



# NORMES ET BONNES PRATIQUES INFORMATIQUES

2024 - 2025



# **CHAPITRE 2**

# **INITIATION À ISO 27001**





# PROGRAMME

## 1. Fondamentaux de la norme ISO 27001

- Normes, Mesures, Risque, Vulnérabilité, etc.

## 2. Les types de mesures de sécurité

- Technologiques, Managériales, administratives, légales

## 3. Conception d'un SMSI (Atelier en groupe)

- Identifier les risques
- Proposer les mesures contre les risques
- Choisir les éléments constituants des mesures
- Architecturer un SMSI

## 4. Implémenter le SMSI

- Technique de mise en œuvre des mesures (ISO 27000)

## 5. Pré audit de son SMSI selon ISO 27001

- Analyse des écarts
- Améliorations
- Les **8 exigences** de l'ISO 27001



# FONDAMENTAUX

ISO 27001





# FAMILLES DE NORME ISO 27001

Norme	Nom complet	Rôle simplifié
ISO/IEC 27000	<b>Vue d'ensemble et vocabulaire</b>	Explique <b>les concepts et les termes</b> utilisés dans toutes les autres normes.
ISO/IEC 27001	Système de management de la sécurité de l'information ( <b>SMSI</b> )	C'est <b>la norme principale</b> : elle dit <b>quoi faire</b> pour sécuriser les infos.
ISO/IEC 27002	<b>Code de bonnes pratiques</b> pour les contrôles de sécurité	Elle <b>détaille comment appliquer</b> les mesures listées dans l'ISO 27001.
ISO/IEC 27003	<b>Lignes directrices pour la mise en œuvre du SMSI</b>	Donne un <b>guide pas à pas</b> pour installer correctement un SMSI.
ISO/IEC 27004	Mesure de la performance de la sécurité de l'information	Aide à <b>mesurer si la sécurité fonctionne bien</b> (indicateurs, métriques).
ISO/IEC 27005	Gestion des risques liés à la sécurité de l'information	Explique <b>comment identifier et gérer les risques</b> informatiques.



# FAMILLES DE NORME ISO 27001

Norme	Nom complet	Rôle simplifié
ISO/IEC 27006	Exigences pour les organismes qui certifient ISO 27001	<input checked="" type="checkbox"/> Norme pour ceux qui <b>délivrent la certification ISO 27001</b> (auditeurs, etc.).
ISO/IEC 27007	Lignes directrices pour l' <b>audit des SMSI</b>	 Aide à faire <b>des audits internes</b> pour vérifier la conformité au SMSI.
ISO/IEC 27017	Lignes directrices pour la <b>sécurité du cloud</b>	 Donne des <b>bonnes pratiques</b> spécifiques à la <b>sécurité dans le cloud</b> .
ISO/IEC 27018	<b>Protection des données personnelles dans le cloud</b>	 Spécialement pour <b>protéger les données personnelles hébergées dans le cloud</b> .
ISO/IEC 27019	Sécurité pour les <b>systèmes de contrôle dans l'énergie</b>	 Ciblée pour les <b>réseaux électriques et industriels</b> (SCADA, OT, etc.).
ISO/IEC 27701	Extension pour la <b>gestion de la vie privée</b> (RGPD, etc.)	 Ajoute la <b>protection de la vie privée</b> au système ISO 27001 (compatible RGPD).



# Qu'est-ce qu'un système de management ?

## ISO/IEC 27000, article 3.41

**Définition :** ensemble d'éléments corrélés ou interactifs d'un organisme visant à établir des politiques, des objectifs et des processus permettant d'atteindre ces objectifs

- Toutes les organisations disposent d'une forme ou d'une autre de système de management, c'est-à-dire d'un mode de fonctionnement.
- Un système de management cohérent et fonctionnel combine processus, ressources, outils et main-d'œuvre.
- Les systèmes de gestion peuvent avoir des degrés de formalité divers : de moins formels à bien définis et documentés.
- Un niveau approprié de documentation est préférable pour assurer la cohérence, l'amélioration continue et la conservation des connaissances organisationnelles.



À mesure que le contexte interne et externe d'une organisation évolue, le système de management doit être agile, adaptable et réactif à ces changements.

Les organisations **mettent en œuvre les systèmes de management** afin d'améliorer leurs opérations et renforcer leur **performance commerciale**, tout en augmentant la satisfaction des clients

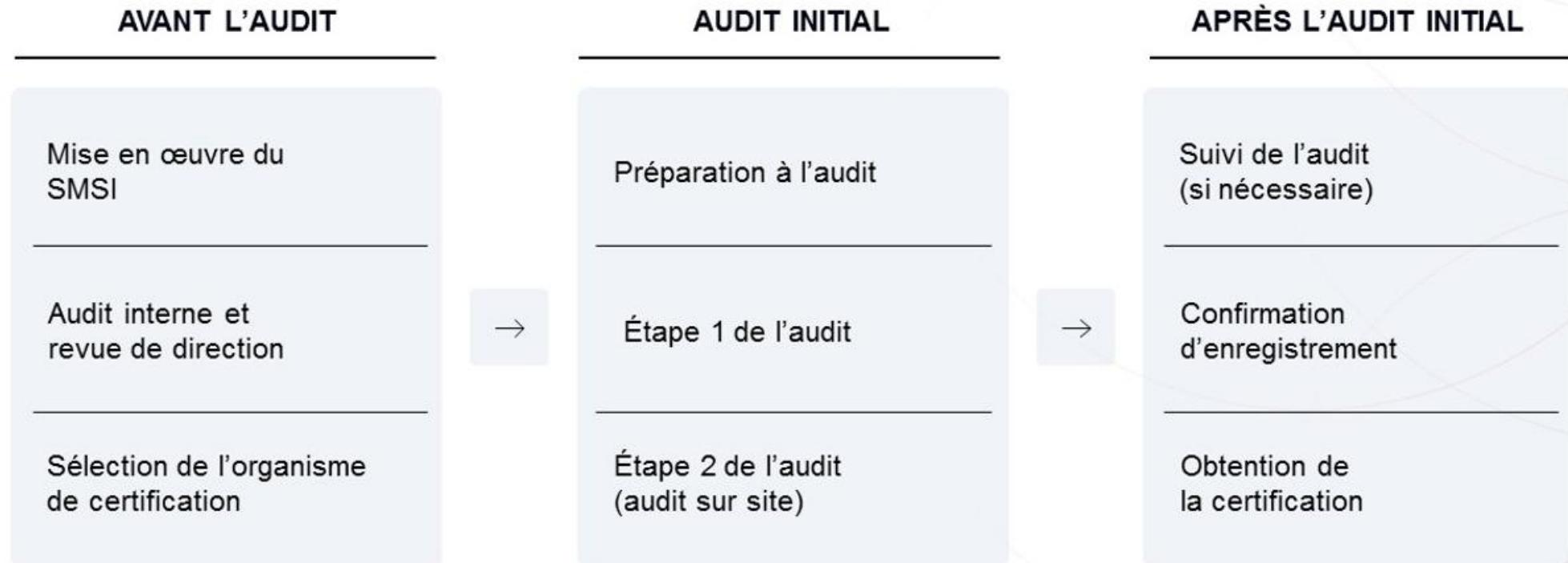
# Autres normes relatives aux systèmes de management

Outre la norme ISO/IEC 27001, les organisations peuvent être certifiées conformément aux normes primaires suivantes :





# Processus de certification



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

# Préparation à l'audit de certification

## Recommandations

1 Comprendre la norme



2 Identifier les experts métier



3 Allouer suffisamment de ressources



4 Effectuer une auto-évaluation



5 Préparer le personnel



6 Préparer les informations documentées



# Qu'est-ce qu'un système de management de la sécurité de l'information ?

## ISO/IEC 27000, article 4.2.1

**Définition :** 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.



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.

Un SMSI utilise une approche systématique visant à :



la sécurité de l'information d'une organisation afin que celle-ci atteigne ses objectifs commerciaux.

# Avantages d'un SMSI conformément à la norme ISO/IEC 27001

La mise en œuvre d'un SMSI conformément à la norme ISO/IEC 27001 confère plusieurs avantages :



