

## **Management de la sécurité de l'information**

### **S**ystème de **m**anagement de la **s**écurité de l'**i**nformation **Mise de place d'un SMSI**

## **ISO 27001 / ISO 27002**

---

PRÉPARÉ PAR : AMAL HADRI  
E-MAIL: A.HADRI@EMSI.MA

# Plan

2

- I. Enjeux de la sécurité SI:
- II. Systèmes de management (SM) :
  - 1. Définitions ;
  - 2. Principaux SM :
  - 3. Propriétés et apports des SM :
  - 4. Démarche qualité : le modèle PDCA
- I. Norme ISO 27001 :
  - a. Objectifs :
  - b. Structure de la norme :
- 1. Construction d'un système de management de la sécurité des systèmes d'information (SMSI) :
- 2. Apports de la famille ISO2700x et la mise en place d'un SMSI :
- 3. Etapes de mise en place d'un SMSI :
  - a. Planification « PLAN » :
  - b. Déploiement « DO » :
  - c. Vérification « CHECK » :
  - d. Ajustement « ACT » :
- 4. Processus de certification ISO 27001 pour les organismes :
- 5. Processus de certification ISO 27001 pour les individus :
- 6. Rappel de la sécurité périmétrique

# Constat

3

- ❑ **Systèmes informatiques: complexes, interconnectés, reliés à internet**
- ❑ **La sécurité** est devenue un **enjeu majeur** : **RSSI**
- ❑ **Sécurité informatique ou sécurité de l'information?**
- ❑ **Sécurité informatique**: pare feu, ACL, sécurité Unix,..... déjà existante
- ❑ **Le chaînon manquant**: véritable **chef d'orchestre**
- ❑ **Les références normatives d'un SMSI**: **ISO 27001** et **ISO 27002**

# Système de Management : SM

4

- ☐ Un **SMSI** c'est d'abord un **SM**
- ☐ La notion du **SM** est historiquement reliée à la **qualité**

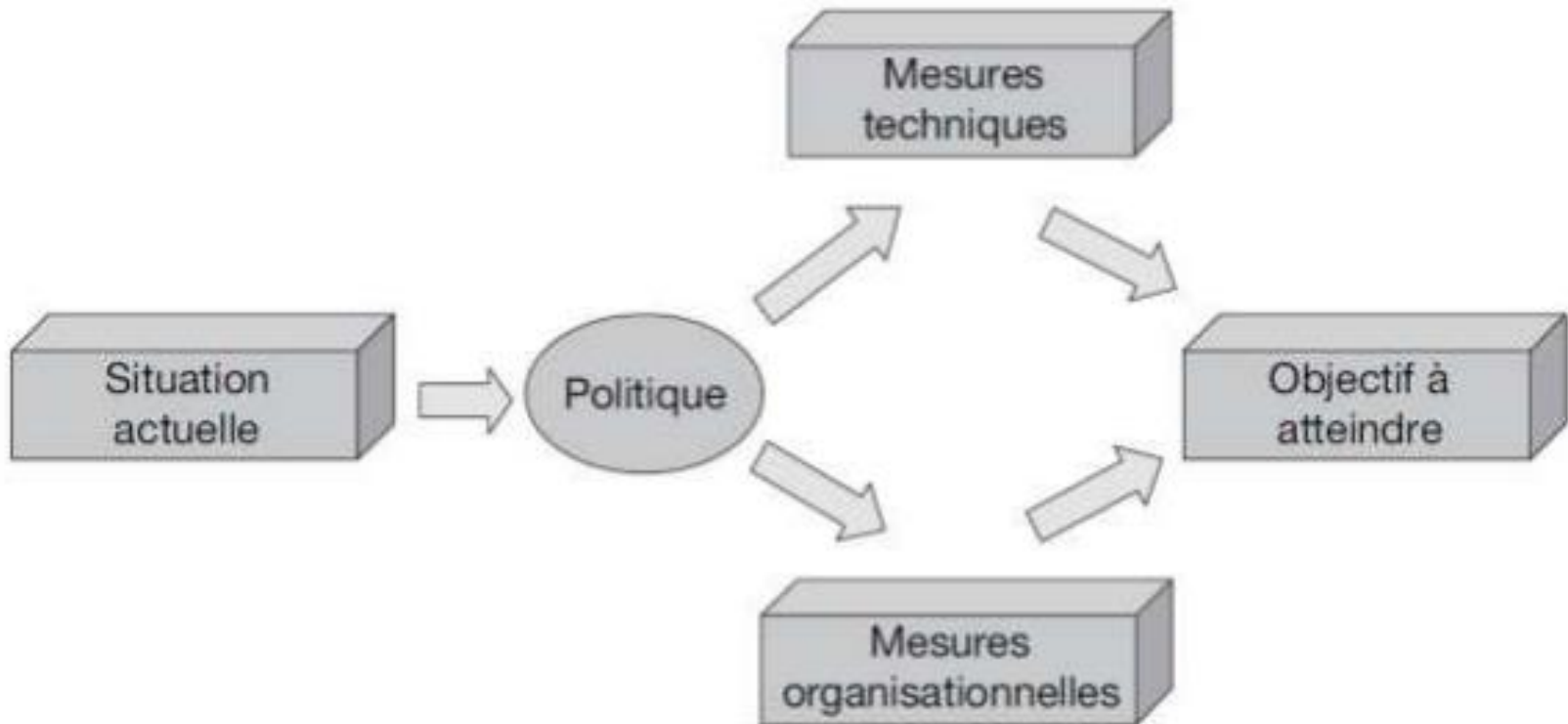
La norme **ISO 9000** stipule: Un **SM** est un système permettant de:

- ☐ Etablir une politique;
- ☐ Etablir des objectifs;
- ☐ Atteindre ces objectifs;

# Système de Management : SM

5

Système de management est un ensemble **de mesures organisationnelles et techniques** visant à atteindre un objectif.



Vision empirique d'un système de management

# Principaux SM

6

- Les **SM** sont historiquement liés à **la qualité** mais ne se limite pas à celle-ci.
- Des référentiels existent pour chaque SM.

Référentiel	Domaine
ISO 9001	Qualité : <b>SMQ</b>
ISO 14001	Environnement : <b>SME</b>
ISO 27001	Sécurité de l'information : <b>SMSI</b>
ISO 20000	Services informatiques : <b>SMS</b>
ISO 22000	Sécurité alimentaire
OHSAS18001	Santé-sécurité du personnel au travail

# Les apports des SM

7

**Certifier son organisme dans un domaine donne confiance aux **parties prenantes** (**Stakeholders, interested parties**):**

- Actionnaires;
- Autorités;
- Clients;
- Utilisateurs;
- Partenaires;
- Fournisseurs;
- Personnel;

➔ Les **SM** existent grâce à **des parties prenantes** et pour **les parties prenantes**

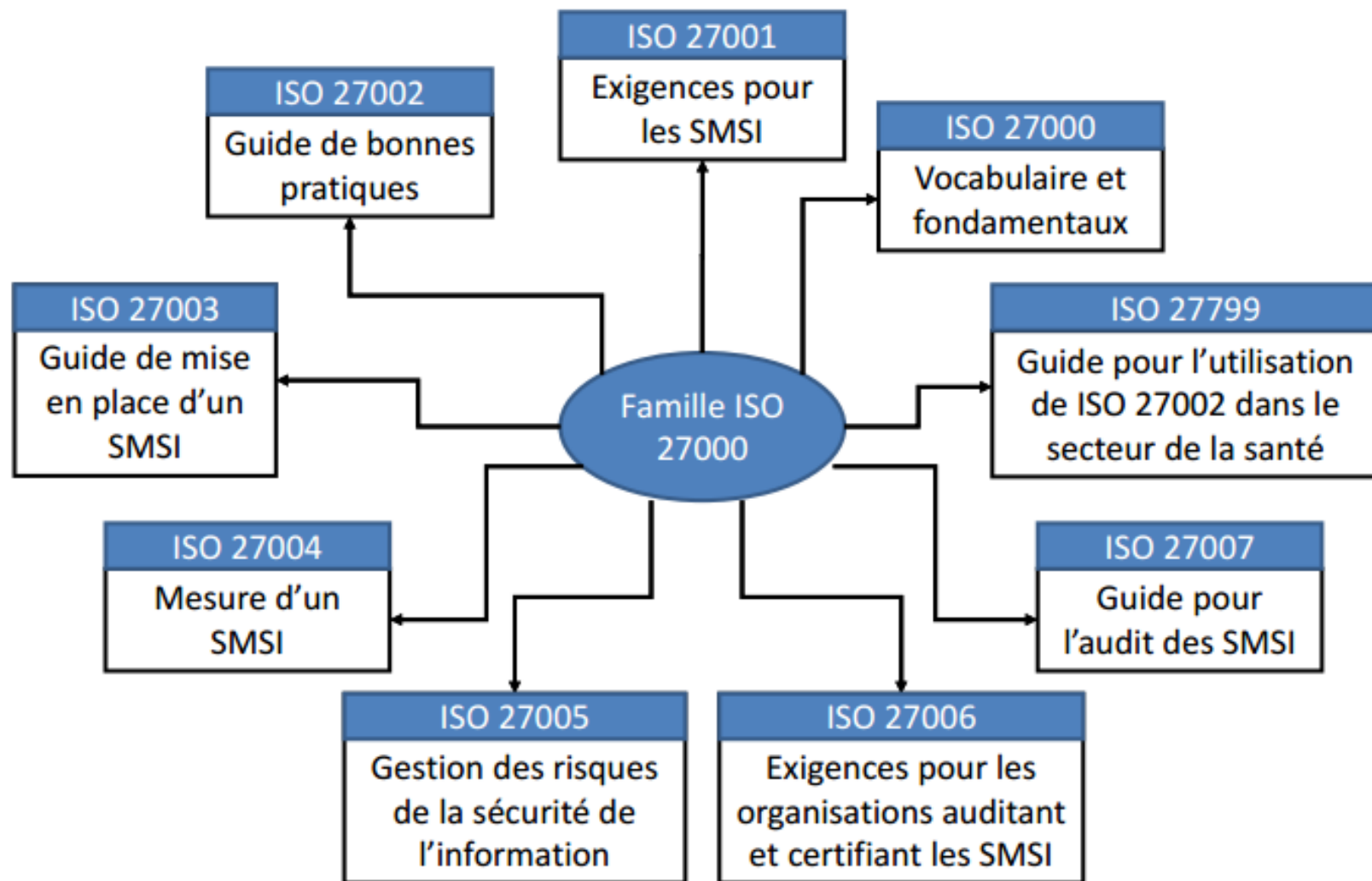
SMSI= SM(système de management) + SI( sécurité de l'information)

- Partie du système de gestion global, basée sur une approche du **risque** lié à l'activité, visant à établir, mettre en œuvre, exploiter, surveiller, réexaminer, tenir à jour et améliorer la sécurité de l'information (clause 3.7)
- Le principal objectif d'un SMSI est de faire en sorte de préserver la **confidentialité**, **l'intégrité** et **disponibilité** pour les informations les plus sensibles de l'entreprise. La norme ISO 27001 insiste sur ces notions.



