Management de la sécurité de l'information

Implémentation ISO 270001

Pr B. REGRAGUI

PLAN

- Les systèmes de management de la sécurité de l'information
- La norme ISO 27001
- La norme ISO 27002
- Implémenter un SMSI

Les systèmes de management de la sécurité de l'information

Introduction

- **Pendant très longtemps la sécurité a été considérée comme**
  - ✓ Le parent pauvre de l'informatique
  - ✓ Ne générant aucun revenu pour l'entreprise
- **Depuis l'interconnexion des systèmes informatiques la donne à changé**
- **De nos jours la sécurité est un enjeu majeur; la généralisation:**
  - ✓ Ingénieur sécurité
  - ✓ Consultant sécurité
  - ✓ **R**esponsable **S**écurité des **S**ystèmes d'**I**nformation (RSSI)
- **Sur le plan technique; beaucoup d'amélioration**
  - ✓ Sécuriser les serveurs Unix et Windows
  - ✓ Protéger les routeurs
  - ✓ Configurer les pare-feux

Introduction

- **Cependant, plusieurs sociétés sont victimes d'actes de malveillance**

- **Principales raisons**
  - ✓ Les mesures de sécurité sont souvent déployées au jour le jour, sans prendre la peine de chercher les vulnérabilités ni se préoccuper des besoins réels de l'entreprise en matière de sécurité.
  - ✓ Manque d'un chef orchestre qui fixe les objectifs, donne les priorités et coordonne les actions de sécurité

- **Le chef d'orchestre → SMSI (Systèmes de Management de la Sécurité de l'Information**

Les systèmes de management

Qu'est ce qu'un système de management?

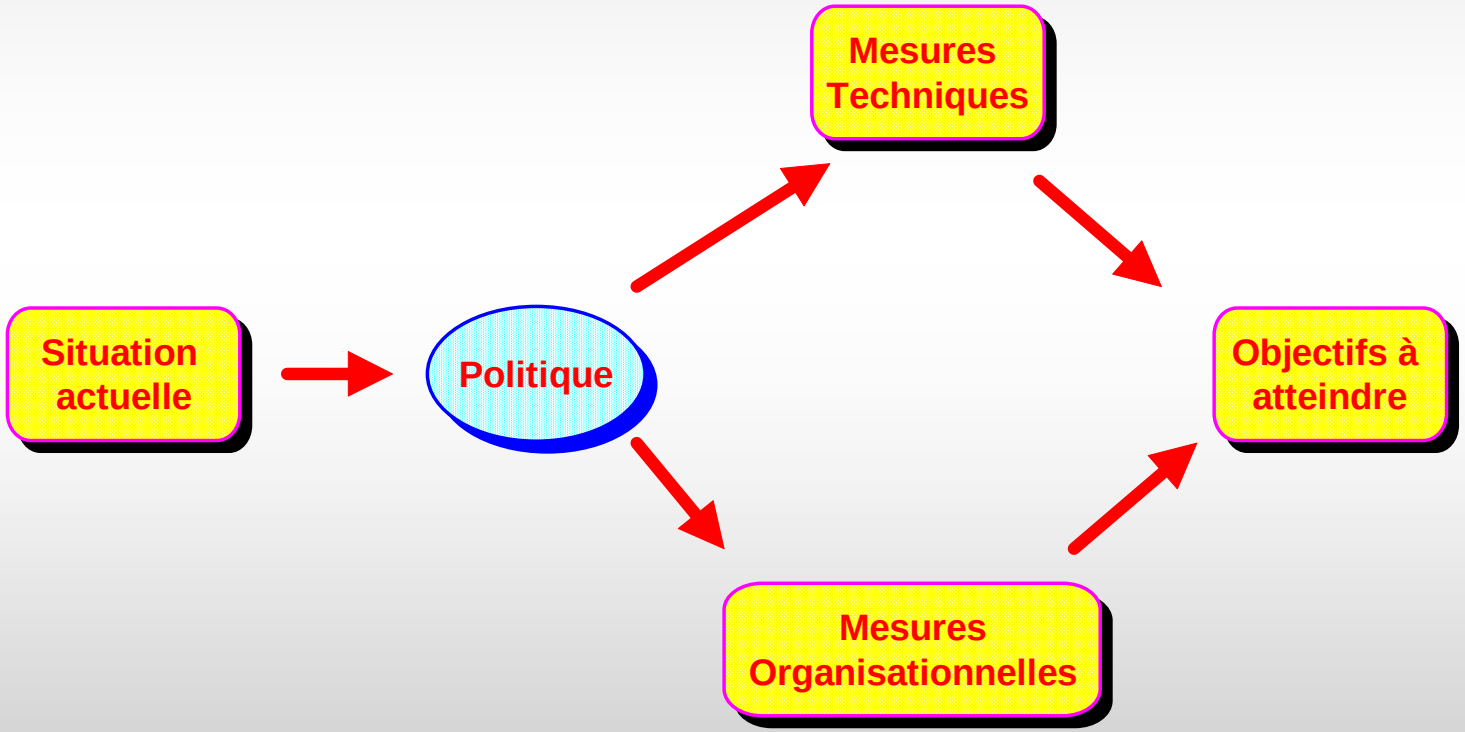
Selon la norme ISO 9000

- **Un système de management est un système permettant**
  - ✓ D'établir une politique
  - ✓ D'établir des objectifs
  - ✓ D'atteindre ces objectifs

- **Un système de management est un ensemble de mesures organisationnelles et techniques visant à atteindre un objectif et à s'y tenir, voire à le dépasser.**

Qu'est ce qu'un système de management?

Selon la norme ISO 9000



Principaux systèmes de management

Standard	Domaines
ISO 9001	Qualité
ISO 14001	Environnement
ISO 27001	Sécurité de l'information
ISO 20000	Services informatiques
ISO 22000	Sécurité alimentaire
OHSAS 18001	Santé/Sécurité du personnel

Propriétés des systèmes de management

- **Large spectre de métiers et de compétences**

  Quel que soit le périmètre (du plus petit au plus ambitieux) le SI implique un nombre important de métiers et de compétences. (Aspect transversal)

- **Un projet fédérateur et mobilisateur**

  Un SI implique toute la hiérarchie de l'entreprise. (Aspect vertical)

- **Importance de l'écrit**

  La formalisation des politiques et des procédures de l'entreprise est indispensable.

- **Auditabilité**

  L'audit est indissociable du SI. Un SI implique systématiquement la mise en place d'un processus d'audit.

Apport des systèmes de management

- **L'adoption des bonnes pratiques**

  Les SI se basent sur des guides de bonnes pratiques dans le domaine qui les concerne (qualité, sécurité, environnement)

- **l'augmentation de la fiabilité**

  Les SI imposent la mise en place de mécanismes d'amélioration continue favorisant la capitalisation sur retour d'expérience.

- **La confiance**

  Les SI fournissent la confiance envers les parties prenantes (actionnaires, autorité de tutelles, clients, fournisseurs, personnel, opinion publique)

Le modèle PDCA

Les SI fonctionnent selon un modèle en 4 temps (PDCA)

- **Phase Plan**

  Exprimer ce que l'on va faire dans un domaine particulier (qualité, environnement, sécurité,…)

- **Phase Do**

  Faire ce que l'on a exprimé dans le domaine

- **Phase Check**

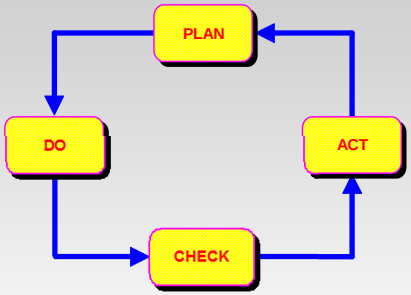
  Vérifier qu'il n'y a pas d'écart entre ce que l'on a dit et ce que l'on a fait.

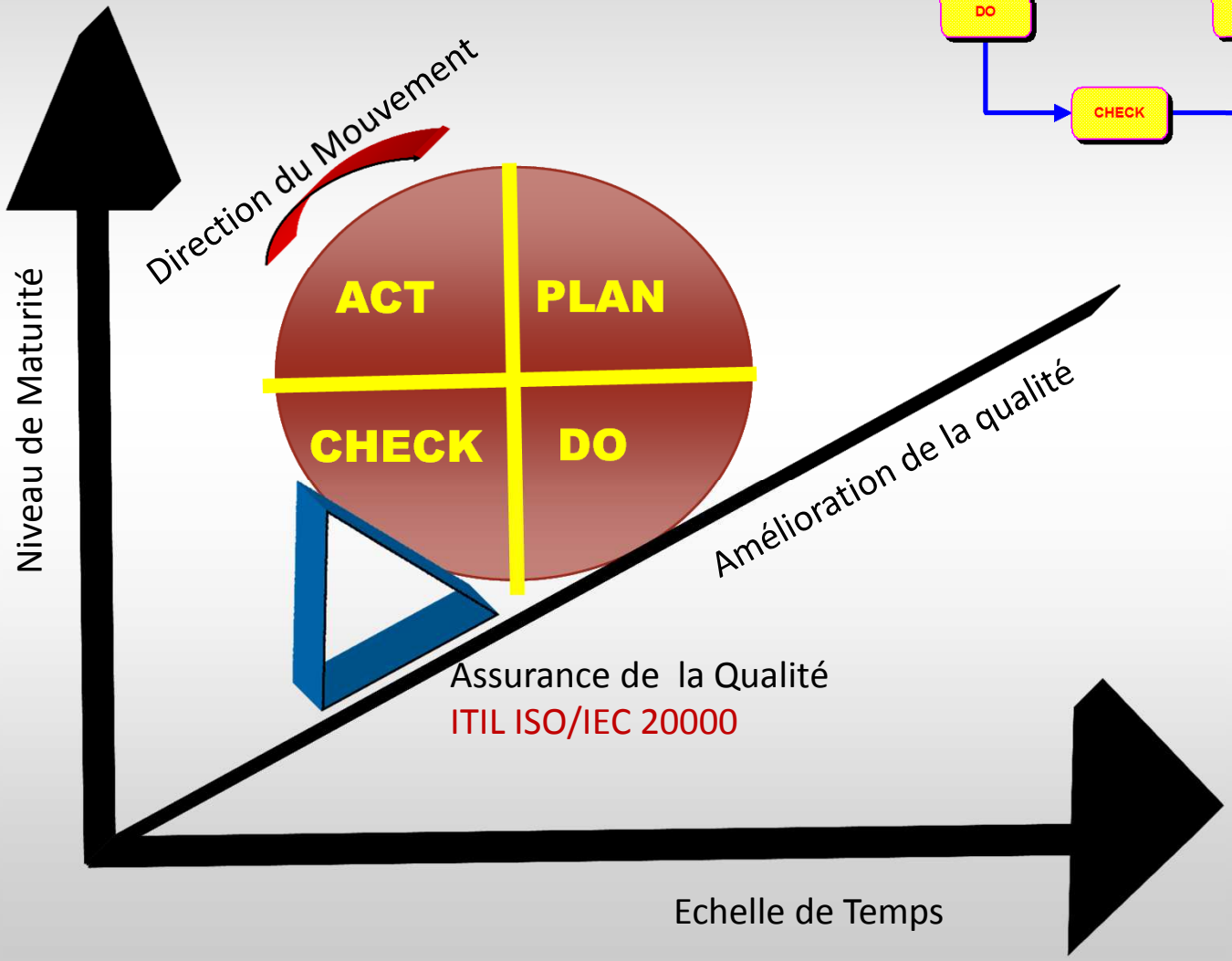
- **Phase Act**

  Entreprendre les actions correctives pour régler tout écart qui aurait été constaté précédemment

Le modèle PDCA

Les SI fonctionnent selon un modèle en 4 temps (PDCA)





Sécurité de l'information

Il s'agit de la sécurité de l'information

- au sens large du terme (pas seulement de la sécurité informatique).
- Sous toutes ses formes indépendamment du support (logiciel, matériel, humain, papier…

Réduire le SMSI à son coté strictement informatique serait une erreur.

Sécurité de l'information

Il s'agit de mettre tous œuvre tout ce qui peut assurer

- **Confidentialité:** l'information ne doit pas être divulguée à toute personne, entité ou processus non autorisé.
- **Intégrité:** le caractère correct et complet des actifs doit être préservé. L'information ne peut être modifiée que par ceux qui ont en le droit.
- **Disponibilité:** l'information doit être rendu accessible et utilisable sur demande par une entité autorisée.

La norme ISO 27001

La norme ISO 27001

L'ISO 27001 est imposé… Management de la Séc…

le jour de l'audit de certification, les auditeurs ne se borneront pas à la mise en place du SMSI, il vérifieront sa mise en place et s'il s'améliore dans le temps

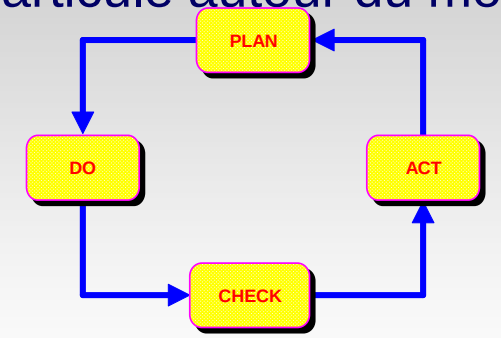
- Disponible sur site ISO, AFNOR, BSI…
- Les organismes visés par la norme sont de tout type (*administrati… …treprise commerciale*, *organisation non gouvernementale*)
- **L'objectif général** est de spécifier les exigences pour *mettre en place*, *exploiter* et *améliorer* un SMSI documenté.

Certaines multinationales, notamment au Japon, sont certifiées ISO 27001. Inversement, des PME françaises qui ne comptent pas plus d'une centaine d'employés le sont aussi.

- La norme spécifie les exige… besoins de l'organisation (ch…
- La norme fait en sorte que les mesures de sécurités … …oyées en fonction du *contexte* (ni trop sévère, ni trop laxiste)
- La norme insiste sur le fait que la mise en place d'un SI… le déploiement de mesures de sécurité appropriées doivent permettre de **p… …ger les actifs de l'information** (bien, patrimoine informationnel, bien sensi…e…)
- La norme précise que les indications de la norme sont génériques

La norme ISO 27001

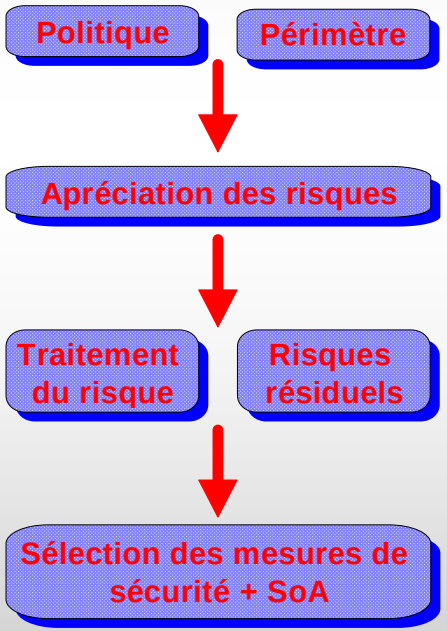
Le noyau dur de la norme (chapitre 4) est articulé autour du modèle Plan, Do, Check, Act.



➢ Phase Plan du SMSI

Cette phase se décompose en 4 grandes étapes:

- ✓ **Etape 1:** définir le périmètre et la politique.
- ✓ **Etape 2:** apprécier les risques
- ✓ **Etape 3:** traiter les risques et identifier le risque résiduel
- ✓ **Etape 4:** sélectionner les mesures de sécurité



La norme ISO 27001 (Phase Plan du SMSI)

- **Etape 1: Définir le périmè**

Il peut ne comprendre que l'une des activités de l'entreprise sur un site particulier tout comme cela peut s'étendre à toutes les activités de tous les sites.

Le périmètre et la politique constitu[illegible] pierre angulaire du système de management.

- ✓ **Périmètre:** c'est le domaine d'application du SMSI. Le but est d'inclure dans le périmètre toutes les activités dont les parties prenantes exigent de la confiance.
- ✓ **Politique:** il s'agit de préciser le niveau de sécurité qui sera appliqué dans le domaine défini dans le périmètre

politique du SMSI : le niveau de sécurité que l'entreprise s'engage à atteindre
politique de sécurité : donne plus de précisions pratiques.
Ces deux documents sont généralement complémentaires.

La norme ne donne aucune directive sur la manière de choisir le périmètre et la politique du SMSI.

Elle ne formule des exigences que sur la forme.

La norme ISO 27001 (Phase Plan du SMSI)

➢ **Etape 2:** Apprécier les risques

✓ Le besoin d'apprécier les risques n'est pas nouveau car les entreprises sont depuis toujours exposées à des menaces.

✓ La norme
d'appré

- **EBIOS:** Méthodologie d'identification des menaces et des vulnérabilités, analyse de risques, spécification des exigences de la sécurité
- **MEHARI: ME**thode **H**armonisée d'**A**nalyse des **Ri**sques

Méthode	Origine	Organisme	Gratuit
Ebios	France	DCSSI	Oui
Mehari	France	Clusif	Oui
CRAMM	Royaume-Uni	CCTA	Non
Octave	Etats-Unis	CERT	Oui

La norme ISO 27001 (Phase Plan du SMSI)

- **Etape 2:** Apprécier les risques

- La norme exige un **cahier de charge très strict** qui spécifie toutes les étapes clés de l'appréciation des risques.(Toute méthode ne respectant pas l'un de ces points est considérée comme étant non conforme à la norme)

  - ✓ Il suffit (au responsable chargé de l'appréciation du risque) de vérifier que la méthode utilisée, pour l'appréciation des risques, soit compatible avec les exigences de la norme.