Sécurité de l'information



Réponse efficace aux menaces pour la sécurité



Bonne gouvernance et culture

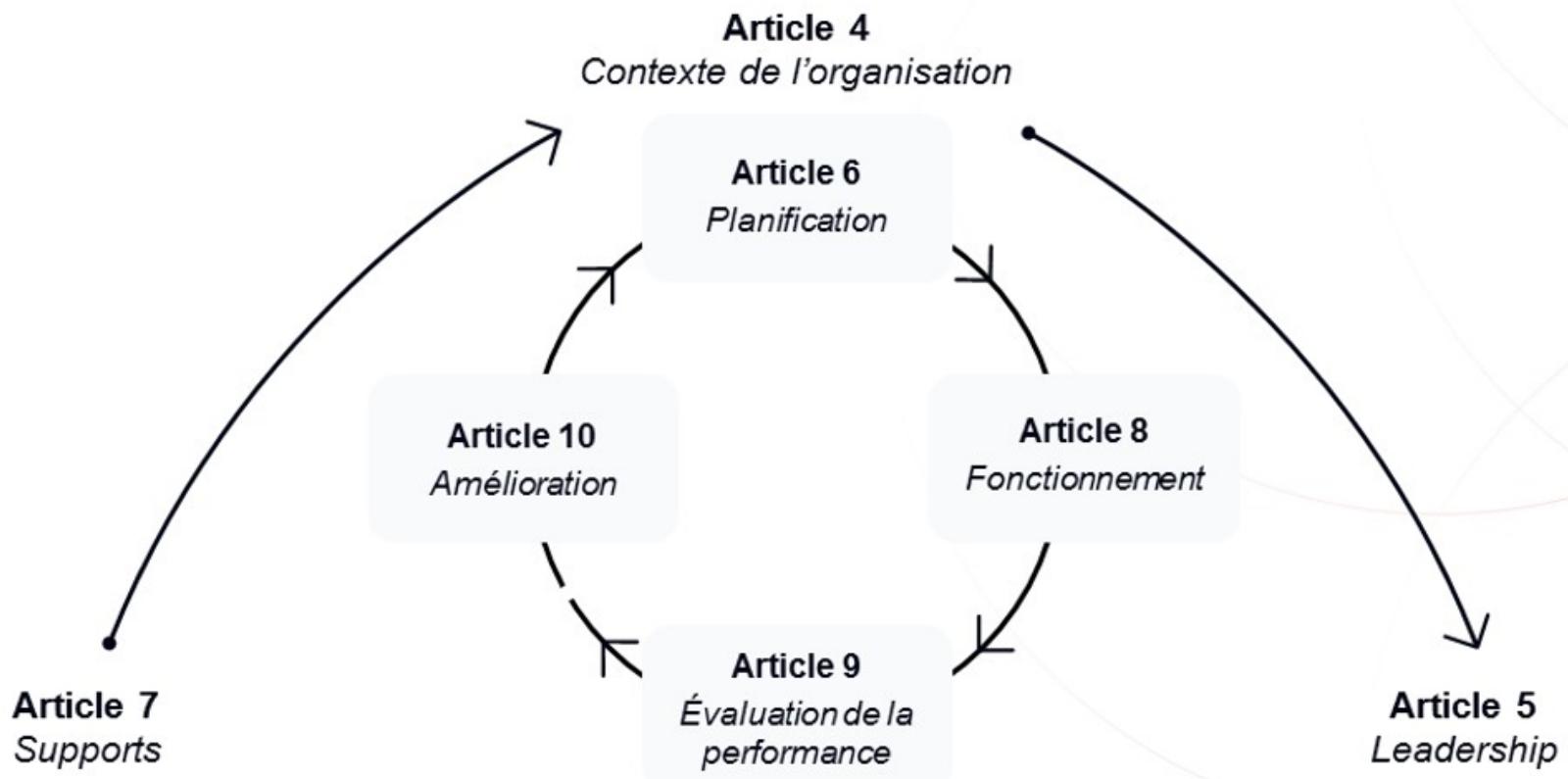


Réduction des coûts liés à la sécurité de l'information



Conformité avec d'autres lois et réglementations

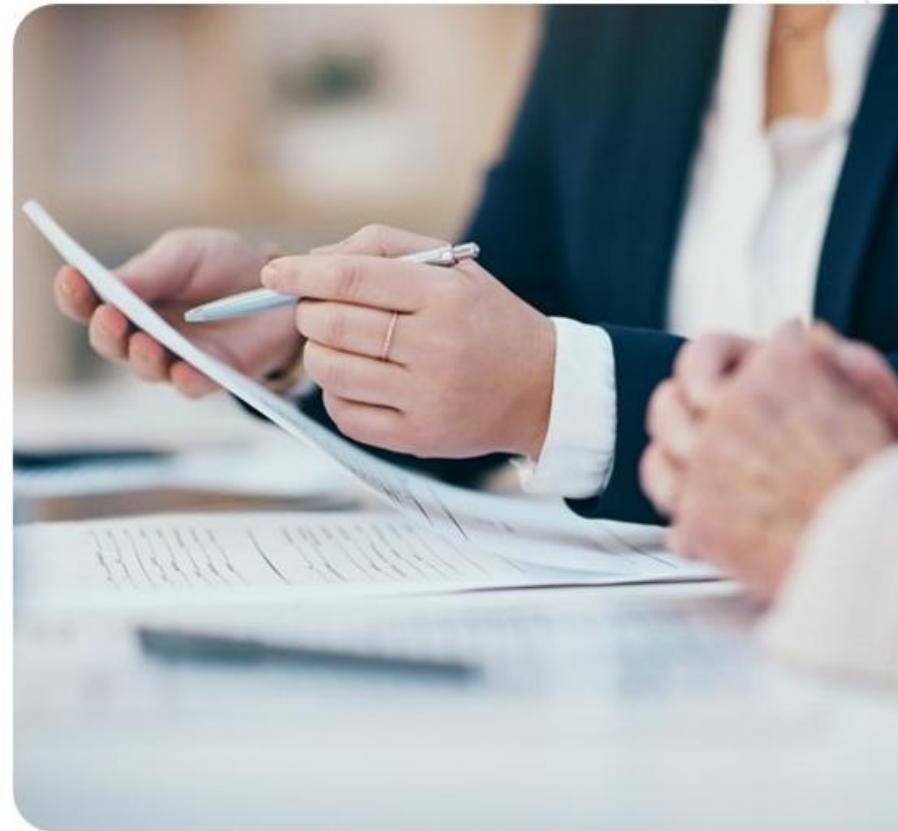
# Structure de la norme ISO/IEC 27001:2022



**Annexe A**  
Référencement des mesures de sécurité de l'information

## Annexe A

- L'Annexe A fait partie de la norme ISO/IEC 27001 et contient 93 mesures de sécurité qu'il convient de prendre en compte pour se conformer à la norme.
- La liste des mesures de sécurité de l'information de l'Annexe A n'est pas exhaustive. L'organisation peut, au besoin, ajouter des mesures supplémentaires provenant d'autres sources.
- Si une mesure particulière n'est pas applicable, il convient que l'organisation fournisse une justification acceptable de son exclusion.



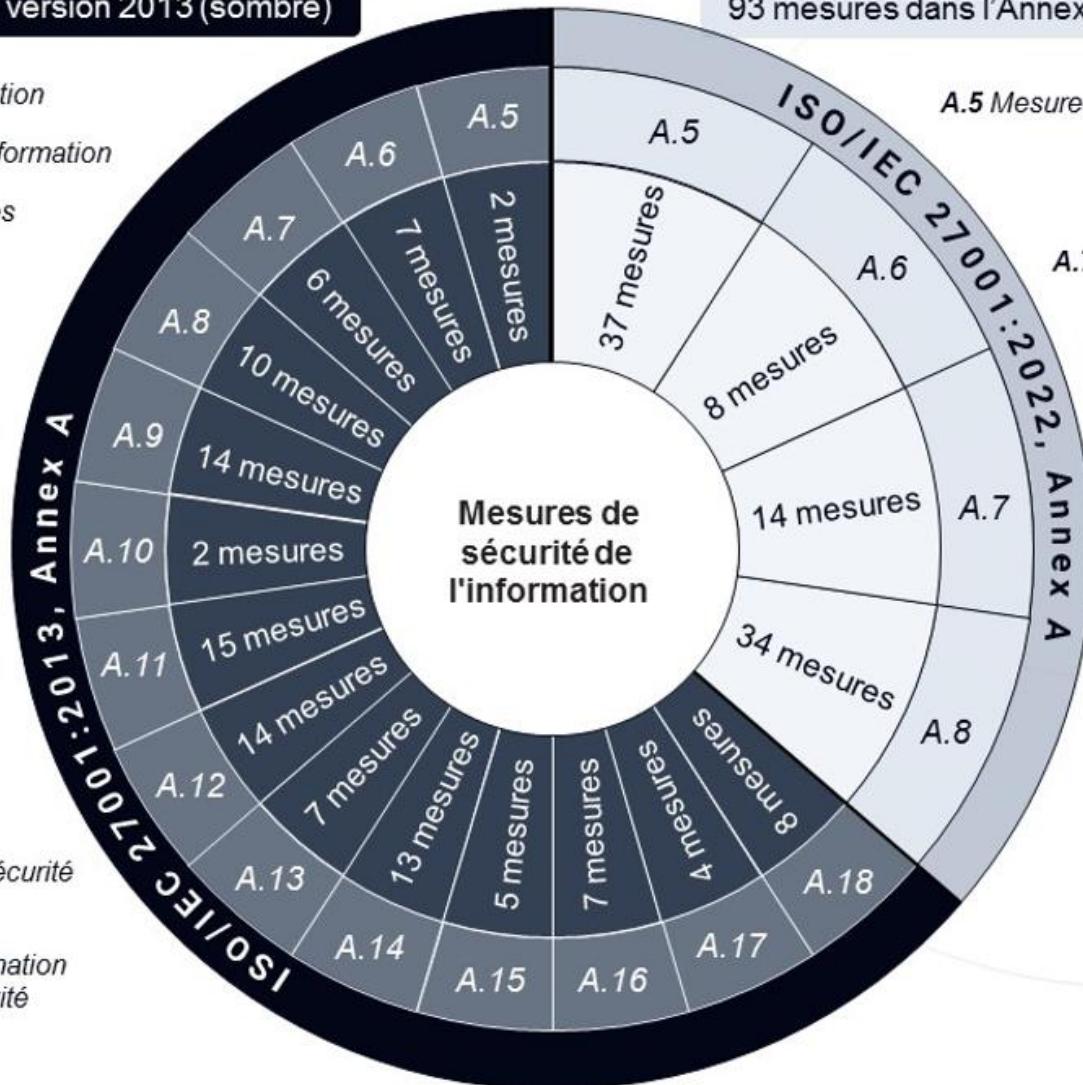


114 mesures dans l'Annexe A, version 2013 (sombre)

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

93 mesures dans l'Annexe A, version 2022 (claire)

- A.5 Mesures de sécurité organisationnelles
- A.6 Mesures de sécurité applicables aux personnes
- A.7 Mesures de sécurité physique
- A.8 Mesures de sécurité technologiques



# Information et actif

ISO 9000, article 3.8.2 et ISO 55000, article 3.2.1

## Définitions

- **Information** : données porteuses de sens
- **Actif** : élément ou entité ayant une valeur potentielle ou réelle pour une organisation



Les actifs personnels ou individuels comprennent :

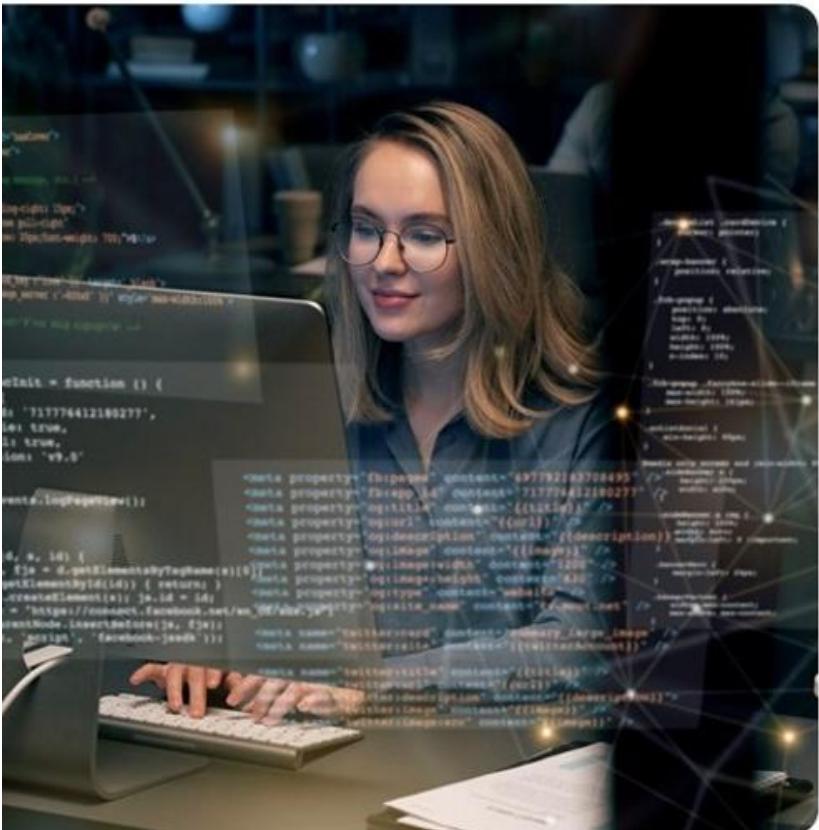
- Les actifs virtuels, tels que les comptes bancaires, les données médicales, les comptes de messagerie électronique et les identités numériques des clients
- Les actifs physiques, tels que les appareils personnels et les PC

Les actifs organisationnels comprennent :

- Les actifs virtuels, tels que l'image de marque en ligne, la réputation, les plans d'affaires et la propriété intellectuelle
- Les actifs physiques, tels que les serveurs, les câbles connectés et les postes de travail



# Sécurité de l'information



- L'article 3.28 de la norme ISO/IEC 27000 définit la sécurité de l'information comme étant la « *protection de la vie privée, de l'intégrité et de la disponibilité de l'information* ».
- La sécurité de l'information détermine les informations qui doivent être protégées, pourquoi elles doivent l'être, comment le faire et contre quoi les protéger.
- La sécurité de l'information couvre les informations de toute nature, imprimées ou manuscrites, transmises par e-mail ou sur site Web, mentionnées au cours d'une conversation, etc.
- Les organisations peuvent assurer la sécurité de l'information en mettant en œuvre des politiques et des mesures appropriées qui sont alignées sur leurs objectifs et qui réduisent les vulnérabilités et atténuent les menaces.

# Confidentialité, intégrité et disponibilité

ISO/IEC 27000, articles 3.7, 3.10 et 3.36

## Définitions

### 3.10 Confidentialité

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

### 3.36 Intégrité

*propriété d'exactitude et de complétude*

### 3.7 Disponibilité

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

# Confidentialité



Assurer la confidentialité des informations implique que seuls les utilisateurs autorisés ont accès aux données sensibles.

Les organisations peuvent y parvenir par les actions suivantes :

- Utiliser des méthodes d'authentification, par exemple l'authentification multifactorielle, qui imposent l'identification de l'utilisateur et un mot de passe pour accéder aux données confidentielles
- Mettre en place une politique d'accès aux données
- Mettre en œuvre des contrôles d'accès qui permettent aux utilisateurs d'accéder uniquement aux informations dont ils ont besoin pour effectuer leur travail
- Chiffrer les informations pour en dissimuler le sens



# Intégrité

Assurer l'intégrité de l'information implique que :

- Les informations ne sont pas modifiées lorsqu'elles sont stockées ou qu'elles sont en transit
- Seules les modifications autorisées sont apportées
- Les données sont précises, cohérentes, fiables et protégées contre tout accès non autorisé

Parmi les contrôles permettant de garantir l'intégrité des informations, on peut citer la conversion des données en un code secret accessible uniquement aux personnes autorisées, la mise en place de contrôles d'accès et de versions, ainsi que l'établissement de procédures de sauvegarde.



# Disponibilité

Garantir la disponibilité de l'information signifie que l'information est accessible :

- à la demande
- au moment voulu
- à l'endroit voulu
- à la personne qui en fait la demande

Pour y parvenir, il convient que les organisations maintiennent et améliorent leurs infrastructures physiques, notamment les serveurs et les disques, et mettent en place des politiques de conservation des enregistrements, des procédures de sauvegarde et de récupération des données, des procédures de gestion des incidents, des procédures de traitement de l'information et des procédures de contrôle de l'utilisation des systèmes.