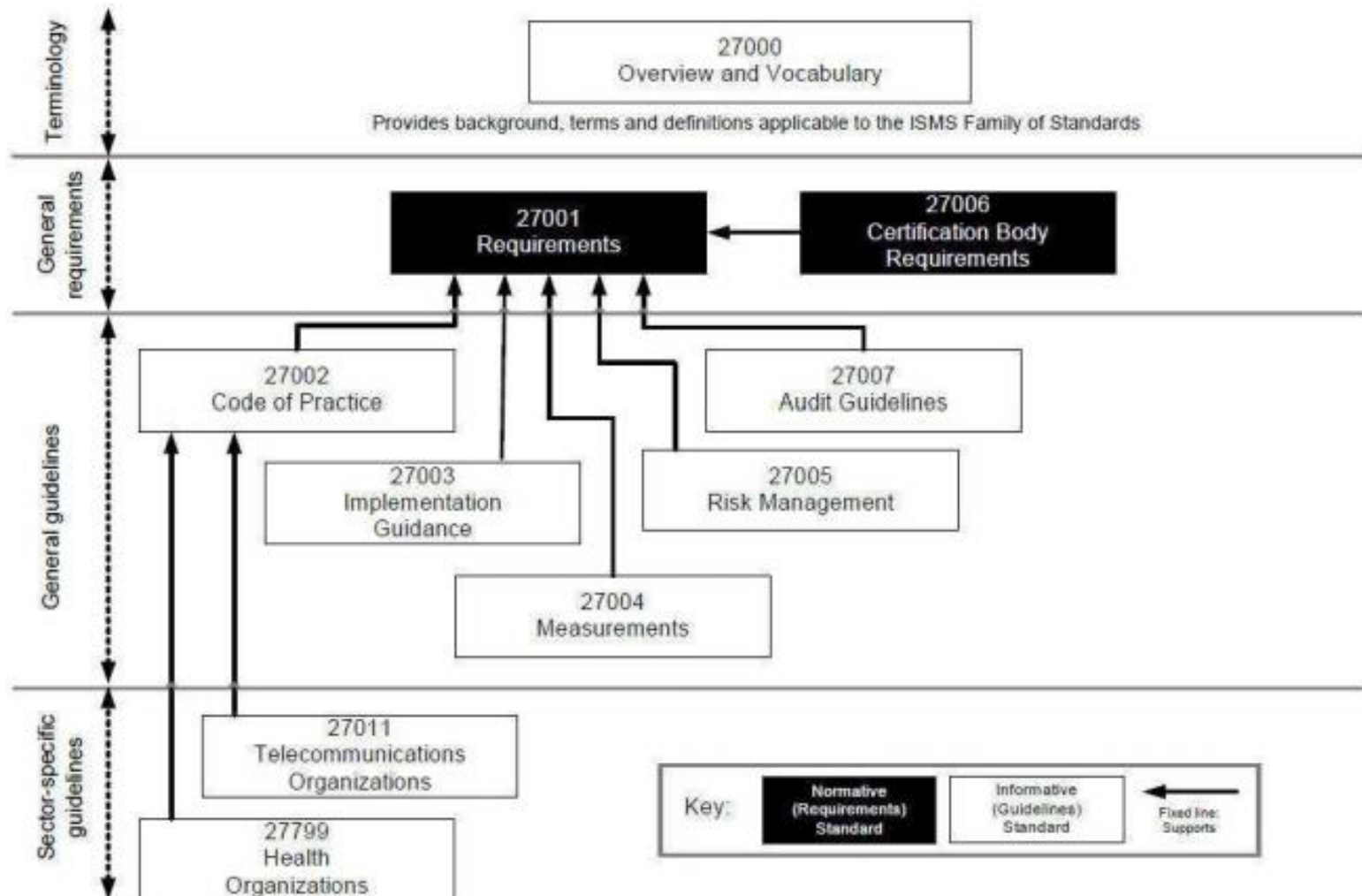
# SMSI: Les norms de la famille 2700X

9



# Références Normatives pour la mise en place d'un SMS

10



# ISO 27001

11

- Appréhender la sécurité de l'information sous l'angle du management permet de dépasser le stade purement technique de la SSI.



# La norme ISO 27001

12

## **ISO 27001: gestion de la sécurité de l'information Spécification pour les SMSI:**

- Spécifie les exigences pour la conception, la mise en place et la documentation des SMSI (<> directive)
- Spécifie les exigences pour la mise en œuvre de contrôles conformément aux besoins des organisations
- L'annexe A se compose de 11 sections comportant 133 contrôles de ISO 27002
- Les organismes peuvent postuler à la certification à cette norme
- Voir clause 0.1

# La norme ISO 27001, Annexe A

13

- ❑ Chapitre 5 : Politique de sécurité.
- ❑ Chapitre 6 : Organisation de la sécurité de l'information
- ❑ Chapitre 7 : Gestion des biens.
- ❑ Chapitre 8 : Sécurité liée aux ressources humaines
- ❑ Chapitre 9 : Sécurité physique et environnementale.
- ❑ Chapitre 10 : Gestion des communications et de l'exploitation.
- ❑ Chapitre 11 : Contrôles d'accès
- ❑ Chapitre 12 : Acquisition, développement et maintenance des systèmes d'information.
- ❑ Chapitre 13 : Gestion des incidents liés à la sécurité de l'information.
- ❑ Chapitre 14 : Gestion de la continuité d'activité.
- ❑ Chapitre 15 : Conformité légale et réglementaire.

# La norme ISO 27001

14

- Chacune des 11 sections
  - ▣ spécifie les objectifs à atteindre
  - ▣ énumère un ensemble de **133 mesures ou « best practices »** pour atteindre ces objectifs
  
- La norme ISO ne détaille pas ces mesures car:
  - ▣ chaque organisation est différente
  - ▣ les risques sont différents pour chaque organisation
  - ▣ **l'évaluation des risques et de leur impact est donc propre à l'organisation**
  - ▣ les « best practices » sont donc plus ou moins appropriées

# Clauses obligatoires de l'ISO 27001

15

## ☐ Clause 4 : SMSI

- Clause 4.2.1 : Mise en place
- Clause 4.2.2 : Implantation et opération
- Clause 4.2.3 : Contrôle et revue
- Clause 4.2.4 : Maintien et améliorations

## ☐ Clause 5 : Responsabilités de la direction

## ☐ Clause 6 : Audit interne

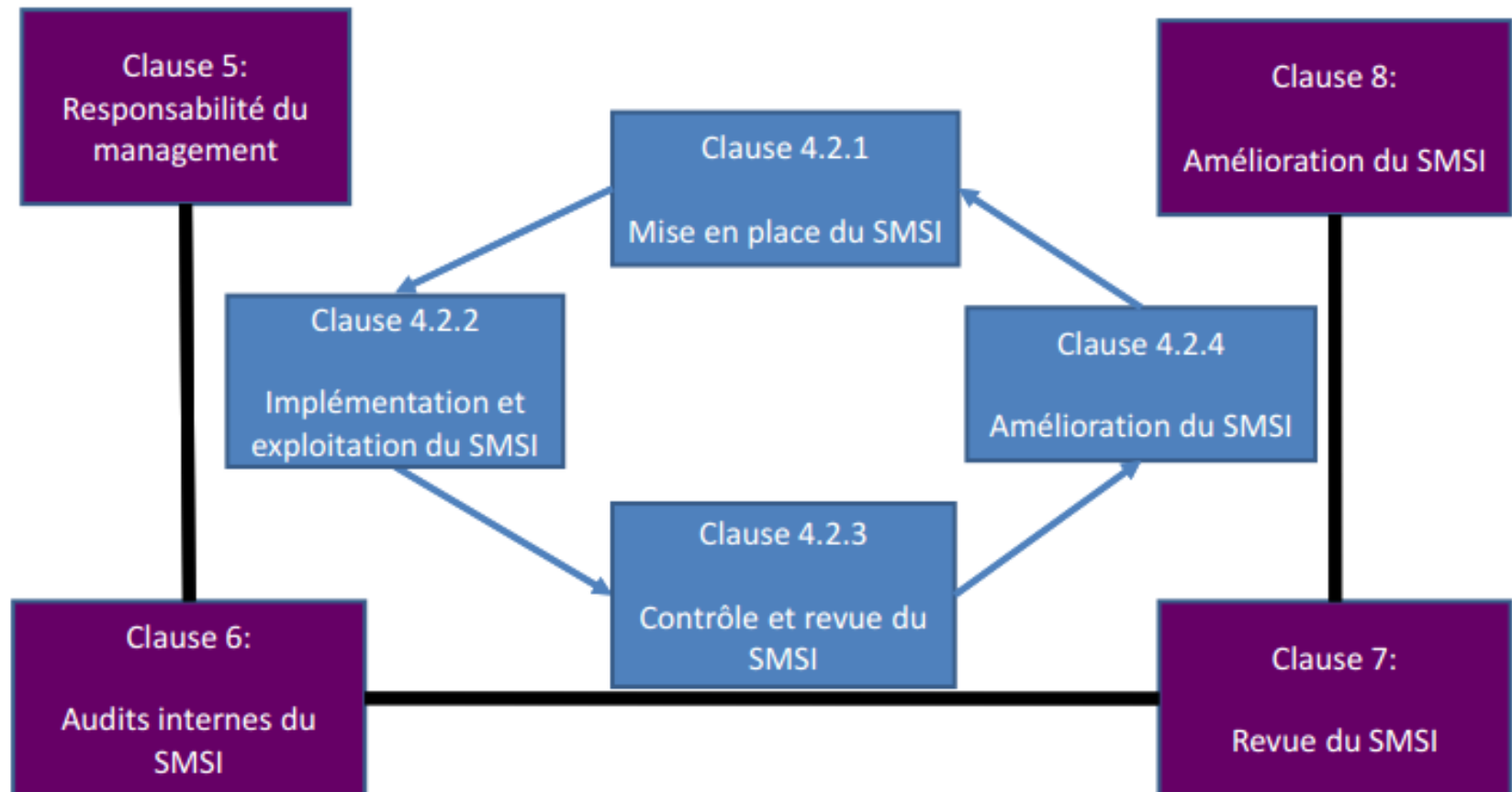
## ☐ Clause 7 : Revue de direction du SMSI