  - ✓ L'entreprise peut très bien inventer sa propre méthode maison, *en respectant rigoureusement le cahier des charges de l'ISO 27001*.

La norme ISO 27001 (Phase Plan du SMSI)

➢ **Etape 2:** Apprécier les risques

Les étapes suivantes sont très importantes dans l'appréciation des risques

1. Identifier les actifs
2. Identifier les personnes responsables
3. Identifier les vulnérabilités
4. Identifier les menaces
5. Identifier les impacts
6. Evaluer la vraisemblances
7. Estimer les niveaux de risque

1. *Identifier les actifs*

Faire la liste de tout ce qui revêt une im au sein du périmètre du SMSI.

Trois problèmes se posent

- ✓ Le choix du **bon niveau de granularité**
- ✓ La définition de la **liste des biens**
- ✓ La **différentiation entre les actifs et les actifs d'information**

La norme ISO 27001 (Phase Plan du SMSI)

- **Etape 2:** Apprécier les risques

1. *Identifier les actifs*

Faire la liste de tout ce qui revêt un importance en matière d'information au sein du périmètre du SMSI.

Trois problèmes se posent

- ✓ Le choix du bon niveau de granularité**:** Il dépend de la taille du périmètre. L'actif d'information concerne aussi bien les logiciels et matériels classiques, mais aussi tout ce qui sert comme support à l'information.
- ✓ La définition de la liste des biens
- ✓ La différentiation entre les actifs et les actifs d'information

La norme ISO 27001 (Phase Plan du SMSI)

- **Etape 2:** Apprécier les risques

1. *Identifier les actifs*

Faire la liste de tout ce qui revêt un importance en matière d'information au sein du périmètre du SMSI.

Trois problèmes se posent

- ✓ Le choix du bon niveau de granularité:
- ✓ La définition de la liste des biens: Ne pas oublier de recenser des biens importants, sinon une analyse de risques risquerait de passer à coté des principales menaces.
- ✓ La différentiation entre les actifs et les actifs d'information

La norme ISO 27001 (Phase Plan du SMSI)

- **Etape 2:** Apprécier les risques

1. *Identifier les actifs*

Faire la liste de tout ce qui revêt un importance en matière d'information au sein du périmètre du SMSI.

Trois problèmes se posent

- ✓ Le choix du bon niveau de granularité:
- ✓ La définition de la liste des biens
- ✓ La différentiation entre les actifs et les actifs d'information**:** les actifs sont tout ce qui possède de la valeur pour l'entreprise. Les actifs d'information sont tout ce qui possède de l'importance en matière d'information.

La norme ISO 27001 (Phase Plan du SMSI)

- **Etape 2:** Apprécier les risques

2. *Identifier les personnes responsables*

Tout bien doit avoir un responsable. C'est la **personne** qui connait le mieux la valeur et les conséquences d'une compromission en termes de ***disponibilité***, ***d'intégrité*** et de ***confidentialité*** de l'actif.

➢ **Etape 2:** Apprécier les risques

3. *Identifier les vulnérabilités*

Chaque actif présente ses propres vulnérabilités. **Une vulnérabilité est une propriété intrinsèque du bien qui l'expose à des menaces**

Exemple: vulnérabilité d'un ordinateur portable

Quelle est la principale vulnérabilité d'un ordinateur portable? La réponse qui vient le plus spontanément est le **vol**. Pourtant, c'est faux.

Le vol n'est pas une vulnérabilité.

La principale vulnérabilité de l'ordinateur portable est sa **portabilité**. En effet, la portabilité est une propriété intrinsèque à ce bien. C'est parce que de tels ordinateurs sont portables qu'ils connaissent le succès qu'on sait. Cependant, **cette propriété pose des problèmes en termes de sécurité**.

➢ **Etape 2:** Apprécier les risques

4. *Identifier les menaces*

Les vulnérabilités exposent les biens d'information à des menaces. La norme impose d'identifier les menaces pour chaque bien recensé.

Exemple: menace principale pour un ordinateur portable

La **principale menace** est le **vol**.
En effet, **le vol exploite la principale vulnérabilité de l'ordinateur, c'est-à-dire sa portabilité**.

La norme ISO 27001 (Phase Plan du SMSI)

➢ **Etape 2:** Apprécier les risques

5. *Identifier les impacts*

Une perte de confidentialité, de disponibilité ou d'intégrité sur un actif aura des conséquences. La norme oblige à évaluer ces impacts pour chaque actif.

Pour **chaque actif**, on donne une **note en trois dimensions** (une pour la ***confidentialité***, une pour la ***disponibilité*** et une autre pour ***l'intégrité***.

La norme laisse l'implémenteur libre de définir ses propres critères.

Exemple:
Si notre critère va de 0 (pour pas d'impact) à 3 (pour un impact majeur),
voici la note que nous pouvons donner pour les deux actifs: ***fichier client*** et ***serveur pilotant un robot*** :
FichierClient (confidentialité: 3 ; intégrité: 2 ; disponibilité: 1) ;
ServeurPilotantRobot (confidentialité: 1 ; intégrité: 3 ; disponibilité: 3).

La norme ISO 27001 (Phase Plan du SMSI)

➢ **Etape 2:** Apprécier les risques

6. *Evaluer la vraisemblance*

Il s'agit de **remettre les biens d'information dans leur contexte** et de **considérer les mesures de sécurité** qui sont déjà en place.

Il ne faut plus considérer les biens d'information un par un en faisant abstraction de leur environnement.

Exemple:
Si le **fichier client est chiffré**, alors la vraisemblance de voir sa confidentialité compromise est **limitée**.
Si le **serveur pilotant le robot est sécurisé** (durcissement du système d'exploitation, scellement des fichiers de configuration, protection par pare-feu), alors la vraisemblance que son intégrité soit compromise est **réduite**.

La norme ISO 27001 (Phase Plan du SMSI)

➢ **Etape 2:** Apprécier les risques

7. *Estimer les niveaux de risque*

Cette étape consiste à donner une note finale pour chaque actif d'information.

Elle **reflètera le niveau de risque réel**, compte tenu de tous les éléments récoltés dans les étapes précédentes de l'analyse.

La norme **n'impose aucune formule**.

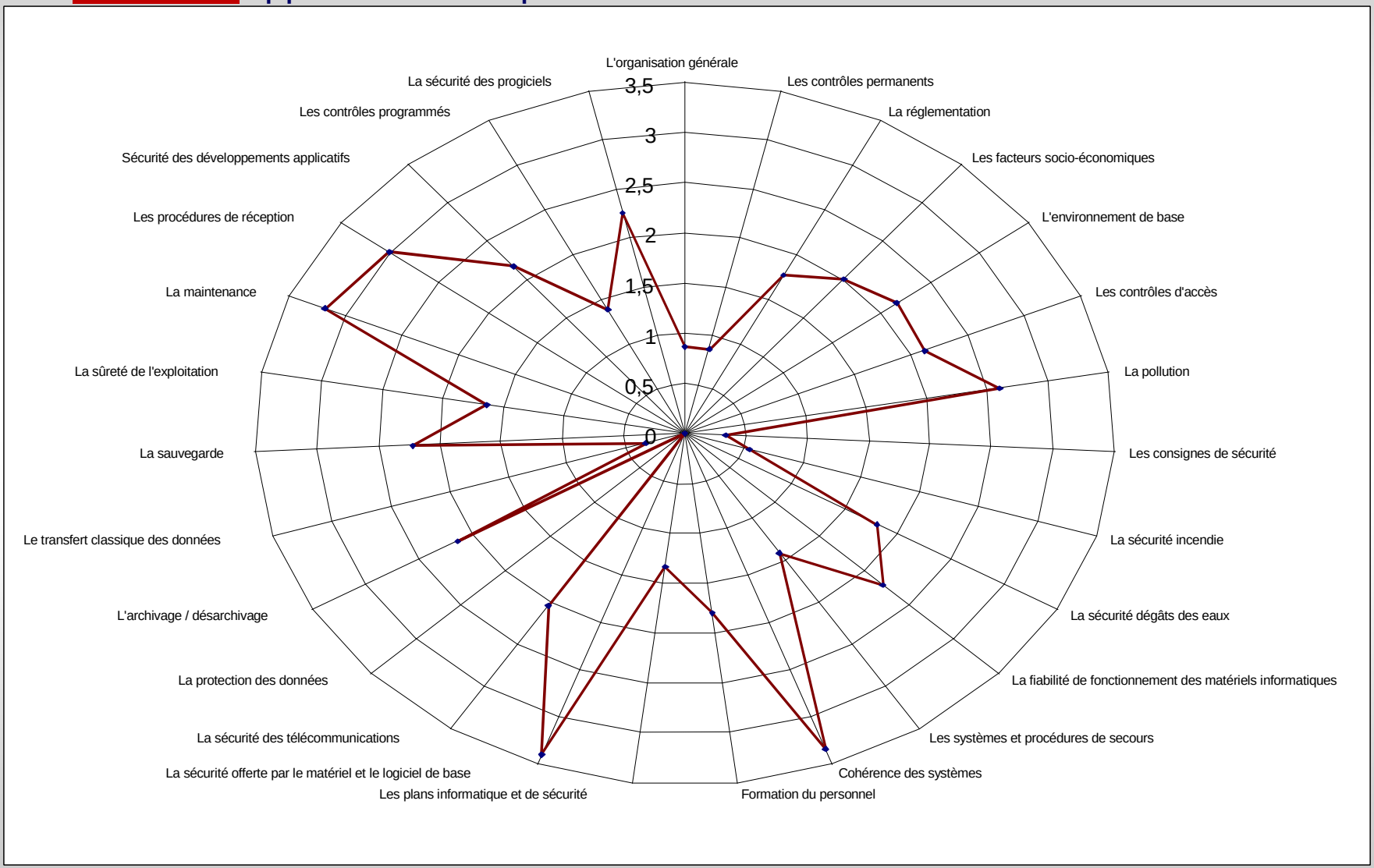
L'implémenteur est libre. Il peut choisir une note allant de 0 à 10 ou de 0 à 100 ou utiliser des couleurs (rouge, orange, vert)

Exemple:
Nous pouvons donner la formule suivante:
Risque = Max (confidentialité, intégrité, disponibilité) x Vraisemblance.
Si on évalue la vraisemblance à 1 sur une échelle de 5, ceci donne pour le fichier client de l'exemple précédent un risque égal à 3 :

Risque = Max (3,2,1) x I.

La norme ISO 27001 (Phase Plan du SMSI)

➢ Etape 2: Apprécier les risques



La norme ISO 27001 (Phase Plan du SMSI)

➢ **Etape 3:** Traiter le risque

La norme identifie quatre conformer

1. **L'acceptation** supplémentai

2. **L'évitemen** jugées inacc risque.

3. **Le transfert:** lorsque le risque ne peut pas être évité, mais que l'e (s

4. **La réduction:** mettre en place toutes les mesures techniques et organisationnelles afin de réduire le risque à un niveau jugé acceptable.

L'acceptation se justifie principalement dans le cas où les **conséquences d'une attaque sont faibles**.

L'évitement du risque est un traitement parfaitement justifié dans les cas où il y a **une exigence de risque zér**o. Au fond, cela consiste à se retirer d activité dont on veut éviter le risque ➔ l nombreuses activités. Donc, ce traiteme que dans des cas très ponctuels, dûmer

Le transfert de risque ne dispense pas l' mettre en place des mesures de sécurit Aucune société d'assurance n'accepte d'assurer un organisme n'ayant pas mis en place des mesures essentielles de protection contre l'incendie (détection de fumée, gaz FM-200 pour éteindre le feu, etc.). .

- ***Accepter***
- ***Eviter***
- ***Transférer***
- ***Réduire***

Il existe d'autres traitements du risque, en plus des 4 spécifiés dans la norme. Cependant, pour être conforme à l'ISO 27001, un SMSI doit absolument considérer ces 4 traitements du risque

La norme ISO 27001 (Phase Plan du SMSI)

- **Etape 3:** Traiter le risque et *identifier le risque résiduel.*

Dès que le traitement de risque est décidé, il reste à identifier les risques résiduels.

Le **risque résiduel** est celui qui reste une fois que l'on a mis en place les mesures de sécurité.

Il faut traiter ce genre de risque.

1. S'il est **jugé inacceptable** alors *appliquer des mesures de sécurité supplémentaires pour tendre à réduire ce risque jusqu'à ce qu'il atteigne un niveau acceptable*

2. En général, il reste toujours un risque résiduel. La **norme** oblige le management soit *de les accepter en connaissance de cause* soit *de les refuser et de prendre les actions appropriées*.

La norme ISO 27001 (Phase Plan du SMSI)

- **Etape 4:** Sélectionner les mesures de sécurité

L'objectif est d'identifier les mesures de sécurité qui permettront de réduire le risque de façon raisonnable.

La norme présente 133 mesures de sécurité, classées selon 11 catégories, qui peuvent être implémentées (Annexe A: liste de mesure sans aucune aide d'implémentation).

Une fois l'appréciation des risques effectué, de même que le traitement; la norme oblige à considérer chacun des risques à traiter, et à sélectionner dans l'annexe A la (les) mesure (s) de sécurité la (les) plus appropriée (s).

La norme ISO 27001 (Phase Plan du SMSI)

- **Etape 4:** Sélectionner les mesures de sécurité

La dernière étape dans la phase ***Plan***, consiste à dresser un tableau récapitulatif, reprenant les 133 mesures de l'annexe A, et en précisant pour chacune d'entre elle, celles qui ont été retenues pour réduire le risque et celles qui ont été écartées (tableau appelé *déclaration d'applicabilité = SoA Statement of Application)*.

Toute sélection de chaque mesure ou son abondant doit être justifié. C'est une exigence de la norme.

La norme ISO 27001

Le noyau dur de la norme (chapitre 4) est articulé autour du modèle Plan, Do, Check, Act.

Phase Do du SMSI

Une fois les objectifs du SMSI fixés (*dans la phase Plan*), il faut les mettre en œuvre. Plusieurs actions sont à entreprendre:

- ✓ **Action1:** Planifier de traitement des risques
- ✓ **Action2:** Déployer les mesures de sécurité
- ✓ **Action3:** Générer les indicateurs
- ✓ **Action4:** Former et sensibiliser le personnel
- ✓ **Action5:** Gérer le SMSI au quotidien
- ✓ **Action6:** Détection et réaction rapide aux incidents

La norme ISO 27001 (Phase Do du SMSI)

- **Action1:** Planifier le traitement des risques

Le **SoA** identifie les mesures de sécurité à déployer sans préciser comment les mettre en œuvre, ni dans quel ordre les traiter.

Plusieurs cas de figures peuvent se présenter:

1. Certaines mesures de sécurité sélectionnées dans le SoA sont déjà en place depuis longtemps.
2. Certaines autres mesures ne le sont que partiellement. (Mesures exploitées au quotidien mais dont l'application n'est pas conforme au modèle PDCA)
3. Certaines mesures doivent être intégralement déployées, mais leur mise en œuvre est assez simple.
4. D'autres mesures de sécurité nécessitent un long travail de préparation

La norme ISO 27001 (Phase Do du SMSI)

- **Action1:** Planifier le traitement des risques

Le SoA identifie les mesures de sécurité à déployer sans préciser comment les mettre en œuvre, ni dans quel ordre les traiter.

En outre, il faut:

1. Gérer les **relations temporelles** (relation de précédence) qui existent entre les différentes actions.
2. Tenir compte de certains éléments tel que
   - ✓ la liste des actions à entreprendre
   - ✓ Les moyens nécessaires
   - ✓ La définition des responsabilité et des priorités

La norme ISO 27001 (Phase Do du SMSI)

- **Action2:** Déployer les mesures de sécurité

Déployer les mesures de sécurité retenues dans le SoA, tel qu'il est précisé dans le plan de traitement des risques et sous la responsabilité du directeur du projet.

cette étape est essentiellement du ressort d'un **directeur de projet** qui prendra soin de vérifier que les actions se déroulent comme convenu, et qui saura réagir aux difficultés qui ne manqueront pas de survenir

La norme ISO 27001 (Phase Do du SMSI)

- **Action3:** Générer les in

Afin de vérifier le bo
d'indicateurs perme

L'implémenteur est

Les indicateurs en matière de SI sont un domaine de réflexion très actifs. Cependant, il existe d'indicateurs

1. **Les indicateurs de performances:** qui permettent de savoir si les mesures de sécurité sont efficaces.
2. **Les indicateurs de conformités:** qui permettent de savoir si le SMSI est conforme à ses spécifications.

