management Body of
Knowledge*)



ISO/IEC 27003
Lignes directrices pour la
mise en œuvre d'un
système de management
de la sécurité de
l'information

PECB

99

ISO10006: Systèmes de management de la qualité – Lignes directrices pour le management de la qualité dans les projets. ISO10006 donne des conseils sur l'application du management de la qualité aux projets. Elle est applicable à des projets de taille, de durée et de complexité variées, dans des environnements variés, quel que soit le type de produits ou de processus. Il peut être nécessaire d'adapter ces conseils à un projet précis.

Source: www.iso.org

Guide PMBOK (Project Management Body of Knowledge): Le Guide PMBOK identifie et décrit les connaissances et les pratiques applicables à la plupart des projets. Il reconnaît cinq processus de base: démarrage, planification, exécution, surveillance et maîtrise, et finalement clôture. Les processus sont décrits en termes d'éléments d'entrée (documents, plans, conceptions, etc.), d'outils et de techniques (mécanismes appliqués aux éléments d'entrée) et d'éléments de sortie (documents, produits, etc.). Le Guide PMBOK définit également dix domaines de connaissances: Gestion de l'intégration du projet, Gestion du périmètre du projet, Gestion de l'échéancier du projet, Gestion des coûts du projet, Gestion de la qualité du projet, Gestion des ressources du projet, Gestion des communications du projet, Gestion des risques du projet, Gestion des approvisionnements du projet et Gestion des parties prenantes du projet

Source: www.pmi.org

Méthodologie basée sur ISO/IEC 27003



ISO/IEC 27003

- Fournit un cadre méthodologique et des lignes directrices (aucun outil n'est fourni)
- Décrit à haut niveau les étapes de mise en œuvre, la liste des activités et des livrables associés à un SMSI

Note importante : L'utilisation de la méthodologie PECB n'est pas une condition préalable à l'obtention de la certification SMSI.

PECB

100

Méthodologie PECB

- Décrit une méthodologie opérationnelle, étape par étape, basée sur les lignes directrices d'ISO/IEC 27003
- Inclut des exemples et des modèles de mise en œuvre

ISO/IEC27003 décrit les principales étapes de la mise en œuvre d'un SMSI. Elle guide l'utilisateur tout au long du processus et facilite la mise en œuvre efficace du SMSI. La norme contient les sections suivantes:

1. Introduction
2. Domaine d'application
3. Termes et définitions
4. Contexte de l'organisation
5. Leadership
6. Planification
7. Support
8. Opération
9. Évaluation de la performance
10. Amélioration

Le cadre méthodologique proposé par ISO/IEC27001 est générique et applicable à tous les types d'organismes, quels que soient leur taille, leur type ou leur activité. Cependant, ISO/IEC 27003 n'est pas une référence exhaustive et elle ne prétend pas d'être universelle. Ce cadre n'est pas une méthodologie formelle, car il ne contient pas d'approche opérationnelle outillée. Il est à noter que son utilisation n'est pas une exigence en soi pour obtenir la certification ISO/IEC 27001.

Veuillez noter qu'ISO/IEC 27003 est rédigée de manière à communiquer les exigences d'ISO/IEC 27001 de telle sorte qu'il ne soit plus nécessaire d'avoir ISO/IEC 27001 à portée de main.

Page de notes

PECB

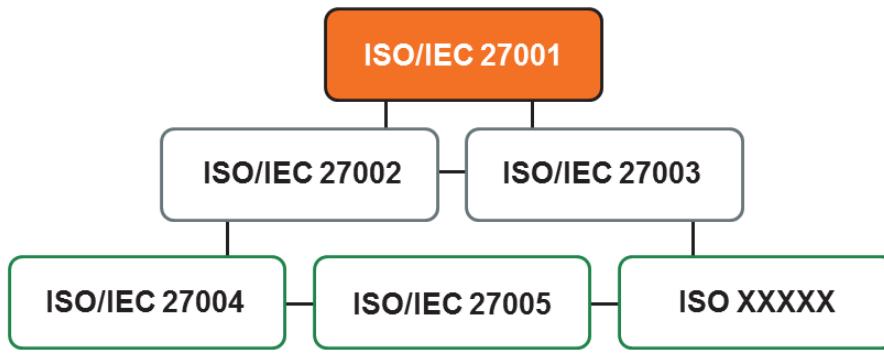
101

La méthodologie proposée par PECB est basée en partie sur l'approche décrite dans la norme ISO/IEC27001 mais ne prétend pas la remplacer. L'objectif de cette méthodologie est d'introduire une mise en œuvre opérationnelle, étape par étape, du SMSI. Autrement dit, elle explique à l'aide d'exemples et d'outils, le «comment» à partir de «quoi», comme décrit dans ISO/IEC27001.

Note importante: Pendant cette formation, tous les sujets ne sont pas abordés en détail. Par conséquent, les sujets brièvement mentionnés ici ne doivent pas nécessairement être considérés comme négligeables.

S'aligner sur les bonnes pratiques

Utilisation des normes ISO



Note : ISO XXXXX se réfère à des normes qui seront développées dans l'avenir.

PECB

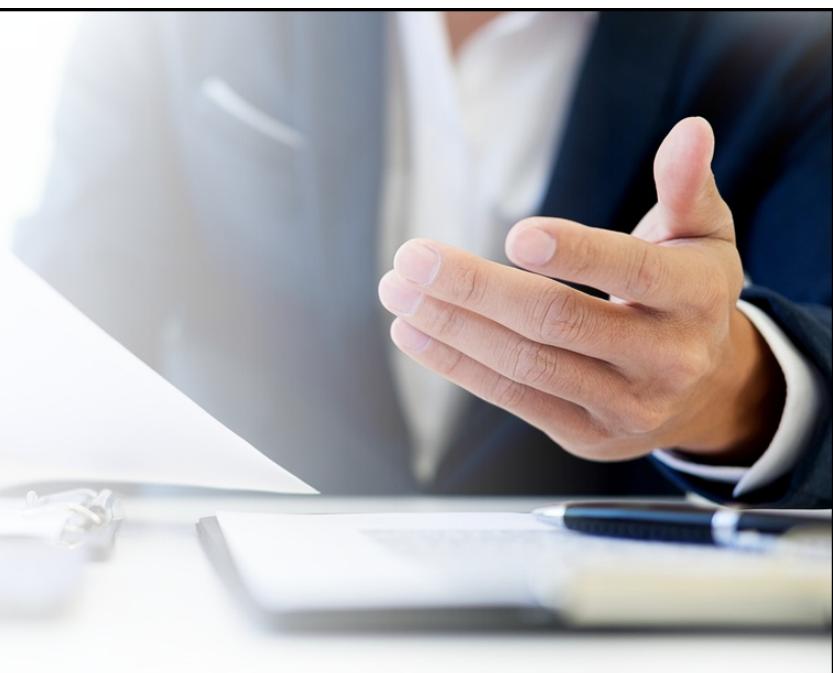
102

L'essentiel des bonnes pratiques incluses dans les différentes normes ISO permet d'avoir accès aux connaissances qui font l'objet d'un consensus auprès des experts de la sécurité de l'information. Ces bonnes pratiques ne doivent pas être confondues avec les exigences des normes. Une bonne pratique est une recommandation et non une exigence. Cela signifie que chaque organisme est libre de s'y référer ou non, voire de l'appliquer ou non.

Par choix, ce sont les bonnes pratiques publiées dans les différentes normes ISO qui sont présentées dans cette formation. Cependant, il existe plusieurs autres corpus de bonnes pratiques telles que les normes ANSI ou la bibliothèque ITIL. Un organisme peut aussi se référer à ISO/IEC27035 pour élaborer son processus de gestion des incidents. Il pourrait tout aussi bien se baser sur ITIL ou encore sur les guides du CERT (Computer Emergency Response Team) en la matière.

Note de terminologie:

1. «Bonne pratique» signifie qu'il est généralement reconnu que la mise en œuvre de recommandations associées à des pratiques décrites correspond aux activités, aux outils et aux techniques largement utilisés par les spécialistes du domaine.
2. «Généralement reconnu» signifie que les connaissances et les pratiques présentées sont le plus souvent applicables à la majorité des organismes, de même que leurs valeurs et leur utilité font l'objet d'un consensus assez large.



Questions ?

PECB

103

Section 6

Compréhension de l'organisme et de son contexte

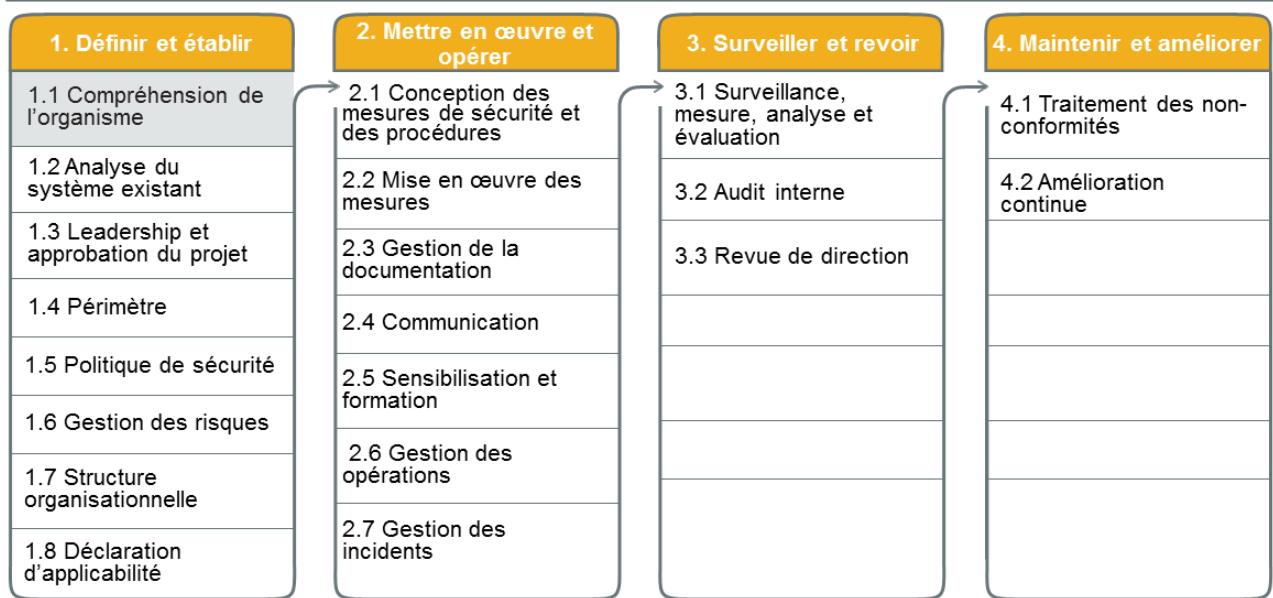
- Mission, objectifs, valeurs, stratégies de l'organisme
- Environnement interne et externe
- Principaux processus et activités
- Parties intéressées
- Exigences métier
- Objectifs du SMSI
- Définition préliminaire du périmètre

PECB

104

La présente section fournira des informations qui aideront le participant à comprendre l'importance de l'identification des facteurs internes et externes qui peuvent influer sur la mise en œuvre d'un SMSI, les processus clés et les parties intéressées impliquées dans la mise en œuvre d'un SMSI, et les informations requises pour planifier la mise en œuvre du SMSI.

1.1 Compréhension de l'organisme



PECB

105

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.



PECB

106

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

1. Être en mesure de démontrer que son SMSI est aligné avec sa mission, ses objectifs et ses stratégies d'affaires
2. Identifier et documenter les activités de l'organisme, ses fonctions, ses services, ses produits, ses partenariats, ses chaînes d'approvisionnement et ses relations avec les parties intéressées
3. Définir les facteurs externes et internes qui peuvent influencer le SMSI
4. Connaître et tenir compte des difficultés relatives à la sécurité de l'information dans son secteur industriel, comme le risque, les obligations légales et réglementaires et les exigences du client
5. Établir et documenter les objectifs du SMSI

ISO/IEC 27001 Exigences

ISO/IEC 27001, article 4.2

L'organisation doit déterminer:

- a) les parties intéressées qui sont concernées par le système de management de la sécurité de l'information; et
- b) les exigences de ces parties intéressées concernant la sécurité de l'information.