## CAS PRATIQUE

Dans chacun des scénarios suivants, **analyser le critère de sécurité qui a été compromis**

Un employé envoie accidentellement une fiche de paie au mauvais destinataire par email.

Un virus modifie des fichiers de base de données clients sans que cela soit immédiatement détecté.

Un attaquant intercepte des communications non chiffrées entre deux collaborateurs via Wi-Fi public.

Un technicien restaure une version ancienne d'un fichier sans alerter, provoquant la perte de données récentes.

Un stagiaire ajoute une règle incorrecte dans le pare-feu, empêchant tous les employés d'accéder à l'intranet.

Un compte administrateur est compromis et utilisé pour consulter les données de tous les employés sans autorisation.



## CAS PRATIQUE

Scénario	Description réaliste et complexe
<b>1. Intrusion furtive et accès non détecté</b>	Un attaquant exploite une faille non corrigée dans un serveur web public. Il obtient un accès discret aux logs de connexion internes, sans modifier les fichiers ni interrompre les services. L'accès reste non détecté pendant trois semaines.
<b>2. Corruption silencieuse de base de données</b>	Suite à une mauvaise configuration d'un module d'intégration tiers, certaines données clients sont mises à jour automatiquement avec des valeurs incorrectes pendant plusieurs jours, sans que personne ne s'en rende compte immédiatement.
<b>3. Fuite par ingénierie sociale ciblée</b>	Un cadre intermédiaire est manipulé par téléphone pour transmettre par email un fichier de planification stratégique confidentiel à une adresse externe, pensant qu'il s'agit d'un collègue légitime.
<b>4. Ransomware et double extorsion</b>	Un ransomware chiffre tous les fichiers partagés du service RH. Les hackers menacent ensuite de publier les dossiers médicaux du personnel volés avant le chiffrement, si une rançon n'est pas payée.



## CAS PRATIQUE

Scénario	Description réaliste et complexe
<b>5. Mise à jour automatique défaillante</b>	Une mise à jour automatique d'un logiciel de gestion comptable, non testée en préproduction, écrase plusieurs fichiers critiques sans avertissement. L'équipe s'en rend compte 48h plus tard.
<b>6. Déni de service distribué ciblé (DDoS)</b>	Le site e-commerce de l'entreprise subit une attaque DDoS le jour du lancement d'un produit. Le portail client est inaccessible pendant 10 heures, entraînant une perte financière et une dégradation de l'image.
<b>7. Reprise après sinistre mal préparée</b>	Après un incendie dans le data center principal, la bascule automatique vers le site de secours fonctionne, mais les dernières sauvegardes n'étaient pas synchronisées depuis 5 jours. Des données sont perdues.
<b>8. Exploitation d'un compte à priviléges par un employé mécontent</b>	Un administrateur IT en cours de licenciement utilise ses accès étendus pour copier discrètement des fichiers confidentiels et supprimer des journaux d'audit. Son activité n'est découverte que 2 semaines plus tard.

# Vulnérabilité

ISO/IEC 27000, article 3.77



## Définition

*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 menaces correspondantes peuvent ne pas nécessiter de mesures, mais il convient de les identifier et de les surveiller afin de détecter les changements.
- Les mesures de sécurité qui ne sont pas correctement mises en œuvre ou qui fonctionnent mal pourraient devenir des vulnérabilités.



# Menaces

ISO/IEC 27005, articles 3.1.9 et 7.2.1



Définition :

*cause potentielle d'un incident lié à la sécurité de l'information qui peut entraîner des dommages pour un système ou porter préjudice à un organisme*

---

*Une menace exploite une vulnérabilité d'un bien pour compromettre la confidentialité, l'intégrité et/ou la disponibilité des informations correspondantes.*

# Exemples de menaces

ISO/IEC 27005, Tableau A.11 (extrait)

<i>Catégorie</i>	<i>Description de la menace</i>
<i>Menaces physiques</i>	<ul style="list-style-type: none"><li>— Feu (A, D, E)</li><li>— Eau (A, D, E)</li><li>— Poussière, corrosion, congélation (A, D, E)</li></ul>
<i>Menaces naturelles</i>	<ul style="list-style-type: none"><li>— Phénomène climatique (E)</li><li>— Phénomène sismique (E)</li></ul>
<i>Défaillances des infrastructures</i>	<ul style="list-style-type: none"><li>— Coupure d'alimentation (A, D, E)</li><li>— Défaillance d'un réseau de télécommunication (A, D, E)</li></ul>
<i>Défaillances techniques</i>	<ul style="list-style-type: none"><li>— Défaillance des machines ou du système (A)</li><li>— Violation de la maintenabilité du système d'information (A, D)</li></ul>
<i>Actions humaines</i>	<ul style="list-style-type: none"><li>— Terrorisme, attaque, sabotage (D)</li><li>— Ingénierie sociale (D)</li><li>— Traitement non autorisé de données à caractère personnel (A, D)</li></ul>
<i>Compromission de fonctions ou de services</i>	<ul style="list-style-type: none"><li>— Erreur d'utilisation (A)</li><li>— Abus de droits ou de permissions (A, D)</li><li>— Falsification de droits ou de permissions (D)</li></ul>
<i>Menaces organisationnelles</i>	<ul style="list-style-type: none"><li>— Manque de personnel (A, E)</li><li>— Manque de ressources (A, E)</li><li>— Violation de la législation ou de la réglementation (A, D)</li></ul>

*Type de source de risque : D = Délibéré (intentionnel) ; A = Accidentelle ; E = Environnementale*



## Vulnérabilités

- Entrepôt non protégé et sans surveillance
- Procédures compliquées de traitement des données
- Absence de protection de mot de passe
- Données non chiffrées
- Utilisation de logiciels piratés
- Pas de revue des droits d'accès
- Absence de procédures de sauvegarde des données



## Menaces

- Vol
- Erreur d'entrée des données par le personnel
- Piratage
- Vol de données
- Virus
- Accès non autorisé aux anciens employés
- Coupure d'alimentation électrique

# Conséquences

## Exemples



### Conséquences sur la confidentialité

- Atteinte à la vie privée des utilisateurs ou des clients
- Atteinte à la vie privée des employés
- Fuite d'informations confidentielles

### Conséquences sur la disponibilité

- Interruption du service
- Indisponibilité du service
- Perturbations des opérations

### Conséquences sur l'intégrité

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



# Risque lié à la sécurité de l'information



Selon la norme NIST SP 800-30, le risque lié à la sécurité de l'information est défini comme « *le risque pour les opérations organisationnelles, les actifs organisationnels, les personnes, les organisations et la nation d'être impactés par la possibilité d'un accès, d'une utilisation, d'une divulgation, d'une perturbation, d'une modification ou d'une destruction non autorisés des informations et/ou des systèmes d'information* ».

---

La gestion des risques liés à la sécurité de l'information est le processus d'identification, d'analyse et d'atténuation de ces risques et de minimisation de leur impact.

---

Cette gestion des risques est essentielle pour identifier et traiter les menaces et les vulnérabilités potentielles en matière de sécurité de l'information.

# Classification des mesures de sécurité par type



## Mesures techniques

Mesures de sécurité liées à l'utilisation de mesures techniques ou technologiques, telles que les pare-feu, les systèmes d'alarme, les caméras de surveillance et les systèmes de détection d'intrusion (IDS).



## Mesures administratives

Mesures de sécurité liées à la structure organisationnelle, telles que la séparation des tâches, les rotations de postes, les descriptions de postes et les processus d'approbation.



## Mesures légales

Mesures de sécurité liées à l'application d'une législation, des exigences réglementaires ou des obligations contractuelles.



## Mesures managériales

Mesures de sécurité liées à la gestion du personnel, y compris la formation des employés, les revues de direction et les audits internes.



## CAS PRATIQUE

Une entreprise de **services financiers** (ex : une assurance) héberge des données sensibles de ses clients (identité, revenus, santé, etc.). L'entreprise **se conformer à l'ISO/IEC 27001** pour **réduire les risques, rassurer ses clients et se mettre en règle avec le RGPD**.

**Quels sont les mesures de sécurité que l'entreprise peut adopter ?**



# Classification des mesures de sécurité par fonction

## Mesures préventives

Mesures de sécurité visant à éviter ou à prévenir l'apparition des risques



## Mesures détectives

Mesures de sécurité visant à rechercher, détecter et identifier les risques

## Mesures correctives

Mesures de sécurité visant à résoudre les risques identifiés et à prévenir leur réapparition



## CAS PRATIQUE

Une entreprise de **150 employés** utilise un service de messagerie (Outlook, Exchange ou Google Workspace) pour toutes ses communications internes et externes. Récemment, deux incidents majeurs ont été signalés :

- Un **compte de direction compromis après une attaque par hameçonnage (phishing)**.
- Un **document sensible envoyé à la mauvaise adresse par erreur**.

**L'entreprise veut renforcer la sécurité autour de la messagerie électronique, en appliquant des mesures préventives, détectives et correctives.**



## CAS PRATIQUE

### MESURES PRÉVENTIVES

Mesure	Explication
Activation de la <b>double authentification</b> (2FA)	Empêche les intrusions même en cas de vol de mot de passe
<b>Formation</b> des utilisateurs à détecter les emails frauduleux (phishing)	Réduit les erreurs humaines dues à la méconnaissance des menaces
Mise en place d'une <b>politique de classification des données sensibles.</b>	Encourage les bonnes pratiques selon la nature (confidentiel, interne, etc.)
Restriction d'envoi vers des domaines externes non approuvés.	Prévient les envois accidentels de documents sensibles à de mauvais destinataires



## CAS PRATIQUE

MESURES DÉTECTIVES	
Mesure	Explication
<b>Journalisation des connexions</b> et des activités de messagerie	Permet de retracer les actions en cas de comportement suspect
Déploiement d'une <b>solution antiphishing</b> / passerelle de messagerie	Filtre les attaques avant qu'elles n'atteignent l'utilisateur final
<b>Tableau de bord de supervision</b> de la messagerie	Fournit une vision en temps réel au RSSI pour détecter des anomalies

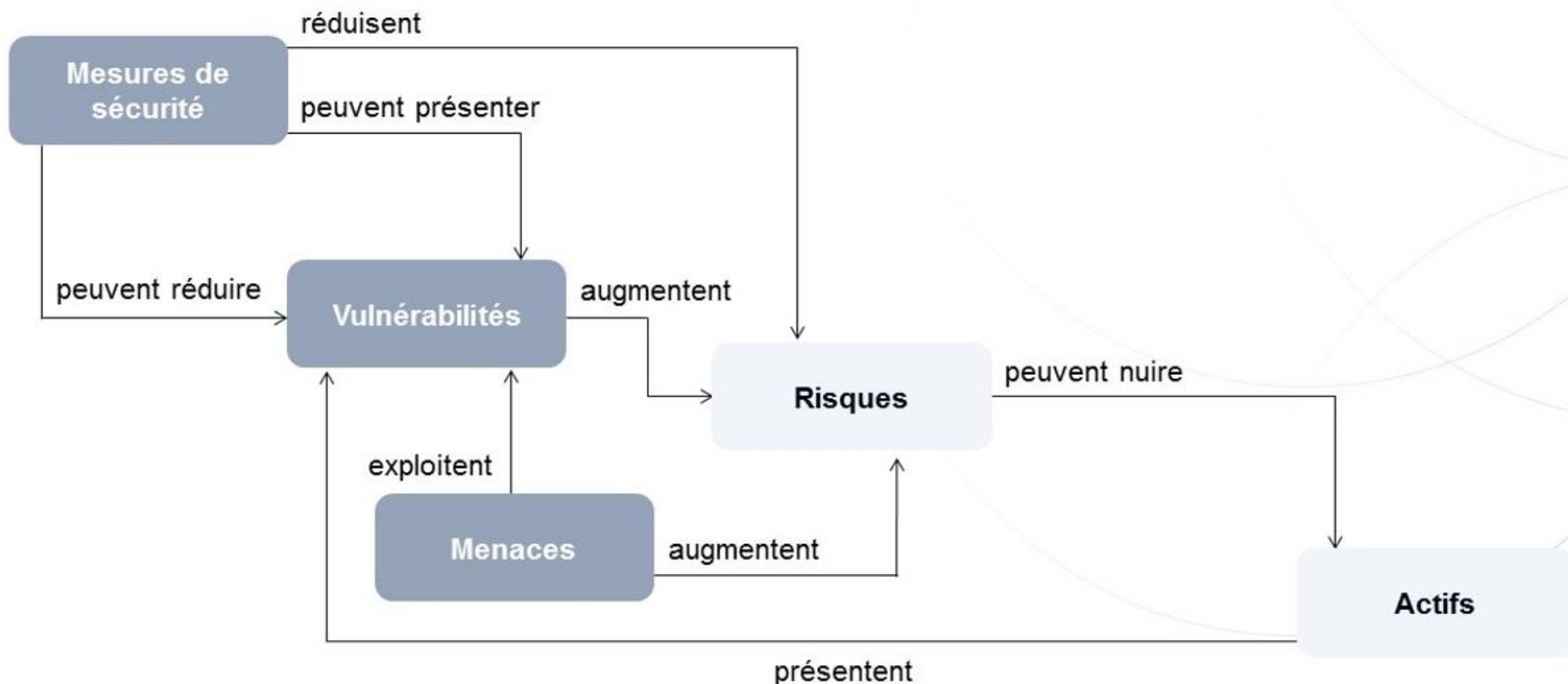


## CAS PRATIQUE

MESURES CORRECTIVES	
Mesure	Explication
<b>Réinitialisation immédiate</b> du mot de passe du compte compromis	Stoppe l'accès non autorisé
<b>Blocage temporaire d'un compte</b> en cas de comportement suspect	Contient la menace jusqu'à vérification
Déclaration de l'incident à la <b>CNIL</b> (Commission Nationale de l'Informatique et des Libertés) si données personnelles concernées	Obligatoire selon le RGPD (sous 72h)
Mise à jour du plan de réponse aux incidents	Permet d'intégrer les leçons apprises et d'améliorer le SMSI