Exemple: nombre d'incidents de sécurité
Le nombre mensuel d'incidents de sécurité rapportés par les utilisateurs est un ndicateur

Exemple: nombre de réunions du comité de sécurité
Si les procédures internes du SMSI spécifient que le comité de sécurité doit se réunir un certain nombre de fois dans le semestre, la fréquence de réunion de cette instance devient un indicateur de conformité,

Remarque

Il faut éviter toute inflation d'indicateurs (risque d'asphyxie du SMSI), commencer avec le moins d'indicateurs possibles, quitte à en ajouter si c'est nécessaire

La norme ISO 27001 (Phase Do du SMSI)

- **Actio**

Un SM
à la sé

Forma

Form
outil

C'est
en fonction des p par le personnel et les chefs de service.

Exemples

Les points ci-dessous sont souvent abordés lors des séances de sensibilisation du personnel de la sécurité:
- ne pas écrire son mot de passe sur un *post-it;*
- respecter des règles de base pour choisir un mot de passe;
- ne pas laisser un visiteur arpenter les locaux de l'entreprise sans être accompagné;
- éviter les codes utilisateurs et mots de passe collectifs permettant â plusieurs collaborateurs d'accéder â une application;
- signaler sans délai tout événement qui semblerait suspect.

Sensibilation:

Sensibiliser tout un chacun consiste à

- ✓ Expliquer les principes de base de la sécurité (langage simple)
- ✓ Rappeler les engagements de l'organisme en matière de sécurité

En général, une séance de sensibilisation est adressée à 10 jusqu'à 20 personnes et dure une demie journée

La norme ISO 27001 (Phase Do du SMSI)

- **Action5:** Gérer le SMSI au quotidien

Pour être conforme à l'ISO 27001, il ne suffit pas d'avancer des déclarations de bonnes intentions:

il faut en plus prouver que le SMSI fonctionne concrètement.

Il s'agit de bien gérer les ressources nécessaires (*humaines, organisationnelles, financières, matériels et logiciel*), mais aussi de produire, pour chacun des processus du système de management, les traces qui prouveront son bon fonctionnement à l'auditeur.

La norme ISO 27001 (Phase Do du SMSI)

- **Action6:** Détection et réaction rapide aux incidents.

Un SMSI opérationnel se doit de **détecter rapidement tout incident**, qu'il soit **d'origine malveillante** ou **accidentelle,** risquant d'altérer la **disponibilité**, la **confidentialité** ou **l'intégrité** de l'information.

Le principe de la sécurité axée sur le temps est de mise

Idées de départ:

- ✓ Toute attaque prend un certain temps à l'agresseur avant de réussir
- ✓ Toute attaque prend un certain temps à être détectée par le défenseur
- ✓ Les actions entreprises par le défenseur pour contrecarrer l'attaque prennent un certain temps

Il faut assurer que:

Le temps de détection + temps de réaction

<

temps nécessaire à l'agresseur pour réussir sont attaque

La norme ISO 27001 (Phase Check du SMSI)

Le noyau dur de la norme (chapitre 4) est articulé autour du modèle Plan, Do, Check, Act.

Phase Check du SMSI

La norme impose la **mise en place de moyen** de **contrôle** est de **surveiller** en **permanence :**

1. L'efficacité du SMSI
2. Sa conformité par rapport aux spécifications

Trois familles d'outils permettent à l'implémenteur de répondre à cette exigence:

- ✓ **Les audits internes**
- ✓ **Le contrôle interne**
- ✓ **Les revues (ou encore réexamen)**

La norme ISO 27001 (Phase Check du SMSI)

Les audits internes;

Le **but** de l'**audit** consiste à vérifier la conformité et l'efficacité du système de management.

Les audits **internes sont planifiés** à l'avance et toutes **les personnes en sont informées**.

L'auditeur doit

- ✓ **Étudier les documents pertinents (**politiques, procédures, enregistrements**)**
- ✓ **Observer les activités des employés**
- ✓ **Rencontrer les responsables ainsi que les opérateurs**

➔ **Recouper toutes les informations qu'il a obtenues pour constater soit l'écart, soit la conformité du SMSI par rapport aux points audités**

La norme ISO 27001 (Phase Check du SMSI)

Les audits internes;

Conseils:

- ✓ **L'audit ne doit pas être effectué** par les personnes ayant été impliquées dans la mise en œuvre ou l'exploitation du processus audité (Impartialité des constats)
- ✓ Il est souhaitable que les auditeurs n'aient **aucun lien hiérarchique avec les personnes qu'ils rencontrent** (objectivité des constats).
- ✓ **Les rapports doivent être consignés**, car ils constituent l'enregistrement prouvant que les audits se déroulent comme prévu.
- ✓ **Le périmètre de l'audit doit être bien défini**.
  - Il peut couvrir l'ensemble du SMSI (l'application de toutes les clauses (4 à 8) de l'ISO 27001, ainsi que toutes les mesures de sécurité sélectionnées dans le SoA (« audit à blanc » juste avant de lancer l'audit de certification).
  - Il peut être limité soit à quelques clauses de l'ISO 27001, soit à quelques mesures de sécurité sur quelques processus du SMSI.

La norme ISO 27001 (Phase Check du SMSI)

- **Le contrôle interne;**

Le **contrôle interne** consiste à vérifier en permanence que le processus fonctionne comme prévu.

Les contrôle doivent être **inopinés** sur certains points bien ciblés.

L'objectif est de vérifier que les employés appliquent les procédures correctement au quotidien-hors des périodes d'audit.

L'effet de surprise est pour des raisons d'efficacité. Il ne s'agit pas de piéger les employés.

Pour des raisons de viabilité, un SMSI doit obtenir l'adhésion du personnel

La norme ISO 27001 (Phase Check du SMSI)

- **Les revues;**

La **mission de la revue** est de **garantir l'adéquation du SMSI par rapport à son environnement.**

La revue de direction

Réunions (annuelles) au cours de lesquelles les managers jettent un coup d'œil rétrospective sur le SMSI.

Ce qui permet

- ✓ **d'avoir une vision globale de l'évolution du SMSI ainsi que de son contexte.**
- ✓ **de tenir compte des changements survenus dans l'entreprise pour que le SMSI reste conforme aux exigences de l'ISO 27001**

La norme ISO 27001 (Phase Check du SMSI)

- **Les revues;**

La mission de la revue est de garantir l'adéquation du SMSI par rapport à son environnement.

La revue de direction

Les **points** les **plus importants** discutés généralement:

- ✓ Résultats des audits internes de l'année:
- ✓ Retours des parties prenantes
- ✓ Etat des lieux sur les actions en cours (préventives et correctives)
- ✓ Menaces mal appréhendées lors de l'application des risques
- ✓ Interprétation des risques
- ✓ Nouvelles priorités
- ✓ Changements survenus dans l'entreprise (réorganisation, fusion, acquisition)

Les managers vont fixer de nouvelles priorités et décider des moyens nécessaires pour les mener à bien.

La norme ISO 27001 (Phase Check du SMSI)

- **Les revues;**

La mission de la revue est de garantir l'adéquation du SMSI par rapport à son environnement.

Les revues ponctuelles

La [illegible] annuelle du SMSI doit être tenue dans tous les cas.

Cepe[illegible]tains **changement** significatifs dans la vie de l'entreprise peuvent **justifi[illegible] ponctuelle et sans délai du SMSI**.

Exemple: **fusion de deux entreprises**

La fusion d'une entreprise déjà certifiée ISO 27001 avec une autre justifie de réviser sans tarder:

- le périmètre du SMSI, puisqu'il doit couvrir maintenant les activités des deux sociétés;
- la politique du SMSI, car les priorités de l'entreprise issue de la fusion ne sont peut-être plus les mêmes qu'auparavant;
- l'appréciation des risques, puisque l'élargissement du périmètre nécessite de faire un nouvel inventaire des actifs, une nouvelle liste de vulnérabilités, etc.

La norme ISO 27001 (Phase Act du SMSI)

Le noyau dur de la norme (chapitre 4) est articulé autour du modèle Plan, Do, Check, Act.

Phase Act du SMSI

Toutes les activités de contrôle réalisées lors de la phase « **Check** » sont susceptible de mettre en lumière un certain nombre de dysfonctionnement

Les constats peuvent être de plusieurs ordres

- ✓ Ecarts entre le SMSI et les exigences de la norme
- ✓ Ecarts entre les spécifications du SMSI et la pratique constatée.
- ✓ Mesures de sécurité inefficaces ou insuffisamment performantes
- ✓ Risques oubliés lors de l'appréciation des risques
- ✓ Changements de contexte entraînant de nouveaux risques
- ✓ Problèmes récurrents

La norme ISO 27001 (Phase Act du SMSI)

- Phase Act du SMSI : **Les actions;**

La norme impose d'identifier systématiquement des actions correctives, préventives ou d'amélioration pour chacun de ces constats.

Actions correctives

Elles sont entreprises lorsqu'un incident ou un écart a été constaté. Le **but** est **d'agir d'abord sur les effets** pour **corriger l'écart**, puis **sur les causes** pour **éviter que l'écart ne se reproduise à nouveau**.

Actions préventives

Elles sont lancer lorsqu'on détecte une **situation qui risque d'entraîner un écart ou un incident si rien n'est fait**. Les actions préventives consistent à agir sur les causes avant que l'écart ne se produise.

Actions amélioration

Leur **but** n'est pas de corriger ni d'éviter un écart, mais **d'améliorer la performance d'un processus du SMSI**

La norme ISO 27001 (Phase Act du SMSI)

- **Les actions;**

- ✓ L'implémenteur doit vérifier que les actions correctives, préventives ou d'amélioration une fois appliquées ont bien permis d'atteindre des objectifs fixés.
- ✓ Il informera ensuite toutes les partie du résultat obtenu.
- ✓ Ces actions contribuent à rendre le SMSI plus fiable et plus efficace dans la durée.
- ✓ Ce qui renforce indirectement la sécurité du système d'information et, par transitivité, la confiance des parties prenantes.

La norme ISO 27002

La norme ISO 27002

L'ISO 27001 décrit les mesures nécessaires à la mise en place d'un SMSI

Fixe l'objectif à atteindre, mais ne précise pas comment

L'ISO 27002 présente un guide de bonnes pratiques pour les différentes actions que l'implémenteur va entreprendre (abordant les aspects **techniques** et **organisationnels**)

- **Deux approches de la sécurité**
  - ***Les formalisateurs*: proposent une approche fondée sur la réflexion au sujet de questions stratégiques
  - ***Les techniciens*: cherchent plutôt des solutions concrètes

La norme ISO 27002

- **Les formalisateurs;**

  Les questions probables avant d'agir:

  - ✓ Quel est l'objectif de l'entreprise
  - ✓ Quel est le cadre au sein duquel on peut agir
  - ✓ Qui est responsable de quoi
  - ✓ Qui va faire quoi

- Ils modélisent les relations d'ordre ainsi que les dépendances entre les différents processus.
- Ils posent par écrit tout ce qu'il faut faire en formalisant les procédures
- Ils prennent en charge tout ce qui est communication, sensibilisation.
- Ils sont prompts à formaliser les procédures, mais réticents à se plonger dans la technique

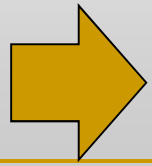
La norme ISO 27002

- **Les techniciens;**

  Les questions principales:

  - ✓ Les applications gèrent-elles bien les sessions?
  - ✓ Les champs de saisie résistent –ils aux attaques d'injection SQL?
  - ✓ Les services qui tournent sur les machines sont-ils à jours?
  - ✓ Les droits sur les fichiers sont-ils les bons?
  - ✓ Les règles des pare-feux sont-elles bien configurées?

- Ils n'hésitent pas à plonger dans les problèmes techniques pour enquêter et trouver des solutions concrètes
- Ils garantissent la sécurité techniques des infrastructures.



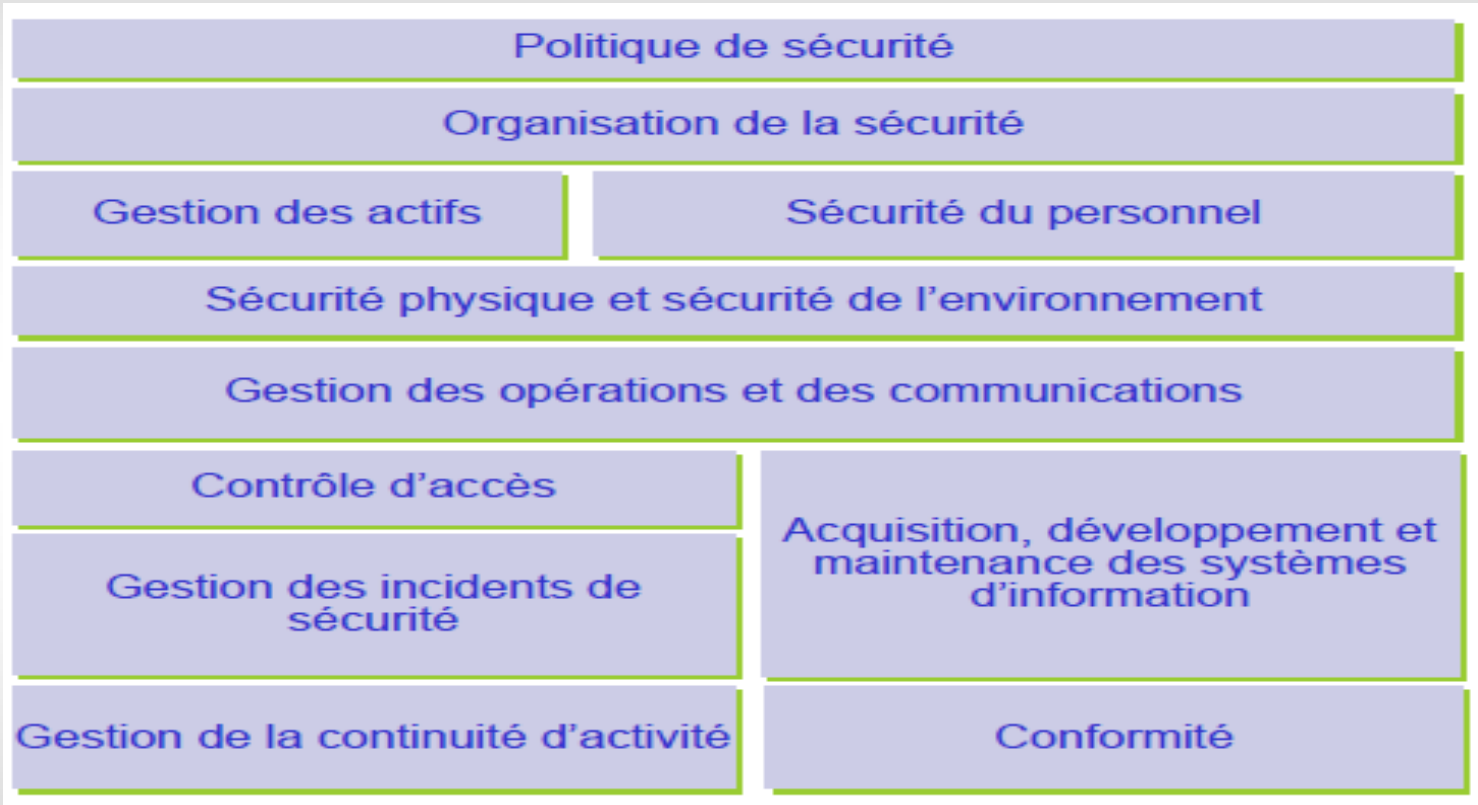
Présentation de la norme;

Structurée sur trois niveaux:

- ✓ Les chapitres (*niveau 1*)
- ✓ Les objectifs de sécurités (*niveau 2*)
- ✓ Les mesures de sécurité *(niveau 3)*

La norme ISO 27002 (Présentation de la norme1)

Structure générale:



Les 11 chapitres de la norme ISO 27002

La norme ISO 27002 (Présentation de la norme1)

Structure générale:

La norme peut être vue comme un dictionnaire à 133 entrées (***mesures de sécurité***).

Chaque mesure de sécurité est décrite en 4 parties

- **Numéro de référence et intitulé de la mesure:** *permet de référencer la mesure sans ambiguïté*
- **Mesure:** *brève description de la mesure permettant de dire clairement de quoi il s'agit*
- **Préconisation de mise en œuvre:** *les préconisations sont développées et éventuellement accompagnées d'exemples pour les illustrer (être aussi concret que possible)*
- **Informations supplémentaires:** *informations jugées utiles, mains non abordées dans les préconisations*

La norme ISO 27002 (Présentation de la norme)

➢ **Structure générale:**

✓ Pour une meilleure lisibilité, ***les 133 mesures de sécurité sont classées en 11 grands chapitres***. Chacun des 11 chapitres est subdivisé en sous- chapitres (niveau 2 où *sont définis les objectifs de sécurités*)[2]

✓ Chaque sous-chapitre est précédé de la rubrique « ***Objectif*** » qui décrit l'objectif général des mesures de sécurité regroupées dans ce sous-chapitre et qui constitue le but final à atteindre (où *sont définies les mesures de sécurité*).[3]

➢ **Chapitres de l'ISO 27002**

L'ISO 27002 est constituée de 11 chapitres important (du 5 au 15) couvrant l'essentiel des données relatives à la sécurité de l'information.

Chapitre 5: Politique de sécurité

Regroupe toutes les questions concernant la rédaction de la politique de sécurité.