NOTE: Les exigences des parties intéressées peuvent inclure des exigences légales et réglementaires et des obligations contractuelles.

PECB

107

Définitions reliées au concept de «l'organisme»

- **Organisme:** personne ou groupe de personnes ayant un rôle avec les responsabilités, l'autorité et les relations lui permettant d'atteindre ses objectifs (ISO9000, 3.2.1)
- **Infrastructure:** système des installations, équipements et services nécessaires au fonctionnement d'un organisme (ISO9000, 3.5.2)
- **Exigence:** besoin ou attente formulé, généralement implicite ou obligatoire (ISO9000, 3.6.4)

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, un travailleur indépendant, 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/IEC27001 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/IEC27005.
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).

Page de notes

PECB

108

ISO/IEC 27003 article 4.1 Compréhension de l'organisme et de son contexte

Les enjeux externes sont ceux qui échappent au contrôle de l'organisme. On y réfère souvent comme à l'environnement de l'organisation. L'analyse de cet environnement peut comprendre les aspects suivants: social et culturel; politique, légal, normatif et réglementaire; financier et macroéconomique; technologique; naturel; et compétitif.

Les enjeux internes sont soumis au contrôle de l'organisme. L'analyse des enjeux internes peut inclure les aspects suivants: culture de l'organisme; politiques, objectifs et stratégies pour les atteindre; gouvernance, structure organisationnelle, rôles et responsabilités; normes, lignes directrices et modèles adoptés par l'organisme; relations contractuelles qui peuvent affecter directement les processus de l'organisme inclus dans le périmètre du SMSI; processus et procédures; capacités, en termes de ressources et de connaissances (par exemple, capital, temps, personnes, processus, systèmes et technologies); infrastructure physique et environnement; systèmes d'information, flux d'information et processus décisionnels (formels et informels); et résultats des audits précédents et analyses d'appreciation des risques précédentes.

À mesure que les enjeux externes et internes changent, les enjeux et leur influence sur le périmètre, les contraintes et les exigences du SMSI devraient être régulièrement revus.

ISO/IEC 27003 article 4.2 Compréhension des besoins et des attentes des parties intéressées

Les parties intéressées externes peuvent comprendre: régulateurs et législateurs; actionnaires y compris les propriétaires et les investisseurs; fournisseurs y compris les consultants et les sous-traitants; associations industrielles; concurrents; clients et consommateurs; et groupes d'activistes.

Les parties intéressées internes peuvent comprendre: décideurs, y compris la haute direction; propriétaires de processus, de systèmes et d'informations; fonctions de soutien telles que les TI ou les ressources humaines; employés et utilisateurs; et professionnels de la sécurité de l'information.

1.1 Compréhension de l'organisme

Liste des activités

1.1.1

Comprendre la mission, les objectifs, les valeurs et les stratégies

1.1.6

Déterminer les objectifs du SMSI

1.1.2

Analyser l'environnement interne et externe

1.1.7

Déterminer le périmètre préliminaire

1.1.3

Identifier les principaux processus et activités

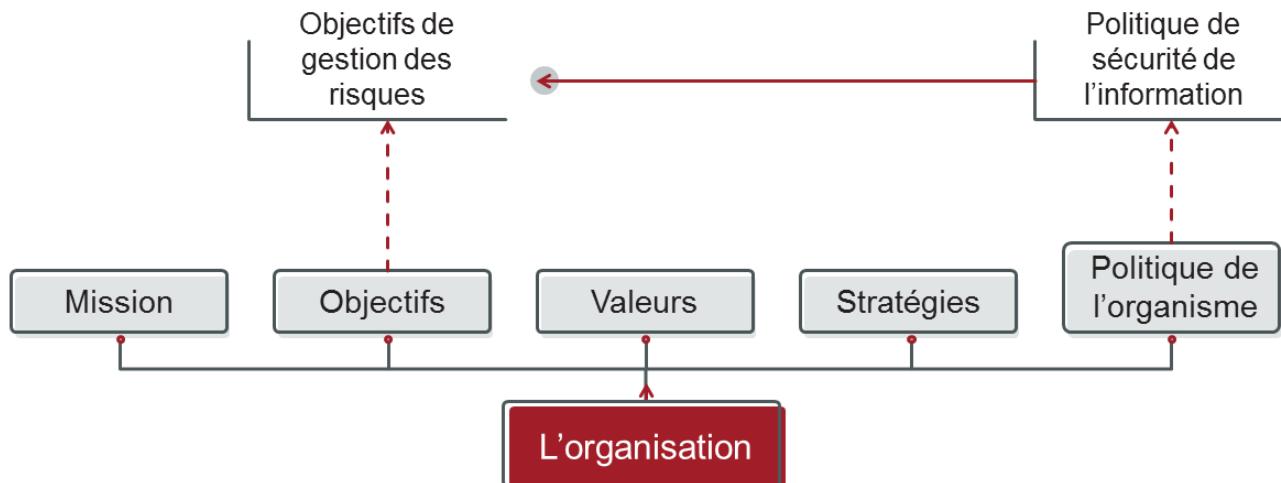
1.1.4

Identifier et analyser les parties intéressées

1.1.5

Identifier et analyser les exigences métier

1.1.1 Comprendre la mission, les objectifs, les valeurs et les stratégies



PECB

110

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. Des informations générales sur l'organisme devraient être recueillies afin de mieux comprendre sa mission, ses stratégies, ses principaux objectifs, ses valeurs, etc. Cela permet de veiller à la cohérence et à l'alignement entre les objectifs stratégiques établis pour la sécurité de l'information et la mission de l'organisme.

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

Implications pour la gestion des risques: La gestion des risques de la sécurité de l'information a pour objectif de soutenir l'organisme dans l'accomplissement de sa mission de protection de ses actifs informationnels. Le SMSI doit donc être aligné sur la mission de l'entreprise.

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.

Implications pour la gestion des risques: Les valeurs de l'organisme influencent les choix faits par les professionnels de la gestion des risques TI (par exemple, les valeurs peuvent influencer les priorités et les politiques en matière d'évaluation des risques).

Objectifs: Les objectifs sont le résultat que l'organisme veut atteindre. Les objectifs sont généralement prédéterminés, quantifiés et limités dans le temps (par exemple, augmenter la part de marché de 5% au cours des 24 mois suivants).

Implications pour la gestion des risques: Quant à la stratégie, le management des risques doit être aligné sur les objectifs de l'organisme en identifiant les risques liés à l'information qui doivent être gérés par l'organisme.

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

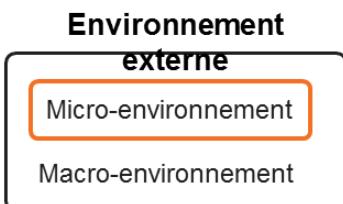
Implications pour la gestion des risques: Les choix de traitement et les actions qui en découlent seront également fonction de la stratégie définie par l'organisme.

1.1.2 Analyser l'environnement interne et externe

- **P**olitique
- **E**conomique
- **S**ocial
- **T**echnologique

Avis pratiques

- Étant donné qu'ISO/IEC 27005 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 utiles.
- Plusieurs méthodologies existent pour comprendre le fonctionnement d'un organisme
- L'important est d'identifier les caractéristiques des facteurs internes et externes qui influenceront la gestion des risques : mission, principales activités, parties intéressées, etc.



PECB

111

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.

Voici certains des modèles les plus fréquemment utilisés:

Analyse SWOT (Strengths, Weaknesses, Opportunities, Threats – Forces, Faiblesses, Opportunités, Menaces): L'analyse SWOT est utilisée pour effectuer une analyse approfondie des forces, des faiblesses, des opportunités et des menaces d'un organisme. L'analyse est effectuée dans le but de formuler des politiques et de déterminer où l'organisme devrait investir ses ressources (Tirer parti des opportunités? Réduire les faiblesses? Faire face aux menaces?). Les forces et les faiblesses visent à évaluer les enjeux internes, tandis que les opportunités et les menaces servent à évaluer les enjeux externes d'un organisme.

Analyse PEST (Political, Economic, Social, Technological – Politique, Économique, Social, Technologique): L'analyse PEST permet à l'organisme d'analyser les forces du marché et les opportunités dans les quatre domaines suivants: social, technologique, économique et politique. Certains auteurs ont ajouté deux catégories supplémentaires: environnementale et légale.

L'analyse des cinq forces de Porter: L'analyse des cinq forces de Porter examine le niveau de compétitivité des organismes en utilisant les cinq facteurs qui influencent l'environnement d'affaires d'une industrie. Ces cinq forces sont l'intensité de la rivalité entre concurrents, le pouvoir de négociation des clients, la menace de nouveaux venus potentiels sur le marché, le pouvoir de négociation des fournisseurs et la menace de produits de remplacement.

Analyser l'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 ?)



112

PECB

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 de la répartition des tâches, des responsabilités, de l'autorité et de la communication dans l'organisme. Il convient également d'identifier les fonctions externalisées aux sous-traitants.

La structure de l'organisme peut être de différents types:

1. La structure divisionnaire: chaque division est placée sous l'autorité d'un directeur de division responsable des décisions stratégiques, administratives et opérationnelles au sein de cette unité.
2. La structure fonctionnelle: l'autorité fonctionnelle est exercée sur les procédures, sur la nature du travail et parfois sur les décisions ou la planification (ex.: la production, les technologies de l'information, les ressources humaines, le marketing, etc.).

Notes:

- Une division au sein de l'organisme ou une structure divisionnaire peut être organisée en structure fonctionnelle et inversement.
- On dit qu'un organisme a une structure matricielle lorsque l'ensemble de l'organisme est basé sur les deux types de structure.
- Quelle que soit la structure, les niveaux suivants sont distingués:
 1. Le niveau décisionnel (responsable de l'élaboration des politiques et des stratégies)
 2. Le niveau de pilotage (responsable de la coordination et de la gestion des activités)
 3. Le niveau opérationnel (responsable de la production et des activités de soutien)

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.

Contexte interne – Aspects principaux

ISO/IEC 27000, article 3.38

Le contexte interne peut inclure :

- la gouvernance, la structure organisationnelle, les rôles et les responsabilités;*
- les politiques, objectifs et stratégies mises en place pour atteindre ces derniers;*
- les capacités, en termes de ressources et de connaissances (par exemple : capital, temps, personnel, processus, systèmes et technologies);*
- les systèmes d'information, flux d'information et processus de prise de décision (formels et informels);*
- les relations avec les parties prenantes internes, les perceptions et valeurs associées à celles-ci;*
- la culture de l'organisme;*
- les normes, lignes directrices et modèles adoptés par l'organisme;*
- la forme et l'étendue des relations contractuelles.*

PECB

113

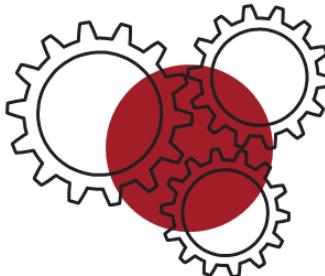
ISO/IEC 27000, article 3.38 Contexte interne

environnement interne dans lequel l'organisme cherche à atteindre ses objectifs

1.1.3 Identifier les 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 ?

Note :

À cette étape, il ne s'agit pas d'effectuer une cartographie complète des processus, mais seulement d'établir une liste générale.

PECB

114

Il est essentiel que le gestionnaire de projet SMSI connaisse les **activités de l'organisme** qui ont une incidence sur la sécurité de l'information. En effet, le type de produits et services offerts par l'organisme aura une influence majeure sur son modèle d'affaires. De plus, ces produits et services peuvent exposer l'organisation à des risques particuliers, comme les risques liés à la sécurité de l'information, les pénalités, les amendes, etc.

Le gestionnaire de projet SMSI devrait également comprendre les **processus opérationnels** de l'organisation puisque ces processus exposent l'organisation à de nombreux risques de sécurité de l'information. Le gestionnaire des risques doit donc analyser et comprendre la nature de ces processus et déterminer quels sont les risques directs et indirects auxquels l'organisme s'expose en menant ses activités.