## ☐ Clause 8 : Amélioration continue

# ISO 27001: Structure de la norme

16

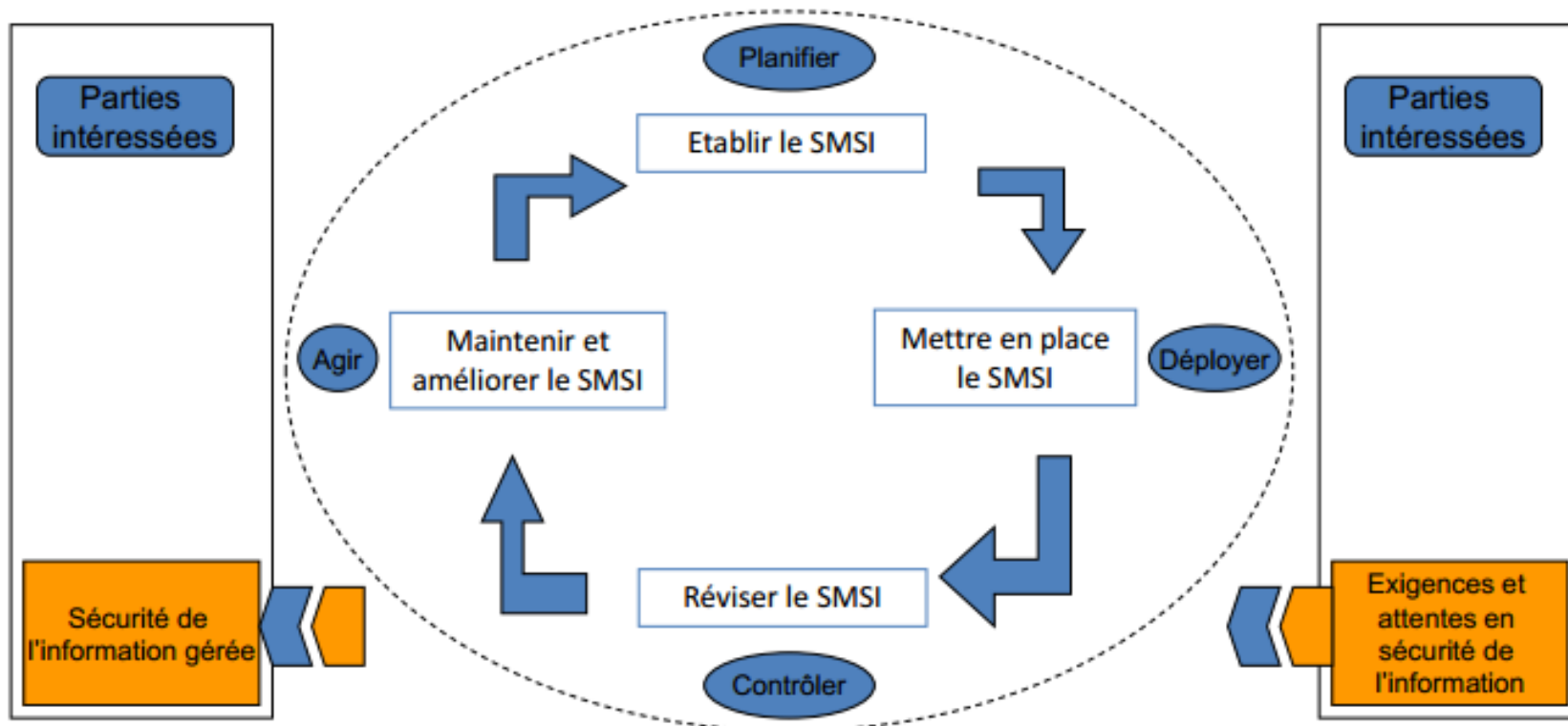
Pour être en conformité avec la norme ISO/CEI 27001, les SMSI doivent répondre à toutes les exigences comprises entre les chapitres 4 et 8:





# SMSI: Modèle PDCA; roue de deming

17



**modèle PDCA(Plan, DO, Check, Act)**

# SMSI: Modèle PDCA

18

- Les **SM** fonctionnent suivant le **modèle PDCA : Roue de Deming**
- caractéristiques du modèle PDCA :
  - **Cyclique**: C'est ce cycle Plan, Do, Check, Act qui permet d'atteindre les objectifs (de sécurité, de qualité, d'environnement ou autre) fixés par le management. En revanche, que se passe-t-il une fois que l'objectif a été atteint ? Un nouveau cycle doit être entrepris. C'est pour cela que l'on peut voir une flèche (figure slide 13) entre la phase Act et la phase Plan. Cette flèche bleu permet à l'entreprise non seulement d'atteindre ses objectifs, mais aussi de s'y tenir dans la durée. Un système de management est donc un processus qui tourne indéfiniment.
  - **Fractale**: Quelle que soit l'échelle à laquelle on observe les systèmes de management, on doit retrouver le modèle Plan, Do, Check, Act

# La norme ISO/CEI 27001 (Le modèle PDCA):

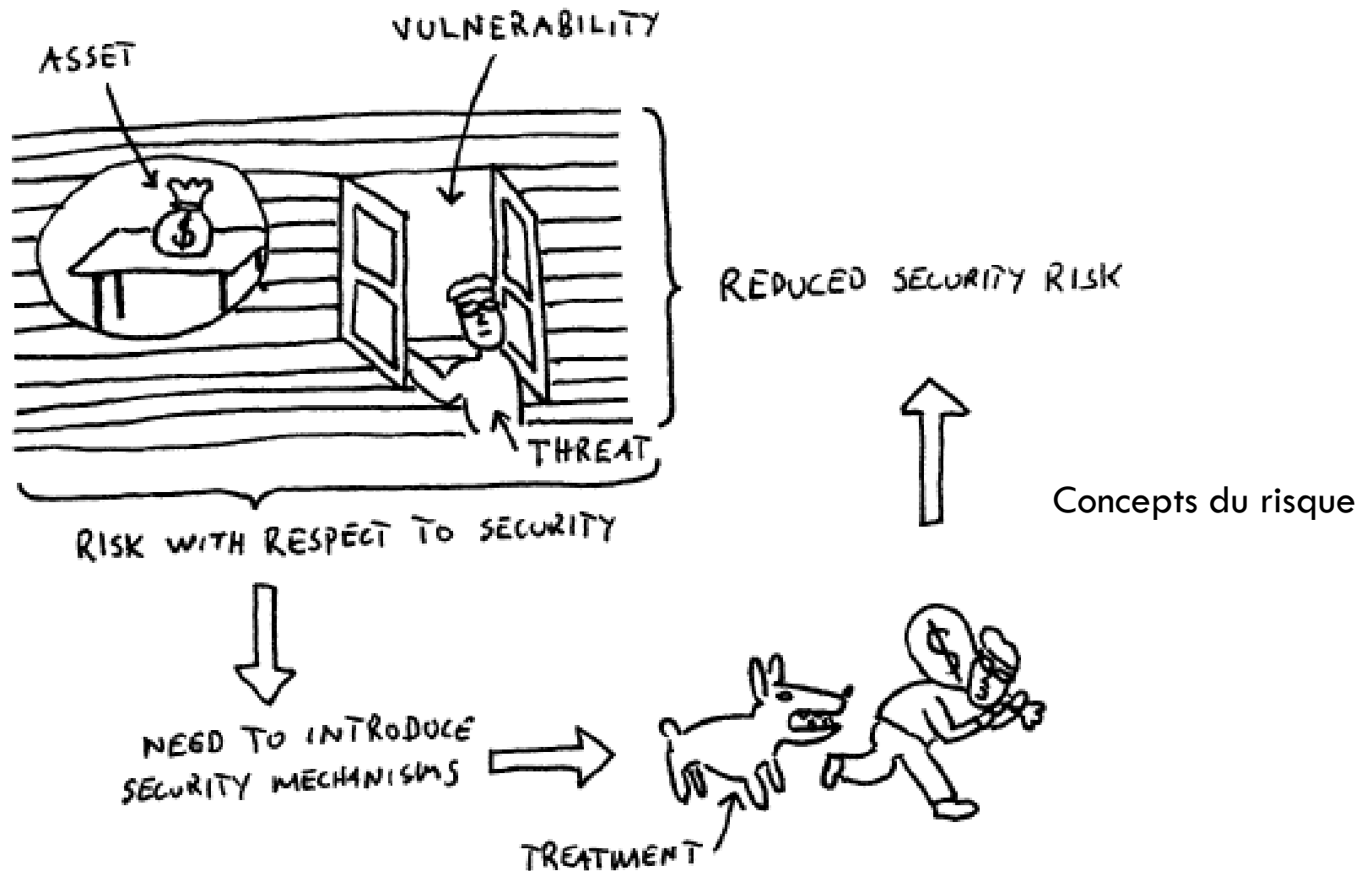
19

- 1. Phase Plan** : dire ce que l'on va faire dans un domaine particulier (qualité, environnement, sécurité, etc.).
- 2. Phase Do** : faire ce que l'on a dit dans ce domaine.
- 3. Phase Check** : vérifier qu'il n'y a pas d'écart entre ce que l'on a dit et ce que l'on a fait.
- 4. Phase Act** : entreprendre des actions correctives pour régler tout écart qui aurait été constaté précédemment.