# Liens entre les éléments de sécurité de l'information

## Vue d'ensemble



# Mise en application de l'approche de mise en œuvre proposée

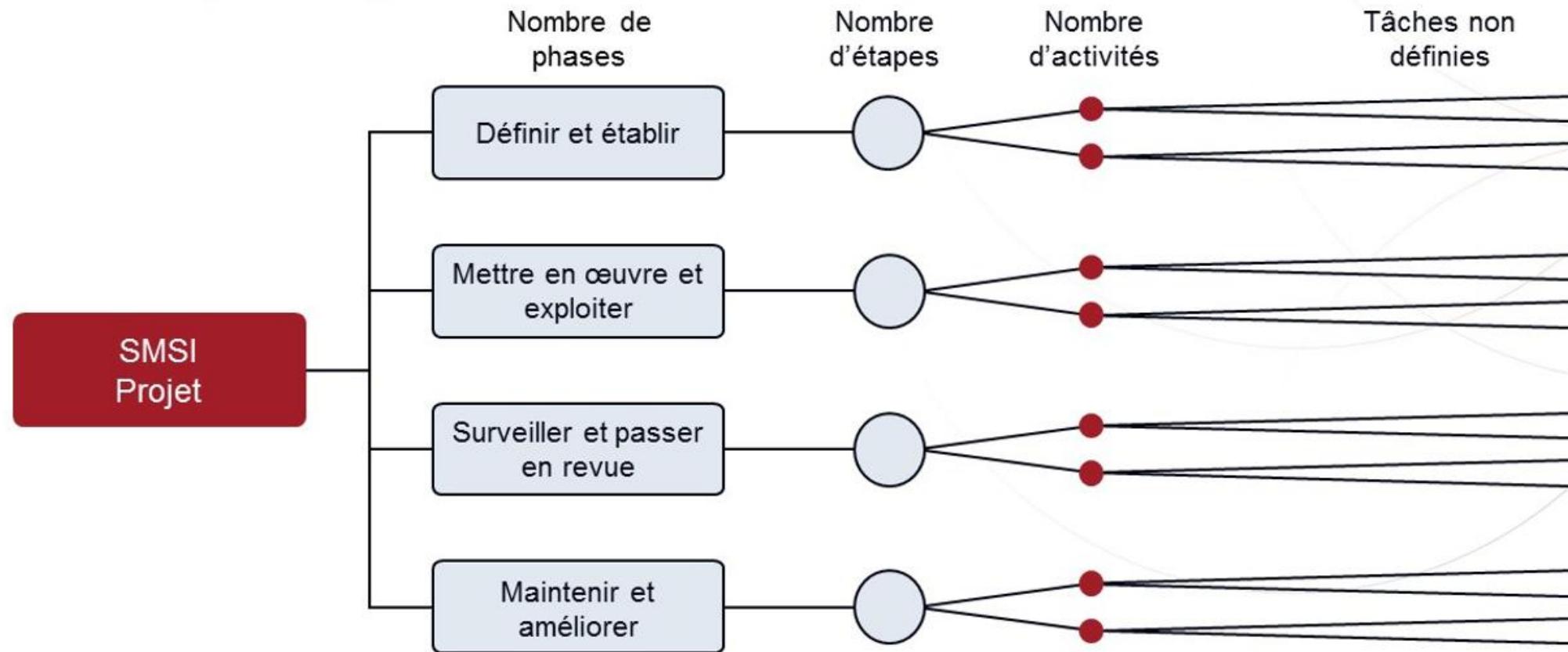
## Recommandations

1. Désigner et nommer un chef de projet SMSI
2. S'assurer du soutien de la direction générale
3. Impliquer les parties intéressées
4. Intégrer le SMSI dans les processus existants
5. Éviter l'intégration de nouvelles technologies
6. Mettre en application les principes de l'amélioration continue



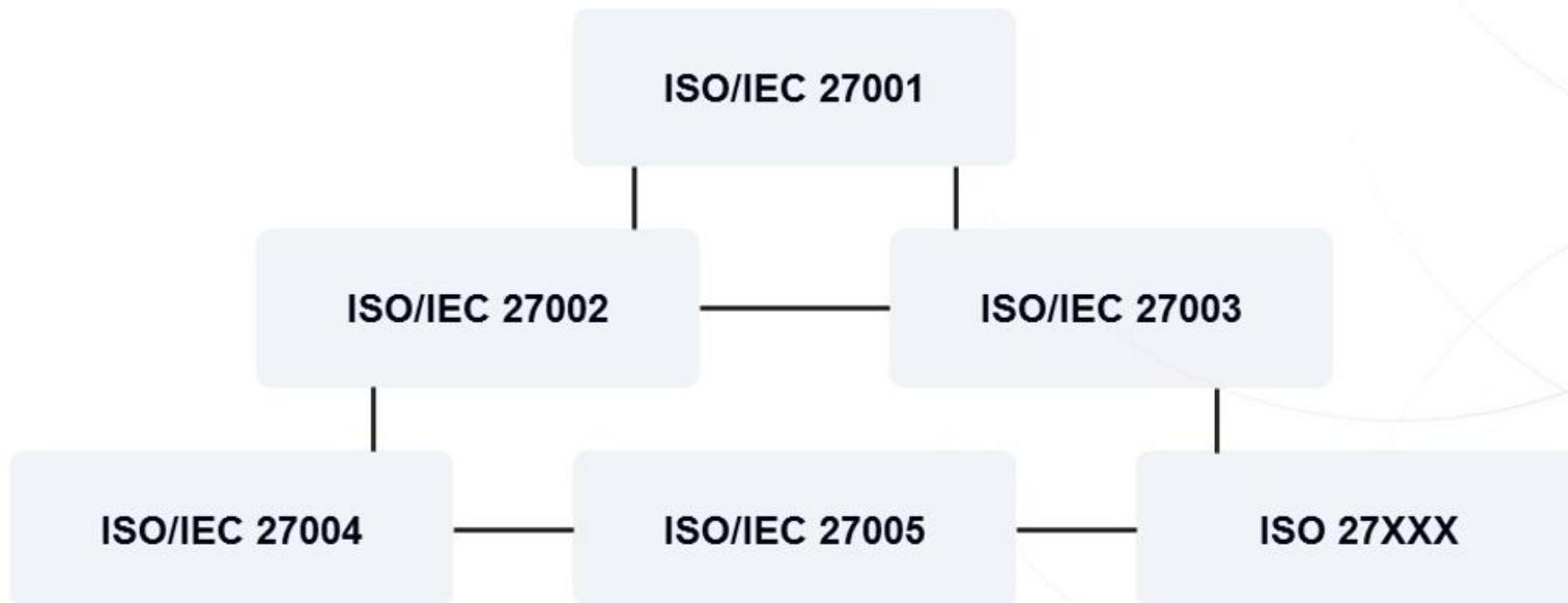
# Integrated Implementation Methodology for Management Systems and Standards

## Méthodologie PECB pour la mise en œuvre du SMSI



# Arrimage aux bonnes pratiques

## Utilisation des normes ISO



# Approche et méthodologie

Basée sur les bonnes pratiques



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

**ISO/IEC 27003**  
Sécurité de  
l'information  
Mise en œuvre du  
système de  
management  
Lignes directrices

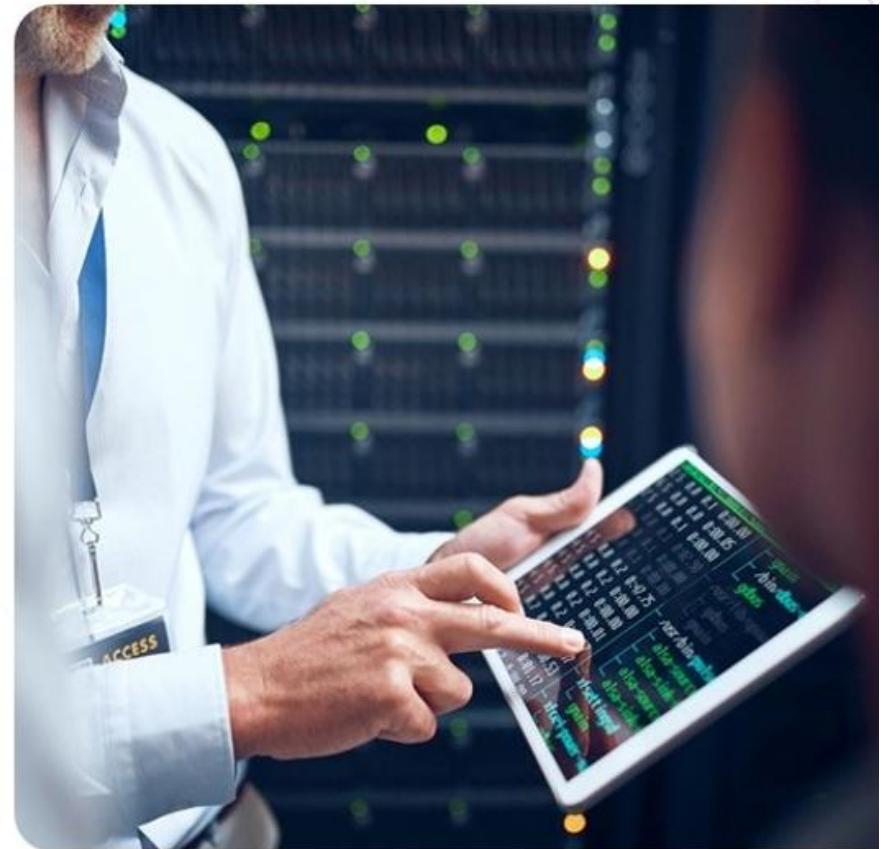


**PMBOK**  
Gestion de projet  
Bibliothèque de  
connaissances

# Exigences de la norme ISO/IEC 27001 relatives à la compréhension de l'organisation et de son contexte

## ISO/IEC 27001, article 4.1

- *L'organisation doit déterminer les enjeux externes et internes pertinents compte tenu de sa mission et qui ont une incidence sur sa capacité à obtenir le(s) résultat(s) attendu(s) de son système de management de la sécurité de l'information.*
- *L'organisation doit déterminer si les changements climatiques sont un enjeu pertinent.*



## 1.1.2 Déterminer les objectifs du SMSI

### ISO/IEC 27001:2022, article 6.2

*L'organisation doit établir, aux fonctions et niveaux concernés, des objectifs de sécurité de l'information. L'organisation doit conserver des informations documentées sur les 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 comme approprié ;

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

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

# Exemples d'objectifs SMSI

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

- Réaliser la conformité aux exigences légales, réglementaires et contractuelles
- Faire preuve de diligence raisonnable
- Inspirer confiance aux parties intéressées de l'organisation
- Protéger les actifs critiques de l'organisation
- Assurer la sécurité de l'information en respectant 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

La détermination des objectifs devrait prendre en compte :

- Événements historiques au sein de l'organisation
- Expositions au risque courantes et émergentes
- Perturbations et incidents opérationnels antérieurs
- Coût associé aux éventuelles perturbations
- Coûts financiers
- Passifs
- Responsabilités sociales
- Succès et échec d'autres projets et programmes de sécurité de l'information

## 1.1.3 Déterminer le domaine d'application préliminaire

Pour définir le domaine d'application d'un SMSI, une organisation peut prendre les mesures suivantes :

- **Déterminer le domaine d'application préliminaire** : Cette activité devrait être menée par un petit groupe représentatif de la direction générale de l'organisation.
- **Déterminer le domaine d'application de l'amélioration** : Les unités fonctionnelles situées à l'intérieur et à l'extérieur du domaine d'application préliminaire devraient être revues, éventuellement suivies de l'inclusion ou de l'exclusion de certaines de ces unités fonctionnelles afin de réduire le nombre d'interfaces le long des limites du domaine d'application. Lors de l'amélioration du domaine d'application préliminaire, toutes les fonctions nécessaires pour soutenir les activités métier du domaine d'application devraient être prises en compte.
- **Déterminer le domaine d'application final** : Il convient que le domaine d'application amélioré soit évalué par la direction générale de l'organisation. Il convient également de l'ajuster et de l'expliquer avec précision.
- **Approuver le domaine d'application** : Les informations documentées décrivant le domaine d'application devraient être formellement approuvées par la direction générale.