Ne comporte que 2 mesures:

- **5.1.1** *indique les différents points susceptibles d'être abordés dans une politique*.
- **5.1.2** *précise que la politique doit être revue régulièrement*

➢ Chapitre 5: Politique de sécurité

L'objectif est, pour la Direction, de:

- ✓ Exprimer formellement la stratégie de sécurité de la société
- ✓ Communiquer clairement son appui à sa mise en œuvre.

Un **document** exposant la politique de sécurité doit être approuvé

Il doit être ***révisé et adapté périodiquement*** en prenant en compte ***l'efficacité*** de ses mesures, le ***coût*** et ***l'impact*** des contrôles sur l'activité, les ***effets des évolutions*** technologiques.

La sécurité est une **responsabilité partagée** par tous les membres de l'équipe de direction.

Un *comité de direction multifonction* doit être formé pour assurer un pilotage clair et une visibilité élevée de l'engagement de la direction.

Il définit les rôles et responsabilités, les méthodes et procédures, approuve et supporte les initiatives de communication internes.

Chapitre 5: Politique de sécurité

Politique de sécurité de l'information

Objectif : Apporter à la sécurité de l'information une orientation et un soutien de la part de la direction, conformément aux exigences métier et aux lois et règlements en vigueur.

Document de politique de sécurité de l'information

Mesure: Un document de politique de sécurité de l'information doit être approuvé par la direction, puis publié et diffusé auprès de l'ensemble des salariés et des tiers concernés.

Réexamen de la politique de sécurité de l'information

Mesure: Pour garantir la pertinence, l'adéquation et l'efficacité de la politique de sécurité de l'information, la politique doit être réexaminée à intervalles fixés préalablement ou en cas de changements majeurs

Chapitre 6: Organisation de la sécurité de l'information

Ce chapitre est divisé en 2 objectifs:

- **Organisation interne:** les mesures de **6.1** abordent *la gouvernance de la sécurité, les relations avec les autorités ainsi que la participation aux groupes spécialisés*
- **Relations avec les tiers:** traiter avec les tiers expose l'organisme à un certain nombre de risques que l'entreprise doit identifier et contre lesquels elle doit se protéger. Les mesures de **6.2** mettent *l'accents sur les accords passés avec les tiers et des exigences de sécurité qui doivent être tenues en compte.*

Chapitre 6: Organisation de la sécurité de l'information

Organisation interne
Objectif : Gérer la sécurité de l'information au sein de l'organisme.

Implication de la direction vis-à-vis de la sécurité de l'information
Mesure: La direction doit soutenir activement la politique de sécurité au sein de l'organisme au moyen de directives claires, d'un engagement démontré, d'attribution de fonctions explicites et d'une reconnaissance des responsabilités liées à la sécurité de l'information.

Coordination de la sécurité de l'information
Mesure: Les activités relatives à la sécurité de l'information doivent être coordonnées par des intervenants ayant des fonctions et des rôles appropriés représentatifs des différentes parties de l'organisme

Chapitre 6: Organisation de la sécurité de l'information

Attribution des responsabilités en matière de sécurité de l'information
Mesure: Toutes les responsabilités en matière de sécurité de l'information doivent être définies clairement.

Système d'autorisation concernant les moyens de traitement de l'information
Mesure: Un système de gestion des autorisations doit être défini et mis en œuvre pour chaque nouveau moyen de traitement de l'information.

Engagements de confidentialité
Mesure: Les exigences en matière d'engagements de confidentialité ou de non-divulgation, conformément aux besoins de l'organisme, doivent être identifiées et réexaminées régulièrement.

Chapitre 6: Organisation de la sécurité de l'information

Relations avec les autorités

Mesure: Des relations appropriées doivent être mises en place avec les autorités compétentes.

Relations avec des groupes de spécialistes

Mesure: Des contacts appropriés doivent être entretenus avec des groupes de spécialistes, des forums spécialisés dans la sécurité et des associations professionnelles.

Réexamen indépendant de la sécurité de l'information

Mesure: Des réexamens réguliers et indépendants de l'approche retenue par l'organisme pour gérer et mettre en œuvre sa sécurité (c'est-à-dire le suivi des objectifs de sécurité, les politiques, les procédures et les processus relatifs à la sécurité de l'information) doivent être effectués ; de tels réexamens sont également nécessaires lorsque des changements importants sont intervenus dans la mise en œuvre de la sécurité

.

Chapitre 6: Organisation de la sécurité de l'information

Tiers

Objectif : *Assurer la sécurité de l'information et des moyens de traitement de l'information appartenant à* l'organisme et consultés, traités, communiqués ou gérés par des tiers.

Identification des risques provenant des tiers

Mesure: Les risques pesant sur l'information et les moyens de traitement de l'organisme qui découlent d'activités impliquant des tiers doivent être identifiés, et des mesures appropriées doivent être mises en œuvre avant d'accorder des accès

Chapitre 6: Organisation de la sécurité de l'information

Tiers

La sécurité et les clients

Mesure: Tous les besoins de sécurité doivent être traités avant d'accorder aux clients l'accès à l'information ou aux actifs de l'organisme.

La sécurité dans les accords conclus avec des tiers

Mesure : Les accords conclus avec des tiers qui portent sur l'accès, le traitement, la communication ou la gestion de l'information, ou des moyens de traitement de l'information de l'organisme, ou qui portent sur l'ajout de produits ou de services aux moyens de traitement de l'information, doivent couvrir l'ensemble des exigences applicables en matière de sécurité.

.

Chapitre 7: Gestion des biens

Les mesures de sécurité de ce chapitre sont indispensables à l'application de la clause 4.2.1.d.1 de l'ISO 27001. Il faut donc *procéder à un inventaire des actifs et désigner, pour chacun d'eux, un responsable*:

- **Responsabilité relative aux biens: 7.1** *couvre l'inventaire, la propriété et la définition de l'utilisation correcte des biens.*
- **Classification des informations:** les mesures de **7.2** concernent *la classification des actifs* (opération très utile lors de l'appréciation des risques)

Chapitre 7: Gestion des biens

L'***objectif*** est de maintenir le niveau de protection adapté à chaque actif d'information en accord avec la politique de sécurité.

- ✓ Tout élément d'actif important doit être répertorié et alloué à un responsable nominatif.
- ✓ L'information doit être classifiée en fonction du besoin, de la priorité et du degré de sa sécurité.

Les ***procédures de classification*** des informations doivent être définies et couvrir la manipulation des informations sous forme physique aussi bien que électronique, et pour les différentes activités de copie, stockage, transmission et destruction.

Chapitre 7: Gestion des biens

Responsabilités relatives aux actifs

Objectif *:* Mettre en place et maintenir une protection appropriée des actifs de l'organisme.

Inventaire des actifs

Mesure*:* Tous les actifs doivent être clairement identifiés et un inventaire de tous les actifs importants doit être réalisé et géré.

Propriété des actifs

Utilisation correcte des actifs

Chapitre 7: Gestion des biens

Responsabilités relatives aux actifs

Inventaire des actifs

Propriété des actifs

Mesure*:* La propriété de chaque information et des moyens de traitement de l'information doit être 'attribuée' à une partie définie de l'organisme.

Utilisation correcte des actifs

Mesure*:* Des règles permettant l'utilisation correcte de l'information et des actifs associés aux moyens de traitement de l'information doivent être identifiées, documentées et mises en œuvre.

Chapitre 7: Gestion des biens

Classification des informations

Objectif *: Garantir un niveau de protection approprié aux informations.*

Lignes directrices pour la classification *Mesure*

Mesure: Les informations doivent être classées en termes de valeur, d'exigences légales, de sensibilité et de criticité.

Marquage et manipulation de l'information

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

Cas pratique

Chapitre 8: Sécurité liée aux ressources humaines

Ce chapitre aborde toutes les questions relatives au personnel. Il est composé de 3 objectifs à mettre en place chronologiquement

- **Avant l'embauche: 8.1** tout est mis en ouvre pour *la définition préalable des rôles et responsabilités de chacun en matière de sécurité .*
- **Pendant la durée du contrat:** les mesures de **8.2** visent à *informer le personnel sur ses responsabilités en matière de sécurité* (même les sanctions disciplinaires).
- **Au départ de l'employé: 8.3** concerne *le retrait des droits d'accès pour le personnel quittant l'entreprise de même que la restitution par ce dernier de tous les biens qu'il a reçus pour travailler*.

➢ Chapitre 8: Sécurité liée aux ressources humaines

Plus de 60% des incidents proviennent de l'intérieur de l'entreprise !.

L'objectif est de:

- ✓ Réduire le risque d'erreur, de vol, de fraude ou de mauvais usage des moyens de traitement.
- ✓ Assurer que les utilisateurs sont informés des risques et menaces concernant les informations.
- ✓ Assurer que les utilisateurs sont formés et sont équipés pour appliquer la politique de sûreté lors de leurs activités normales.
- ✓ Minimiser les dommages en cas d'incident.
- ✓ Apprendre de ces incidents.

Chapitre 8: Sécurité liée aux ressources humaines

Avant le recrutement (ou changement de domaine d'activité)

Objectif *: Garantir que les salariés, contractants et utilisateurs tiers connaissent leurs responsabilités et qu'ils* conviennent pour les fonctions qui leur sont attribuées et réduire le risque de vol, de fraude ou de mauvais usage des équipements.

Rôles et responsabilités

Mesure*:* Les rôles et responsabilités en matière de sécurité des salariés, contractants et utilisateurs tiers doivent être définis et documentés conformément à la politique de sécurité de l'information de l'organisme.

Sélection

Chapitre 8: Sécurité liée aux ressources humaines

Avant le recrutement (ou changement de domaine d'activité)

Rôles et responsabilités

Sélection

Mesure*:* Qu'il s'agisse de postulants, de contractants ou d'utilisateurs tiers, les vérifications des informations concernant tous les candidats doivent être réalisées conformément aux lois, aux règlements et à l'étique et doivent être proportionnelles aux exigences métier, à la classification des informations accessibles et aux risques identifiés.

➢ Chapitre 8: Sécurité liée aux ressources humaines

Conditions d'embauche

Mesure*:* Dans le cadre de leurs obligations contractuelles, les salariés, contractants et utilisateurs tiers doivent se mettre d'accord sur les modalités du contrat d'embauche les liant et le signer. Ce contrat doit définir leurs responsabilités et celles de l'organisme quant à la sécurité de l'information.

Pendant la durée du contrat

Objectif *: Veiller à ce que tous les salariés, contractants et utilisateurs tiers soient conscients des menaces pesant* sur la sécurité de l'information, de leurs responsabilités financières ou autres, et disposent des éléments requis pour prendre en charge la politique de sécurité de l'organisme dans le cadre de leur activité normale et réduire le risque d'erreur humaine.

Responsabilités de la direction

Mesure: La direction doit demander aux salariés, contractants et utilisateurs tiers d'appliquer les règles de sécurité conformément aux politiques et procédures établies de l'organisme.

➢ Chapitre 8: Sécurité liée aux ressources humaines

Conditions d'embauche.

Pendant la durée du contrat

Responsabilités de la direction

Mesure*:* La direction doit demander aux salariés, contractants et utilisateurs tiers d'appliquer les règles de sécurité conformément aux politiques et procédures établies de l'organisme.

➢ Chapitre 8: Sécurité liée aux ressources humaines

Sensibilisation, qualification et formations en matière de sécurité de l'information

Mesure*:* L'ensemble des salariés d'un organisme et, le cas échant, les contractants et utilisateurs tiers doivent suivre une formation adaptée sur la sensibilisation et doivent recevoir régulièrement les mises à jour des politiques et procédures de l'organisme, pertinentes pour leurs fonctions.

Processus disciplinaire

Mesure*:* Un processus disciplinaire formel doit être élaboré pour les salariés ayant enfreint les règles de sécurité.

Fin ou modification du contrat

Objectif *:* Veiller à ce que les salariés, contractants et utilisateurs tiers quittent un organisme ou changent de poste selon une procédure définie.

➢ Chapitre 8: Sécurité liée aux ressources humaines

Responsabilités en fin de contrat

Mesure: Les responsabilités relatives aux fins ou aux modifications de contrats doivent être clairement définies et attribuées.

Restitution des actifs

Mesure: Tous les salariés, contractants et utilisateurs tiers doivent restituer la totalité des actifs de l'organisme qu'ils ont en leur possession à la fin de leur période d'emploi, contrat ou accord.

Retrait des droits d'accès

Mesure: Les droits d'accès de l'ensemble des salariés, contractants et utilisateurs tiers à l'information et aux moyens de traitement de l'information doivent être supprimés à la fin de leur période d'emploi, ou modifiés en cas de modification du contrat ou de l'accord.

Chapitre 9: Sécurité physique et environnementale

La sécurité physique s'applique aux locaux et aux équipements qui s'y trouvent

- **Sécurité des locaux: 9.1** *traite de questions très variées*; définition des différentes zones de sécurité dans l'entreprise, des contrôles d'accès physique aux locaux, de la protection contre les menaces extérieures, la sécurité des zones de livraison.
- **Sécurité du matériel:** le but des mesures de **9.2** est de *protéger le matériel en le plaçant dans des lieux appropriés* (avec air conditionné, alimentation électrique, câblage normalisé). Les questions relatives à la maintenance sont abordées.

Chapitre 9: Sécurité physique et environnementale

L'objectif est de:

- ✓ Prévenir les accès non autorisés, les dommages et les interférences sur les informations, les activités et les locaux de l'organisation.
- ✓ Prévenir la compromission ou le vol d'information ou de moyens de traitement.

➢ Chapitre 9: Sécurité physique et environnementale

Zones sécurisées

Objectif *: Empêcher tout accès physique non autorisé, tout dommage ou intrusion dans les locaux ou portant sur* les informations de l'organisme.

Périmètre de sécurité physique

Mesure*:* Les zones contenant des informations et des moyens de traitement de l'information doivent être protégées par des périmètres de sécurité (obstacles tels que des murs, des portes avec un contrôle d'accès par cartes, ou des bureaux de réception avec personnel d'accueil).

Contrôles physiques des accès

Sécurisation des bureaux, des salles et des équipements

Chapitre 9: Sécurité physique et environnementale

Zones sécurisées

Périmètre de sécurité physique

Contrôles physiques des accès

Mesure*:* Les zones sécurisées doivent être protégées par des contrôles à l'entrée adéquats pour s'assurer que seul le personnel habilité est admis.

Sécurisation des bureaux, des salles et des équipements

Mesure*:* Des mesures de sécurité physique doivent être conçues et appliquées pour les bureaux, les salles et les équipements.

➢ Chapitre 9: Sécurité physique et environnementale

Protection contre les menaces extérieures et environnementales

Mesure*:* Des mesures de protection physique contre les dommages causés par les incendies, les inondations, les tremblements de terre, les explosions, les troubles civils et autres formes de catastrophes naturelles ou de sinistres provoqués par l'homme, doivent être conçues et appliquées.

Travail dans les zones sécurisées

Mesure*:* Des mesures de protection physique et des directives pour le travail en zone sécurisée doivent être conçues et appliquées.

Zones d'accès public, de livraison et de chargement

Chapitre 9: Sécurité physique et environnementale

Protection contre les menaces extérieures et environnementales

Travail dans les zones sécurisées

Zones d'accès public, de livraison et de chargement

Mesure: Les points d'accès tels que les zones de livraison/chargement et les autres points par lesquels des personnes non habilitées peuvent pénétrer dans les locaux doivent être contrôlés. Les points d'accès doivent également, si possible, être isolés des moyens de traitement de l'information, de façon à éviter les accès non autorisés.

➢ Chapitre 9: Sécurité physique et environnementale

A.9.2 Sécurité du matériel

Objectif *: Empêcher la perte, l'endommagement, le vol ou la compromission des actifs et l'interruption des activités* de l'organisme.

Choix de l'emplacement et protection du matériel

Mesure*:* Le matériel doit être situé et protégé de manière à réduire les risques de menaces et de dangers environnementaux et les possibilités d'accès non autorisé.

Services généraux

Mesure *:* Le matériel doit être protégé des coupures de courant et autres perturbations dues à une défaillance des services généraux.

Sécurité du câblage

Maintenance du matériel

Chapitre 9: Sécurité physique et environnementale

A.9.2 Sécurité du matériel

Objectif *: Empêcher la perte, l'endommagement, le vol ou la compromission des actifs et l'interruption des activités* de l'organisme.

Choix de l'emplacement et protection du matériel

Services généraux

Sécurité du câblage

Mesure*:* Les câbles électriques ou de télécommunications transportant des données doivent être protégés contre toute interception d'information ou dommage.

Maintenance du matériel

Mesure*:* Le matériel doit être entretenu correctement pour garantir sa disponibilité permanente et son intégrité.

Chapitre 9: Sécurité physique et environnementale

Sécurité du matériel hors des locaux

Mesure*:* La sécurité doit être appliquée au matériel utilisé hors des locaux de l'organisme en tenant compte des différents risques associés au travail hors site.

Mise au rebut ou recyclage sécurisé(e) du matériel

Mesure*:* Tout le matériel contenant des supports de stockage doit être vérifié pour s'assurer que toute donnée sensible a bien été supprimée et que tout logiciel sous licence a bien été désinstallé ou écrasé de façon sécurisée, avant sa mise au rebut.