L'**identification des actifs informationnels de l'organisme** est un élément déterminant de l'élaboration d'un SMSI. En effet, les environnements de gestion technique de plus en plus complexes tendent à accroître le taux de difficulté de la protection des actifs, du fait que ces actifs sont soumis à une évolution et à un progrès constants. Ainsi, le gestionnaire du projet SMSI doit accorder une attention particulière à:

- Identifier clairement les propriétaires des actifs
- Faire comprendre de façon cohérente et claire aux propriétaires les contours des actifs dont ils sont responsables
- Définir un ensemble complet d'exigences connexes en matière de sécurité de l'information pour chaque actif
- Décrire de façon non équivoque où les actifs sont stockés, déplacés et utilisés (que ce soit de façon physique ou logique)
- Déterminer la valeur que l'organisme attache aux actifs évalués, cette valeur pouvant être absolue (par exemple, un coût d'achat ou de remplacement) ou relative (le coût direct ou indirect occasionné par la perte de cet actif).

Identification de l'infrastructure

Catégorie	Définition	Exemples
Matériel informatique	Éléments physiques qui soutiennent les processus	Serveur, ordinateur portable, imprimante, lecteur CD-ROM, etc.
Logiciels	Programmes qui contribuent au traitement de données	Système d'exploitation, processeur de texte, logiciel de comptabilité, etc.
Réseaux	Équipements de télécommunication utilisés pour connecter physiquement des éléments dans un système d'information	Routeur, coupe-feu, câble réseau, commutateur (<i>switch</i>), pont (<i>bridge</i>), etc.
Sites	Endroits physiques où les opérations ont lieu	Bureau, salle de serveur, résidence des employés, zone sécurisée, système d'air conditionné, etc.

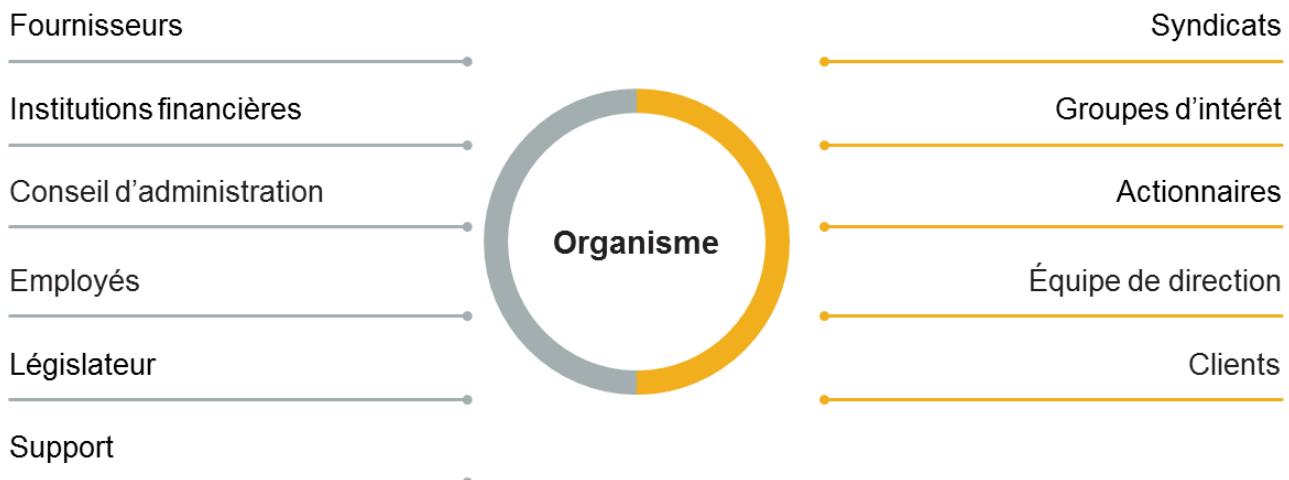
PECB

115

Malgré le fait qu'ISO/IEC 27001 se préoccupe de la protection de l'ensemble des actifs informationnels et non exclusivement des actifs liés aux technologies de l'information, le gestionnaire de projet SMSI doit bien comprendre les processus et infrastructures TI de l'organisme, car ces processus occupent une part vitale dans le traitement, le transfert et la maintenance de l'information organisationnelle.

Dans la norme ISO/IEC27005, les infrastructures TI font partie de la catégorie des actifs en support. Dans l'AnnexeB.1.3, on définit des sous-catégories pour chaque catégorie d'actifs en support, avec des exemples. Durant le deuxième jour de la formation, nous verrons de façon plus détaillée l'identification et l'analyse des risques liés aux actifs.

1.1.4 Identifier et analyser les parties intéressées



Note : Dans ce contexte, l'expression **partie intéressée** est synonyme de **partie prenante**, c'est pourquoi ces termes sont utilisés de façon interchangeable.

PECB

116

ISO/IEC 27001 soulève souvent la question des parties intéressées, ce qui, dans ce contexte, désigne à la fois les parties intéressées internes et externes de l'organisme ayant des intérêts dans le processus du management de la sécurité de l'information.

La norme ISO/IEC27001 stipule également que le SMSI vise à assurer le choix de mesures de sécurité appropriées et proportionnelles pour protéger les actifs et pour donner confiance aux parties intéressées.

Note terminologique: ISO/IEC 27005 utilise également le terme « parties prenantes » sans classification. Certains experts définissent les parties prenantes en tant que sous-catégorie des parties intéressées. Les parties prenantes sont celles qui interagissent directement avec le SMSI (employés, clients ou fournisseurs). Les médias ou les législateurs seront catégorisés comme des parties intéressées, car ils n'interagissent généralement pas directement avec le SMSI.

Définitions

ISO9000, article3.2.3 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, Partie1. La définition initiale a été modifiée par l'ajout de l'Exemple.

Page de notes

PECB

117

ISO9000, article3.2.4 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.

Note 1 à l'article : Un prestataire peut être interne ou externe à l'organisme.

Note 2 à l'article : Dans une situation contractuelle, le prestataire peut être appelé « contractant ».

Il est plutôt difficile d'identifier, d'analyser et de gérer les parties prenantes, car un certain nombre de questions peuvent se poser. Certaines questions sont conceptuelles, comme la façon de gérer les différences culturelles. D'autres sont procédurales:

- Comment aborder et procéder avec la gestion des parties prenantes?
- Comment équilibrer efficacement les intérêts conflictuels des parties prenantes?
- Comment cartographier les parties prenantes lorsque les frontières entre les groupes ne sont pas claires, lorsqu'il existe appartenances multiples à un groupe ou lorsque des coalitions fortes entre les groupes sont apparentes?

Identifier et analyser les parties intéressées

Analyse de leurs exigences et attentes

L'organisation peut utiliser un certain nombre d'outils pour l'identification et l'analyse des parties intéressées. L'une des méthodes les plus courantes est présentée ci-dessous :

1. Identifier leurs exigences et leurs attentes

- Identifier l'ensemble des parties intéressées ainsi que leurs exigences et attentes
- Les exigences et leurs attentes peuvent être implicites ou explicites
- Exemple : Taux de disponibilité d'un service à 99,5 %

2. Valider leurs exigences et leurs attentes

- Analyser les enjeux de sécurité de l'information et confirmer si l'organisme répond ou non à ces préoccupations en ce moment
- Peut s'effectuer par l'envoi d'un questionnaire, par la réalisation d'entrevues ou encore par l'animation de groupes de discussion

3. Définir leurs rôles et responsabilités

- Définir ce que l'on attend des différentes parties intéressées dans le projet : les rôles, responsabilités et niveaux de participation demandés
- Établir un consensus avec elles pendant la phase de planification de leur participation

PECB

118

Dans un premier temps, l'équipe de projet SMSI devrait identifier l'ensemble des parties intéressées ainsi que leurs exigences et leurs attentes en matière de sécurité de l'information. Il est essentiel d'identifier toutes les parties intéressées afin qu'elles puissent s'impliquer dans le processus de mise en œuvre du SMSI. Une exigence pourrait être qu'une violation de la sécurité de l'information n'entraînera aucun préjudice financier grave ou ne portera aucunement atteinte à l'organisme. Une attente pourrait être que, si un incident grave survient, par exemple une panne du système informatique, l'organisme dispose de suffisamment de personnes formées aux procédures adéquates pour réduire l'impact de cet incident et de rétablir rapidement les services.

Dans un deuxième temps, l'équipe de projet SMSI devrait analyser les enjeux de sécurité de l'information des parties intéressées et confirmer que l'organisme répond à leurs préoccupations. Cette activité peut s'effectuer par l'envoi d'un questionnaire, par la réalisation d'entrevues ou encore par l'animation de groupes de discussion. Il convient aussi de prendre en compte les accords de services conclus et d'analyser les exigences SMSI (explicites ou implicites) qu'ils contiennent.

Enfin, l'équipe de projet SMSI devrait définir ce qui est attendu des différentes parties intéressées dans le cadre du projet, y compris les rôles, responsabilités et niveaux de participation exigés. Il convient d'en arriver ainsi à un consensus sur leur implication avec les parties prenantes pendant l'étape de planification.

Page de notes

PECB

119

L'organisme doit prévoir du temps dans le projet pour soutenir les parties intéressées dans les tâches qui vont leur être confiées (en répondant aux questions, en consolidant des rapports, en présentant l'avancement du projet, etc.).

William C. Frederick, James E. Post et Keith Davis écrivent dans leur livre Business and Society: Corporate Strategy, Public Policy, Ethics qu'il y a six étapes pour mener une analyse des parties prenantes:

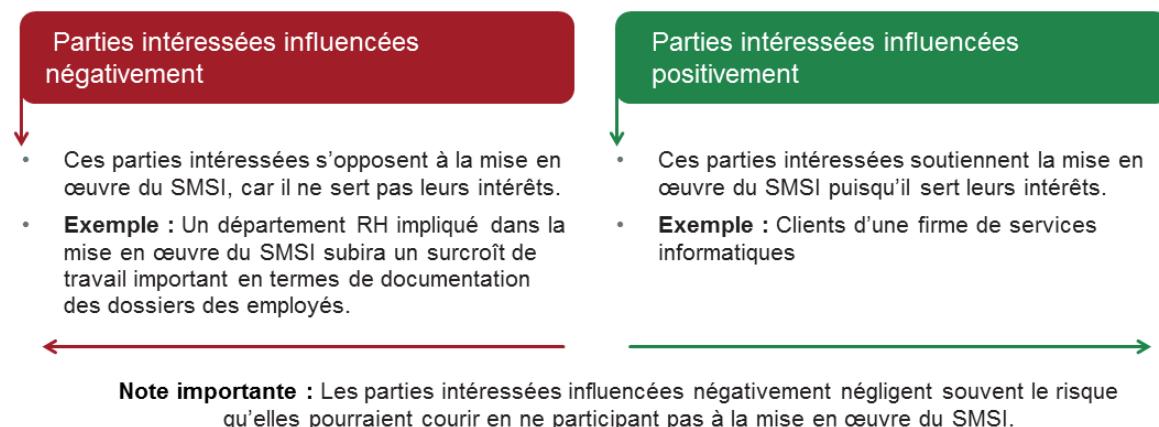
1. Cartographier les relations avec les parties prenantes
2. Cartographier les coalitions des parties prenantes
3. Évaluer la nature de l'intérêt de chaque partie prenante
4. Évaluer la nature du pouvoir de chaque partie prenante
5. Construire une matrice des priorités des parties prenantes
6. Surveiller les coalitions changeantes

Note importante : L'organisme est tenu d'informer toutes les parties intéressées des mesures prises concernant le SMSI, ainsi que de l'impact et des responsabilités qu'elles y assument.

Identifier et analyser les parties intéressées

Influence positive et négative

Nous pouvons classer les parties intéressées en deux catégories :



PECB

120

La prise en compte des exigences et des attentes des parties intéressées est nécessaire au succès du projet de mise en œuvre du SMSI. Leurs exigences et leurs attentes devraient être parfaitement comprises pour assurer que les processus et les mesures de sécurité soient adaptés à ces exigences. On peut classer les parties intéressées en deux catégories: celles qui sont en faveur du projet et celles qui s'y opposent.

Les parties intéressées positives aident à la mise en œuvre du SMSI.

Par exemple, le CIO d'un organisme peut considérer que le SMSI apportera de nouvelles perspectives d'action à l'équipe de gestion, ce qui facilitera l'appréciation des incidents de sécurité ; ainsi, il est perçu comme pouvant améliorer positivement le processus de rapport à la direction.

Stratégie: Participation active en tant que partie intéressée.