## Avis pratiques

- La norme ISO/IEC 27001 ne prévoit pas d'approche pratique expliquant comment analyser le contexte d'une organisation. À ce titre, les organisations sont libres de choisir l'approche qu'elles jugent la plus appropriée à leur contexte.
- Il existe de nombreuses approches qui aident à comprendre le fonctionnement d'une organisation. Lors de l'adoption d'une approche, il est important d'identifier les caractéristiques des facteurs internes et externes qui influencent la mission d'une organisation, ses principales activités, les parties intéressées, etc.

P Politique

E Économique

S Social

T Technologique

Environnement externe

Micro-environnement

Macro-environnement

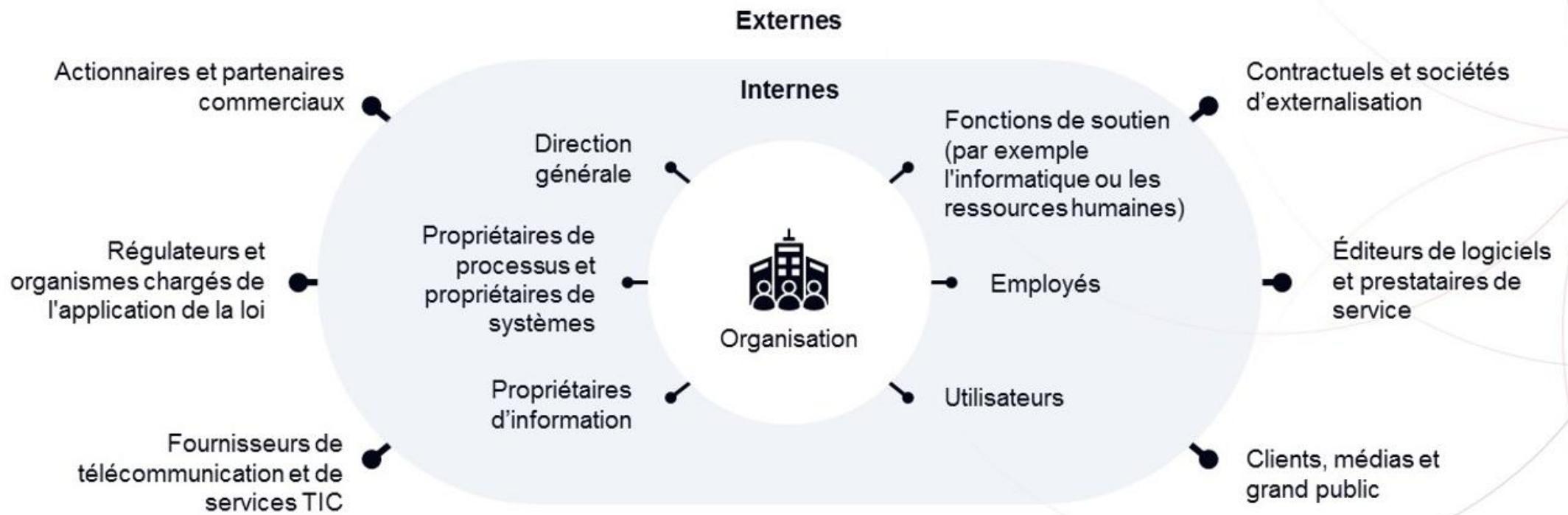
S Strengths

W Weaknesses

O Opportunities

T Threats

# Exemples de parties intéressées externes et internes





# DIFFÉRENCE ENTRE POLITIQUE, PROCESSUS ET PROCÉDURE

Élément	Définition simple	Rôle dans l'organisation	<input checked="" type="checkbox"/> Exemple concret
 Politique	Un <b>ensemble de principes directeurs</b> et de règles générales décidées par la direction.	Donne le <b>cadre global</b> et les intentions stratégiques.	« La <b>politique de sécurité de l'information</b> interdit le stockage de données sur clé USB. »
 Processus	Une <b>suite d'activités interconnectées</b> visant un objectif.	Définit " <b>quoi faire</b> " pour produire un résultat.	« Le <b>processus de gestion des incidents IT</b> décrit comment identifier, traiter et clôturer un incident. »
 Procédure	Une <b>description détaillée et pas-à-pas</b> de la manière de réaliser une tâche.	Explique " <b>comment faire</b> " concrètement une activité.	« Pour signaler un incident, l'utilisateur doit remplir le formulaire X et l'envoyer au support. »



## DIFFÉRENCE ENTRE POLITIQUE, PROCESSUS ET PROCÉDURE

	Politique	Processus	Procédure
Niveau	Stratégique	Organisationnel	Opérationnel
Focus	Pourquoi et dans quel esprit ?	Quoi faire ?	Comment faire ?
Auteur typique	DIRECTION GÉNÉRALE / RSSI	Responsable de service	Technicien, analyste, opérateur
Forme	Document d'engagement ou de principes	Cartographie de processus	Fiche ou guide étape par étape



## DIFFÉRENCE ENTRE POLITIQUE, PROCESSUS ET PROCÉDURE

**Exemple :** Une entreprise veut sécuriser ses accès aux systèmes d'information.

Élément	Contenu dans le contexte
Politique	"L'accès aux systèmes d'information doit être limité aux utilisateurs autorisés, selon les besoins métier."
Processus	Processus de gestion des accès : inclut les demandes d'accès, la validation, la mise en œuvre, la suppression des droits.
Procédure	Étapes précises à suivre pour créer un compte utilisateur dans l'Active Directory (ex : remplir le formulaire, validation RH, création du compte, envoi du mot de passe initial).



# **Exigences de la norme ISO/IEC 27001 relatives à la définition du domaine d'application du SMSI**

## **ISO/IEC 27001, article 4.3**

*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.*

*Lorsque l'organisation établit ce domaine d'application, elle 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 ;*
- c) les interfaces et les dépendances existant entre les activités réalisées par l'organisation et celles réalisées par d'autres organisations.*



# L'importance de déterminer le domaine d'application du SMSI

Un domaine d'application clairement défini est essentiel à la réussite de la mise en œuvre du SMSI. Il facilite les tâches suivantes :



Obtenir le soutien de la direction générale



Mobiliser les parties intéressées pour le projet



Justifier une valeur ajoutée aux parties intéressées

**Note :** La définition du domaine d'application est une activité clé de la mise en œuvre du SMSI qui sert de point de référence continu pour d'autres activités participant à ce processus.



## 1.2 Domaine d'application du SMSI

### Liste des activités

1.2.1

Définir les limites organisationnelles

1.2.2

Définir les limites du système d'information

1.2.3

Définir les limites physiques

1.2.4

Définir le domaine d'application du SMSI



# Limites du SMSI

Il y a trois dimensions à prendre en compte lors de la définition des limites du domaine d'application du SMSI :



**Limites organisationnelles**



**Limites du système d'information**



**Limites physiques**

## 1.2.1 Définir les limites organisationnelles

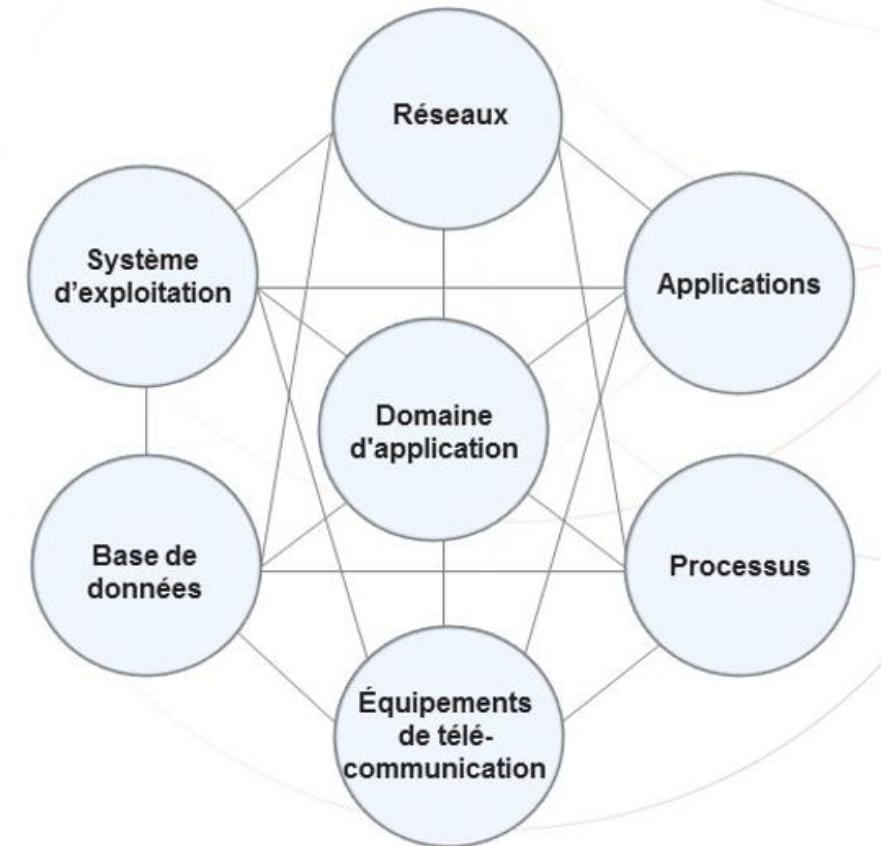
Les limites organisationnelles du domaine d'application peuvent inclure :



## 1.2.2 Définir les limites du système d'information

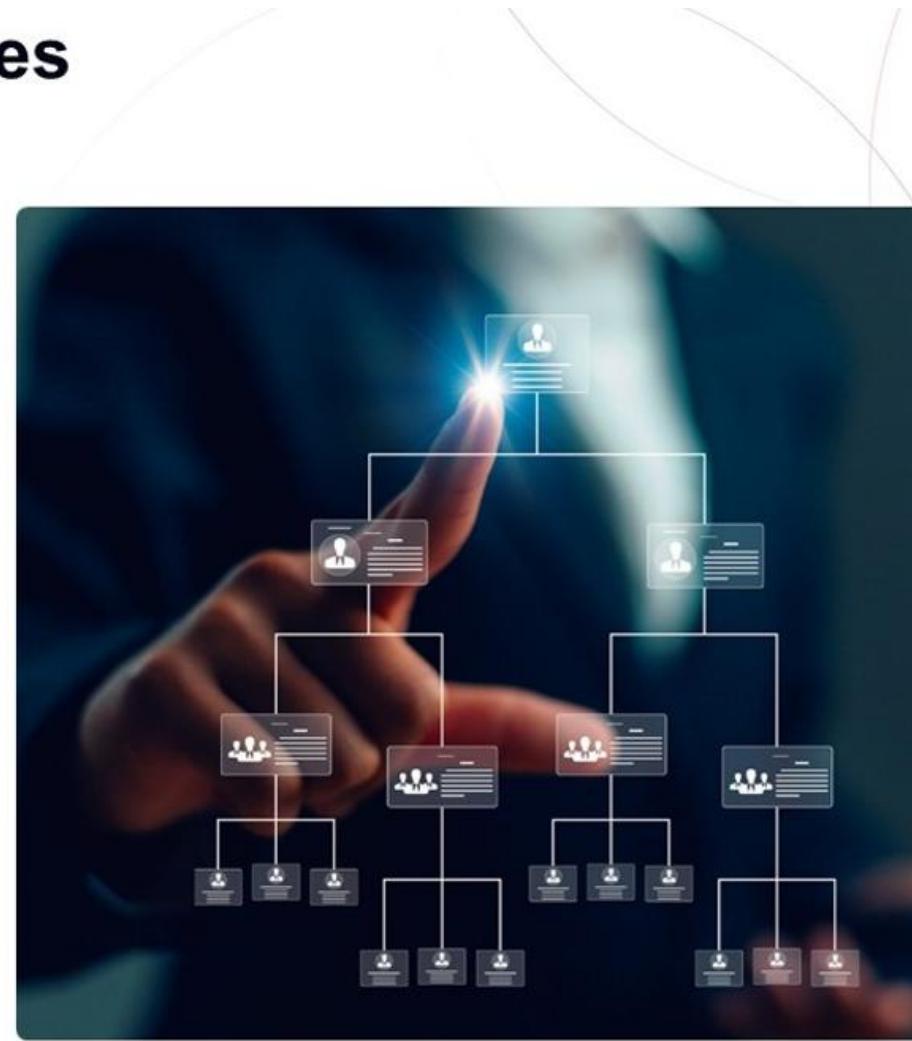
- Toutes les composantes du système devraient être prises en compte ; l'accent ne devrait pas être mis uniquement sur les composantes matérielles.
- Pour ce qui est des limites des systèmes d'information, l'ensemble des éléments des systèmes devrait être pris en considération, et non se limiter aux éléments matériels tels que les serveurs et l'équipement de télécommunication. Il faut également considérer les contraintes technologiques et les obligations contractuelles de l'organisation.