*Les termes français pour nommer le modèle PDCA pourraient être « Planification », « Action », « Vérification » et « Correction ».*

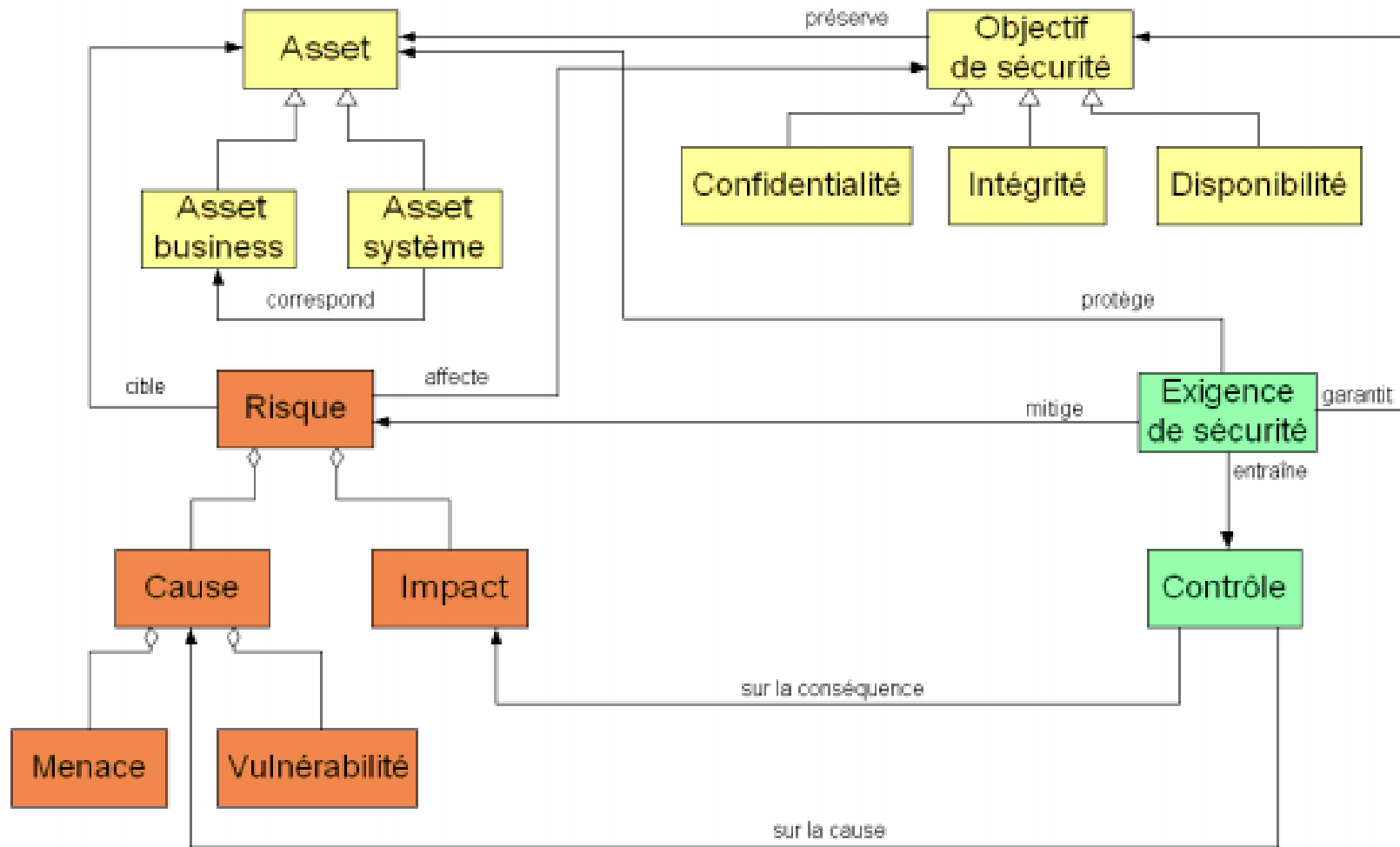
# Les concepts du risque

20



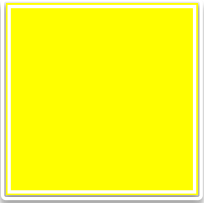
# Gestion des risques de sécurité des systems d'information : Concepts

21



# Gestion des risques de sécurité des systems d'information : Composants

22



1. L'organisme cible définie par ces assets (business, systèmes) et ses objectifs de sécurité



2. Les mesures de sécurité mises en place pour traiter le risque



3. Les risques pesants sur les actifs.

# Gestion des risques de sécurité des systems d'information: Processus

23

1

Identification du contexte des assets

2

Détermination des objectifs de sécurité

3

Analyse des risques

4

Définition des exigences de sécurité

5

Sélection des contrôles

6

Implémentation des contrôles



# Processus générique de gestion des risques de sécurité des systems d'information

24

1

## Identification du contexte des assets

Cette étape consiste en l'identification du domaine et des assets. Dans cette partie, il est question de prendre connaissance avec l'organisation, son environnement, son SI et de déterminer précisément les limites du système sur lequel va porter l'étude de gestion des risques. Une fois notre système borné, on procède en premier lieu à l'identification des assets business constituant la valeur de l'organisation. Ensuite, le lien sera fait entre ces assets business et les assets système, sur lesquels on identifiera et corrigera les risques d'un point de vue technique et organisationnel



# Processus générique de gestion des risques de sécurité des systems d'information

25

2

Détermination des objectifs de sécurité

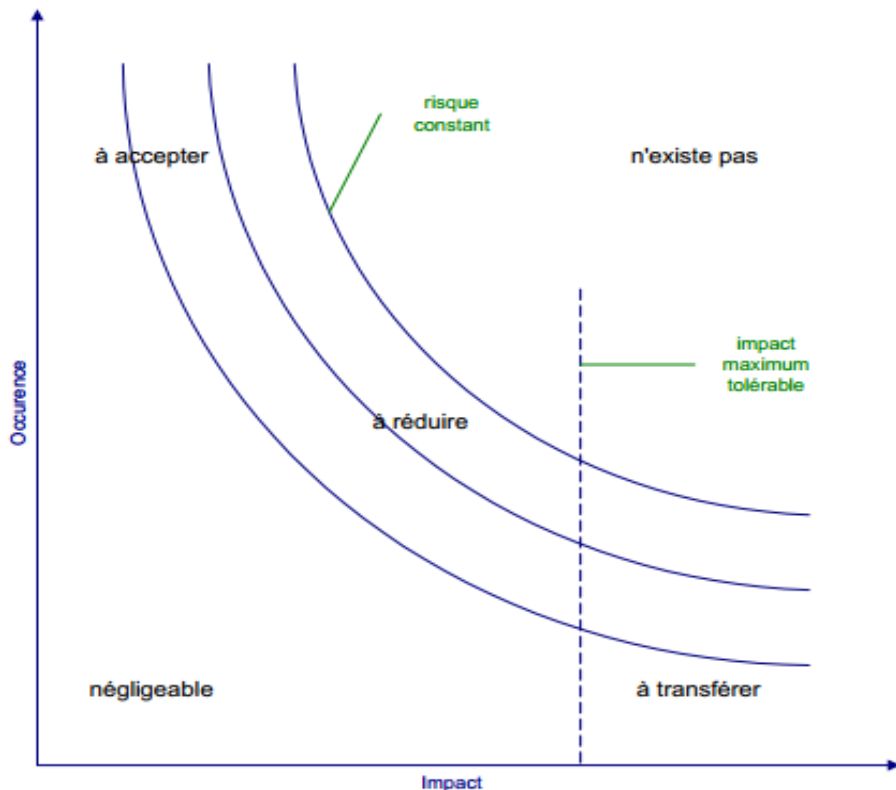
La détermination des objectifs de sécurité vise à spécifier les besoins en termes de confidentialité, intégrité et disponibilité des assets, en particulier au niveau business. Le lien entre les assets business et les assets système étant fait en amont, on retrouve donc les besoins en sécurité au niveau du système

# Processus générique de gestion des risques de sécurité des systems d'information

26

3

## Analyse des risques



« l'analyse des risques » est un processus essentiel qui permet de définir des exigences de sécurité qui seront traduites en objectifs de sécurité qui à leur tour vont impliquer la mise en place de mesures de sécurité adaptées. Dans ce cadre, plusieurs référentiels utiles à la mise en œuvre d'un tel système sont disponibles.

La gestion du risque comporte deux grandes étapes : **l'appréciation des risques** et **le traitement des risques**

# Processus générique de gestion des risques de sécurité des systems d'information

27

- ☐ Les risques ayant une occurrence et un impact faible sont négligeables.
- ☐ Les risques ayant une forte occurrence et un impact important ne doivent pas exister, autrement une remise en cause des activités de l'entreprise est nécessaire (**éviter le risque**).
- ☐ Les risques ayant une occurrence forte et un impact faible sont acceptés, leur coût est généralement inclus dans les coûts opérationnels de l'organisation (**accepter le risque**).
- ☐ Les risques ayant une occurrence faible et un impact lourd sont à transférer. Ils peuvent être couverts par une assurance ou un tiers (**transférer le risque**).
- ☐ les autres risques, en général majoritaires, sont traités au cas par cas et sont au centre du processus de gestion des risques ; l'objectif, étant de diminuer les risques en les rapprochant au maximum de à un niveau acceptable (**réduire le risque à l'aide de contrôles**).

# Processus générique de gestion des risques de sécurité des systems d'information

28

4

Définition des exigences de sécurité

Une fois l'analyse des risques effectuée, la définition des exigences de sécurité permettra de réduire les risques identifiés. Comme précédemment, en fonction des méthodes, cette étape pourra être effectuée avec l'assistance de référentiels, ou aiguillée par la connaissance d'experts système/sécurité.