Les parties intéressées négatives entravent le bon déroulement du projet.

Par exemple, le gestionnaire d'un département responsable de la gestion des droits d'accès des utilisateurs pourrait voir d'un mauvais œil la mise en place de mesures de sécurité supplémentaires, car elles pourraient nuire à l'efficacité de son équipe à accorder les droits d'accès à temps, ou parce que cela pourrait amener son équipe à faire des heures supplémentaires difficiles à intégrer dans le travail quotidien.

Stratégie: Communiquer avec eux au sujet des objectifs, mettre en évidence l'intérêt pour eux et pour leur société, faire des compromis ou neutraliser leur influence en dernier recours.

Page de notes

PECB

121

Autres exemples positifs:

- Le CFO trouve que le SMSI est un bon outil d'estimation de la valeur (même relative) des actifs immatériels de l'organisme.
- Le responsable qualité est motivé par le fait que cette conformité à ISO/IEC 27001 contribuera à réactiver les processus de management de la qualité qui avaient été un peu négligés depuis la dernière certification ISO 9001. La combinaison des deux normes semble également être une bonne stratégie pour élaborer des pratiques économiques efficaces en l'interne.
- Les clients de l'entreprise perçoivent la conformité à ISO/IEC 27001 comme une meilleure garantie que leurs données personnelles seront efficacement protégées par leur fournisseur..

Autres exemples négatifs:

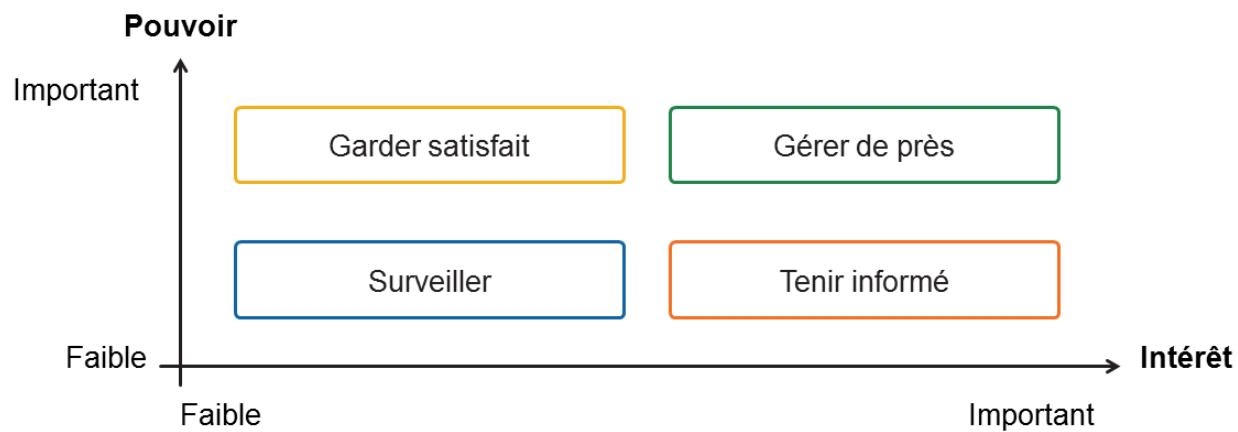
- Le directeur des RH perçoit le SMSI comme un vecteur d'une certaine lourdeur et d'un certain impact sur le bon fonctionnement de son service.
- Le responsable de la sécurité physique (gérée par une société externe) voit le SMSI comme un élément perturbateur dans son rôle puisque le SMSI distribue les rôles et les responsabilités à un plus grand nombre de personnes ; ainsi, le responsable de la sécurité physique a l'impression que sa contribution ne sera pas aussi importante qu'auparavant.

Une façon de gérer les attitudes négatives par rapport à la mise en place d'un SMSI pourrait être de désigner un «champion du SMSI». Cette personne, généralement membre de l'équipe dirigeante ou responsable d'assez haut niveau dans l'organisme concerné, pourrait alors jouer le rôle de «chevalier blanc», de protecteur du projet SMSI et garant de son succès.

Cette personne est alors censée incarner l'engagement de la direction à la réussite de la mise en œuvre du système. À ce titre, elle dispose du pouvoir et de l'autorité lui permettant de soutenir et d'aider à finaliser le projet. Par opposition à ce rôle de protecteur, on voit parfois se développer une sorte «d'anti-champion» ou de «leader négatif» qui symbolise les intérêts incompatibles à la concrétisation du projet, quelles qu'en soient les raisons. Le rôle de champion est dès lors tout à fait utile pour contrer les actions hostiles qui pourraient émaner des parties intéressées négatives incarnées par des leaders négatifs..

Identifier et analyser les parties intéressées

Matrice pouvoir/intérêt



PECB

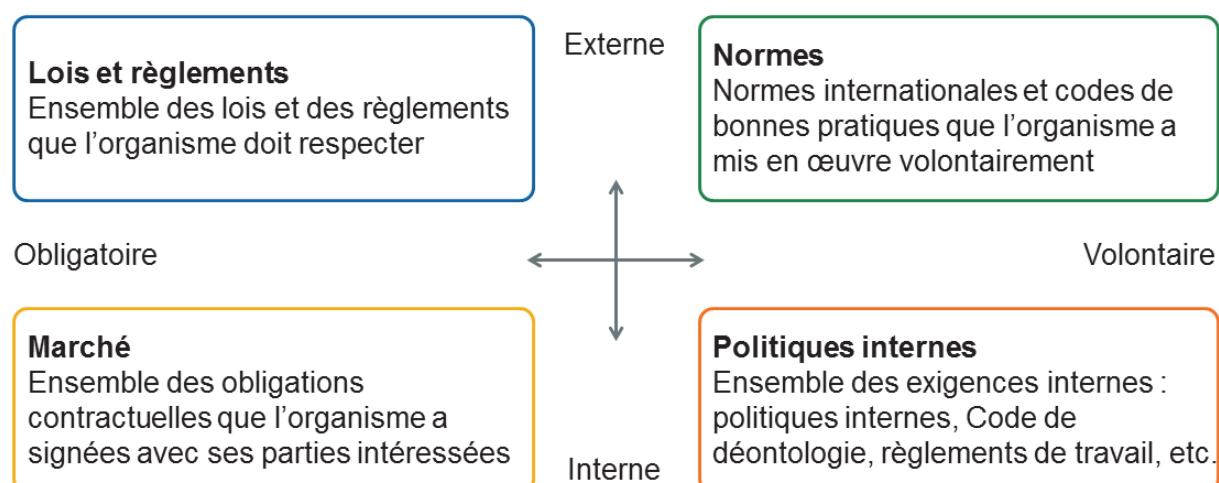
122

La matrice mise au point par Johnson et Scholes, la matrice pouvoir/intérêt, constitue un outil qui aide à déterminer et à gérer les parties intéressées. La présente matrice montre la relation entre deux variables importantes, la variable intérêt montrant l'intérêt des parties intéressées dans les décisions et les activités de l'organisme, et la variable pouvoir montrant le pouvoir qu'ont les parties intéressées sur les activités et les décisions de l'organisme. Grâce à cette matrice, les organismes peuvent prioriser les efforts nécessaires pour répondre aux exigences et aux attentes des parties intéressées.

Les organismes peuvent également cartographier les différentes parties intéressées dans la matrice en fonction des priorités:

- Identifier et répertorier les parties intéressées pertinentes
- Déterminer les exigences et les attentes des parties intéressées en utilisant différentes méthodes de recherche
- Classer en fonction du pouvoir/intérêt
- Établir des priorités et des objectifs et ainsi réduire le risque de ne pas répondre aux exigences et aux attentes

1.1.5 Identifier et analyser les exigences métier



PECB

123

L'organisme doit tenir compte des exigences commerciales, légales ou réglementaires, de même que des obligations contractuelles qu'il a conclues avec différentes parties intéressées. Pour y parvenir, il doit identifier et 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.

Il faut noter que, pour l'identification et l'analyse des exigences légales et contractuelles, il convient d'impliquer des conseillers juridiques ou des juristes qualifiés dans le domaine. Un expert en sécurité de l'information n'est généralement pas en mesure, par exemple, d'analyser les implications juridiques et, par conséquent, pourrait ne pas être en mesure de déterminer les exigences juridiques et contractuelles.

Les exigences SMSI pour tous les organismes, petits ou grands, émanent principalement de quatre sources:

1. **Lois et règlements:** Voir la diapositive suivante.
2. **Normes:** Les organismes doivent se conformer à un ensemble de normes internationales et de codes de pratique liés à leur secteur industriel. Bien que la mise en œuvre des cadres réglementaires soit volontaire, du point de vue de la sécurité de l'information, ils deviennent des obligations à respecter (avec le risque de perdre sa certification en cas de défaut grave).
3. **Marché:** Les exigences de marché comprennent l'ensemble des obligations contractuelles que l'organisme a signées avec ses parties prenantes. Un manquement à des obligations contractuelles peut conduire à des pénalités (lorsqu'elles sont indiquées dans les contrats) ou à des poursuites civiles en dommages. Les exigences de marché sont toutes des règles implicites qu'un organisme devrait respecter pour mener ses activités. Par exemple, même si l'organisme n'a aucune obligation contractuelle de livrer ses produits comme prévu, il va de soi qu'il s'agit d'une politique commerciale de base de respecter les délais de livraison prévus, et le manquement à cette obligation entraînera une perte de parts de marché, de confiance des clients, de profits, etc.
4. **Politiques internes:** Les politiques internes sont des principes, règles et lignes directrices qui incluent toutes les exigences définies à l'intérieur de l'organisme: politiques internes (ressources humaines, management de la sécurité alimentaire, chaîne d'approvisionnement, etc.), codes de déontologie, règles de travail, etc.

Identifier et analyser les exigences métier

Conformité légale

- Les lois applicables et les règlementations doivent être appliquées par l'organisme.
- Dans la plupart des pays, la mise en œuvre d'une norme ISO est une décision volontaire de l'organisme, pas une condition légale.
- Dans tous les cas, les lois prévalent sur les normes.



PECB

124

ISO/IEC 27002, article 18 Conformité

18.1 Conformité aux obligations légales et réglementaires

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

18.1.1 Identification de la législation et des exigences contractuelles applicables

Mesure Il convient, pour chaque système d'information et pour l'organisation elle-même, de définir, documenter et mettre à jour explicitement toutes les exigences légales, réglementaires et contractuelles en vigueur, ainsi que l'approche adoptée par l'organisation pour satisfaire à ces exigences.

Préconisations de mise en œuvre De la même façon, il convient de définir et de documenter les mesures spécifiques et les responsabilités individuelles mises en place pour répondre à ces exigences.

Il convient que les responsables identifient toutes les législations applicables à l'organisation afin de répondre aux exigences liées à leur type d'activité. Si l'organisation mène des activités dans d'autres pays, il convient que les responsables étudient la conformité aux règles des pays concernés.

Conformité légale et réglementaire

Principaux thèmes à surveiller

- 1 Protection des données
- 2 Protection de la vie privée
- 3 Délits informatiques
- 4 Signature numérique
- 5 Propriété intellectuelle
- 6 Paiements électroniques
- 7 Gestion des enregistrements

PECB

125

Il est généralement souhaitable que l'expert en sécurité de l'information travaille avec des conseillers juridiques pour identifier les sujets à analyser et expliquer les enjeux de sécurité concernés. Par exemple, il devrait expliquer à l'avocat impliqué dans cette analyse le mode de fonctionnement du système de surveillance du réseau, afin que l'avocat puisse mieux estimer s'il viole une loi sur la protection de la vie privée ou tout autre règlement interne de l'organisme.

Par ailleurs, les nouvelles législations liées aux enjeux de confidentialité, les obligations financières et la gouvernance des entreprises obligent celles-ci à surveiller leur infrastructure TI avec plus de réactivité et d'efficacité qu'auparavant. Plusieurs organismes publics et privés qui traitent avec ces entreprises sont mandatés pour assurer un niveau de sécurité minimum. En l'absence d'une sécurité proactive, les dirigeants d'entreprise peuvent être exposés à des poursuites judiciaires (civiles ou même pénales) pour violation de leurs responsabilités fiduciaires et légales. Dans les grandes entreprises, les demandes d'avis légal peuvent principalement porter sur:

1. **Protection des données** – Dans plusieurs pays, il existe des lois spécifiques qui couvrent la protection de la confidentialité et de l'intégrité des données, souvent limitées au contrôle des données personnelles (par exemple le Règlement général sur la protection des données de l'Union européenne). De la même façon que des incidents de sécurité doivent pouvoir être attribués aux individus les ayant générés, les informations personnelles devraient également être assujetties à une gestion et à des enregistrements adéquats. Une approche structurée de la gestion des incidents liés à la sécurité de l'information devrait donc gérer les mesures les plus appropriées pour protéger la vie privée et les données personnelles.