Sortie d'un actif

Mesure*:* Un matériel, des informations ou des logiciels ne doivent pas être sortis des locaux de l'organisme sans autorisation préalable.

.

Chapitre 10: Gestion de l'exploitation et des télécommunications

Il comporte de très nombreuses mesures de sécurité, à la fois techniques et organisationnelles, et couvrant tous les aspects de l'exploitation du systèmes d'information.

- **Procédures d'exploitation et responsabilités: 10.1** aborde la *formalisation des procédures d'exploitation* (points essentiels dans la mise en place d'un SMSI) de même que *la gestion des droits afin d'éviter le phénomène de collusion*, ainsi que *la séparation des environnements de développement, de test et de production*.

La norme ISO 27002 (Gestion de l'exploitation et des télécom)

Il comporte de très nombreuses mesures de sécurité, à la fois techniques et organisationnelles, et couvrant tous les aspects de l'exploitation du systèmes d'information.

- **Prestation de service par un tiers:** les3 mesures de 10.2 concernent les relations avec les tiers. 3 questions y sont posées

  1. Qui est le responsable de quoi?
  2. Quelles dispositions prend le client pour contrôler le travail du prestataire?
  3. Comment les changements chez le prestataire sont-ils approuvés par le client?
  4. Etc

La norme ISO 27002 (Gestion de l'exploitation et des télécom)

Il comporte de très nombreuses mesures de sécurité, à la fois techniques et organisationnelles, et couvrant tous les aspects de l'exploitation du systèmes d'information.

- **Planification et acceptation du système: l**es 2 mesures de **10.3** abordent *la gestion de la capacité des systèmes et les critères de recettes des environnements*.
- **Protection contre le code malveillant:** *la protection contre le code mobile et les codes malveillant* font l'objet de **10.4**.
- **Sauvegarde:** l'unique partie de cette partie **10.5.1** aborde la *question des sauvegardes*
- **Gestion de la sécurité des réseaux:** Cette partie **10.6** comporte *2 mesures relatives à la sécurité du réseau*.

La norme ISO 27002 (Gestion de l'exploitation et des télécom)

- **Manipulation des supports:** *Tout ce qui a trait à la manipulation des support* **10.7** ((stockage des supports, sécurité de la documentation système et la sécurisation des supports lors de leur mise en rebut).
- **Echange des informations:** Toute information appelée à être échangée avec l'extérieur peut faire l'objet de mesures de sécurité 10.8 (qu'il s'agisse d'accords formels ou de mesures de protection purement techniques.
- **Commerce électronique:** Les mesures décrites dans 10.9 ne concernent pas uniquement le commerce électronique. Dès qu'une information est rendue publiquement accessible par un organisme, des mesures de protection sont nécessaires.
- **Surveillance:** La partie 10.10 met l'accent sur la traçabilité des actions des utilisateurs et des administrateurs. Elle insiste sur le fait que les journaux doivent être protégés contre les accès illicites.

Chapitre 10: Gestion de l'exploitation et des télécommunications

Exploitation et Réseaux

L'objectif est de:

- ✓ Assurer une exploitation correcte et sûre des moyens de traitement.
- ✓ Minimiser les risques de pannes et leur impact.
- ✓ Assurer l'intégrité et la disponibilités des informations, des traitements et des communications.
- ✓ Prévenir les dommages aux actifs et les interruptions de service.
- ✓ Prévenir les pertes, les modifications et les mauvaises utilisations d'informations échangées entre organisations.

Chapitre 10: Gestion de l'exploitation et des télécommunications

Procédures et responsabilités liées à l'exploitation

Objectif *: Assurer l'exploitation correcte et sécurisée des moyens de traitement de l'information.*

Procédures d'exploitation documentées

Mesure*:* Les procédures d'exploitation doivent être documentées, tenues à jour et disponibles pour tous les utilisateurs concernés.

Management des modifications

Mesure: Les changements apportés aux systèmes et moyens de traitement de l'information doivent être contrôlés.

Séparation des tâches

Mesure*:* Les tâches et les domaines de responsabilité doivent être séparés pour réduire les occasions de modification ou de mauvais usage non autorisé(e) ou involontaire des actifs de l'organisme.

Séparation des équipements de développement, d'essai et d'exploitation

Mesure: Les équipements de développement, d'essai et d'exploitation doivent être séparés pour réduire les risques d'accès ou de changements non autorisés au système d'information en exploitation

Chapitre 10: Gestion de l'exploitation et des télécommunications

Procédures et responsabilités liées à l'exploitation

Procédures d'exploitation documentées

Séparation des tâches

Mesure*:* Les tâches et les domaines de responsabilité doivent être séparés pour réduire les occasions de modification ou de mauvais usage non autorisé(e) ou involontaire des actifs de l'organisme.

Séparation des équipements de développement, d'essai et d'exploitation

Mesure*:* Les équipements de développement, d'essai et d'exploitation doivent être séparés pour réduire les risques d'accès ou de changements non autorisés da ns le système d'information en exploitation

Chapitre 10: Gestion de l'exploitation et des télécommunications

Gestion de la prestation de service conclus avec un tiers

Objectif *: Mettre en œuvre et maintenir un niveau de sécurité de l'information et de service adéquat et conforme* aux accords de prestation de service conclus avec un tiers.

Prestation de service

Mesure*:* Il doit être assuré que les mesures de sécurité, les définitions du service et les niveaux de prestation prévus dans l'accord de prestation de service tiers sont mis en œuvre, appliqués et tenus à jour par le tiers.

Surveillance et examen des services tiers

Gestion des modifications dans les services tiers

Chapitre 10: Gestion de l'exploitation et des télécommunications

Gestion de la prestation de service conclus avec un tiers

Prestation de service

Surveillance et examen des services tiers

Mesure*:* Les services, rapports et enregistrements fournis par les tiers doivent être régulièrement contrôlés et réexaminés, et des audits doivent être régulièrement réalisés.

Gestion des modifications dans les services tiers

Mesure*:* Les changements effectués dans la prestation de service, comprenant le maintien et l'amélioration des politiques, procédures et mesures existant en matière de sécurité de l'information, doivent être gérés en tenant compte de la criticité des systèmes et processus de gestion concernés et de la réévaluation du risque.

Chapitre 10: Gestion de l'exploitation et des télécommunications

Planification et acceptation du système

Objectif *: Réduire le plus possible le risque de pannes du système.*

Dimensionnement

Mesure*:* L'utilisation des ressources doit être surveillée et ajustée au plus près, et des projections doivent être faites sur les dimensionnements futurs pour assurer les performances requises par le système.

Acceptation du système

Mesure*:* Les critères d'acceptation doivent être fixés pour les nouveaux systèmes d'information, les nouvelles versions et les mises à niveau, et les tests adaptés du (des) système(s) doivent être réalisés au moment du développement et préalablement à leur acceptation

Chapitre 10: Gestion de l'exploitation et des télécommunications

Protection contre les codes malveillant et mobile

Objectif *: Protéger l'intégrité des logiciels et de l'information.*

Mesures contre les codes malveillants

Mesure*:* Des mesures de détection, de prévention et de recouvrement pour se protéger des codes malveillants ainsi que des procédures appropriées de sensibilisation des utilisateurs doivent être mises en œuvre.

Mesures contre le code mobile

Sauvegarde

Sauvegarde des informations

Chapitre 10: Gestion de l'exploitation et des télécommunications

Protection contre les codes malveillant et mobile
Mesures contre les codes malveillants

Mesures contre le code mobile
Mesure*:* Lorsque l'utilisation de code mobile est autorisée, la configuration doit garantir que le code mobile fonctionne selon une politique de sécurité clairement définie et tout code mobile non autorisé doit être bloqué.

Sauvegarde
Objectif *: Maintenir l'intégrité et la disponibilité des informations et des moyens de traitement de l'information.*

Sauvegarde des informations
Mesure*:* Des copies de sauvegarde des informations et logiciels doivent être réalisées et soumises régulièrement à essai conformément à la politique de sauvegarde convenue.

Chapitre 10: Gestion de l'exploitation et des télécommunications

Gestion de la sécurité des réseaux

Objectif *: Assurer la protection des informations sur les réseaux et la protection de l'infrastructure sur laquelle elles* s'appuient.

Mesures sur les réseaux

Mesure*:* Les réseaux doivent être gérés et contrôlés de manière adéquate pour qu'ils soient protégés des menaces et pour maintenir la sécurité des systèmes et des applications utilisant le réseau, notamment les informations en transit.

Sécurité des services réseau

Mesure*:* Pour tous les services réseau, les fonctions réseau, les niveaux de service et les exigences de gestion doivent être identifiés et intégrés dans tout accord sur les services réseau, qu'ils soient fournis en interne ou en externe.

Chapitre 10: Gestion de l'exploitation et des télécommunications

Manipulation des supports

Objectif *: Empêcher la divulgation, la modification, le retrait ou la destruction non autorisé(e) d'actifs et l'interruption* des activités de l'organisme.

Gestion des supports amovibles

Mesure*:* Des procédures doivent être mises en place pour la gestion des supports amovibles.

Mise au rebut des supports

Procédures de manipulation des informations

Sécurité de la documentation système

Chapitre 10: Gestion de l'exploitation et des télécommunications

Manipulation des supports

Gestion des supports amovibles

.

Mise au rebut des supports

Mesure*:* Les supports qui ne servent plus doivent être mis au rebut de façon sûre, en suivant des procédures formelles.

Procédures de manipulation des informations

Mesure*:* Des procédures de manipulation et de stockage des informations doivent être établies pour protéger ces informations d'une divulgation non autorisée ou d'un mauvais usage.

Sécurité de la documentation système

Mesure*:* La documentation système doit être protégée contre les accès non autorisés.

Chapitre 10: Gestion de l'exploitation et des télécommunications

Echange des informations

Objectif *: Maintenir la sécurité des informations et des logiciels échangés au sein de l'organisme et avec une entité* extérieure.

Politiques et procédures d'échange des informations

Mesure*:* Des politiques, procédures et mesures d'échange formelles doivent être mises en place pour protéger les échanges d'informations liées à tous types d'équipements de télécoms.

Accords d'échange

Mesure*:* Des accords doivent être conclus pour l'échange d'informations et de logiciels entre l'organisme et la partie externe.

Supports physiques en transit

Messagerie électronique

Chapitre 10: Gestion de l'exploitation et des télécommunications

Echange des informations

Objectif *: Maintenir la sécurité des informations et des logiciels échangés au sein de l'organisme et avec une entité* extérieure.

Politiques et procédures d'échange des informations

Accords d'échange

Supports physiques en transit

Mesure*:* Les supports contenant des informations doivent être protégés contre les accès non autorisés, le mauvais usage ou l'altération lors du transport hors des limites physiques de l'organisme.

Messagerie électronique

Mesure*:* Les informations liées à la messagerie électronique doivent être protégées de manière adéquate.

Chapitre 10: Gestion de l'exploitation et des télécommunications

Services de commerce électronique

Objectif *: Assurer la sécurité des services de commerce électronique, ainsi que leur utilisation sécurisée.*

Commerce électronique

Mesure*:* Les informations liées au commerce électronique transmises sur les réseaux publics doivent être protégées contre les activités frauduleuses, les litiges sur les contrats et la divulgation et la modification non autorisées.

Transactions en ligne

Informations à disposition du public

Chapitre 10: Gestion de l'exploitation et des télécommunications

Services de commerce électronique

Commerce électronique

Transactions en ligne

Mesure*:* Les informations liées aux transactions en ligne doivent être protégées pour empêcher la transmission incomplète, les erreurs d'acheminement, la modification non autorisée, la divulgation non autorisée, la duplication non autorisée du message ou la réémission.

Informations à disposition du public

Mesure*:* L'intégrité des informations mises à disposition sur un système accessible au public doit être protégée pour empêcher toute modification non autorisée.

Chapitre 10: Gestion de l'exploitation et des télécommunications

Surveillance

Objectif *: Détecter les traitements non autorisés de l'information.*

Journaux d'audit

Mesure*:* Les journaux d'audit, qui enregistrent les activités des utilisateurs, les exceptions et les événements liés à la sécurité doivent être produits et conservés pendant une période préalablement définie afin de faciliter les investigations ultérieures et la surveillance du contrôle d'accès.

Surveillance de l'exploitation du système

Protection des informations journalisées

Chapitre 10: Gestion de l'exploitation et des télécommunications

Surveillance

Journaux d'audit

Surveillance de l'exploitation du système

Mesure*:* Des procédures permettant de surveiller l'utilisation des moyens de traitement de l'information doivent être établies et les résultats des activités de surveillance doivent être réexaminés périodiquement.

Protection des informations journalisées

Mesure*:* Les équipements de journalisation et les informations journalisées doivent être protégés contre le sabotage et les accès non autorisés.

Chapitre 10: Gestion de l'exploitation et des télécommunications

Journal administrateur et journal des opérations

Mesure*:* Les activités de l'administrateur système et de l'opérateur système doivent être journalisées.

Rapports d'anomalies

Mesure*:* Les éventuels défauts doivent être journalisés et analysés et les mesures appropriées doivent être prises.

Synchronisation des horloges

Mesure*:* Les horloges des différents systèmes de traitement de l'information d'un organisme ou d'un domaine de sécurité doivent être synchronisées à l'aide d'une source de temps précise et préalablement définie.

➢ *Chapitre 11: Contrôle d'accès*

Hormis le contrôle d'accès physique (traité dans 9.1), toutes les mesures se rapportant au contrôle d'accès sont réunies dans ce chapitre.

- **Politique:** La mesure 11.1.1 donne des pistes pour formaliser la procédure de contrôle d'accès.
- **Utilisateurs:** Les mesures décrites dans 11.2 traitent de l'enregistrement des utilisateurs, la gestion des droits d'accès ainsi que des mots de passe.
- **Responsabilités des utilisateurs:** La partie 11.3 revient sur les mots de passe et donne des conseil pour protéger les équipements laissés sans surveillance.
- **Réseau:** Partie 11.4 très technique. Elle aborde tous les moyens pratiques pour protéger l'accès aux réseaux (depuis l'authentification des utilisateurs distants jusqu'au cloisonnement par DMZ, en passant par le routage.

➢ *Chapitre 11: Contrôle d'accès*

Hormis le contrôle d'accès physique (traité dans 9.1), toutes les mesures se rapportant au contrôle d'accès sont réunies dans ce chapitre.

- **Système d'exploitation:** La section 11.5 couvre les mesures de contrôle d'accès aux systèmes d'exploitation, à la limitation du temps de connexion, à l'accès aux utilitaires systèmes …
- **Applications :** Contient 2 mesures essentielles. Mesure 11.6.1 donne des conseils permettant de ne donner accès aux utilisateurs qu'aux informations et fonctions dont ils ont besoins. Mesure 11.6.2 préconise d'isoler les systèmes particulièrement sensibles des autres systèmes.
- **Information mobile et télétraitement:** La section 11.7 donne des conseils se rapportant à l'usage de l'informatique mobile (consistant à se connecter au SI de l'entreprise lorsque l'on est en déplacement) et le télétraitement (personnes travaillant depuis leur domicile avec un contrat de travail approprié).

➢ *Chapitre 11: Contrôle d'accès*

L'objectif est de:

- ✓ gérer et contrôler l'accès aux informations
- ✓ prévenir les accès non autorisés
- ✓ assurer la protection des systèmes en réseau
- ✓ détecter les activités non autorisées

La politique de contrôle comprend notamment:

- ✓ l'enregistrement unique de chaque utilisateur,
- ✓ une procédure écrite de délivrance d'un processus d'authentification signée du responsable hiérarchique,
- ✓ des services de déconnexion automatique en cas d'inactivité,
- ✓ une politique de révision des mots de passe

➢ *Chapitre 11: Contrôle d'accès*

Exigences métier relatives au contrôle d'accès
Objectif *: Maîtriser l'accès à l'information.*

Politique de contrôle d'accès
Mesure*:* Une politique de contrôle d'accès doit être établie, documentée et réexaminée sur la base des exigences métier et de sécurité.

Gestion des accès des utilisateurs
Objectif *: Contrôler l'accès des utilisateurs autorisés et empêcher les accès non autorisés aux systèmes* d'information.

Enregistrement des utilisateurs
Mesure*:* Une procédure formelle d'inscription et désincription des utilisateurs destinée à accorder et à supprimer l'accès à tous les systèmes et services d'information doit être définie.

➢ *Chapitre 11: Contrôle d'accès*

Gestion des privilèges

Mesure*:* L'attribution et l'utilisation des privilèges doivent être restreintes et contrôlées.

Gestion du mot de passe utilisateur

Mesure*:* L'attribution de mots de passe doit être réalisée dans le cadre d'un processus formel.

Réexamen des droits d'accès utilisateurs

Mesure *:* La direction doit réexaminer les droits d'accès utilisateurs à intervalles réguliers par le biais d'un processus formel. examinée sur la base des exigences métier et de sécurité.

➢ *Chapitre 11: Contrôle d'accès*

Responsabilités de l'utilisateurs

Objectif *: Empêcher l'accès d'utilisateurs non habilités et la compromission ou le vol d'informations et de moyens de* traitement de l'information.