# Processus générique de gestion des risques de sécurité des systems d'information

29

5

## Sélection des contrôles

Le dernier niveau de raffinement est constitué par la sélection des contrôles (ou contremesures) de sécurité. Les contrôles sont l'instanciation des exigences de bas niveau pour le système cible étudié. Ici sont définis les choix techniques des solutions de sécurité, influencés par le système déjà en place, les compétences disponibles, les coûts de mise en oeuvre

# Processus générique de gestion des risques de sécurité des systems d'information

30

6

Implémentation des contrôles

Une fois les contrôles sélectionnés, il reste alors à les implémenter dans le SI et à éventuellement les tester et les évaluer. Il subsiste alors indéniablement une part de risques traités partiellement ou non, qui constitue ce que l'on appelle le risque résiduel

# Processus de gestion des risques de sécurité des systems d'information : Exercice

31

## L'organisme cible:

- ❑ Un site de e-commerce dispose d'une base de données clients, présente sur un serveur de son parc informatique et contenant les informations bancaires de ces derniers.
  
- ❑ Suivez le processus de gestion des risques afin d'apprécier et d'analyser le risque

# Mise en place d'un SMSI

32

La norme NF ISO/CEi 27001 nous donne la définition suivante du SMSI :

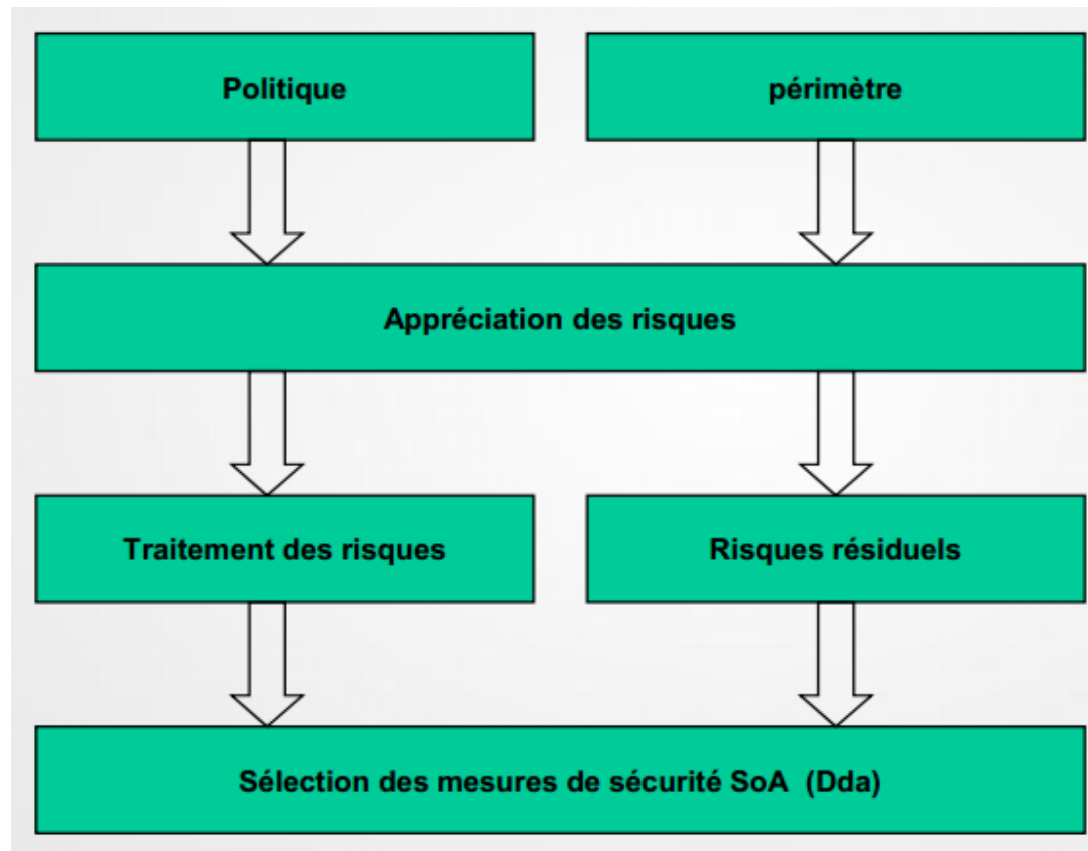
« Partie du système de management global, basée sur une approche du risque lié à l'activité, visant à établir, mettre en œuvre, exploiter, surveiller, réexaminer, tenir à jour et améliorer la sécurité de l'information »



# 1. PLAN

33

**Cette phase est découpée en 4 grandes étapes:**



*Processus de déroulement de la phase Plan*

### ☐ Pierres angulaires d'un SMSI

- ☐ ISO 27001 exige un périmètre sans imposer un à l'implémenter : 2 éléments de **souveraineté**
- ☐ La politique du SMSI spécifie le niveau de sécurité qui sera adopté dans le périmètre choisi
- ☐ Il **s'agit** de la **politique du SMSI** # **politique de la sécurité informatique**
- ☐ La norme exige une politique SMSI et non une politique de la sécurité informatique : cette dernière est également souvent utilisé dans les organisme
- ☐ La norme ne précise aucun niveau de sécurité : **deuxième levier de souveraineté**

**Périmètre** : domaine d'application du SMSI. **Son choix est libre**, mais il doit être bien défini, car il doit comprendre toutes les activités pour lesquelles les parties prenantes exigent de la confiance. **(Premier levier de souveraineté)**

**Politique** : niveau de sécurité (intégrité, confidentialité, disponibilité de l'information) qui sera pratiqué au sein de l'entreprise. **La norme n'impose pas de niveau minimum** de sécurité à atteindre dans le SMSI. **(deuxième levier de souveraineté)**

- Existence d'une **pléthore de méthodes** d'appréciation des risques
- ISO 27001 exige l'appréciation des risques sans spécifier une méthode
- ISO 27001 exige cependant un **cahier de charges** à respecter lors de l'appréciation des risques.

### Quelques méthodes d'appréciation des risques

Méthodes	Origine	Organisme	Gratuit	Téléchargement
<b>Ebios</b>	France	DCSSI	Oui	<a href="http://Dcssi.gouv.fr">Dcssi.gouv.fr</a>
<b>Mehari</b>	France	Clusif	Oui	<a href="http://Clusif.asso.fr">Clusif.asso.fr</a>
<b>CRAMM</b>	Royaume-Uni	CCTA	Non	
<b>Octave</b>	Etats-Unis	CERT	Oui	<a href="http://Cert.org/octave">Cert.org/octave</a>

### Critères de choix de la méthode d'appréciation des risques:

- **l'origine géographique de la méthode la langue de la méthode;**
- **l'existence d'outils:** logiciels en facilitant l'utilisation;
- **l'existence d'un club d'utilisateurs** afin d'avoir un retour d'expériences;
- **la qualité de la documentation;**
- **la facilité d'utilisation et le pragmatisme de la méthode;**
- **la compatibilité** avec une norme nationale ou internationale;
- **le coût** de la mise en œuvre;
- **la quantité de moyens humains** qu'elle implique et la durée de mobilisation;
- **la taille de l'entreprise** à laquelle elle est adaptée;
- **le support de la méthode** par son auteur, une méthode abandonnée n'offre plus la possibilité de conseil et de support de la part son éditeur;
- **Sa popularité**, une méthode très connue offre un réservoir de personnels qualifiés pour la mettre en œuvre.

Le cahier des charges imposé par l'ISO 27001:



### a. Identifiers les actifs:

Cet actif(Information Asset) peut être:

- ☐ **Matériel:** pour tous les équipements réseau et système.
- ☐ **Physique:** pour les bureaux, lieux de production, de livraisons.
- ☐ **Logiciel:** pour les bases de données, fichiers, les systèmes d'exploitation.
- ☐ **Humain:** pour tous les collaborateurs de l'organisme.
- ☐ **Documents:** pour les documents papier, manuels d'utilisation.
- ☐ **Immatériel:** pour le savoir-faire de l'organisme.

### b. Identifier les responsables :

- ❑ Cette étape vise à attribuer pour chaque actif d'information un « **propriétaire** ». La norme définit le propriétaire comme étant la personne qui connaît le mieux la valeur et les conséquences d'une compromission en termes de disponibilité, d'intégrité et de confidentialité de l'actif.
- ❑ ISO 27001 exige qu'un **responsable** soit désigné pour **chaque bien**



### c. Identifier les vulnérabilités :

- ☐ Cette étape consiste en l'identification des vulnérabilités des actifs recensés. La vulnérabilité est la **propriété intrinsèque** du bien qui l'expose aux menaces.
- ☐ Chaque actif présente des vulnérabilités qui lui sont propres.
- ☐ **Exemple:** un ordinateur portable ?

### d. Identifier les vulnérabilités :

❑ **Exemple:** un ordinateur portable est vulnérable au vol mais sa vulnérabilité n'est pas le vol mais sa portabilité. Dans ce cas l'identification de la vulnérabilité est la portabilité.

### e. Identifier les menaces:

- ☐ Vulnérabilités exposent les biens d'information aux menaces
- ☐ ISO 27001 exige d'identifier les menaces pour chaque bien recensé
- ☐ Exemple : Pc portable ?

### f. Identifiers les menaces:

- ❑ l'ordinateur portable, la menace est dans ce cas le vol.

### g. Identifiers les impacts:

- ☐ Cette étape vise à évaluer l'impact d'une perte de la **confidentialité**, de la **disponibilité** ou de **l'intégrité** sur les actifs. Pour mesurer cet impact on peut par exemple utiliser une matrice des risques, la norme n'impose aucun critère de mesure.
  
- ☐ La norme laisse l'implémenteur libre de choisir la méthode

### h. Identifiers les impacts:

☐ exemples: sans impact = 0, impact mineur = 1, impact moyen = 2, impact majeur = 3

**Actif 1 = (C, D, I) = (3, 2, 1)**

**Actif 2 = (C, D, I) = (1, 3, 3)**

....

### i. Identifiers la vraisemblance:

- ☐ Vraisemblance (**likelihood**) = probabilité d'occurrence
  
- ☐ Cette étape consiste à évaluer la vraisemblance des précédentes étapes du processus en plaçant dans leur contexte les actifs. Il s'agit par exemple de considérer les mesures de sécurité déjà en vigueur dans l'organisme. Si l'ordinateur portable possède une clef d'authentification, un cryptage de ses données ou un accès VPN pour travailler, alors la vraisemblance d'observer un impact sur la confidentialité, la disponibilité ou l'intégrité de ses données est limitée.