Page de notes

PECB

126

2.Respect de la vie privée – Conformément aux législations applicables, beaucoup d'organismes choisissent d'établir une Politique de protection de la vie privée, souvent conçue pour atteindre les objectifs suivants:

- Augmenter la sensibilisation aux exigences réglementaires, légales et métier en ce qui concerne le traitement et la protection des informations personnelles
- Établir une politique d'entreprise claire et complète pour le traitement des informations personnelles
- Définir la responsabilité de toutes les personnes traitant des informations personnelles
- Permettre à l'organisme de respecter sa responsabilité commerciale, légale et réglementaire en ce qui concerne les informations personnelles

3.Identification et poursuite des crimes informatiques – Le crime informatique représente une menace considérable, via Internet, pour les systèmes d'information d'un organisme. Les dégâts occasionnés peuvent être vraiment accablants et se traduire en pertes financières directes, en perte de réputation ou encore en perte de temps pour l'organisme touché. Le cybercrime a de nombreux visages et ne connaît pas de frontières. Sa nature générique et instable nécessite du responsable de l'organisation (avec pratiquement toute structure étant connectée à un réseau externe) une prise de conscience ainsi que la mise en place de contre-mesures adéquates en conformité avec les lois applicables. S'assurer que la collecte de preuve respecte la législation. Les mesures de protection ne peuvent pas être elles-mêmes des crimes (par exemple, répondre au pourriel par des contre-mesures comme le dépassement de mémoire [buffer overflow]).

4.Utilisation de la signature numérique – Aujourd'hui, la loi reconnaît la validité des conventions sur la preuve, comme le faisait déjà la jurisprudence fondée sur le caractère non impératif des règles sur la preuve. La rédaction de ces conventions ne peut pas se faire n'importe comment, elle doit s'opérer en fonction du contexte dans lequel elles s'inscrivent pour pouvoir être considérées comme valides en cas de contentieux. Dans certains pays, les enregistrements numériques doivent garantir la préservation de «traces» comme preuve d'intégrité selon des procédures de sécurité élaborées sur la base de normes reconnues relatives à l'archivage électronique (par exemple, en France, la norme AFNOR NF Z 42-013 ou, plus internationalement, la norme ISO 14721 qui concerne les Systèmes de transfert des informations et données spatiales – Système ouvert d'archivage de l'information – Modèle de référence).

5.Propriété intellectuelle – Le produit des efforts intellectuels est souvent reconnu par les conventions nationales et internationales comme un droit de propriété intellectuelle permettant de protéger certains actifs immatériels. Pour les petites et moyennes entreprises, l'utilisation efficace des droits de propriété intellectuelle peut permettre de rivaliser avec des entreprises de plus grande taille. La propriété intellectuelle offre aux PME un fort potentiel en termes de protection juridique, de technologie de l'information et d'avantage concurrentiel. Le but

est donc ici de renforcer la position concurrentielle de l'entreprise.

6.Commerce et paiements électroniques – D'un point de vue légal, dans la plupart des pays, il est tout à fait essentiel de pouvoir prouver devant un tribunal qu'un client a acheté le produit ou le service vendu par l'entreprise. Il devrait être également possible de prouver à l'autorité fiscale à quelle période ont eu lieu les différentes transactions. La grande différence entre le commerce électronique et le commerce papier est le support sur lequel les transactions sont conservées. Avec des preuves papier, une modification physique est difficile alors que la modification d'un fichier électronique est plus aisée. Un autre aspect consiste en la possibilité qu'un concurrent offre les mêmes produits depuis un serveur localisé dans un paradis fiscal. Enfin, quand un consommateur achète un produit sur un site Web, il n'est pas toujours évident de définir quelle législation nationale s'applique.

Page de notes

PECB

127

7.Gestion des enregistrements – Certaines législations nationales exigent que les entreprises maintiennent à jour des enregistrements relatifs à leurs activités afin de les revoir dans le cadre d'un processus d'audit annuel.

8.Des exigences similaires existent au niveau gouvernemental. Dans certains pays, les organismes sont légalement tenus de remettre ce type de rapports ou de fournir des enregistrements à des fins légales (par exemple, dans des cas d'infractions impliquant la pénétration d'un système gouvernemental sensible).

ISO/IEC 27001 et cadres réglementaires

Exemples

États-Unis:

- **Federal Information Security Management Act (2002)** : FISMA (législation sur le management de la sécurité de l'information) impose un ensemble de procédures à suivre pour tout système d'information utilisé par le gouvernement fédéral américain, ses sous-traitants ou ses fournisseurs.
- **NIST 800-53** : NIST 800-53 (National Institute of Standards and Technology) fournit des lignes directrices pour sécuriser les systèmes d'information au sein du gouvernement fédéral en choisissant et en précisant les mesures de sécurité. Ces lignes directrices s'appliquent à toutes les parties d'un système d'information qui traitent, stockent ou transmettent des informations de nature fédérale. Il est émis par le département du Commerce des États-Unis.

Notez que NIST 800-53 comprend un tableau de concordance entre ses mesures et celles de l'Annexe A de la norme ISO/IEC 27001.

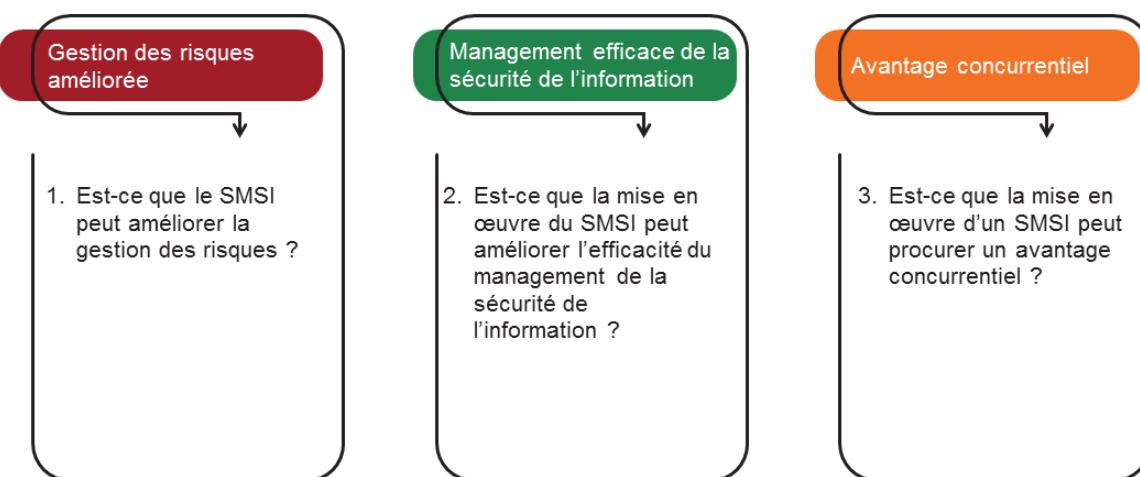
Europe:

- **Règlement général sur la protection des données – RGPD:** Ce règlement établit des règles relatives à la protection des personnes physiques en ce qui concerne le traitement des données à caractère personnel et les règles relatives à la libre circulation des données à caractère personnel.
- **Regulation (EC) n°45/2001:** Règlement relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données. Le texte comprend des dispositions garantissant un niveau élevé de protection des données personnelles traitées par les institutions et organismes communautaires. Il prévoit également la création d'un organe de surveillance indépendant chargé de surveiller l'application de ces dispositions..

Référentiels internationaux et industriels:

- **Principes directeurs de l'OCDE (2002):** L'OCDE (Organisation de coopération et de développement économiques) a élaboré les Lignes directrices de l'OCDE régissant la sécurité des systèmes et réseaux d'information sur la base de neuf principes: sensibilisation, responsabilité, réaction, éthique, démocratie, appréciation des risques, conception et mise en œuvre de la sécurité, gestion de sécurité et réappréciation
- **COBIT (1994+)** : Développé par ISACA et l'ITGI, COBIT (Control Objectives for Information and related Technology) est un cadre de référence pour gérer la gouvernance des systèmes d'information. COBIT fournit aux responsables de la technologie de l'information, aux auditeurs et aux utilisateurs des indicateurs, des processus et des bonnes pratiques pour les aider à maximiser les avantages découlant du recours aux technologies de l'information et de l'élaboration de la gouvernance et du contrôle d'un organisme..

1.1.6 Déterminer les objectifs du SMSI



PECB

128

Les objectifs d'un programme de management du SMSI sont l'expression de l'intention de l'organisation de traiter les risques identifiés et de se conformer aux exigences établies. Néanmoins, il est nécessaire d'établir d'abord les objectifs du SMSI avec les parties intéressées.

Ces objectifs du SMSI sont nécessaires à la détermination du périmètre et devront être validés au plus haut niveau de l'organisme. Les objectifs peuvent être affinés en cours de projet, particulièrement après la réalisation de l'analyse des risques. Les objectifs doivent être correctement documentés.

ISO/IEC27001, 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.

Déterminer les objectifs du SMSI

Quelques exemples de formulations d'objectifs reliés à la mise en œuvre du SMSI :

- S'assurer de la conformité aux exigences légales, réglementaires et contractuelles de l'organisme
- Faire preuve de diligence raisonnable
- Créer un environnement de mesures internes
- Inspirer confiance aux parties prenantes de l'organisme
- Valider la conformité à des contraintes légales, réglementaires ou contractuelles spécifiques
- Protéger les actifs critiques de l'organisme
- Structurer efficacement le management de la sécurité de l'information selon 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 de l'activité
- S'assurer de la conformité à la sécurité de l'information pour un projet, la livraison d'un service ou d'un produit, etc.

PECB

129

La détermination des objectifs devrait prendre en considération:

- Historique des événements de risque dans l'organisme
- Expositions au risque courantes et émergentes
- Tendances d'interruption opérationnelle et incidents qui les précèdent
- Augmentations des coûts et pertes de revenu à la suite d'interruptions potentielles
- Coûts de financement des risques
- Responsabilités (Liabilities)
- Responsabilités sociales
- Succès et échec d'autres projets et programmes de sécurité de l'information

1.1.7 Déterminer le 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, article 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.*

130

Les éléments suivants devraient être considérés lors de la prise de décisions initiale concernant le périmètre du SMSI:

- a. Quels sont les mandats du management de la sécurité de l'information établis par la direction de l'organisme et les engagements imposés extérieurement à l'organisme?
- b. La responsabilité des systèmes à intégrer dans le périmètre est-elle partagée par plus d'une équipe de gestion (par ex. les responsables de différentes filiales ou divisions)?
- c. Comment les documents du SMSI seront-ils communiqués dans l'organisme (par ex. sur papier ou sur l'intranet corporatif)?
- d. Les systèmes de management actuels peuvent-ils soutenir les besoins de l'organisme? Sont-ils complètement opérationnels, bien maintenus, et fonctionnent-ils comme prévu?

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

f.Déterminer le périmètre préliminaire: cette activité devrait être menée par un petit groupe de management, néanmoins représentatif.

g.Déterminer le périmètre raffiné: les unités fonctionnelles à l'intérieur et à l'extérieur du périmètre préliminaire devraient être revues, éventuellement suivies d'une inclusion ou d'une exclusion de certaines de ces unités fonctionnelles afin de réduire le nombre d'interfaces le long des limites. Lors du raffinage du périmètre préliminaire, toutes les fonctions nécessaires pour soutenir les activités commerciales dans le périmètre doivent être prises en considération.

h.Déterminer le périmètre final: il doit être évalué par toute la direction inclus dans le périmètre final. Si nécessaire, il doit être ajusté et décrit précisément.

i.Approuver le périmètre: l'information documentée décrivant le périmètre devrait être formellement approuvée par la haute direction.