**Note :** En théorie, l'absence d'infrastructure technique n'empêche pas une organisation d'obtenir une certification ISO/IEC 27001.



### 1.2.3 Définir les limites physiques

- L'ensemble des emplacements physiques, autant internes qu'externes, inclus dans le SMSI, devraient être pris en considération.
- Les sites comprennent tous les emplacements situés dans le domaine d'application ou dans une partie du domaine d'application, ainsi que les moyens physiques nécessaires à leur fonctionnement.
- Dans le cas de sites loués, les interfaces avec le SMSI et les accords de service applicables doivent être pris en compte. Par exemple, si un centre de traitement des données est loué, l'organisation doit tenir compte de l'emplacement géographique où se trouve le centre, même s'il n'en est pas le propriétaire.



## 1.2.4 Définir le domaine d'application du SMSI

### ISO/IEC 27003, article 4.3

*Le domaine d'application d'un SMSI peut être très différent d'une mise en œuvre à une autre. Par exemple, le domaine d'application peut inclure :*

- a) un ou plusieurs processus spécifiques ;*
- b) une ou plusieurs fonctions spécifiques ;*
- c) un ou plusieurs services spécifiques ;*
- d) une ou plusieurs sections ou emplacements spécifiques ;*
- e) une entité juridique entière ; et*
- f) une entité administrative entière et un ou plusieurs de ses fournisseurs.*

*Il convient que l'organisation tienne également compte des activités ayant un impact sur le SMSI ou des activités externalisées, soit vers d'autres parties de l'organisation, soit vers des fournisseurs indépendants. Pour de telles activités, il convient que les interfaces (physique, technique, et organisationnelle) et leur influence sur le domaine d'application soient identifiées.*



# MISE EN PLACE DU SMSI

# Rôle de la direction générale dans le projet SMSI

## OBJECTIF

### Aligner le SMSI sur les objectifs et la stratégie de l'entreprise

1. Fixer les objectifs de sécurité de l'information et définir la stratégie pour le SMSI
2. Valider les rôles et responsabilités des principales parties intéressées par le projet
3. Passer en revue et approuver les politiques de sécurité du SMSI
4. Définir les critères d'acceptation du risque
5. Approuver le plan de traitement des risques et faciliter la mise en œuvre du SMSI
6. Allouer les ressources nécessaires à la mise en œuvre et à la mise à jour du SMSI

## Missions

Direction générale (PDG, DSI, DF, etc.)

## Fréquence des réunions

Tenir des réunions pour marquer les jalons du projet (p. ex., après avoir rédigé le rapport d'analyse du risque, le plan de traitement des risques, la déclaration d'applicabilité).

Déterminer les exigences du SMSI en termes de ressources

Planifier le projet SMSI

Constituer l'équipe de projet SMSI

Assurer l'approbation par la direction générale de la mise en œuvre du projet SMSI

# Analyse du système existant

Définir et établir		Mettre en œuvre et opérer		Surveiller et passer en revue		Maintenir et améliorer	
1.1	Compréhension de l'organisation et de son contexte	2.1	Sélection et conception des mesures	3.1	Surveillance, mesurage, analyse et évaluation	4.1	Traitement des non-conformités
1.2	Domaine d'application du SMSI	2.2	Mise en œuvre des mesures	3.2	Audit interne	4.2	Amélioration continue
1.3	Leadership et approbation du projet	2.3	Gestion des informations documentées	3.3	Revue de direction		
1.4	Structure organisationnelle	2.4	Communication				
1.5	Analyse du système existant	2.5	Compétence et sensibilisation				
1.6	Politique de sécurité de l'information	2.6	Gestion des opérations de sécurité				
1.7	Gestion des risques						
1.8	Déclaration d'applicabilité						

# Analyse des écarts

## Comprendre l'analyse des écarts

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



## Une analyse des écarts se déroule comme suit :

---

1

Déterminer l'état actuel :

L'organisation a mis en œuvre un processus de réponse aux incidents liés à la sécurité de l'information. Toutefois, il n'a pas documenté de processus de planification et de préparation pour la gestion des incidents et les rôles et responsabilités connexes.

---

2

Identifier l'état souhaité (cibles) :

La documentation de gestion des incidents doit inclure un processus documenté pour gérer efficacement les incidents de sécurité de l'information afin de se conformer aux exigences d'ISO/IEC 27001.

---

3

Effectuer l'analyse des écarts :

L'organisation doit élaborer, mettre en œuvre et communiquer un plan de gestion des incidents de sécurité de l'information qui explique clairement les processus de gestion des incidents ainsi que les rôles et responsabilités du personnel en cas d'incident de sécurité de l'information.

# Collecte d'information



## Observations

Observer les opérations, le système et le personnel de l'organisation afin de bien les comprendre



## Questionnaires

Envoyer des questionnaires à un groupe de personnes qui représentent les parties intéressées



## Entretiens

Mener des entretiens avec des personnes clés à différents niveaux hiérarchiques de l'organisation



## Revue de la documentation

Lire et analyser les informations documentées pertinentes (par exemple, les politiques internes, les procédures, les rapports d'audit précédents, les contrats)



## Outils d'analyse

Utiliser des outils technologiques pour détecter les vulnérabilités techniques, établir une liste d'actifs susceptibles d'avoir un impact sur un réseau, effectuer une revue de code, etc.

## Analyse des écarts et niveaux de maturité

Les objectifs en matière de processus et de mesures de sécurité de l'information peuvent être fixés en fonction des niveaux de maturité visés :

Il y a une absence totale de processus identifiables.

0

Inexistants

Les processus sont mis en œuvre au cas par cas sans aucune méthode.

1

À l'état initial

Des processus non standards sont en place.

2

Gérés

Les processus sont documentés et communiqués.

3

Définis

Les processus sont surveillés et mesurés.

4

Gérés quantitativement

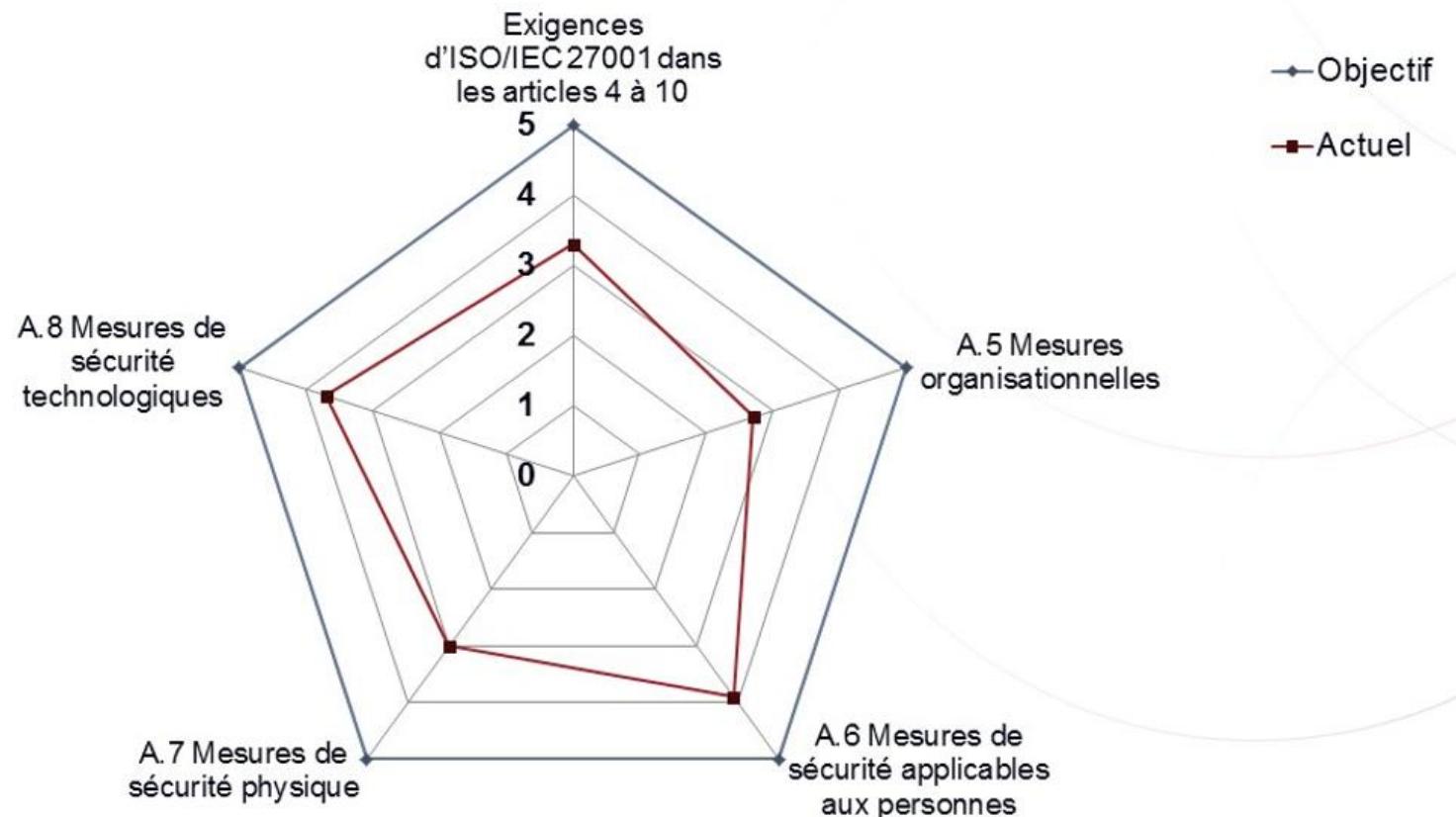
Les processus sont optimisés.

5

Optimisés

# Rapport d'analyse des écarts

## Exemple de représentation graphique



# Gestion des risques

Définir et établir		Mettre en œuvre et opérer		Surveiller et passer en revue		Maintenir et améliorer	
1.1	Compréhension de l'organisation et de son contexte	2.1	Sélection et conception des mesures	3.1	Surveillance, mesurage, analyse et évaluation	4.1	Traitement des non-conformités
1.2	Domaine d'application du SMSI	2.2	Mise en œuvre des mesures	3.2	Audit interne	4.2	Amélioration continue
1.3	Leadership et approbation du projet	2.3	Gestion des informations documentées	3.3	Revue de direction		
1.4	Structure organisationnelle	2.4	Communication				
1.5	Analyse du système existant	2.5	Compétence et sensibilisation				
1.6	Politique de sécurité de l'information	2.6	Gestion des opérations de sécurité				
1.7	Gestion des risques						
1.8	Déclaration d'applicabilité						



## ISO 31000

La norme ISO 31000 fournit des lignes directrices pour la gestion des risques auxquels sont confrontées les organisations de tout type d'industrie ou de secteur.