### j. Identifiers le niveau de risque:

Le risque est qualifié en fonction de **l'impact** qu'il peut avoir et de **sa probabilité d'occurrence (vraisemblance)**. Pour analyser les risques on va passer par deux étapes :

- **détermination / identification des risques** : on détermine quels sont les principaux risques qui pèsent sur les éléments du SI ;
- **valorisation des risques** : on calcule une valeur (un poids) pour chacun des risques en fonction de **la probabilité d'occurrence d'une menace, de la facilité d'exploitation d'une vulnérabilité, et des impacts** qui en découlent.



**j. Identifiers le niveau de risque:**

L'appréciation des risques consiste, d'une part, à les **identifier**, et d'autre part à les **évaluer** c'est-à-dire les **exprimer avec une valeur qui caractérise leur importance**.

**Définition des échelles de valeurs**

Avant de commencer, il est important de se doter de diverses échelles de notation et d'évaluation qui seront nécessaires pour « quantifier » les risques et leur affecter une priorité (abaque).

1. une échelle de valeur des actifs (quels sont les actifs les plus importants ?) ;
2. une échelle de vraisemblance des menaces (quelles sont les menaces les plus probables ou les plus vraisemblables ?) ;
3. une échelle de facilité d'exploitation des vulnérabilités ;
4. une échelle d'importance des impacts ;
5. un tableau de classification des risques.

### j. Identifier le niveau de risque:

#### 1. Les niveaux de valorisation des actifs

- valeur négligeable (**coefficient 0**) : si cet actif vient à manquer, les effets ne sont pas décelables ;
- valeur faible (**coefficient 1**) : si cet actif vient à manquer, les effets affectent essentiellement des éléments de confort ;
- valeur significative (**coefficient 2**) : si cet actif vient à manquer, les effets affaiblissent la performance ;
- valeur élevée (**coefficient 3**) : si cet actif vient à manquer toute l'unité est impactée ;
- valeur critique (**coefficient 4**) : si cet actif vient à manquer les missions essentielles de l'organisme sont mises en danger.

### j. Identifiers le niveau de risque:

#### 2. Échelle d'estimation des menaces

On évalue les menaces à partir de leur vraisemblance (ou leur probabilité d'occurrence). La vraisemblance d'une menace se mesure à partir de scénarios d'attaques : types de menaces environnementales ou humaines, existence d'attaquants, motivations d'attaque...

On trouvera une liste de 42 méthodes d'attaques possibles dans le volet ISO 27005 ou dans la méthode Ebios (comme par exemple, l'incendie, le vol, les écoutes réseau, etc.).

L'estimation des menaces peut ainsi s'évaluer sur une échelle à trois niveaux selon la vraisemblance ou probabilité d'occurrence : **probabilité faible, moyenne et forte, notées de 1 à 3**

### j. Identifiers le niveau de risque:

#### 3. Échelle d'estimation des vulnérabilités (facilité d'exploitation) (1/2)

Il convient dans un premier temps de répertorier les vulnérabilités présentes sur les actifs de soutien, puis pour chacune d'elles, de déterminer leurs facilités d'exploitation en tenant compte des mesures de protection existantes.

Pour chaque actif de soutien de l'unité on va estimer la facilité d'exploitation de leurs vulnérabilités :

- **vulnérabilité très facile à exploiter (coefficient 1)** : par exemple une salle serveur peut avoir comme vulnérabilité d'avoir une climatisation défectueuse ou de capacité insuffisante. L'augmentation de température qui peut s'ensuivre peut être un facteur de déclenchement d'incendie. Le déclenchement d'un incendie qu'il soit d'ordre environnemental ou intentionnel ne nécessite aucune compétence et est de ce fait facile à exploiter ;

### j. Identifiers le niveau de risque:

#### 3. Échelle d'estimation des vulnérabilités (facilité d'exploitation) (2/2)

- **vulnérabilité moyenne (coefficient 2)** : par exemple, le système de messagerie peut laisser passer certains documents comportant des virus. Les PC de l'unité ne sont pas tous équipés d'antivirus. Cette vulnérabilité est moyennement facile à exploiter du fait que certaines mesures antivirales sont déjà prises dans l'unité, et que l'unité a une architecture réseau sécurisée (réseau segmenté en vlan et filtres entre les réseaux) qui minimise les diffusions virales ;
- **vulnérabilité difficile à exploiter (coefficient 3)** : par exemple, le logiciel de gestion du service de noms (DNS) souffre d'un bogue de sécurité permettant de corrompre le cache des adresses IP de l'internet. Cette vulnérabilité potentiellement très dangereuse et spectaculaire nécessite toutefois des compétences très importantes relevant de spécialistes pour être exploitée.

### j. Identifiers le niveau de risque:

#### 4. Établissement des critères d'impact

Il faut répondre à la question : à partir de quel niveau juge-t-on qu'un impact est assez important pour que le risque soit pris en compte ? Les niveaux d'impact peuvent être confondus avec les niveaux de valorisation d'un actif définis précédemment, à sa perte ou sa dégradation.

Cinq niveaux dans les critères d'impacts / conséquences :

- **négligeables** : les effets ne sont pas décelables (**coefficient 0**) ;
- **faibles** : les effets affectent essentiellement des éléments de confort (**coefficient 1**) ;
- **significatifs** : les effets affaiblissent la performance de l'unité (**coefficient 2**) ;
- **élevés** : toute l'unité est impactée (**coefficient 3**) ;
- **critiques** : les effets mettent en danger les missions essentielles de l'organisme (**coefficient 4**).

### j. Identifiers le niveau de risque:

Exemple :

- **impact important (coefficient 3 à 4)** : l'incendie de la salle serveur en raison de la défaillance d'une climatisation peut avoir un impact catastrophique pendant plusieurs semaines pour la poursuite des activités de l'unité ;
- **impact moyen (coefficient 2 à 3)** : en l'absence de dispositif de sauvegarde de données, la perte ou le vol d'un PC peut compromettre une expérimentation et les activités d'une équipe sans toutefois paralyser l'unité entière ;
- **impact faible (coefficient 1)** : dans des conditions de sécurité déjà présentes (présence d'antivirus sur la majorité des PC de l'unité, sensibilisation permanente des utilisateurs et filtrage sur les serveurs de messagerie) la contamination de quelques PC dans l'unité fera perdre tout au plus quelques heures à l'utilisateur et au service informatique.

**j. Identifiers le niveau de risque:**

- ☐ Cette étape consiste à attribuer une note finale reflétant les risques pour chacun des actifs d'information. La norme n'impose aucune formule, on peut par exemple utiliser un code couleur (rouge pour un niveau de risque très élevé, orange pour moyen et vert pour faible).
- ☐ Donner une **note finale** pour chaque actif recensé;
- ☐ SO 27001 n'impose pas le comment;
- ☐ Risque = fonction (impact, menace, vulnérabilité)
- ☐ **Exemple:**

$$\text{Risque} = (\text{menace} + \text{vulnérabilité} + \text{impact}) - 2$$


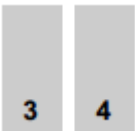




**j. Identifiers le niveau de risque:**

Vraisemblance de la menace		Faible (1)			Moyenne (2)			Forte (3)		
		Basse (1)	Moy. (2)	Elevée (3)	Basse (1)	Moy. (2)	Elevée (3)	Basse (1)	Moy. (2)	Elevée (3)
Impact (Valeur d'actif)	0	0	1	2	1	2	3	2	3	4
	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	5	6	7
	4	4	5	6	5	6	7	6	7	8

Le risque est maximal (valeur de 8) dans le cas d'un impact critique (4) avec de fortes probabilités de menaces (haute) et une vulnérabilité élevée (facile)

**j. Identifiers le niveau de risque:**

0	Risques nuls (0)	Risques acceptables
	Risques négligeable (1-2)	Risques acceptables
	Risques significatifs (3-4)	Risques à traiter cas par cas
	Risques graves (5-6)	Risques à traiter systématiquement
	Risques vitaux (7-8)	Refus du risqué tant qu'il n'a pas été traité

# 1. PLAN

## Étape 1.3: Traiter le risque et identifier le risqué résiduel

59

❑ La norme ISO 27001 décrit quatre moyens pour le traitement des risques :

**1. L'acceptation du risque:** ne déployer aucune mesure de sécurité autre que celles déjà en place si le risque n'a aucun impact constaté sur l'organisme(stratégique)

**2. La réduction du risque:** prendre de mesures techniques et organisationnelles pour ramener le risque à un niveau acceptable. C'est le traitement le plus courant.

**\*\* Après avoir sélectionné le traitement et mis en place les mesures de sécurité, un risque peut persister → le risque résiduel**

**3. Le transfert du risque:** Lorsque l'organisme ne peut ou ne souhaite pas mettre en place les mesures de sécurité qui permettrait de le réduire (souscription d'assurance ou sous-traitance)

**4. L'évitement du risque:** supprimer l'activité ou le matériel offrant le risque

# 1. PLAN

## Étape 1.3: Traiter le risque et identifier le risque résiduel

60

- ❑ **Risque résiduel**: restant après la mise en place des mesures de sécurité.
- ❑ Identifier les **risques**+ les **risques résiduels**

Risques résiduels:

- ❑ Acceptables: **Les accepter** en connaissance de cause
- ❑ Inacceptables: appliquer des **mesures de sécurité supplémentaires**

# 1. PLAN

## Étape 1.4: Sélectionner les mesures de sécurité (Contrôles)

61

Pour chaque Menace qui pèse sur un actif de soutien à travers une vulnérabilité donnée, en fonction du niveau de risque calculé, on détermine alors s'il faut traiter le risque (Inutile, Envisageable, Nécessaire, Obligatoire) et quel type de traitement du risque adopter :

**Accepter**-> Ne rien changer !

**Diminuer**-> Engager des actions pour réduire le risque

**Transférer**-> Engager des actions pour déplacer le risque

**Eviter**-> Refuser le risque !

# 1. PLAN

## Étape 1.4: Sélectionner les mesures de sécurité (Contrôles)

62

- ☐ Identifier les **mesures de sécurité** pour chaque risque : **Annexe A** contenant les **133 mesures**
- ☐ **Annexe A**: ne donne aucun conseil ni explication. C'est **ISO 27002** qui le fait (**préconisations d'implémentation**)
- ☐ ISO 27001 exige d'établir la **déclaration d'applicabilité** (**SoA : Statement Of Applicability**):
  - ☐ Tableau récapitulant les 133 mesures de l'annexe A;
  - ☐ Spécifier si la mesure est retenue ou rejetée;
  - ☐ Justification.