Page de notes

PECB

131

L'organisme devrait également envisager des activités ayant un impact sur le SMSI ou des activités externalisées, à d'autres parties de l'organisme ou à des fournisseurs indépendants. Pour de telles activités, les interfaces (physique, technique et organisationnelle) et leur influence sur le périmètre doivent être identifiées.

Les informations documentées décrivant le périmètre devraient inclure:

- j.Le périmètre organisationnel, les limites et les interfaces
- k.Le périmètre, les limites et les interfaces des technologies de l'information et de la communication
- l.Le périmètre physique, ses limites et ses interfaces

Exercice 3

PECB

132

Exercice3: Établir le contexte de management du SMSI

Fiers du taux de croissance rapide de leurs activités, les dirigeants de Scientia Online Library sont soudainement préoccupés par les aspects de mesure et de sécurité, surtout depuis qu'il y a eu récemment quelques incidents de sécurité. Parce qu'ils vous connaissent bien et qu'ils connaissent votre expertise en sécurité de l'information, ils vous confient le mandat de les aider dans la mise en place d'un système de management de la sécurité de l'information et dans la préparation à la certification ISO/IEC27001.

La première étape de votre mandat est d'établir le contexte du management de la sécurité de l'information dans l'organisme. Pour eux, c'est le jargon des spécialistes. Ils veulent que vous proposiez une version qu'ils approuveront plus tard.

Pour y parvenir, identifiez, en vous basant sur les informations contenues dans l'étude de cas, quelles seraient les trois plus importantes sources potentielles d'exigences de conformité pour l'organisme. En outre, identifiez quels seraient les deux actifs informationnels ainsi que les deux processus d'affaires que vous jugez les plus critiques pour l'organisme.

Durée de l'exercice: 30 minutes

Commentaires: 15 minutes

Questions ?

PECB

133

Section 7

Analyse du système existant

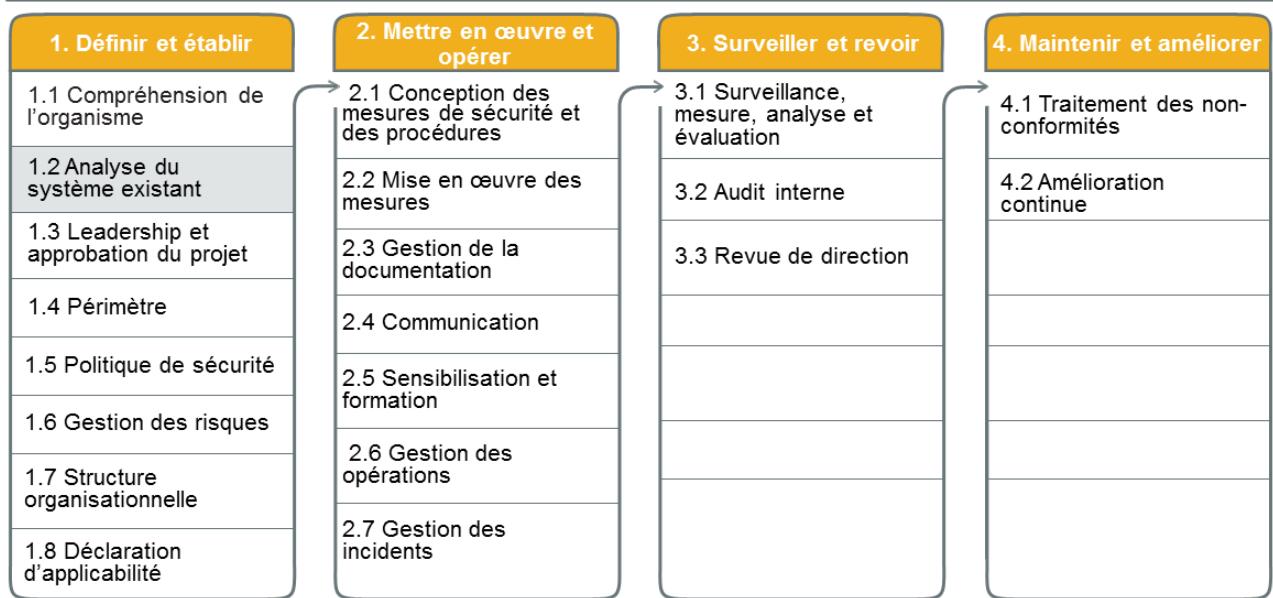
- Déterminer l'état actuel
- Effectuer l'analyse des écarts
- Détermination des objectifs et publication du rapport d'analyse des écarts

PECB

134

La présente section fournit des informations qui aideront le participant à comprendre le processus d'analyse des écarts.

1.2 Analyse du système existant



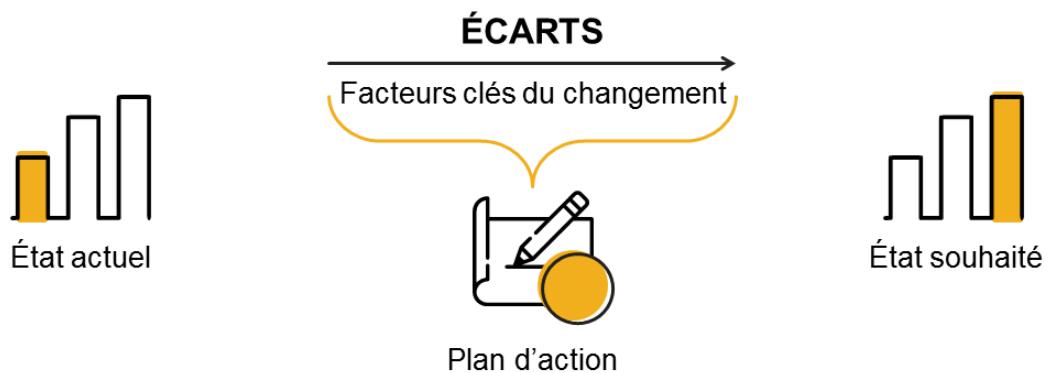
PECB

135

Technique d'analyse des écarts

Comprendre l'analyse des écarts

L'analyse des écarts (*Gap analysis*) est une technique permettant de déterminer les mesures à prendre pour passer d'un état actuel à un état futur souhaité.



PECB

136

L'analyse des écarts traite des questions suivantes:

- Quelle est notre situation actuelle?
- Quel est notre état souhaité (objectif)?
- Quelle est la différence entre notre situation actuelle et notre état souhaité (objectif)?

1.2 Analyse du système existant

Liste des activités

1.2.1

Déterminer l'état actuel

1.2.2

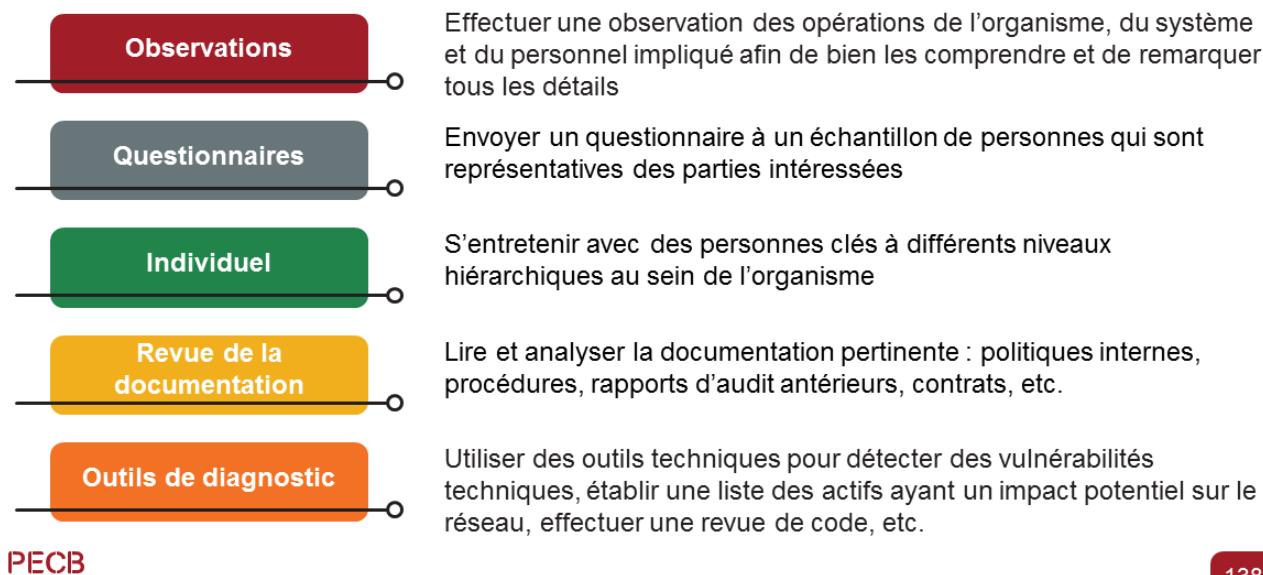
Effectuer l'analyse des écarts

1.2.3

Déterminer les objectifs et publier un rapport d'analyse des écarts

1.2.1 Déterminer l'état actuel

Collecte d'information



138

L'équipe de projet devrait acquérir une connaissance détaillée du système de management existant en recueillant des informations auprès de multiples parties intéressées.

Pour déterminer un état donné en fonction d'une situation à un moment donné, le choix de la méthode de collecte des données dépend souvent du type de données à recueillir, des personnes à interroger, des compétences et connaissances des intervieweurs, ainsi que des ressources disponibles (temps, budget, etc.). Il existe de nombreuses méthodes de collecte de données.

Ainsi, pour récolter les informations appropriées dans l'organisme, il peut être utile de mener les actions suivantes:

- Observer sur site les mesures de sécurité physique
- Mener des entretiens avec les personnes responsables du management de la sécurité de l'information et celles responsables des opérations quotidiennes des mesures de sécurité
- Consulter les documents contenant des informations sur les mesures de sécurité (processus et procédures de management de la sécurité de l'information, description des mesures de sécurité, rapports, etc.)
- Consulter les résultats de l'audit interne

Note importante: Même si certaines personnes au sein de l'organisation peuvent prétendre qu'il n'y a pas de système en place, ce n'est presque jamais le cas. Même si elles sont très informelles, il existe toujours une série de mesures de sécurité gérées de manière plus ou moins efficace.

Mener un entretien

-  Utiliser des questions ouvertes et éviter les questions fermées ou guidées
-  S'assurer de couvrir l'ensemble des sujets en maîtrisant le temps disponible pour l'entretien
-  Prendre des notes durant l'entretien
-  Poser des questions pour clarifier une réponse ou une situation

PECB

139

L'expérience montre que, plus on prépare un entretien, plus la rencontre sera productive. Une stratégie qui peut être utilisée pour mener des entretiens efficaces consiste à créer une liste de contrôle, garantissant que les entretiens sont menés de manière systématique et que des preuves pertinentes sont obtenues. La liste de contrôle peut inclure une liste de définitions pour assurer l'uniformité des réponses. La liste de contrôle devrait permettre d'insérer des réponses, des commentaires et des observations. Elle devrait aussi mentionner la référence à la norme concernée. La personne interrogée peut recevoir la liste de contrôle avant l'entretien, lui permettant d'être bien préparée pour l'entretien.

Lors des entretiens, il peut être utile de clarifier certains termes liés à la sécurité de l'information, tels que **menaces** et **vulnérabilités**, en un langage plus significatif pour les parties prenantes non expérimentées. On peut, par exemple, utiliser la formulation suivante: «Qu'essayez-vous d'éviter?» ou «Que craignez-vous qu'il n'arrive avec cette ressource particulière?»

L'entretien peut être enregistré si la personne l'accepte. Cependant, la pratique la plus commune est simplement de prendre des notes. L'enregistrement de l'entretien peut être interprété comme intimidant par la personne interrogée et cela pourrait avoir un impact négatif sur les résultats de l'entretien. De plus, nous avons rarement le temps d'écouter un enregistrement d'entretien.