Elle s'applique à tout type de risque, indépendamment de sa nature ou de ses conséquences.

Cette norme ne se prête pas à des fins de certification.

## ISO/IEC 27005

La norme ISO/IEC 27005 fournit des lignes directrices pour la gestion des risques liés à la sécurité de l'information et prend en charge les concepts spécifiés dans la norme ISO/IEC 27001.

Elle s'applique à toute organisation qui entend gérer des risques susceptibles de compromettre sa sécurité de l'information.

Les organisations ne peuvent pas obtenir de certification selon cette norme.



```
graph LR; A((ISO/IEC 27001, articles 6.1.1, 6.1.2, 6.1.3 et 8.2 à 8.3)) --> B[ISO/IEC 27005  
Cadre générique de gestion des risques appliqué à la sécurité de l'information]; A --> C[ISO 31000  
Cadre générique de gestion des risques]
```

**ISO/IEC 27001,  
articles 6.1.1,  
6.1.2, 6.1.3 et 8.2  
à 8.3**

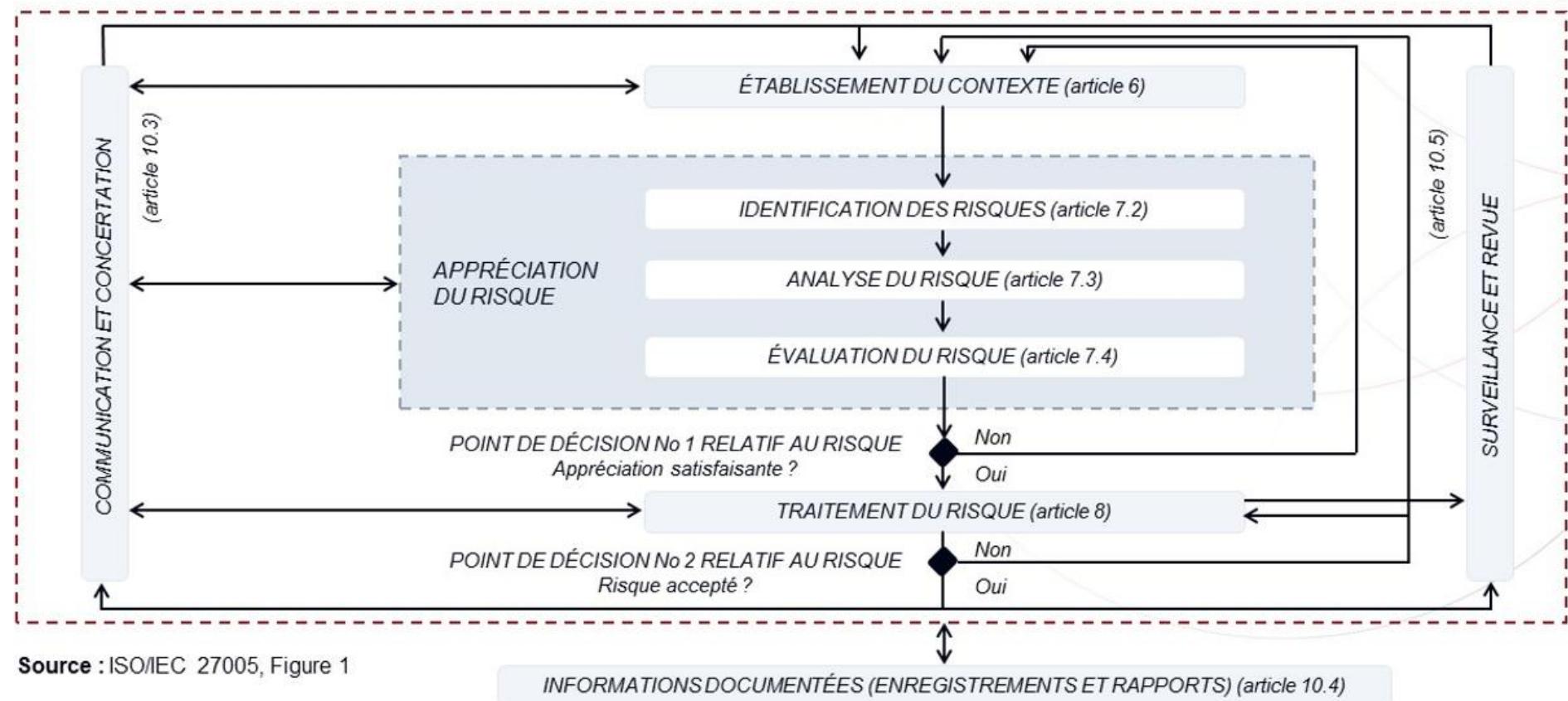
**ISO/IEC 27005**

Cadre générique de gestion des risques appliqué à la sécurité de l'information

**ISO 31000**

Cadre générique de gestion des risques

# Processus de gestion des risques liés à la sécurité de l'information





## Liste des activités

1.7.1

1.7.2

1.7.3

1.7.4

1.7.5

Établissement du contexte

Identification du risque

Analyse du risque

Évaluation du risque

Traitement des risques

1.7.6

1.7.7

1.7.8

Communication et concertation

Enregistrement et élaboration de rapports

Surveillance et revue des risques

# Techniques d'analyse du risque

## ISO/IEC 27005, article 7.3.1

*Les techniques d'analyse du risque basées sur les conséquences et la vraisemblance peuvent être les suivantes:*

a)

*qualitative, en utilisant une échelle d'attributs qualificatifs (par exemple, élevé, moyen, faible); ou*

b)

*quantitative, en utilisant une échelle avec des valeurs numériques (par exemple, le coût monétaire, la fréquence ou la probabilité d'occurrence); ou*

c)

*semi-quantitative, utilisant des échelles qualitatives avec des valeurs attribuées.*

# Appréciation des conséquences potentielles

## ISO/IEC 27005, article 7.3.2

*L'incapacité à préserver de manière adéquate la sécurité des informations peut entraîner la perte de leur confidentialité, de leur intégrité ou de leur disponibilité. La perte de confidentialité, d'intégrité ou de disponibilité peut avoir d'autres conséquences sur l'organisme et ses objectifs. L'analyse de ces autres conséquences peut être effectuée de manière ascendante à partir des conséquences de l'incapacité à préserver la sécurité de l'information. En général, le propriétaire du risque peut réaliser l'estimation des conséquences si l'événement se produit. Il convient de tenir compte des éléments suivants:*

- *l'estimation (ou la mesure basée sur l'expérience) des pertes (de temps ou de données) dues à l'événement suite à l'interruption ou à la perturbation des opérations;*
- *l'estimation/perception de la gravité des conséquences (par exemple, exprimée en termes financiers);*
- *les coûts de récupération, suivant la possibilité d'effectuer ou non la récupération en interne (par l'équipe du propriétaire du risque) ou s'il est nécessaire de faire appel à une entité externe.*



## Sélection des options de traitement des risques

Les options de traitement du risque peuvent impliquer un ou plusieurs des éléments suivants:

- **Modification du risque** – Introduction, retrait ou modification de moyens de maîtrise pour que le risque résiduel puisse être considéré comme acceptable
- **Prise de risque** – Décision d'accepter le niveau de risque actuel
- **Refus du risque** – Annulation ou modification d'une ou plusieurs activités liées aux risques
- **Partage du risque** – Décision de partager les risques avec des tiers (p. ex. assurance ou sous-traitance)

# Formulation et approbation du plan de traitement des risques

ISO/IEC 27005, article 8.6.1

*Un plan de traitement du risque est un plan qui vise à modifier le risque de manière à ce qu'il réponde aux critères d'acceptation du risque de l'organisme.*

- *Une fois que l'organisme a choisi l'option pertinente de traitement des risques, il doit la planifier et la mettre en œuvre en conséquence.*
- *Il convient de classer par ordre de priorité les activités à entreprendre pour mettre en œuvre l'option de traitement des risques.*
- *Il convient que l'organisme alloue les ressources nécessaires à la mise en œuvre efficace de l'option de traitement des risques choisie.*
- *Il convient que le plan de traitement des risques soit approuvé par les propriétaires du risque.*



# Plan de traitement des risques

## Exemple

<b>Scénario de risque</b>	Les utilisateurs non autorisés peuvent se connecter via l'extranet à Microsoft SharePoint et rechercher des fichiers sensibles de l'organisation avec l'ID demandé.
<b>Niveau de risque</b>	Six
<b>Priorité</b>	Élevé
<b>Option de traitement</b>	Refus
<b>Moyen de maîtrise</b>	Rendre SharePoint inaccessible
<b>Ressources requises</b>	10 heures pour reconfigurer et tester le système
<b>Responsable</b>	David Smith, administrateur Microsoft SharePoint ; John McGee, administrateur du pare-feu
<b>Date de début/date de fin :</b>	Du 20 février 2022 au 20 février 2022
<b>Maintenance nécessaire/commentaires</b>	Effectuer des revues périodiques de la sécurité du système pour garantir qu'une sécurité adéquate est assurée pour Microsoft SharePoint

# Déclaration d'applicabilité

- Une déclaration d'applicabilité (DdA) est un énoncé documenté énumérant les mesures pertinentes et applicables au SMSI de l'organisation.
- La DdA contient non seulement les justifications de l'organisation d'inclure certaines mesures de l'Annexe A, mais également les justifications d'exclure d'autres mesures de l'Annexe A.
- La déclaration d'applicabilité est plus qu'une liste de contrôle des mesures de sécurité de l'Annexe A d'ISO/IEC 27001 à mettre en œuvre dans le système de management de la sécurité de l'information de l'organisation. C'est un document clé du SMSI qui sert de référence pour l'auditeur externe durant l'audit de certification ; ainsi, c'est l'une des premières informations documentées qui fera l'objet d'une analyse. C'est également l'une des informations documentées que la direction générale de l'organisation doit valider et approuver avant de lancer les opérations du SMSI.



Revue et sélection  
des mesures de  
sécurité de  
l'information  
applicables

Justifier les mesures  
sélectionnées

Justifier les mesures  
exclues

Finaliser la  
déclaration  
d'applicabilité

Obtenir l'approbation  
de la direction  
générale





L'organisation doit justifier l'exclusion de chaque mesure de sécurité présentée dans l'Annexe A de la norme ISO/IEC 27001.

### Les raisons d'exclusions les plus souvent invoquées sont les suivantes :



Cela conduirait à la violation d'une prescription légale, réglementaire ou contractuelle, par exemple ISO/IEC 27001, Annexe A.6.1 examen préalable.



Aucune activité liée à cette mesure n'est présente dans l'organisation, par exemple, ISO/IEC 27001, Annexe A.6.7 télétravail.

## 1.8.4 Finaliser la déclaration d'applicabilité

### Exemple

Mesure de sécurité	Applicable	Description	Justification	Documentation	Responsable
ISO/IEC 27001, <i>Annexe A.5.1 Politiques de sécurité de l'information</i>	Oui	<p>La politique de sécurité de l'information, approuvée par la direction générale, est en vigueur depuis le mercredi 21 décembre 2022.</p> <p>Une copie a été transmise à tous les employés et parties prenantes concernées. La version officielle est disponible sur l'intranet</p>	La politique sera mise en œuvre afin de fournir des recommandations sur la sécurité de l'information et de s'assurer que les pratiques de sécurité de l'information sont conformes aux exigences commerciales, aux lois et aux réglementations.	Politique de sécurité-3213PO	Responsable de la sécurité de l'information
ISO/IEC 27001 Annexe A.6.7 Travail à distance	Non	-----	Notre organisation n'a aucune activité liée au travail à distance.	N/A	Responsable des TI



## 1.8.5 Obtenir l'approbation de la direction générale



- Une collaboration étendue, du temps, des efforts et un engagement fort de la part de la direction générale sont essentiels à la planification des DdA au niveau de l'entreprise.
- La DdA obtenue devrait être un tableau de mesures concis, soumis à l'examen et à l'approbation de la direction générale ou de l'autorité compétente.

# Sélection et conception des mesures

## Planification et contrôle opérationnels

- L'organisation doit planifier, mettre en œuvre, contrôler et améliorer en permanence les processus nécessaires pour répondre aux exigences de sécurité de l'information.
- Il convient que l'organisation choisisse et mette en œuvre des mesures de sécurité de l'information en fonction des résultats de l'appréciation des risques.
- Il convient que les informations documentées soient régulièrement maintenues afin de s'assurer que les processus ont été effectués comme prévu.
- Il convient de contrôler les changements planifiés et non planifiés afin d'atténuer leurs conséquences et leurs effets négatifs.
- Il convient que l'organisation s'assure également que les processus externalisés sont correctement identifiés et contrôlés.