Utilisation du mot de passe

Mesure*:* Il doit être demandé aux utilisateurs de respecter les bonnes pratiques de sécurité lors de la sélection et de l'utilisation de mots de passe.

Matériel utilisateur laissé sans surveillance

Politique du bureau propre et de l'écran vide

➢ *Chapitre 11: Contrôle d'accès*

Responsabilités de l'utilisateurs

Utilisation du mot de passe

Matériel utilisateur laissé sans surveillance

Mesure*:* Les utilisateurs doivent s'assurer que tout matériel laissé sans surveillance est doté d'une protection appropriée.

Politique du bureau propre et de l'écran vide

Mesure*:* Une politique du bureau propre doit être adoptée pour les documents papier et les supports de stockage amovibles, et une politique de l'écran vide doit également être adoptée pour les moyens de traitement de l'information.

➢ *Chapitre 11: Contrôle d'accès*

Contrôle d'accès réseau
Objectif *: Empêcher les accès non autorisés aux services disponibles sur le réseau.*

Politique relative à l'utilisation des services en réseau
Mesure *:* Les utilisateurs doivent avoir uniquement accès aux services pour lesquels ils ont spécifiquement reçu une autorisation.

Authentification de l'utilisateur pour les connexions externes
Mesure*:* Des méthodes d'authentification appropriées doivent être utilisées pour contrôler l'accès des utilisateurs distants.

Identification des matériels en réseaux
Mesure*:* L'identification automatique de matériels doit être considérée comme un moyen d'authentification des connexions à partir de lieux et matériels spécifiques.

➢ *Chapitre 11: Contrôle d'accès*

Protection des ports de diagnostic et de configuration à distance
Mesure*:* L'accès physique et logique aux ports de diagnostic et de configuration à distance doit être contrôlé.

Cloisonnement des réseaux
Mesure*:* Les groupes de services d'information, d'utilisateurs et de systèmes d'information doivent être séparés sur le réseau.

Mesure relative à la connexion réseau

Contrôle du routage réseau

.

➢ *Chapitre 11: Contrôle d'accès*

Protection des ports de diagnostic et de configuration à distance

Cloisonnement des réseaux

Mesure relative à la connexion réseau

Mesure *:* Pour les réseaux partagés, en particulier les réseaux qui s'étendent au-delà des limites de l'organisme, la capacité de connexion réseau des utilisateurs doit être restreinte, conformément à la politique de contrôle d'accès et aux exigences relatives aux applications métier

Contrôle du routage réseau

Mesure*:* Des mesures du routage des réseaux doivent être mises en œuvre afin d'éviter que les connexions réseau et les flux d'informations ne portent atteinte à la politique de contrôle d'accès des applications métier.

.

➢ *Chapitre 11: Contrôle d'accès*

Contrôle d'accès au système d'exploitation
Objectif *: Empêcher les accès non autorisés aux systèmes d'exploitation.*

Ouverture de sessions sécurisées
Mesure*:* L'accès aux systèmes d'exploitation doit être soumis à une procédure sécurisée d'ouverture de session.

Identification et authentification de l'utilisateur
Mesure*:* Un identifiant unique et exclusif doit être attribué à chaque utilisateur et une technique d'authentification doit être choisie, permettant de vérifier l'identité déclarée par l'utilisateur.

Système de gestion des mots de passe
Mesure*:* Les systèmes qui gèrent les mots de passe doivent être interactifs et doivent fournir des mots de passe de qualité.

➢ *Chapitre 11: Contrôle d'accès*

Emploi des utilitaires système

Mesure*:* L'emploi des programmes utilitaires permettant de contourner les mesures d'un système ou d'une application doit être limité et contrôlé étroitement.

Déconnexion automatique des sessions inactives

Mesure*:* Les sessions inactives doivent être déconnectées après une période d'inactivité définie.

Limitation du temps de connexion

Mesure*:* Les temps de connexion doivent être restreints afin d'apporter un niveau de sécurité supplémentaire aux applications à haut risque.

.

.

➢ *Chapitre 11: Contrôle d'accès*

Contrôle d'accès aux applications et à l'information

Objectif *: Empêcher les accès non autorisés aux informations stockées dans les applications.*

Restriction d'accès à l'information

Mesure*:* Pour les utilisateurs et le personnel chargé de l'assistance technique, l'accès aux informations et aux fonctions applicatives doit être restreint conformément à la politique de contrôle d'accès.

Isolement des systèmes sensibles

Mesure*:* Les systèmes sensibles doivent disposer d'un environnement informatique dédié (isolé).

Informatique mobile et télétravail

Informatique et communications mobiles

Télétravail

➢ *Chapitre 11: Contrôle d'accès*

Contrôle d'accès aux applications et à l'information

Restriction d'accès à l'information

Isolement des systèmes sensibles

Informatique mobile et télétravail

Objectif *: Garantir la sécurité de l'information lors de l'utilisation d'appareils informatiques mobiles.*

Informatique et communications mobiles

Mesure*:* Une procédure formelle et des mesures de sécurité appropriées doivent être mises en place pour assurer une protection contre le risque lié à l'utilisation d'appareils et de communication mobiles.

Télétravail

Mesure*:* Une politique, des procédures et des programmes opérationnels spécifiques au télétravail doivent être élaborés et mis en œuvre.

➢ *Chapitre 12: Acquisition développement et maintenance des SI*

Toutes les mesures de sécurité relatives au développement et à la maintenance des plates-formes et des applications

- **Exigence de la sécurité:** La mesure 12.1.1 insiste sur l'importance de tenir compte des exigences de sécurité lors de l'acquisition ou de la conception d'un SI ou de l'un de ses éléments constitutifs.
- **Bon fonctionnement des applications:** L'objectif de la mesure 12.2 est d'empêcher toute erreur de traitement, perte, divulgation ou altération de données Il s'agit des données en entrée et en sortie).
- **Chiffrement:** La mesure 12.3 aborde les questions de chiffrement et de la gestion des clés.

➢ *Chapitre 12: Acquisition développement et maintenance des SI*

Toutes les mesures de sécurité relatives au développement et à la maintenance des plates-formes et des applications

- **Systèmes de fichiers:** L'objet des mesures de la section 12.4 est la protection de l'accès au code source, la protection des données de test l'installation de logiciels dans l'environnement de production .
- **Développement et support :** les mesures de sécurité de la partie 12.5 traitent les procédures de mises en production et la validation des changements
- **Vulnérabilité :** La mesure 12.6.1 prodigue des conseils en matière de veille en vulnérabilité.

➢ *Chapitre 12: Acquisition développement et maintenance des SI*

L'objectif est de:

- ✓ Assurer que la sécurité est incluse dès la phase de conception.
- ✓ Prévenir la perte, la modification ou la mauvaise utilisation des informations dans les systèmes.
- ✓ Protéger la confidentialité, l'intégrité et la disponibilité des informations.
- ✓ Assurer que les projets et les activités de maintenance sont conduits de manière sûre.
- ✓ Maintenir la sécurité des systèmes d'application, tant pour le logiciel que pour les données..

➢ *Chapitre 12: Acquisition développement et maintenance des SI*

Exigences de sécurité applicables aux systèmes d'information

Objectif *: Veiller à ce que la sécurité fasse partie intégrante des systèmes d'information.*

Analyse et spécification des exigences de sécurité

Mesure*:* Les exigences métier relatives aux nouveaux systèmes d'information ou les améliorations apportées aux systèmes d'information existants doivent spécifier les exigences de sécurité.

Bon fonctionnement des applications

Validation des données en entrée

Mesure relative au traitement interne

➢ *Chapitre 12: Acquisition développement et maintenance des SI*

Exigences de sécurité applicables aux systèmes d'information

Analyse et spécification des exigences de sécurité

Bon fonctionnement des applications

Objectif *: Empêcher toute erreur, perte, modification non autorisée ou tout mauvais usage des informations dans* les applications.

Validation des données en entrée

Mesure*:* Les données entrées dans les applications doivent être validées afin de vérifier si elles sont correctes et appropriées.

Mesure relative au traitement interne

Mesure*:* Des contrôles de validation doivent être inclus dans les applications afin de détecter les éventuelles altérations de l'information dues à des erreurs de traitement ou des actes délibérés.

➢ *Chapitre 12: Acquisition développement et maintenance des SI*

Intégrité des messages

Mesure*:* Les exigences permettant d'assurer l'authentification et la protection de l'intégrité des messages dans les applications doivent être identifiées, et des mesures appropriées doivent être identifiées et mises en œuvre.

Validation des données en sortie

Mesure*:* Les données de sortie d'une application doivent être validées pour assurer que le traitement des informations stockées est correct et adapté aux circonstances.

Mesures cryptographiques

Politique d'utilisation des mesures cryptographiques

Gestion des clés

.

➢ *Chapitre 12: Acquisition développement et maintenance des SI*

Intégrité des messages
Validation des données en sortie

Mesures cryptographiques
Objectif *: Protéger la confidentialité, l'authenticité ou l'intégrité de l'information par des moyens cryptographiques.*

Politique d'utilisation des mesures cryptographiques
Mesure*:* Une politique d'utilisation des mesures cryptographiques en vue de protéger l'information doit être élaborée et mise en œuvre.

Gestion des clés
Mesure*:* Une procédure de gestion des clés doit favoriser l'utilisation par l'organisme de techniques cryptographiques.

.

➢ *Chapitre 12: Acquisition développement et maintenance des SI*

Sécurité des fichiers systèmes

Objectif *: Garantir la sécurité des fichiers système.*

Mesure relative aux logiciels en exploitation

Mesure*:* Des procédures doivent être mises en place pour contrôler l'installation du logiciel sur les systèmes en exploitation.

Protection des données système d'essai

Mesure*:* Les données d'essai doivent être sélectionnées avec soin, protégées et contrôlées.

Contrôle d'accès au code source du programme

Sécurité en matière de développement et d'assistance technique

.Procédures de contrôle des modifications

➢ *Chapitre 12: Acquisition développement et maintenance des SI*

Sécurité des fichiers systèmes
Mesure relative aux logiciels en exploitation
Protection des données système d'essai

Contrôle d'accès au code source du programme

Mesure*:* L'accès au code source du programme doit être restreint.

Sécurité en matière de développement et d'assistance technique

Objectif *: Garantir la sécurité du logiciel et des informations d'application.*

Procédures de contrôle des modifications

Mesure*:* La mise en œuvre des modifications doit être contrôlée par le biais de procédures formelles.

➢ *Chapitre 12: Acquisition développement et maintenance des SI*

Réexamen technique des applications après modification du système d'exploitation

Mesure*:* Lorsque des modifications sont apportées aux systèmes d'exploitation, les applications critiques métier doivent être réexaminées et testées afin de vérifier l'absence de tout effet indésirable sur l'activité ou sur la sécurité.

Restrictions relatives à la modification des progiciels

Mesure *:* La modification des progiciels ne doit pas être encouragée, et doit être limitée aux changements nécessaires. Un contrôle strict doit également être exercé sur ces modifications.

Fuite d'informations

Externalisation du Développement logiciel

➢ *Chapitre 12: Acquisition développement et maintenance des SI*

Réexamen technique des applications après modification du système d'exploitation

Restrictions relatives à la modification des progiciels

Fuite d'informations

Mesure*:* Toute possibilité de fuite d'informations doit être empêchée.

Externalisation du Développement logiciel

Mesure*:* Le développement logiciel externalisé doit être encadré et contrôlé par l'organisme

➢ *Chapitre 12: Acquisition développement et maintenance des SI*

Gestion des vulnérabilités techniques

Objectif *:* Réduire les risques liés à l'exploitation des vulnérabilités techniques ayant fait l'objet d'une publication.

Mesure relative aux vulnérabilités techniques

Mesure*:* Toute information concernant toute vulnérabilité technique des systèmes d'information en exploitation doit être obtenue à temps, l'exposition de l'organisme aux dites vulnérabilités doit être évaluée et les actions appropriées doivent être entreprises pour traiter le risque associé.

➢ *Chapitre 12: Gestion des incidents liés à la sécurité de l'information*

La gestion des incidents fait l'objet de 2 « objectifs »

- **Signalement des incidents:** les 2 mesures de la partie 13.1 donnent des conseils pour le signalement rapide des incidents et des failles de sécurité.
- **Gestion des incidents :** Elle commence par la répartition des responsabilités dans le processus de gestion des incidents 13.2.1, se poursuit par la réaction rapide aux incidents 13.2.2, puis se conclut par la collecte des preuves permettant d'en comprendre les causes et, éventuellement, d'entreprendre des poursuite 13.2.3..

L'objectif est de:

✓ Assurer que les incidents de sécurité sont enregistrés, résolus et qu'un reporting adéquat est mis en place (ITIL).

➢ *Chapitre 12: Gestion des incidents liés à la sécurité de l'information*

Gestion des incidents liés à la sécurité de l'information et des améliorations

Objectif *: Garantir la mise en place d'une approche cohérente et efficace pour la gestion des incidents liés à la* sécurité de l'information.

Responsabilités et procédures

Mesure*:* Des responsabilités et des procédures doivent être établies, permettant de garantir une réponse rapide, efficace et pertinente en cas d'incident lié à la sécurité de l'information.

Exploitation des incidents liés à la sécurité de l'information déjà survenus

Collecte de preuves

➢ *Chapitre 12: Gestion des incidents liés à la sécurité de l'information*

Gestion des incidents liés à la sécurité de l'information et des améliorations

.

Responsabilités et procédures

Exploitation des incidents liés à la sécurité de l'information déjà survenus

Mesure*:* Des mécanismes doivent être mis en place, permettant de quantifier et surveiller les différents types d'incidents liés à la sécurité de l'information ainsi que leur volume et les coûts associés.

Collecte de preuves

Mesure*:* Lorsqu'une action en justice civile ou pénale est engagée contre une personne physique ou un organisme, à la suite d'un incident lié à la sécurité de l'information, les éléments de preuve doivent être recueillis, conservés et présentés conformément aux dispositions légales relatives à la présentation de preuves régissant la ou les juridiction(s) compétente(s).

➢ *Chapitre 13: Gestion de la continuité de l'activité*

Gestion des incidents liés à la sécurité de l'information et des améliorations

.

Responsabilités et procédures

Exploitation des incidents liés à la sécurité de l'information déjà survenus

Mesure*:* Des mécanismes doivent être mis en place, permettant de quantifier et surveiller les différents types d'incidents liés à la sécurité de l'information ainsi que leur volume et les coûts associés.

Collecte de preuves

Mesure*:* Lorsqu'une action en justice civile ou pénale est engagée contre une personne physique ou un organisme, à la suite d'un incident lié à la sécurité de l'information, les éléments de preuve doivent être recueillis, conservés et présentés conformément aux dispositions légales relatives à la présentation de preuves régissant la ou les juridiction(s) compétente(s).

➢ *Chapitre 13: Gestion de la continuité de l'activité*

L'objectif est de développer la capacité à répondre rapidement aux interruptions des activités critiques de l'organisation, résultant de pannes, d'incident, de sinistre ou de catastrophe.

- ✓ Une analyse de risques à partir de divers scénarii de sinistre et une évaluation de la criticité des applications, permet d'établir différents plans de poursuite des opérations depuis le mode dégradé en cas de dysfonctionnements mineurs jusqu'à la reprise dans un local distant en cas de sinistre grave (incendie, attentat, grève, etc…).

➢ *Chapitre 13: Gestion de la continuité de l'activité*

Gestion de la continuité de l'activité d'un point de vue aspects de la sécurité de l'information

Objectif *: Empêcher les interruptions des activités de l'organisme, protéger les processus métier cruciaux des effets* causés par les défaillances majeures des systèmes d'information ou par des sinistres et garantir une reprise de ces processus dans les meilleurs délais.

Intégration de la sécurité de l'information dans le processus de gestion du plan de continuité de l'activité

Continuité de l'activité et appréciation du risque

.

➢ *Chapitre 13: Gestion de la continuité de l'activité*

Gestion de la continuité de l'activité d'un point de vue aspects de la sécurité de l'information

Intégration de la sécurité de l'information dans le processus de gestion du plan de continuité de l'activité

Mesure*:* Un processus de continuité de l'activité dans l'ensemble de l'organisme doit être élaboré et géré, qui satisfait aux exigences en matière de sécurité de l'information requises pour la continuité de l'activité de l'organisme.

Continuité de l'activité et appréciation du risque

Mesure*:* Les événements pouvant être à l'origine d'interruptions des processus métier doivent être identifiés, tout comme la probabilité et l'impact de telles interruptions et leurs conséquences pour la sécurité de l'information.

➢ *Chapitre 13: Gestion de la continuité de l'activité*

Élaboration et mise en œuvre des plans de continuité intégrant la sécurité de l'information

Mesure*:* Des plans doivent être élaborés et mis en œuvre pour maintenir ou restaurer l'exploitation et assurer la disponibilité des informations au niveau et dans les délais requis suite à une interruption ou une panne affectant les processus métier cruciaux.

Cadre de la planification de la continuité de l'activité

Mise à l'essai, gestion et réévaluation constante des plans de continuité de l'activité

.