Page de notes

PECB

140

Les notes d'entretien devraient contenir les éléments suivants:

Poste de la personne interrogée (habituellement, pas de nom excepté pour les membres de la direction ; confidentialité)

Example: Discussion avec un employé du service des TI, le 3mars 2019

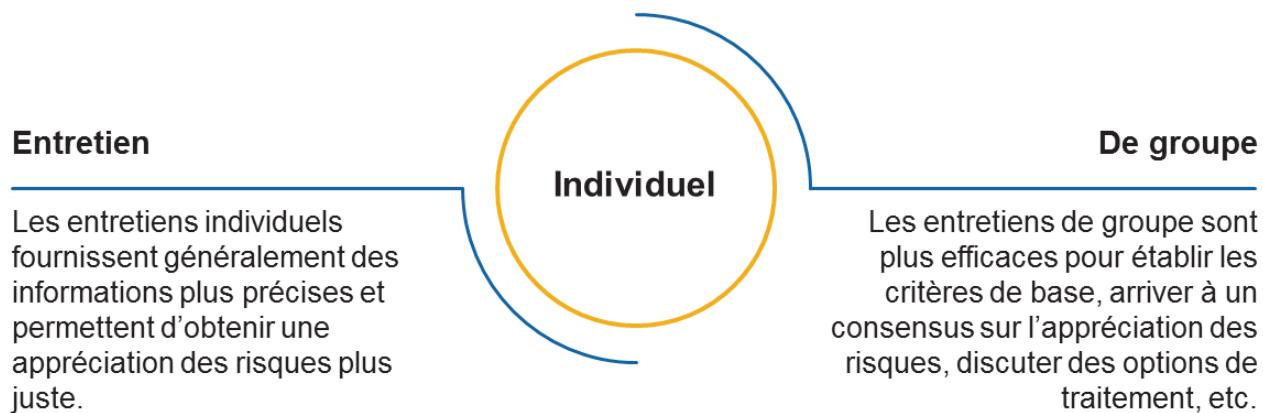
Objectifs de l'entrevue

Exemple: Valider si l'organisation suit convenablement le plan de formation ou non

Résumé de la preuve recueillie

L'information documentée doit être recueillie dans un langage clair, concis et précis. Il convient de noter des faits, pas des opinions. En outre, il convient d'identifier les faiblesses. Ensuite, les faiblesses identifiées seront signalées dans l'analyse des écarts. La référence exacte à la norme doit être indiquée avec le numéro de l'article de la norme..

Entretiens individuel et de groupe



PECB

141

Certains pourraient remettre en cause la valeur de questions détaillées sur le SMSI adressées à des personnes ne disposant pas d'expérience professionnelle en matière de risques liés à la sécurité de l'information. Cependant, la recherche a démontré qu'il est essentiel de connaître l'opinion des parties prenantes (qu'elles soient ou non expertes), sur leur exposition aux activités qu'elles gèrent ou aux tâches qu'elles accomplissent. Les personnes responsables des processus métier fourniront une vision beaucoup plus «opérationnelle» des risques ; par exemple, le responsable des relations publiques indiquera ses préoccupations concernant le risque pour la réputation.

Entretiens individuels

Grâce aux entretiens individuels, il est possible de se concentrer sur une seule personne et généralement d'obtenir des informations plus détaillées sur le SMSI. Les entretiens individuels empêchent tout membre dominant du groupe d'influencer la réaction des autres, ce que l'on appelle «l'effet d'entraînement». Il est donc préférable de mener ce type d'entretien.

Les entretiens individuels permettent de:

- Lire le langage corporel de l'individu interviewé
- Identifier des points de discussion sensibles
- Assurer la confidentialité des échanges avec l'interviewé
- Ajuster les questions de suivi

Entretiens de groupe

La pratique des entretiens de groupe doit être limitée, à moins que l'on ne veuille vérifier l'interaction et la dynamique entre les différents membres du groupe. Au cours d'entretiens de groupe, chaque membre du groupe résume son opinion sur le SMSI.

Questionnaires

Questions ouvertes et fermées

Questions types :

1. Le processus est-il présent dans l'organisme ?
Est-il normalisé ?
2. Est-il suivi par les utilisateurs concernés ?
3. Le processus est-il documenté ?
4. Est-ce qu'un responsable a été nommé pour assurer l'efficacité du processus ? Est-ce que les rôles et responsabilités sont déterminés ?
5. Toutes les parties concernées ont-elles été informées du processus existant ? Y a-t-il des séances de formation disponibles ?
6. Le processus est-il contrôlé ? Le processus est-il mesuré ?
7. Le processus est-il automatisé ? Utilise-t-on des outils ?
8. Le processus est-il mis à jour ?
9. La performance du processus est-elle comparée aux pratiques de l'industrie ?

PECB

142

La détermination de l'état actuel des mesures de sécurité de l'information mises en œuvre peut être effectuée par l'équipe de projet ou confiée à des consultants externes. L'avantage de confier l'analyse à des parties externes est que, théoriquement, on recevra des rapports neutres. La collecte de données pendant la phase d'analyse exige que l'équipe responsable soit très bien informée de la situation actuelle. Dans la plupart des cas, une grande partie de l'analyse sera produite sur la base des réponses à des questionnaires structurés et semi-structurés qui, selon le choix ou le contexte, seront envoyés par écrit (ou électroniquement).

Lors de l'utilisation de questionnaires, les questions posées pourront être:

Question fermée: La personne interrogée est plutôt limitée puisqu'elle n'a pas la liberté de clarifier davantage la réponse à l'intervieweur.

Note: Les questions fermées présentent le risque de suggérer des réponses non spontanées. Elles sont surtout utiles pour l'étude de comportement (nature, fréquence, etc.). Les échelles d'opinion représentent un format particulier de questions fermées. Elles renseignent sur le degré d'adhésion à une proposition: les sujets doivent se positionner sur une échelle «accord-désaccord» à plusieurs niveaux.

Question ouverte: La personne interrogée jouit d'une totale liberté de réponse, ce qui permet d'obtenir des informations plus détaillées.

Note: Grâce à des questions ouvertes, les intervieweurs peuvent recueillir des informations plus riches et plus complètes. Mais elles sont souvent plus difficiles à analyser, car elles génèrent un volume important qu'il faut exploiter par «analyse de contenu». Le taux de réponse à ces questions est souvent moins important, plus approprié pour l'analyse des opinions et attitudes.

1.2.2 Effectuer l'analyse des écarts

Analyse des écarts

Technique permettant de déterminer les mesures à prendre pour passer d'un état actuel à un état futur souhaité :

1. Comparaison entre les performances actuelles du système de management de la sécurité de l'information et les exigences de la norme ISO/IEC 27001
2. Identification des besoins d'amélioration
3. Base pour la rédaction du plan de projet SMSI



PECB

143

L'analyse des écarts est une réponse à trois questions:

- Quelle est notre situation actuelle?
- Quelle est la cible?
- Quelle est la différence entre la situation actuelle et la situation visée?

Une analyse des écarts se déroule comme suit:

- **Déterminer l'état actuel:** Identifier les processus et les mesures de sécurité en place au sein de l'organisme et leurs caractéristiques.
- **Identifier les cibles (objectifs):** Déterminer le niveau de maturité requis pour chaque mesure de sécurité en effectuant des comparaisons avec d'autres organismes (ou d'autres divisions de l'organisme).
- **Analyse des écarts:** Identifier l'écart qui peut exister entre les mesures de sécurité actuellement en place et les exigences de la norme ISO/IEC27001. Ceci permet à l'organisation de déterminer les processus ou les mesures actuels qui doivent être améliorés et de planifier en conséquence pour y remédier.

La principale utilité de l'analyse des écarts est de fournir une base pour identifier et mesurer les investissements nécessaires en temps, argent, ressources humaines et autres pour une mise en œuvre efficace du SMSI proposé.

ISO/IEC 21827 et CMM®

Matrice d'évaluation des niveaux de maturité

ISO/IEC 21827 est une norme visant à améliorer le processus de développement logiciel basé sur le modèle CMM® (*Capability Maturity Model*) qui est :

- Un modèle d'évaluation et d'évolution des capacités sur une grille de maturité hiérarchisée en cinq niveaux
- Un modèle largement repris par les spécialistes pour réaliser une analyse des écarts avec les normes ISO/IEC 27001 et ISO/IEC 27002

PECB

144

ISO/IEC 21827 permet à un organisme de mesurer son niveau de maturité et sa capacité à développer son processus de développement logiciel. Cette norme est basée sur le modèle CMM (*Capability Maturity Model*) initialement développé par le *Software Engineering Institute* de l'Université Carnegie Mellon. Le CMM avait pour objectif de mesurer la qualité des services rendus par les fournisseurs de logiciels du Département de la Défense (DoD) des États-Unis. Ce modèle d'évaluation et de développement de capacité repose sur une grille hiérarchique de cinq niveaux de maturité (voir la prochaine diapositive).

Le modèle proposé par la norme ISO/IEC21827 est désormais largement utilisé par les entreprises de R et D, les services informatiques et les fournisseurs de logiciels pour évaluer et améliorer leur propre développement de produits. Ce modèle a été par la suite adapté à d'autres secteurs d'activités que le génie logiciel dont:

- CMMI (*Capability Maturity Model Integration*) qui détermine le développement pratique et la maintenance des systèmes et des applications.
- CMM-TSP (*Team Software Process*) qui détermine les pratiques normalisées d'un projet d'équipe.
- CMM-PSP (*Personal Software Process*) qui détermine les pratiques normalisées de développement d'une ressource individuelle.
- SSE-CMM (*Systems Security Engineering Capability Maturity Model*) qui détermine les pratiques de sécurité liées aux systèmes d'information.

De nombreux autres modèles et cadres de référence ont adopté l'échelle de maturité du CMM. Le plus connu est sans doute COBIT, publié par l'ISACA (*Information Systems Audit and Control Association*).

Page de notes

PECB

145

our mesurer de manière précise l'amélioration du processus SMSI lors de la mise en œuvre initiale du SMSI, mais aussi durant le cycle de vie du système, il est intéressant de s'appuyer sur les méthodologies commeCMMI. Ce modèle permet, conformément aux principales pratiques en place, d'atteindre un statut proactif pour l'activité de sécurité. Il est toutefois encore insuffisant en soi, car il doit compter avec la culture de l'organisme et accorder à l'organisme un temps considérable pour atteindre la maturité nécessaire..

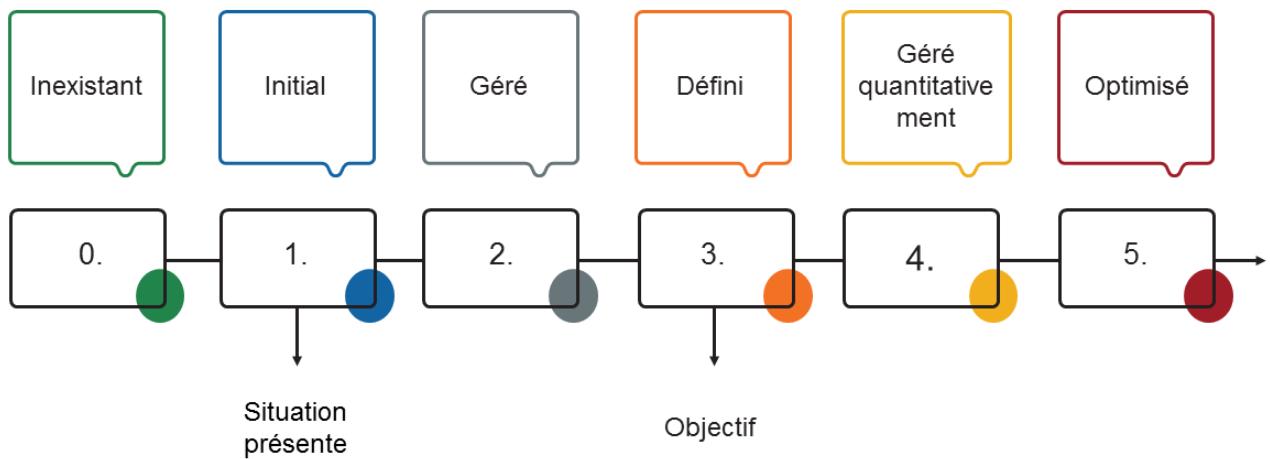
Jumeler ISO/IEC 27001 à d'autres référentiels de bonnes pratiques et de méthodes

De nombreuses entreprises ont récemment pris des mesures concrètes pour mettre en place des références en matière de gouvernance informatique – les plus citées étant CMMI, COBIT et ITIL. Ces différentes normes peuvent se compléter et permettre des économies d'échelle. Par exemple, la mise en œuvre des processus CMMI et ITIL facilitent la mise en œuvre des mesures de sécurité d'ISO/IEC27002. COBIT, avec son approche de la gestion des risques, est également une option qui contribue à la mise en œuvre de la norme ISO/IEC 27001.