- A05. La politique de sécurité de l'information.
- A06. L'organisation de la sécurité de l'information.
- A07. La gestion des actifs.
- A08. La sécurité liée au RH.
- A09. La sécurité physique et environnementale.
- A10. La gestion de l'exploitation et des télécommunications.
- A11. Les contrôles d'accès.
- A12. Les acquisitions, développement et maintenance des systèmes d'information.
- A13. La gestion des incidents liés à la sécurité de l'information .
- A14. La gestion de la continuité de l'activité.
- A15. La conformité.

### Appréciation des risques sur un cas d'école

#### **Utilisation d'un portable par un chercheur:**

- Identifier les risques
- Effectuer une appréciation des risques
- Mettre en place un traitement du risque



### Appréciation des risques sur un cas d'école

#### **Utilisation d'un portable par un chercheur**

Utilisation du portable par un chercheur lors de ses déplacements :

- Le disque dur contient des résultats de recherche et des informations stratégiques (courriels échangés avec des partenaires industriels, rapport de recherche, projet de brevet)
- Ce chercheur se déplace régulièrement à l'étranger et utilise son ordinateur dans des endroits publics exposés : aéroports, gares, hôtels...
- La seule protection utilisée est un simple couple identifiant / mot de passe à l'allumage de l'ordinateur

## Etude de cas 3

66

### **Plateforme de bourses:**

Nous nous basons sur la plateforme actuelle du Ministère de l'Education Nationale, de la Formation Professionnelle, de l'Enseignement Supérieur et de la Recherche Scientifique dans laquelle les étudiants s'inscrivent pour faire la demande d'une bourse.

Nous imaginons une nouvelle fonctionnalité dans la plateforme permettant les professeurs (comité de sélection des boursiers) de se connecter, étudier les dossiers et sélectionner les étudiants ...

## 2. DO

67

- ☐ La phase **Plan** fixe les objectifs
- ☐ La phase **Do** met en œuvre ces objectifs
- ☐ Cette phase consiste à décrire la mise en œuvre des mesures de sécurité sélectionnées dans le SoA à travers quatre étapes.



- ❑ SoA indique les mesures de sécurité à déployer et non pas le comment.
- ❑ Le comment relève d'un plan de traitement des risques.
- ❑ La norme exige ce plan et qu'il contient au minimum :
  - Liste des actions à entreprendre;
  - Moyens nécessaires;
  - Responsabilités;
  - Priorités.

- ☐ mettre en place des indicateurs de **performance** pour vérifier l'efficacité des mesures de sécurité ainsi que des indicateurs de **conformité** pour contrôler la conformité du SMSI aux exigences de l'ISO 27001
- ☐ Il est à noter que la norme ne préconise pas d'indicateurs précis à utiliser mais **L'ISO/CEI 27004** propose une démarche qui peut aider au choix de l'indicateur.
- ☐ **De performance:**  
Ex: Nombre d'incidents de sécurité.
- ☐ **De conformité:**  
Ex: Nombre de réunions tenues; d'audit, de procédures écrites

## Étape 2.3: Formation et sensibilisation des collaborateurs:

70

la sensibilisation à la sécurité du système d'information concerne tous les collaborateurs. Etant donné que les mesures de sécurité de l'information couvrent de nombreux domaines allant de la sécurité organisationnelle à la sécurité physique, en passant par la sécurité des réseaux et autres, les collaborateurs doivent donc maîtriser les outils de sécurité déployés dans les différents domaines.

❑ Un SMSI ne peut exister et durer sans personnel **sensibilisé** et **formé**

❑ **Formation SMSI:**

- ISO 27001 Lead Auditor;
- ISO 27001 Lead implemter.

❑ **Formation technique:**

- Vidéosurveillance;
- Firewall;
- Sécurité UNIX.....

cette démarche consiste à garantir le bon fonctionnement du SMSI et de vérifier que leur documentation est à jour.

☐ Cette action permet donc aux auditeurs externe de contrôler la gestion du SMSI.

Tous les systèmes de management ISO sont concernés par maintenance.

☐ Maintenant que, **les mesures identifiées du SoA fonctionnent, les indicateurs sont implémentés et les collaborateurs formés et sensibilisés à la sécurité du SMSI**, la phase Check du PDCA peut être déclanchée.

### 3. CHECK

72

- ☐ Les phases **Plan** et **Do** opérationnalisent le SMSI;

**Question** : qui garantit la bonne marche et le bon fonctionnement du SMSI ?

- ☐ Les mesures de sécurités fonctionnent bien ?
- ☐ Les procédures sont toutes bien appliquées ?
- ☐ Les indicateurs sont bien collectés et interprétés? ...

ISO 27001 exige des contrôles pour surveiller en permanence le SMSI :

- ☐ Efficacité du SMS;
- ☐ Conformité du SMSI aux exigences de ISO 27001.



### 3. CHECK

73

L'implémenteur possède 3 outils:

1

Les audits internes (Exigences)

2

Les contrôles internes (non  
exigences)

3

Les revues de  
directions (exigences)

- ☐ 'assurer au quotidien que les collaborateurs appliquent correctement leurs procédures.

- ☐ contrôler **la conformité** et l'efficacité du SMSI en recherchant les écarts entre la documentation du système et les activités de l'organisme.
- ☐ La norme exige que la méthode utilisée pour l'audit soit documentée dans une procédure et que les rapports soient enregistrés pour être utilisés lors des revues de direction.

- ❑ revues de Direction (annuelle ou biannuelle par exemple) qui permettent aux dirigeants de l'organisme d'analyser les évènements qui se sont déroulés sur l'année en cours.

## 4. ACT

77

Cette phase consiste à prendre les mesures résultantes des constatations faites lors de la phase de vérification (Check) .

☐ Trois actions sont possible au cours de cette phase:

1

Actions correctives

2

Actions préventives

3

Actions d'amélioration

- ❑ intervention de manière corrective lors qu'un dysfonctionnement ou écart est constaté. Tout d'abord, agir sur les écarts ou dysfonctionnement puis les causes pour éviter qu'il ne se reproduisent.

- ❑ emploi des actions préventives quand une situation à risque est détectée.

Agir sur les causes avant que l'écart ou le dysfonctionnement ne se produisent.

- ❑ ces actions ont pour objectif l'amélioration de la performance du SMSI.

Les résultats des différentes actions doivent être enregistrés et communiqués aux parties prenantes.



## Résumé: Pour une bonne mise en place d'un SMSI il faut:

81

- ☐ Trouver/Choisir/désigner/se faire choisir un chef de projet: futur propriétaire du SMSI;
- ☐ Constituer une équipe que mènera le projet SMSI à terme;
- ☐ Décider des objectifs du SMSI;
- ☐ Déterminer le périmètre;
- ☐ Faire le point sur l'existant et mettre à jour la documentation
- ☐ Décider des actifs sensibles;
- ☐ Faire l'analyse des risques pour ces actifs sensibles;
- ☐ Sélectionner les mesures de sécurité;
- ☐ Rédiger et mettre en place les procédures;
- ☐ Auditer les membres du comité du SMSI;
- ☐ Communiquer;
- ☐ Mettre en place un programme d'audits internes;
- ☐ Rechercher et tester des indicateurs;
- ☐ Refaire l'analyse de risque;
- ☐ Revoir la liste des actifs;
- ☐ Réexaminer le périmètre;
- ☐ Faire soi-même, ne pas faire faire à d'autres;
- ☐ Ne pas nécessairement suivre l'ordre de L'ISO/CEI 27001

# ISO 27001: Processus de certification

82

- ❑ La certification ISO 27001 se déroule sur un cycle de trois ans : **l'audit initial**, **l'audit de surveillance** et **l'audit de renouvellement**.
- ❑ La durée est déterminée dans l'annexe C de la norme **ISO 27006**.

# ISO 27001 Processus de certification : L'audit initial

83

- ❑ **L'audit initial** porte sur l'ensemble du SMSI. L'auditeur ne donne pas la certification, il donne juste un avis qui sera étudié par un comité de validation technique, puis par un comité de certification. Ce n'est qu'après cela que le certificat initial est délivré pour une durée de **trois ans**. Dans le cas contraire, il y a un audit complémentaire dans le délai maximum de trois mois. L'organisme devra, durant ce délai, corriger les problèmes décelés lors de l'audit initial pour obtenir le certificat.

# ISO 27001 Processus de certification : L'audit de surveillance

84

**L'audit de surveillance** a lieu pendant la période de validité du certificat (3 ans) afin de s'assurer que le SMSI est toujours valable. Il y en a un par an.

L'audit porte notamment sur les écarts ou non-conformités relevés lors de l'audit initial ainsi que sur d'autres points :

- le traitement des plaintes ;
- l'état d'avancement des activités planifiées ;
- la viabilité du SMSI ;
- l'utilisation de la marque de l'organisation certificatrice ;
- différentes clauses choisies par l'auditeur.

Si l'auditeur relève des non-conformités, le certificat sera suspendu voire annulé.

L'organisme doit donc être perpétuellement mobilisé.

# ISO 27001 Processus de certification : L'audit de renouvellement

85

- ❑ **L'audit de renouvellement** se déroule à l'échéance du certificat. Il porte sur les **non-conformités** du dernier audit de surveillance ainsi que sur **la revue des rapports** des audits de surveillance précédents et la revue des performances du SMSI sur la période.