Analyser l'architecture de sécurité de l'organisation

Concevoir et décrire les mesures

Préparer la mise en œuvre des mesures



# Mise en œuvre des mesures

- L'Annexe A de la norme ISO/IEC 27001 contient une liste des mesures de sécurité de l'information possibles. Les mesures de sécurité de l'Annexe A sont dérivées de celles d'ISO/IEC 27002.
- L'Annexe A comprend 93 mesures de sécurité de l'information regroupées en quatre catégories.

5

**Mesures de sécurité organisationnelles**

5.1-5.37



6

**Mesures de sécurité applicables aux personnes**

6.1-6.8



7

**Mesures de sécurité physique**

7.1-7.14



8

**Mesures de sécurité technologiques**

8.1-8.34



# Audit interne

Définir et établir		Mettre en œuvre et opérer		Surveiller et passer en revue		Maintenir et améliorer	
1.1	Compréhension de l'organisation et de son contexte	2.1	Sélection et conception des mesures	3.1	Surveillance, mesurage, analyse et évaluation	4.1	Traitement des non-conformités
1.2	Domaine d'application du SMSI	2.2	Mise en œuvre des mesures	3.2	Audit interne	4.2	Amélioration continue
1.3	Leadership et approbation du projet	2.3	Gestion des informations documentées	3.3	Revue de direction		
1.4	Structure organisationnelle	2.4	Communication				
1.5	Analyse du système existant	2.5	Compétence et sensibilisation				
1.6	Politique de sécurité de l'information	2.6	Gestion des opérations de sécurité				
1.7	Gestion des risques						
1.8	Déclaration d'applicabilité						

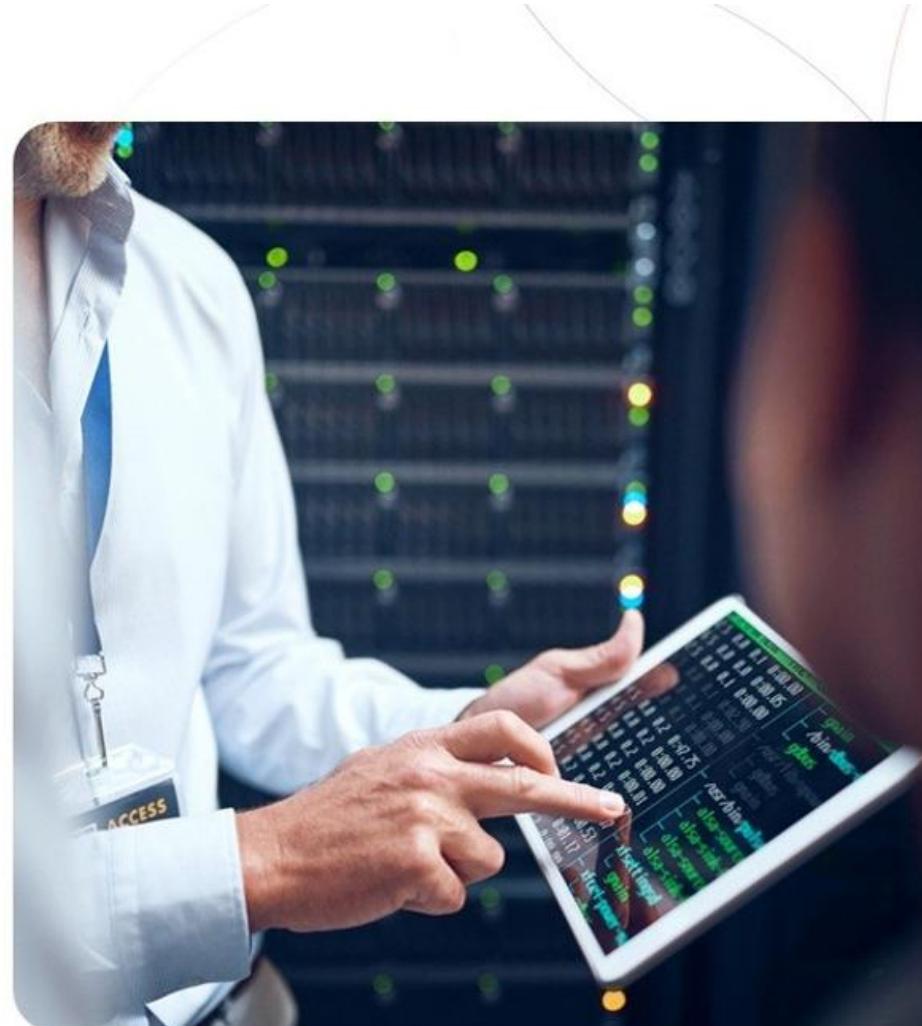
# Qu'est-ce qu'un audit ?

ISO 19011, article 3.1

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

---

Autrement dit, l'audit consiste à demander à l'audité ce qu'il fait et comment il le fait, afin de vérifier si ses pratiques sont conformes aux politiques, procédures et processus organisationnels ainsi qu'aux exigences des normes nationales et internationales.



# Différences entre audits internes et externes

## Principales caractéristiques

Audit interne	Audit externe
1. Indépendant des activités auditées (et non de l'organisation)	1. Indépendant de l'organisation auditee et de ses activités
2. Tient compte de l'efficacité et de l'efficiency du SMSI	2. Tient compte uniquement de l'efficacité du SMSI
3. Rôle de conseil au sein de l'organisation pour l'amélioration du SMSI	3. Aucun rôle de conseil auprès de l'organisation
4. Peut être effectué en continu	4. Toujours mené de manière planifiée et en temps opportun

# Principaux services et activités de l'audit interne

Coordination avec les audits externes

Évaluation du processus d'amélioration continue

Évaluation de la revue du mesurage du SMSI

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

Évaluation des objectifs de sécurité de l'information

Évaluation de la gouvernance du SMSI

Évaluation du processus de gestion des risques

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



# Principaux services et activités de l'audit interne (suite)

Coordination avec les audits externes

Évaluation du processus d'amélioration continue

Évaluation de la revue du mesurage du SMSI

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



# Amélioration continue

		Définir et établir	Mettre en œuvre et opérer	Surveiller et passer en revue	Maintenir et améliorer
1.1	1.1	Compréhension de l'organisation et de son contexte	2.1 Sélection et conception des mesures	3.1 Surveillance, mesurage, analyse et évaluation	4.1 Traitement des non-conformités
1.2	1.2	Domaine d'application du SMSI	2.2 Mise en œuvre des mesures	3.2 Audit interne	4.2 Amélioration continue
1.3	1.3	Leadership et approbation du projet	2.3 Gestion des informations documentées	3.3 Revue de direction	
1.4	1.4	Structure organisationnelle	2.4 Communication		
1.5	1.5	Analyse du système existant	2.5 Compétence et sensibilisation		
1.6	1.6	Politique de sécurité de l'information	2.6 Gestion des opérations de sécurité		
1.7	1.7	Gestion des risques			
1.8	1.8	Déclaration d'applicabilité			

# Exigences de la norme ISO/IEC 27001 relatives à l'amélioration continue

## ISO/IEC 27001, article 10.1



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

- L'amélioration continue est le processus qui consiste à accroître l'efficacité et l'efficiency de l'organisation afin de réaliser sa politique et ses objectifs.
- L'amélioration continue est obtenue en fixant des objectifs de performance organisationnelle, en mesurant et révisant, et en apportant les modifications nécessaires aux processus, systèmes, ressources, etc.



Le SMSI doit être maintenu et mis à jour régulièrement.



Le gestionnaire de la sécurité de l'information devrait être informé des actions convenues pour améliorer les processus afin qu'aucun risque ou élément de risque ne soit négligé ou sous-estimé avant la mise en œuvre des modifications.

# Organismes d'accréditation

- Un organisme d'accréditation est un organisme indépendant qui fait autorité et qui vérifie si un organisme d'évaluation de la conformité répond aux critères établis et s'il est compétent pour effectuer des tâches d'évaluation de la conformité.
- Les activités couvertes par l'accréditation comprennent, entre autres, les essais, l'étalonnage, l'inspection, la certification des systèmes de management, des personnes, des produits, des processus et des services, ainsi que la validation et la vérification.
- Les organismes d'accréditation tirent généralement leur autorité des gouvernements.



INTERNATIONAL  
ACCREDITATION  
SERVICE®



This image cannot  
currently be  
displayed.



Deutsche  
Akkreditierungsstelle



Note : Une liste des  
organismes d'accréditation  
de plusieurs pays est fournie  
dans l'Annexe C du fichier  
des Annexes.



# Organismes de certification



Les organismes de certification certifient des systèmes de management, des personnes, des produits, des processus et des services.

---

Les organismes de certification sont toujours des organismes d'évaluation de la conformité tiers et impartiaux.

---

Un organisme de certification peut être un organisme gouvernemental ou non gouvernemental, avec ou sans autorité réglementaire.



Bien que le terme « organisme de certification » puisse être utilisé pour désigner des organismes qui assurent la certification de personnes (ISO/IEC 17024) et de produits, processus et services (ISO/IEC 17065), dans cette formation, il est utilisé uniquement pour désigner des organismes qui certifient des systèmes de management (comme spécifié dans ISO/IEC 17021-1).



# Processus de certification



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



# Sélection de l'organisme de certification

Les éléments ci-après sont une liste des principaux critères de sélection d'un organisme de certification :

- 1 Notoriété et crédibilité
- 2 Localisation géographique
- 3 Références dans votre secteur
- 4 Possibilité d'un audit combiné
- 5 Compétences et expérience de l'équipe d'audit
- 6 Prix

# Rejet d'un auditeur par le client de l'audit ou l'audité

## ISO/IEC 17021-1, article 9.2.3.5

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



Exemples de raisons valables pour lesquelles l'audité peut rejeter un auditeur :

- Auditeur en situation de conflit d'intérêts (réel ou potentiel).
- Auditeur ayant déjà fait preuve d'un comportement non professionnel.
- Auditeur qui n'a pas l'habilitation de sécurité requise par l'audité.
- Auditeur ayant déjà audité l'organisation dans le passé et client de l'audit n'étant donc pas convaincu que l'audit lui apporte une valeur ajoutée

# Préparation à l'audit de certification

## Recommandations

1 Comprendre la norme



2 Identifier les experts métier



3 Allouer suffisamment de ressources



4 Effectuer une auto-évaluation



5 Préparer le personnel



6 Préparer les informations documentées



# Étape 1 de l'audit



## Visite du site

- Évaluer l'emplacement de l'audité et les conditions propres au site
- Rencontrer le personnel de l'audité
- Observer les technologies utilisées
- Observer les opérations du SMSI



## Entretiens avec les principales parties intéressées

- Valider le domaine d'application du SMSI ainsi que les contraintes légales, réglementaires et contractuelles applicables
- Vérifier si les procédures et les politiques sont respectées
- Préparer l'étape 2 de l'audit



## Revue des informations documentées

- Comprendre le fonctionnement du SMSI
- Évaluer la conception du SMSI ainsi que ses processus ou mesures connexes
- Vérifier la réalisation des audits internes et des revues de direction

Note : La revue des informations documentées est l'activité principale de l'audit de phase 1 ?

## Étape 2 de l'audit



L'étape 2 de l'audit vise à évaluer le système de management de la sécurité de l'information afin de vérifier s'il :

1 Est conforme aux exigences d'ISO/IEC 27001

2 Est mis en œuvre de manière efficace

3 Permet à l'organisation d'atteindre ses objectifs en matière de sécurité de l'information

# Utilisation des marques déposées de l'ISO

- Un audité certifié est autorisé à afficher publiquement sa certification et à s'en servir à des fins de marketing.
- La certification ne peut pas être affichée directement sur un produit ou d'une façon qui laisserait à penser que le produit est certifié.
- L'organisme de certification fournit à l'audité un logo pouvant être utilisé à des fins de marketing.
- L'utilisation non autorisée des marques ISO pourrait induire en erreur, créer de fausses impressions ou prêter à confusion. Par conséquent, les marques ISO ne doivent pas être utilisées dans l'intention d'exprimer la certification d'un produit, d'une personne ou d'une organisation, car l'ISO n'effectue pas de certifications.



# **CONCLUSION**

MERCI POUR VOTRE  
**ATTENTION**