D'autres types de risques sont considérés autres que ceux de la norme ISO/IEC 27001 (risques affectant l'efficacité, la fiabilité et l'efficience des systèmes d'information, en plus des critères orientés vers la sécurité tels que la confidentialité, l'intégrité, la disponibilité ou la conformité), mais les approches restent similaires.

En général, on peut considérer que la série ISO/IEC 27000 approfondit les thèmes de la sécurité de l'information et de la gestion des risques, qui sont traités plus succinctement dans les autres références. Il convient également de noter qu'ISO 20000 et la solution ITIL renvoient désormais directement à la norme ISO/IEC 27001 en ce qui concerne le processus de management de la sécurité de l'information..

1.2.3 Déterminer les objectifs et publier un rapport d'analyse des écarts



PECB

146

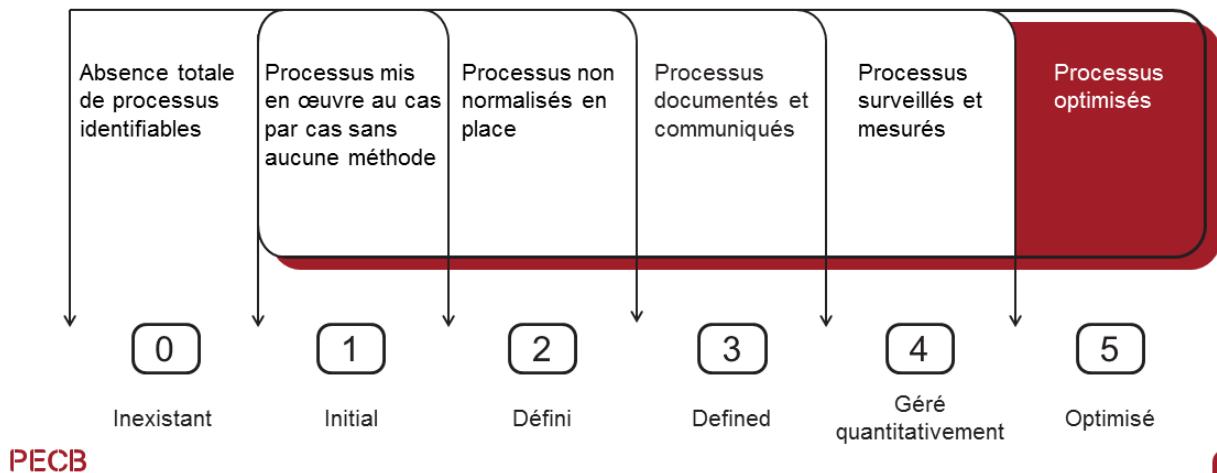
Le rapport d'analyse des écarts devrait comprendre au moins:

1. Description sommaire de la **situation existante** observée
2. Objectif du projet
3. **Description des écarts** entre la situation actuelle et l'objectif à atteindre
4. Diverses recommandations sur **comment** y arriver

Déterminer les objectifs

Analyse des écarts et niveau de maturité

On peut établir les objectifs par des processus et des mesures de sécurité en fonction des niveaux de maturité visés :



147

0. Inexistant: L'entreprise n'est pas consciente de l'absence totale de processus identifiables et de l'importance d'étudier la question.

1. Initial: L'organisation est consciente du problème et de la nécessité de l'étudier ; toutefois, il n'existe pas de processus normalisé à cet effet. Il n'existe pas d'approche générale entérinée par la direction.

2. Géré: Les processus ont été développés jusqu'à un stade où différentes personnes effectuant la même tâche utilisent les mêmes procédures. Il n'y a pas de formation formelle ou de communication des procédures standardisées et la responsabilité est laissée à certaines personnes. L'opération repose beaucoup sur les connaissances individuelles, d'où une probabilité d'erreurs.

3. Défini: Des procédures ont été normalisées, documentées et communiquées lors de séances de formation. Toutefois, leur utilisation est laissée à l'initiative de chacun et il est probable que des défaillances seront constatées. Concernant les procédures, elles ne sont pas sophistiquées mais formalisent des pratiques existantes.

4. Géré quantitativement: Il est possible de surveiller et de mesurer la conformité aux procédures et de réagir lorsque des processus ne fonctionnent pas correctement. Les processus sont en constante amélioration et correspondent aux bonnes pratiques. L'automatisation et l'utilisation d'outils s'effectuent cependant de manière limitée ou partielle.

5. Optimisé: Le processus a atteint le niveau des bonnes pratiques à la suite d'une amélioration constante par rapport aux autres organismes (modèle de maturité). L'ordinateur est utilisé comme un moyen d'automatiser les flux de travail intégré, offrant des outils qui améliorent la qualité et l'efficacité et permettent à l'organisme de s'adapter rapidement.

Déterminer les objectifs et faire l'analyse

Exemple – Analyse des écarts dans le contexte d'ISO/IEC 27001

Article	Exigence	Description de la situation actuelle	Maturité actuelle	Maturité cible	Analyse des écarts	Responsable
A.5.1.1 Politiques de sécurité de l'information	<i>Un ensemble de politiques de sécurité de l'information doit être défini, approuvé par la direction, diffusé et communiqué aux salariés et aux tiers concernés.</i>	Une politique de la sécurité de l'information existe et a été signée par la direction, mais le document n'a jamais été transmis à l'ensemble des employés. Seuls les participants à la mise en œuvre du SMSI doivent l'approuver. En outre, le document n'est pas facile à trouver sur l'intranet de l'entreprise.	3	4	La publication n'est pas distribuée efficacement aux employés et aux autres personnes concernées.	Robert Johnson, CISO

PECB

148

Pour l'identification des mesures de sécurité existantes ou prévues, on peut se servir de la liste des mesures de sécurité d'ISO/IEC27002 (ou l'Annexe A d'ISO/IEC27001). Cela permet d'avoir un aperçu de la situation actuelle en ce qui concerne les bonnes pratiques de sécurité.

Ce document résume l'analyse des écarts qui a été faite au sein d'un organisme en mettant l'accent sur les actions à entreprendre en priorité. Son objectif à court terme est de favoriser la mise en œuvre de mesures correctives ou préventives pour les actifs avec un risque potentiel élevé. À moyen et long terme, ce modèle de rapport permet de suivre les mesures prévues et l'analyse des écarts effectuée, en mettant l'accent sur l'amélioration continue mise en œuvre dans l'organisme.

Déterminer les objectifs et faire l'analyse

Exemple – Analyse des écarts dans le contexte d'ISO/IEC 27001

Article	Exigence	Description de la situation actuelle	Maturité actuelle	Maturité ciblée	Analyse des écarts	Responsable
A.5.1.2 Revue des politiques de sécurité de l'information	<i>Les politiques de sécurité de l'information doivent être revues à intervalles programmés ou en cas de changements majeurs pour garantir leur pertinence, leur adéquation et leur effectivité dans le temps.</i>	La politique existe depuis plus de six mois et il n'y a pas encore eu de revue formelle par la direction. Actuellement, aucune revue n'est prévue. Cependant, il est clair qu'aucun changement majeur n'a été fait dans l'organisme qui nécessiterait une revue du document.	2	5	La politique n'est pas réexaminée périodiquement et, si aucun changement majeur ne survient, elle n'est pas revue du tout. Cependant, la direction est sensible lors de l'examen de la politique si un changement majeur est survenu dans les systèmes d'information.	Robert Johnson, CISO

PECB

149

Rapport d'analyse des écarts

Exemple – Contenu d'un rapport d'analyse des écarts

- Introduction
 - ▷ Objectif du rapport
 - ▷ Méthodologie
- Base de référence des mesures actuelles de la sécurité de l'information
 - ▷ Outils et processus disponibles
 - ▷ Défis posés par les outils, les processus et les ressources disponibles
- Cadre décisionnel axé sur la sécurité de l'information
 - ▷ Identifier et sélectionner un projet
 - ▷ Prévoir les résultats du projet de sécurité de l'information
 - ▷ Mettre en œuvre le projet
- Identification et analyse des écarts
- Options de transition suggérées
- Résumé et étapes suivantes



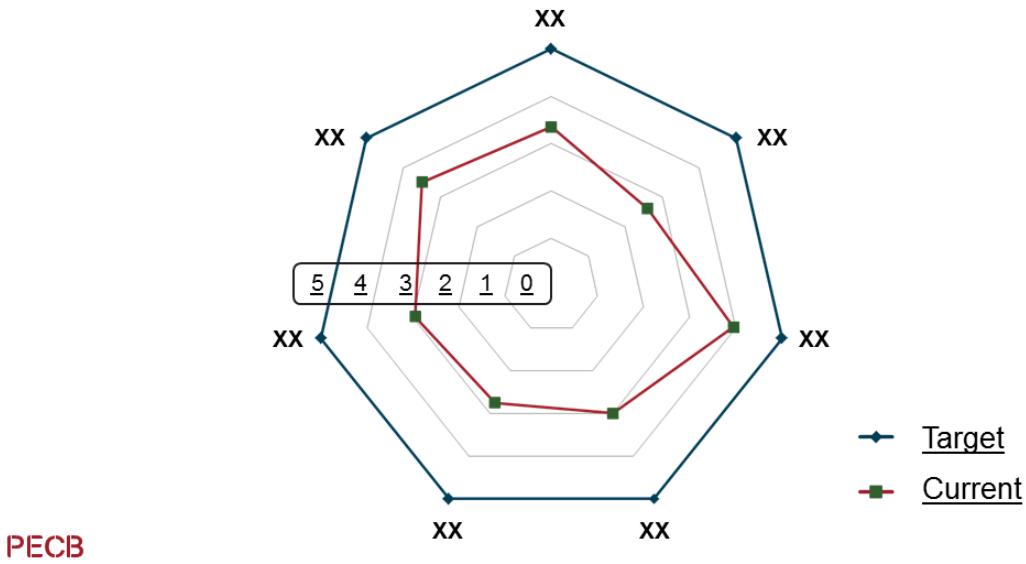
PECB

150

L'exemple montré sur la diapositive représente un potentiel rapport d'analyse des écarts.

Rapport d'analyse des écarts

Exemple de représentation graphique



151

Afin de présenter les différences mesurées, il est préférable de choisir un outil visuel efficace. Les données qui produisent des valeurs numériques basées sur des échelles qualitatives devraient être présentées de manière à ce que l'on puisse immédiatement remarquer les éléments positifs et ceux qui ont besoin d'être améliorés.

Dans le graphique «en radar» (aussi appelé «en toile d'araignée») ci-dessus, il y a autant d'axes qu'il y a de catégories.

Les catégories représentant les éléments du système de management de la sécurité de l'information (ISO/IEC27001), partent toutes du point central selon une séquence horaire classique. Elles sont indiquées autour du graphique (axe des X). Les valeurs de la série (ici, les valeurs attribuées par l'analyse de la maturité des processus) sont affichées à l'intérieur de la toile (axe des Y) sur une échelle impaire allant de 1 à 5.

La présentation en cercles concentriques ici utilisée peut varier selon que les segments de droite (lignes) relient les données d'une série, formant une «toile d'araignée» dont la forme variera donc en fonction du nombre de séries et des valeurs attribuées à chaque catégorie du graphique.

Les avantages de cette représentation comprennent:

- On peut présenter plusieurs séries de données dans un seul graphique.
- Elle est utilisée dans divers domaines pour mettre en valeur une série par rapport à une autre, les «toiles d'araignée» superposées donnant une bonne vue d'ensemble d'une situation.



Exercice 4

PECB

152

Exercice4: Analyse des écarts

En vous référant aux informations fournies dans l'étude de cas sur le fonctionnement du processus de gestion des changements, évaluez le niveau de maturité de ce processus. Également, la direction de l'organisme souhaiterait que vous lui fassiez des recommandations sur l'amélioration des processus actuellement en place afin de mieux se conformer aux exigences de la norme ISO/IEC27001 sur la gestion des changements.

Durée de l'exercice: 30 minutes

Commentaires: 15 minutes



Questions ?

PECB

153

Page de notes

PECB

154

Page de notes

PECB

155