➢ *Chapitre 13: Gestion de la continuité de l'activité*

Élaboration et mise en œuvre des plans de continuité intégrant la sécurité de l'information

Cadre de la planification de la continuité de l'activité

Mesure*:* Un cadre unique pour les plans de continuité de l'activité doit être géré afin de garantir la cohérence de l'ensemble des plans, de satisfaire de manière constante aux exigences en matière de sécurité de l'information et d'identifier les priorités en matière de
mise à l'essai et de maintenance.

Mise à l'essai, gestion et réévaluation constante des plans de continuité de l'activité

Mesure*:* Les plans de continuité de l'activité doivent être testés et mis à jour régulièrement afin de s'assurer qu'ils sont actualisés et efficaces.

➢ *Chapitre 14: Conformité*

Ce chapitre est composé de 5 mesures de sécurité. Il couvre tous les aspects relatifs PCA (*Plan de Continuité d'Activité*); depuis l'analyse d'impact jusqu'aux tests et aux revues du PCA.

➢ *Chapitre 14: Conformité*

Ce chapitre aborde toutes les questions relatives à la conformité avec la réglementation et avec les procédures internes de l'entreprise. Il traite aussi des audits

- **Réglementation :** La partie 15.1 aborde les questions liées à la conformité avec la réglementation (propriété intellectuelle), l'utilisation du chiffrement, la protection des enregistrements contre toute falsification ou accès illicite
- **Procédures internes :** Les mesures traitées dans 15.2 préconisent les moyens à mettre en place pour assurer le conformité du système avec les politiques et les normes de sécurité.
- **Audit du SI:** La partie 15.3 traite les mesures organisationnelles mises en place pour procéder aux audits sans interférer avec le travail des personnes audités. Cet « objectif » rappelle aussi que les outils d'audit doivent être protégés.

➢ *Chapitre 14: Conformité*

La conformité se décline en 3 volets:

- ✓ Le respect des lois et réglementations: licences logiciels, propriété intellectuelle, règles de manipulation des fichiers contenant des informations touchant la confidentialité des personnes,
- ✓ La conformité des procédures en place au regard de la politique de sécurité de l'organisation, c'est à dire quels dispositifs ont été mis en place pour assurer les objectifs décrits par la Direction Générale
- ✓ L'efficacité des dispositifs de traçabilité et de suivi des procédures en place, notamment les journaux d'activités, les pistes d'audit, les enregistrements de transaction.

➢ *Chapitre 14: Conformité*

Conformité aux exigences légales

Objectif *: Eviter toute violation des obligations légales, statutaires, réglementaires ou contractuelles et des* exigences de sécurit

Identification de la législation en vigueur

Mesure *:*Pour chaque système d'information et pour l'organisme, toutes les exigences légales, réglementaires et contractuelles en vigueur doivent être définies, documentées et mises à jour, ainsi que la procédure utilisée par l'organisme pour satisfaire à ces exigences.

Droits de propriété intellectuelle (DPI)

.

Protection des enregistrements de l'organisme

➢ *Chapitre 14: Conformité*

Conformité aux exigences légales

Identification de la législation en vigueur

Droits de propriété intellectuelle (DPI)

Mesure*:* Des procédures appropriées doivent être mises en œuvre, visant à garantir la conformité avec les exigences légales, réglementaires et contractuelles concernant l'utilisation du matériel pouvant être soumis à des droits de propriété intellectuelle et l'utilisation des logiciels propriétaires.

Protection des enregistrements de l'organisme

Mesure*:* Les enregistrements importants doivent être protégés contre la perte, destruction et falsification conformément aux exigences légales, réglementaires et aux exigences métier.

➢ *Chapitre 14: Conformité*

Protection des données et confidentialité des informations relatives à la vie privée

Mesure*:* La protection et la confidentialité des données doivent être garanties, telles que l'exigent la législation ou les réglementations applicables, et les clauses contractuelles le cas échéant.

Mesure préventive à l'égard du mauvais usage des moyens de traitement de l'information

Mesure*:* Les utilisateurs doivent être dissuadés de toute utilisation de moyens de traitement de l'information à des fins illégales.

Réglementation relative aux mesures cryptographiques

Mesure*:* Des mesures cryptographiques doivent être prises conformément aux accords, lois et réglementations applicables.

➢ *Chapitre 14: Conformité*

Conformité avec les politiques et normes de sécurité et conformité technique

Objectif *: S'assurer de la conformité des systèmes avec les politiques et normes de sécurité de l'organisme.*

Conformité avec les politiques et les normes de sécurité

Mesure*:* Les responsables doivent s'assurer de l'exécution correcte de l'ensemble des procédures de sécurité placées sous leur responsabilité en vue de garantir leur conformité avec les politiques et normes de sécurité.

Vérification de la conformité technique

Mesure*:* La conformité des systèmes d'information avec les normes relatives à la mise en œuvre de la sécurité doit être vérifiée régulièrement.

➢ *Chapitre 14: Conformité*

Prises en compte de l'audit du système d'information

Objectif *: Optimiser l'efficacité et réduire le plus possible l'interférence avec le/du processus d'audit du système* d'information.

Contrôles de l'audit du système d'information

Mesure*:* Les exigences d'audit et les activités impliquant des contrôles des systèmes en exploitation doivent être planifiées de manière précise et doivent être le résultat d'un accord afin de réduire le plus possible le risque de perturbations des processus métier.

Protection des outils d'audit du système d'information

Mesure*:* L'accès aux outils d'audit du système d'information doit être protégé afin d'empêcher tous mauvais usage ou compromission éventuels.

La norme ISO 27002

Utilisation de la norme

- ✓ L'ISO 27002 est un référentiel de 112 pages comportant 133 mesures de sécurité.
- ✓ C'est un code de bonnes pratiques devant être consulté comme ouvrage de de référence.
- ✓ Il doit être consulté en cas de doute sur la mise en application d'une mesure de sécurité.

La norme propose et l'implémenteur dispose, en fonction du contexte auquel il est confronté

La norme ISO 27002 ()

La norme ISO 27002 (Mesure de sécurité: exemple1)

- **Mesure de sécurité 11.2.4 de la norme:**

  - ✓ **Références:**11.2.4 Réexamen des droits d'accès des utilisateurs
  - ✓ **Mesure:** il convient que la direction revoie les droits d'accès utilisateurs à intervalles réguliers par le biais d'un processus formel
  - ✓ **Préconisations de mise en œuvre:**
  - ✓ **Informations supplémentaires:**

La norme ISO 27002 (Mesure de sécurité: exemple1)

- **Mesure de sécurité 11.2.4 de la norme:**
  - ✓ **Préconisations de mise en œuvre:** il convient de tenir comptes des lignes directives suivantes:
    - Réexaminer les droits d'accès utilisateurs à intervalles réguliers (6mois), et après tout changement (promotion, rétrogradation ou départ) [11.2.1]
    - Réexaminer et de réattribuer les droits d'accès utilisateurs en cas de changement de fonction au sein de l'organisme
    - Réexaminer les autorisations d'accès accordées aux utilisateurs dotés de privilège spéciaux [11.2.2] à une plus grande fréquence (3mois)
    - Vérifier l'attribution des privilèges à intervalles réguliers pour s'assurer qu'aucun privilège non autorisé n'a été accordé.
    - Journaliser les modifications apportées aux comptes dotés de privilèges pour les besoins de réexamens périodique.
  - ✓ **Informations supplémentaires:** Il est nécessaire de réexaminer à intervalles réguliers les droits d'accès utilisateurs afin de conserver un contrôle sur les accès aux données et aux services d'information

La norme ISO 27002 (Mesure de sécurité: exemple2)

- **Subdivision du chapitre 11:**

Ce chapitre contient 7 sous-chapitres

- ✓ **11.1** Exigences métier relatives au contrôle d'accès
- ✓ **11.2** Gestion de l'accès utilisateurs
- ✓ **11.3** Responsabilités utilisateurs
- ✓ **11.4** Contrôle d'accès au réseau
- ✓ **11.5** Contrôle d'accès au système
- ✓ **11.6** Contrôle d'accès aux applications et à l'information
- ✓ **11.7** Informatique mobile et télétraitement

La norme ISO 27002 (Mesure de sécurité: exemple3)

11.2 Gestion de l'accès des utilisateurs:

Objectif: maintenir l'accès utilisateurs par le biais d'autorisations et empêcher les accès non autorisés aux systèmes d'informations.

Toutes les mesures de sécurité comprises dans le sous-chapitre 11.2 auront pour objectif de maitriser l'accès utilisateur par le biais d'autorisation et d'empêcher les accès non autorisés aux systèmes d'information.

Implémenter un SMSI

Implémenter un SMSI

- **Paradoxe:**

  Alors que plusieurs indices dénotent un réel intérêt pour la norme ISO 27001, force est de constater que le nombre d'entreprises certifier est très insignifiant.

- **Raisons:**

  - ✓ Il ne faut pas croire que le déploiement d'un SMSI se limite:
    - à la rédaction d'une politique
    - à la réalisation d'une appréciation des risques
    - à la formalisation des procédures
  - ✓ Il faut s'approprier le SMSI

Il est difficile d'obtenir des informations concrète sur la façon de mener à bien un projet de déploiement de SMSI

Le projet de mise en place du SMSI

Le projet de mise en place du SMSI

➢ **Nature du projet:**

La mise en place d'un SMSI est un projet fondamentalement transversal, donc difficile à gérer.

✓ **Les acteurs :**

- Le service informatique
- La directions des ressources humaines
- les moyens généraux
- Tous les services métiers impliqués
- …

Le projet concerne toute la hiérarchie de l'entreprise, tout le monde est mis à contribution

Le projet de mise en place du SMSI

➢ **Nature du projet:**

La mise en place d'un SMSI est un projet fondamentalement transversal, donc difficile à gérer.

✓ **Les difficultés:**

Puisque le projet de construction d'un SMSI;

- couvre des domaines très variés (techniques et organisationnels)
- implique de nombreux services de l'entreprise
- entraine la mise en place de très nombreux processus
- …

Il est indispensable de le découper en grandes phases, puis en sous-projets, conduits souvent par des personnes différentes

Le projet de mise en place du SMSI

- **Chef du projet:**
  - ✓ **Profil 1:** *l'idéal*

    Une personne ayant déjà piloté un projet de SMSI ⇨ *profil rarissime*

  - ✓ **Profil 2 :** *un peu plus disponible, mais …*

    Une personne ayant monté avec succès un système de management en qualité

    ⇨ *avantage*

    Connaissance parfaite des points incontournable dans la mise en place d'un système de management;

    ⇨ *Inconvénient*

    Méconnaissance des problèmes et questions relatives à la sécurité

Le projet de mise en place du SMSI

- **Chef du projet:**
  - ✓ **Profil 3:** *à défaut*

  Une personne spécialisée dans la conduite de projets concernant la sécurité ⇨ *profil* plus répandu

  - ✓ **Le Chef de Projet (**les particularités**) :** *Le chef de projet doit:*
    - avoir reçu une formation certifiant qu'il connait bien la norme ISO 27001 (certifications: *implementation* 27001 et *lead auditor* 27001)
    - posséder les qualités requises pour piloter un tel projet
    - posséder le sens de l'organisation
    - posséder le charisme d'un chef de projet

Le projet de mise en place du SMSI

- **Chef du projet:**
  - ✓ **Le Chef de Projet** (les qualités) **:** *Le chef de projet doit savoir échanger avec :*
    - La direction générale: Il doit savoir évaluer les coûts humains et financiers de chaque aspect du projet (savoir présenter et qualifier les apports du SMSI)
    - Les techniciens: Il doit avoir une forte culture technique. Il doit faire comprendre que le SMSI valorise la technique et qu'il n'est pas synonyme de paperasserie administrative.
    - Les utilisateurs: Il doit faire comprendre aux utilisateurs (population diversifiée) que le SMSI impliquera une diminution des incidents et donc une amélioration continue du service

C'est un chef de projet confirmé; c.à.d.

une personne choisie en interne, reconnue pour son ancienneté et connaissant très bien les services de l'organisme

Le projet de mise en place du SMSI

Projet de mise en place du SMSI: (les approches)

Consciente de la difficulté, l'ISO travaille sur la norme ISO 27003,. C'est un guide proposant des solutions pour conduire le projet de construction du SMSI.

Approche primaire

1. Concevoir une politique pour le SMSI
2. Commander une appréciation des risques à un prestataire
3. Commander la rédaction des documents par le même prestataire

Le projet de mise en place du SMSI

Projet de mise en place du SMSI: (les approches)

Consciente de la difficulté, l'ISO travaille sur la norme ISO 270003,. C'est un guide proposant des solutions pour conduire le projet de construction du SMSI.

Approche primaire : Démarche à éviter, car:

1. Ne répond pas aux exigence de la norme
2. Ne responsabilise nullement l'entreprise vis-à-vis de la sécurité

Le projet de mise en place du SMSI

Projet de mise en place du SMSI: (les approches)

Consciente de la difficulté, l'ISO travaille sur la norme ISO 270003,. C'est un guide proposant des solutions pour conduire le projet de construction du SMSI.

Approche Séquentielle (suivre scrupuleusement la norme***)***

1. Conception du périmètre et de la politique du SMSI
2. Appréciation des risques
3. Sélection des mesures de sécurité dans la déclaration d'applicabilité
4. Rédaction du plan de traitement des risques et implémentation des mesures de sécurité nécessaires
5. Mise en place d'une structure de détection d'incidents
6. Contrôle du bon fonctionnement des mesures de sécurité
7. Mise en place d'un audit interne
8. Revue du SMSI
9. Actions correctives et préventives

Le projet de mise en place du SMSI

➢ Projet de mise en place du SMSI: (les approches)

Consciente de la difficulté, l'ISO travaille sur la norme ISO 270003,. C'est un guide proposant des solutions pour conduire le projet de construction du SMSI.

Approche Séquentielle : Démarche dangereuse, car elle oublie de prendre en compte les paramètres suivants:

1. **La réalité du terrain:** Commencer d'abord par l'étude de l'état des lieux sur les pratiques de l'entreprise en matière de sécurité.➔ la connaissance des coûts induits lors de la sélection de tel ou tel périmètre, confronter les objectifs des parties prenantes avec la réalité du terrain.
2. **Les mesures déjà existantes**
3. **La définition des priorités**
4. **La nécessité de paralléliser les tâches**
5. **Certaines tâches manquantes**

Le projet de mise en place du SMSI

Projet de mise en place du SMSI: (les approches)

Consciente de la difficulté, l'ISO travaille sur la norme ISO 270003,. C'est un guide proposant des solutions pour conduire le projet de construction du SMSI.

Approche Séquentielle : Démarche dangereuse, car elle oublie de prendre en compte les paramètres suivants:

1. **La réalité du terrain:**
2. **Les mesures déjà existantes:** Il est absurde de se lancer tête baissée dans une appréciation des risques en faisant abstraction de l'existant, comme si rien n'a été fait au par avant ➔ Comme l'exige la norme, mener à bien une appréciation des risques d'où la sélection des mesures de sécurité adéquates.
3. **La définition des priorités:**
4. **La nécessité de paralléliser les tâches:**
5. **Certaines tâches manquantes:**

Le projet de mise en place du SMSI

Projet de mise en place du SMSI: (les approches)

Consciente de la difficulté, l'ISO travaille sur la norme ISO 270003,. C'est un guide proposant des solutions pour conduire le projet de construction du SMSI.

Approche Séquentielle : Démarche dangereuse, car elle oublie de prendre en compte les paramètres suivants:

1. **La réalité du terrain:**
2. **Les mesures déjà existantes:**
3. **La définition des priorités:** Il est important de comprendre que l'ordre d'apparition des tâches dans la norme n'a aucun rapport avec l'ordre dans lequel il faudra les implémenter.
4. **La nécessité de paralléliser les tâches:**
5. **Certaines tâches manquantes:**

Le projet de mise en place du SMSI

Projet de mise en place du SMSI: (les approches)

Consciente de la difficulté, l'ISO travaille sur la norme ISO 270003,. C'est un guide proposant des solutions pour conduire le projet de construction du SMSI.

Approche Séquentielle : Démarche dangereuse, car elle oublie de prendre en compte les paramètres suivants:

1. **La réalité du terrain:**
2. **Les mesures déjà existantes:**
3. **La définition des priorités:**
4. **La nécessité de paralléliser les tâches:** L'ISO 27001 présente les exigences de façon séquentielle, sans préciser quelles tâches peuvent être conduite en parallèle. Entreprendre toutes les tâches séquentiellement représenterait une perte de temps
5. **Certaines tâches manquantes:**

Le projet de mise en place du SMSI

Projet de mise en place du SMSI: (les approches)

Consciente de la difficulté, l'ISO travaille sur la norme ISO 270003,. C'est un guide proposant des solutions pour conduire le projet de construction du SMSI.

Approche Séquentielle : Démarche dangereuse, car elle oublie de prendre en compte les paramètres suivants:

1. **La réalité du terrain:**
2. **Les mesures déjà existantes:**
3. **La définition des priorités:**
4. **La nécessité de paralléliser les tâches:**
5. **Certaines tâches manquantes:** La norme décrit le SMSI tel qu'il doit être une fois en production, mais elle fait impasse sur certaines tâches qui doivent être entreprise (notamment en amont) pour construire le SMSI car elle n'est pas un « *document projet* ». ➔ se baser exclusivement sur les spécifications de la norme conduit à passer à coté de certaines tâches pourtant incontournables.