# ISO 27001: Processus de certification

86

## **Exercice 4: Risques de projet SMSI**

- Listez les principaux risques liés à un projet de mise en œuvre d'un SMSI en vous appuyant sur vos connaissances en gestion de projet et sur les facteurs propres au SMSI
- Déterminez les 3 risques qui sont selon vous les plus importants et proposez une solution de gestion de chacun de ces risques

# Les 133 points de contrôle de la norme

## Annexe A

### **5 Politique de sécurité**

- 5.1 Politique de sécurité de l'information
  - 5.1.1 Document de politique de sécurité de l'information
  - 5.1.2 Réexamen de la politique de sécurité de l'information

### **6 Organisation de la sécurité de l'information**

- 6.1 Organisation interne
  - 6.1.1 Engagement de la Direction vis-à-vis de la sécurité de l'information
  - 6.1.2 Coordination de la sécurité de l'information
  - 6.1.3 Attribution des responsabilités en matière de sécurité de l'information
  - 6.1.4 Système d'autorisation concernant les moyens de traitement de l'information
  - 6.1.5 Engagements de confidentialité
  - 6.1.6 Relations avec les autorités
  - 6.1.7 Relations avec des groupes de spécialistes
  - 6.1.8 Revue indépendante de la sécurité de l'information
- 6.2 Tiers
  - 6.2.1 Identification des risques provenant des tiers
  - 6.2.2 La sécurité et les clients
  - 6.2.3 La sécurité dans les accords conclus avec des tiers

### **7 Gestion des biens (assets / actifs)**

- 7.1 Responsabilités relatives aux biens
  - 7.1.1 Inventaire des biens
  - 7.1.2 Propriété des biens
  - 7.1.3 Utilisation correcte des biens
- 7.2 Classification des informations
  - 7.2.1 Lignes directrices pour la classification
  - 7.2.2 Marquage et manipulation de l'information

# Les 133 points de contrôle de la norme

## **8 Sécurité liée aux ressources humaines**

### **Annexe A**

- 8.1 Avant le recrutement
  - 8.1.1 Rôles et responsabilités
  - 8.1.2 Sélection
  - 8.1.3 Conditions d'embauche
- 8.2 Pendant la durée du contrat
  - 8.2.1 Responsabilités de la direction
  - 8.2.2 Sensibilisation, qualification et formations en matière de sécurité de l'information
  - 8.2.3 Processus disciplinaire
- 8.3 Fin ou modification de contrat
  - 8.3.1 Responsabilités en fin de contrat
  - 8.3.2 Restitution des biens
  - 8.3.3 Retrait des droits d'accès

## **9 Sécurité physique et environnementale**

- 9.1 Zones sécurisées
  - 9.1.1 Périmètre de sécurité physique
  - 9.1.2 Contrôles physiques des accès
  - 9.1.3 Sécurisation des bureaux, des salles et des équipements
  - 9.1.4 Protection contre les menaces extérieures et environnementales
  - 9.1.5 Travail dans les zones sécurisées
  - 9.1.6 Zones d'accès public, de livraison et de chargement
- 9.2 Sécurité du matériel
  - 9.2.1 Choix de l'emplacement et protection du matériel
  - 9.2.2 Services généraux
  - 9.2.3 Sécurité du câblage
  - 9.2.4 Maintenance du matériel
  - 9.2.5 Sécurité du matériel hors des locaux
  - 9.2.6 Mise au rebut ou recyclage sécurisé(e) du matériel
  - 9.2.7 Sortie d'un bien



# Les 133 points de contrôle de la norme

## Annexe A

### **10 Gestion de l'exploitation et des télécommunications**

#### 10.1 Procédures et responsabilités liées à l'exploitation

##### 10.1.1 Procédures d'exploitation documentées

##### 10.1.2 Gestion des modifications

##### 10.1.3 Séparation des tâches

##### 10.1.4 Séparation des équipements de développement, de test et d'exploitation

#### 10.2 Gestion de la prestation de service par un tiers

##### 10.2.1 Prestation de service

##### 10.2.2 Surveillance et réexamen des services tiers

##### 10.2.3 Gestion des modifications dans les services tiers

#### 10.3 Planification et acceptation du système

##### 10.3.1 Dimensionnement

##### 10.3.2 Acceptation du système

#### 10.4 Protection contre les codes malveillant et mobile

##### 10.4.1 Mesures contre les codes malveillants

##### 10.4.2 Mesures contre le code mobile

#### 10.5 Sauvegarde

##### 10.5.1 Sauvegarde des informations

#### 10.6 Gestion de la sécurité des réseaux

##### 10.6.1 Mesures sur les réseaux

##### 10.6.2 Sécurité des services réseau

#### 10.7 Manipulation des supports

##### 10.7.1 Gestion des supports amovibles

##### 10.7.2 Mise au rebut des supports

##### 10.7.3 Procédures de manipulation des informations

##### 10.7.4 Sécurité de la documentation système

#### 10.8 Échange des informations

##### 10.8.1 Politiques et procédures d'échange des informations

##### 10.8.2 Accords d'échange

##### 10.8.3 Supports physiques en transit

##### 10.8.4 Messagerie électronique

##### 10.8.5 Systèmes d'information d'entreprise

#### 10.9 Services de commerce électronique

##### 10.9.1 Commerce électronique

##### 10.9.2 Transactions en ligne

##### 10.9.3 Informations à disposition du public

#### 10.10 Surveillance

##### 10.10.1 Rapport d'audit

##### 10.10.2 Surveillance de l'exploitation du système

##### 10.10.3 Protection des informations journalisées

##### 10.10.4 Journal administrateur et journal des opérations

##### 10.10.5 Rapports de défaut

##### 10.10.6 Synchronisation des horloges

# Les 133 points de contrôle de la norme

## Annexe A

### 11 Contrôle d'accès

- 11.1 Exigences métier relatives au contrôle d'accès
  - 11.1.1 Politique de contrôle d'accès
- 11.2 Gestion de l'accès utilisateur
  - 11.2.1 Enregistrement des utilisateurs
  - 11.2.2 Gestion des privilèges
  - 11.2.3 Gestion du mot de passe utilisateur
  - 11.2.4 Réexamen des droits d'accès utilisateurs
- 11.3 Responsabilités utilisateurs
  - 11.3.1 Utilisation du mot de passe
  - 11.3.2 Matériel utilisateur laissé sans surveillance
  - 11.3.3 Politique du bureau propre et de l'écran vide
- 11.4 Contrôle d'accès au réseau
  - 11.4.1 Politique relative à l'utilisation des services en réseau
  - 11.4.2 Authentification de l'utilisateur pour les connexions externes
  - 11.4.3 Identification des matériels en réseau
  - 11.4.4 Protection des ports de diagnostic et de configuration à distance
  - 11.4.5 Cloisonnement des réseaux
  - 11.4.6 Mesure relative à la connexion réseau
  - 11.4.7 Contrôle du routage réseau
- 11.5 Contrôle d'accès au système d'exploitation
  - 11.5.1 Ouverture de sessions sécurisées
  - 11.5.2 Identification et authentification de l'utilisateur
  - 11.5.3 Système de gestion des mots de passe
  - 11.5.4 Emploi des utilitaires système
  - 11.5.5 Déconnexion automatique des sessions inactives
  - 11.5.6 Limitation du temps de connexion
- 11.6 Contrôle d'accès aux applications et à l'information
  - 11.6.1 Restriction d'accès à l'information
  - 11.6.2 Isolement des systèmes sensibles
- 11.7 Informatique mobile et télétravail
  - 11.7.1 Informatique mobile et télécommunications
  - 11.7.2 Télétravail

# Les 133 points de contrôle de la norme

## Annexe A

### **12 Acquisition, développement et maintenance des systèmes d'information**

- 12.1 Exigences de sécurité applicables aux systèmes d'information
  - 12.1.1 Analyse et spécification des exigences de sécurité
- 12.2 Bon fonctionnement des applications
  - 12.2.1 Validation des données d'entrée
  - 12.2.2 Mesure relative au traitement interne
  - 12.2.3 Intégrité des messages
  - 12.2.4 Validation des données de sortie
- 12.3 Mesures cryptographiques
  - 12.3.1 Politique d'utilisation des mesures cryptographiques
  - 12.3.2 Gestion des clés
- 12.4 Sécurité des fichiers système
  - 12.4.1 Mesure relative aux logiciels en exploitation
  - 12.4.2 Protection des données système d'essai
  - 12.4.3 Contrôle d'accès au code source du programme
- 12.5 Sécurité en matière de développement et d'assistance technique
  - 12.5.1 Procédures de contrôle des modifications
  - 12.5.2 Réexamen technique des applications après modification du système d'exploitation
  - 12.5.3 Restrictions relatives à la modification des logiciels
  - 12.5.4 Fuite d'informations
  - 12.5.5 Externalisation du développement logiciel
- 12.6 Gestion des vulnérabilités techniques
  - 12.6.1 Mesure relative aux vulnérabilités techniques

# Les 133 points de contrôle de la norme

## **13 Gestion des incidents liés à la sécurité de l'information**

## **Annexe A**

- 13.1 Signalement des événements et des failles liés à la sécurité de l'information
  - 13.1.1 Signalement des événements liés à la sécurité de l'information
  - 13.1.2 Signalement des failles de sécurité
- 13.2 Gestion des améliorations et incidents liés à la sécurité de l'information
  - 13.2.1 Responsabilités et procédures
  - 13.2.2 Exploitation des incidents liés à la sécurité de l'information déjà survenus
  - 13.2.3 Collecte de preuves

## **14 Gestion du plan de continuité de l'activité**

- 14.1 Aspects de la sécurité de l'information en matière de gestion de la continuité de l'activité
  - 14.1.1 Intégration de la sécurité de l'information dans le processus de PCA
  - 14.1.2 Continuité de l'activité et appréciation du risque
  - 14.1.3 Élaboration et mise en oeuvre des PCA intégrant la sécurité de l'information
  - 14.1.4 Cadre de la planification de la continuité de l'activité
  - 14.1.5 Mise à l'essai, gestion et appréciation constante des plans de continuité de l'activité

## **15 Conformité**

- 15.1 Conformité avec les exigences légales
  - 15.1.1 Identification de la législation en vigueur
  - 15.1.2 Droits de propriété intellectuelle
  - 15.1.3 Protection des enregistrements de l'organisme
  - 15.1.4 Protection des données et confidentialité des informations relatives à la vie privée
  - 15.1.5 Mesure préventive à l'égard du mauvais usage des moyens de traitement de l'information
  - 15.1.6 Réglementation relative aux mesures cryptographiques
- 15.2 Conformité avec les politiques et normes de sécurité et conformité technique
  - 15.2.1 Conformité avec les politiques et les normes de sécurité
  - 15.2.2 Vérification de la conformité technique
- 15.3 Prises en compte de l'audit du système d'information
  - 15.3.1 Contrôles de l'audit du système d'information
  - 15.3.2 Protection des outils d'audit du système d'information