Le projet de mise en place du SMSI

➢ Projet de mise en place du SMSI: (les approches)

Consciente de la difficulté, l'ISO travaille sur la norme ISO 270003,. C'est un guide proposant des solutions pour conduire le projet de construction du SMSI.

Approche Projet : Prendre toutes les libertés nécessaires pou garantir le succès du projets.

Contraintes fondamentaux dont il faut tenir compte:

1. **Les exigences de la norme:** le SMSI doit satisfaire toutes les exigences des clases 4 à 8 de la norme
2. **Le modèle PDCA:** doit être respecté tant au niveau global, qu'au niveau processus ou des mesures de sécurité
3. **La cohérence générale:** est nécessaire entre le périmètre du SMSI, la politique, l'appréciation des risques et les mesures de sécurité effectivement mises en place.

Le projet de mise en place du SMSI

- **Projet de mise en place du SMSI: (L'approche projet: les phases)**

  La mise en place d'un SMSI se divise en 4 phases principales.

  Phase 1: Analyse préalable

  Phase 2: Mise en place de la structure de base

  Phase 3: Mise en place de processus du SMSI.

  Phase 4: Démarrage du SMSI

Le projet de mise en place du SMSI

Projet de mise en place du SMSI: (L'approche projet: les phases)

La mise en place d'un SMSI se divise en 4 phases principales.

Phase 1: Analyse préalable

Il s'agit de faire les bons choix stratégiques afin d'éviter toute erreur lourde de conséquence. ➔ 3 étapes préalables :

1. **L'étude de l'opportunité :** Evaluer concrètement l'apport de la mise en place d' SMSI pour l'entreprise. C'est un travail au niveau stratégique. D'où la nécessité de connaître exactement les attentes des parties prenantes. La direction générale est impliquée.
2. **L'état des lieux:** Il s'agit de faire le point sur la situation de l'entreprise vis-à-vis des mécanismes élémentaires du système de management
3. **L'étude des options (politique et périmètre):** compte tenu des résultats de l'étape précédente, plusieurs options de périmètre sont à étudier. L'objectif est d'évaluer le coût de chacune de ces options et de le confronter aux bénéfices attendus. La direction générale retiendra l'option qui lui paraitra la meilleure.

Le projet de mise en place du SMSI

- **Projet de mise en place du SMSI: (**L'approche projet**: les phases)**

La mise en place d'un SMSI se divise en 4 phases principales.

Phase 2: Mise en place de la structure de base

Il s'agit de bâtir le socle de services qui constituera l'infrastructure du SMSI. Quel que soit le périmètre et l'état d'avancement, il sera toujours nécessaire de prendre des décisions de tenir à jours la documentation, de contrôler les processus, de mesurer leur efficacité et de former le personnel (Construction d'une roue PDCA) .

Les principales briques de l'infrastructure SMSI

1. **La gouvernance de la sécurité:** sous projet consiste à mettre en place une **structure** permettant de prendre les *bonnes décisions* en matière de sécurité, *au bon moment et au bon niveau*. Dès l'initiation du projet, il faut valider officiellement la politique et le périmètre du SMSI.
2. **La documentation:** Une procédure de gestion de la documentation doit être créée et validée juste après la mise en place de la gouvernance (**passage à la tradition écrite**). Toute la documentation du SMSI reposera sur les règles fixées dans cette procédure.

Le projet de mise en place du SMSI

➢ Projet de mise en place du SMSI: (L'approche projet: les phases)

La mise en place d'un SMSI se divise en 4 phases principales.

Phase 2: Mise en place de la structure de base

Il s'agit de bâtir le socle de services qui [illegible] et
d'avancement, il sera toujours nécessaire de [illegible]
contrôler les processus, de mesurer leur efficacité et de [illegible] .

Cette phase est très importante: la réussite ou l'échec du SMSI dépend de cette phase

Les principales briques de l'infrastructure SMSI

3. **L'audit interne et le suivi des actions:** l'obj[illegible] les processus du SMSI sont efficaces et conformes aux [illegible] de la norme. La mise en place de l'audit interne va permettre **le contrôle et la correction rapide de toute non-conformité,** garantissant la qualité des processus.

4. **La formation et la sensibilation:** Il est nécessaire de mettre en place, dès que les 3 sous-projets précédents ont été établis, un *processus continu* de **gestion de la formation et de sensibilation du personnel**.

5. **Les indicateurs:** permettront aux différentes instances de décision de connaître le niveau de conformité et de performance du système. Tout processus venant s'intégré au SMSI pourra faire objet d'un indicateur.

Le projet de mise en place du SMSI

Projet de mise en place du SMSI: (L'approche projet: les phases)

La mise en place d'un SMSI se divise en 4 phases principales.

Phase 3: Mise en place des processus du SMSI.

Initiée par une appréciation des risques, elle se poursuit par la mise en place des mesures de sécurité et se conclut par la construction d'un mécanisme de revue.

1. **Appréciation des risques :** c'est un point clé du projet , car elle permettra de sélectionner les mesures de sécurité les plus appropriées par rapport au contexte et la politique du SMSI. Elle doit être conduite avant l'adaptation et l'implémentation des mesures de sécurité.
2. **Adaptation des mesures de sécurité existantes:** les mesures de sécurité déjà en place avant le projet SMSI doivent être mises en conformité avec le modèle PDCA (formaliser les procédures et identifier les enregistrements pertinents.

Le projet de mise en place du SMSI

Projet de mise en place du SMSI: (L'approche projet: les phases)

La mise en place d'un SMSI se divise en 4 phases principales.

Phase 3: Mise en place de processus du SMSI.

Initiée par une appréciation des risques, elle se poursuit par la mise en place des mesures de sécurité et se conclut par la construction d'un mécanisme de revue.

3. **Implémentation des mesures de sécurité manquantes :** les mesures de sécurité sélectionnées dans la déclaration d'applicabilité (SoA) et non encore mises en place devront être implémentées.

4. **Revue:** Ce processus constitue avec l'audit interne, l'essentiel de la phase *Check* du système de management. Il est indispensable dans la construction du SMSI. Cependant, sa mise en place n'est pas urgent, car la revue n'a lieu d'être qu'une fois le SMSI constitué.

Le projet de mise en place du SMSI

Projet de mise en place du SMSI: (L'approche projet: les phases)

La mise en place d'un SMSI se divise en 4 phases principales.

Phase 4: Démarrage du SMSI

Le démarrage du SMSI est progressif. Les processus de la structure de base sont les premiers à produire des enregistrements, suivis de près par l'appréciation des risques, puis par les nombreuses mesures de sécurité.

Lorsque le chef de projet estime que tout est en place, il lui reste à effectuer quelques opérations avant de commander l'audit de certification.

L'objectif est de vérifier que tout est prêt pour réussir la certification du1ier coup

1. **Revue du SMSI:** processus défini à la fin de la phase 3. Il permet de prendre du recul afin de vérifier que le système est bien adapté aux besoins des parties prenantes, qu'il fonctionnent correctement et qu'il est efficace. Il n'est pas prudent de commander un audit de certification, sans avoir fait une revue du SMSI (revue de direction). Normalement, la revue se tient une fois par an, ou à la demande.
2. **Préparation à l'audit:** Il convient de vérifier que tout est fin prêt avant de faire venir les auditeurs

Le projet de mise en place du SMSI

Projet de mise en place du SMSI: (L'approche projet: les phases)

La mise en place d'un SMSI se divise en 4 phases principales.

Phase 4: Démarrage du SMSI

Le démarrage du SMSI est progressif. Les processus de la structure de base sont les premiers à produire des enregistrements, suivis de près par l'appréciation des risques, puis par les nombreuses mesures de sécurité.

Lorsque le chef de projet estime que tout est en place, il lui reste à effectuer quelques opérations avant de commander l'audit de certification.

L'objectif est de vérifier que tout est prêt pour réussir la certification du1ier coup

3. **Audit à blanc :** conduit par un cabinet externe, il consiste à procéder à un audit complet du SMSI en utilisant la même démarche que les auditeurs de certification

4. **Actions correctives et préventives:** tous les écarts identifiés lors de l'audit à blanc nécessiteront d'appliquer des actions correctives et préventives. Il ne reste alors plus qu'à commander l'audit de certification (***l'inauguration officielle du SMSI***)

Le projet de mise en place du SMSI

- **Principales erreurs à éviter**

1. Travailler sans l'appui de la direction générale
2. Travailler seul
3. Ne pas mettre en place une structure de base
4. Se tromper de périmètre
5. Déclaration d'applicabilité
6. Faire « de la procédure »

Le projet de mise en place du SMSI

- **Principales erreurs à éviter**

1. Travailler sans l'appui de la direction générale:

Le SMSI entraîne la création de procédure qui s'imposeront à tout le monde (ne tenant compte ni de la hiérarchie ni …) ➔ susceptibilités entre …

2. Travailler seul

Le RSSI est souvent le 1ier convaincu . Sans l'appui de la direction et l'implication des autres services, il se trouvera avec un tas de documents et de procédures auto-validé et dont personne ne s'en sert.

3. Ne pas mettre en place une structure de base

Il n'est pas suffisant de se baser sur sur la norme IOS 27002 pour monter une SMSI. Le plus important est de construire l'infrastructure qui fera tourner la roue PDCA

Le projet de mise en place du SMSI

- **Principales erreurs à éviter**

4. Se tromper de périmètre

Le choix d'un périmètre trop ambitieux risque d'être trop onéreux et complexe à mettre en place, puis à maintenir. Un périmètre trop restreint risque de s'avérer inutile.

5. Déclaration d'applicabilité

Au moment de la construction du SoA, il faut bien choisir le nombre des indicateurs de mesure. Un nombre très élevé va rendre le SMSI complexe et son exploitation risque de n'être pas conforme avec la norme. La tentation inverse (nb réduit) risque de nous faire omettre certaines mesures indispensables au bon fonctionnement du SMSI.

6. Faire « de la procédure »

Eviter les procédures verbeuses. Plus une procédures est chargée, plus elle est difficile à lire, et surtout, plus il y a de chance que la description ne corresponde pas à la réalité du terrain.

Considérons une société implantée sur un seul site, développant et fabriquant des équipements électroménagers. Elle a mis en place un système de management dont le périmètre ne couvre que les activités de recherche et développement (R&D), ce qui représente un petit périmètre. Dans ces conditions, il parait logique que seules les personnes travaillant dans le laboratoire de R&D soient concernées.

Ce n'est pourtant pas le cas.

-Le service de R&D est hébergé dans les locaux de l'entreprise. Il consomme de l'eau, de l'électricité, de l'air conditionné et tout autre type de servitudes. Les ***personnes des services généraux*** sont donc concernées, même indirectement

-Le service de R&D utilise les ressources informatiques qui sont mises à sa disposition: serveurs, réseau, postes de travail, etc. Les ***informaticiens*** sont donc aussi concernés par le système de management

-Toutes ces personnes (informaticiens, techniciens des services généraux. chercheurs) sont des employés ou des sous-traitants de la société, il est donc logique que le ***service du personnel*** soit impliqué dans le système de management

- Enfin, chaque fois que le service de R&D achète des biens ou des services, cela concerne également la **comptabilité** et les **finances**.

Généralement, les personnes concernées par les systèmes de management sont:

-les membres de la direction générale;

-les principaux responsables des services concernés;

-tous les cadres et employés directement impliqués dans les activités couvertes par le système de management;

- tous les cadres ou employés indirectement impliqués par le système de management.

Importance de l'écrit

Les industriels en général, et le secteur aéronautique en particulier, ont la culture. de la tradition écrite depuis longtemps. Les procédures sont écrites et les décisions sont prises lors de commissions, donnant lieu â des comptes rendus.

Exemple:

Dans une entreprise réunir une commission pour décider du changement de place ou non d'une simple prise de courant.

Il faut dire que la sensibilité de son activité le justifiait amplement.

Dans la mesure où l'entreprise qui a

- mis en place un système de management formalise ses procédures par écrit et
- consigne les principales décisions dans des comptes rendus,

il devient possible à une personne extérieure (un ***auditeur***, par exemple) de venir vérifier que ce qui est pratiqué correspond effectivement à ce qui a été spécifié par écrit.

Un système de management en sécurité de l'information permettra d'adopter des mesures de sécurité appropriées aux besoins de l'entreprise, en ***posant les bonnes questions***.

Quels sont les éléments les plus sensibles de l'entreprise?

Où déployer en priorité les mesures de sécurité?

Comment cloisonner les réseaux? Comment détecter les incidents?

Comment réagir rapidement aux intrusions? Comment améliorer les processus?

Et ainsi de suite ...

Considérons une entreprise qui, dans le cadre de son SMSI, a mis en place une ***procédure de réaction aux incidents de sécurité.***

Lorsqu'une tentative d'intrusion se produit sur le réseau, les équipes savent ce qu'elles ont à faire et agissent en conséquence pour limiter l'impact de cette attaque.

Après coup, l'attaque est analysée et des actions préventives sont entreprises pour éviter qu'une telle agression puisse se reproduire.

Sur la durée, cette organisation rend les attaques de plus en plus difficiles à réaliser.

La confiance

Il s'agit de toute personne, groupe ou instance envers laquelle l'entreprise doit rendre des comptes. Les parties prenantes les plus classiques sont les suivantes:

1. **Les actionnaires:** en tant que propriétaires, ils sont directement concernés par les résultats de l'entreprise.

2. **Les autorités de tutelle:** les administrations doivent rendre des comptes à leurs autorités de tutelle, qui fixent leurs missions.

3. **Les clients:** ils sont la partie prenante par excellence, puisque l'entreprise ne peut vivre sans eux.

4. **Les fournisseurs:** même si la relation client-fournisseur place souvent ceux ci en situation d'infériorité, l'entreprise a des responsabilités envers eux.

5. **Les partenaires:** les relations de partenariat sont devenues indispensables pour le développement de l'entreprise. Si les partenaires n'ont pas confiance, ils ne collaboreront pas.

6. **Les banques et les assurances:** l'entreprise ne peut pas vivre sans leur confiance.

7. **Le personnel:** son adhésion est capitale pour le bon fonctionnement de l'entreprise.

8. **l'opinion publique:** elle a un pouvoir de sanction très important. dont les conséquences peuvent se révéler désastreuses pour l'entreprise.

Exemple: **SMSI observé à l'échelle globale**

Considérons un système de management de la sécurité de l'information dans son ensemble. La ***mise en place d'un SMSI*** *nécessite de produire un certain nombre de documents de politique et d'identifier les actions à entreprendre pour se prémunir contre les actes de malveillance. C'est la* ***phase Plan****. Ensuite, il faut mettre en oeuvre les mesures de sécurité identifiées précédemment C'est la* ***phase Do.*** *L'audit interne permettra de vérifier que ce qui est mis en place est conforme aux politiques et aux procédures. C'est la* ***phase Check****. Enfin, des actions corrigeront ces écarts. C'est la* ***phase Act****.*

Exemple: **SMSI observé à l'échelle d'un processus**

Changeons à présent d'échelle pour ne considérer que ce qui concerne le cloisonnement des réseaux de niveaux de sensibilité différents (c'est-à-dire les DMZ ou zones démilitarisées). La ***phase Plan*** *implique qu'il faut une politique de flux réseau conduisant à l'élaboration* d'une matrice de flux. La ***phase Do*** *consistera à configurer les pare-feux et les routeurs* afin de ne laisser passer que les protocoles nécessaires (TCP, UDp, ports, protocoles) entre les différents segments du réseau. La ***phase Check*** *consistera à vérifier périodiquement que* les règles des pare-feux et des routeurs correspondent bien à ce qui est spécifié dans la matrice de flux. Enfin, la ***phase Act*** *reviendra à corriger tout écart entre les deux.*

Exemple

Le SMSI d'une agence de voyages sur Internet pourra avoir pour missions principales:

- **La *disponibilité:*** *en permettant à ses clients d'acheter un voyage à n'importe quelle* heure du jour ou de la nuit
- ***L:intégrité:*** *en fournissant aux clients une information exacte sur les vols et débiter* exactement le prix convenu, ni plus, ni moins, . ..
-**La *confidentialité:*** *en protégeant les données personnelles de ses clients (compte* bancaire, historique des achats, etc.) contre tout accès illicite,

Les trois notions présentées ci-dessus ne sont pas les seules. On parle aussi de ***trafabilité****,* ***d'authentification****, de* ***non-répudiation****, et de bien d'autres* mécanismes de sécurité, Le fait que ces principes ne soient pas au centre du SMSI ne signifie pas qu'ils ne soient pas importants, Ils seront déployés en fonction des besoins de sécurité de l'entreprise,

Exemple

Pour parvenir à ses objectifs de disponibilité, d'intégrité et de confidentialité, l'agence de voyages déploiera des mécanismes d'authentification par mot de passe utilisateur et certificat serveur, chiffrement des flux. signature, etc.

Exemples

✓ Une société d'infogérance soumise à de très nombreux audits de la part de ses clients peut espérer alléger cette charge en faisant certifier les activités les plus contrôlées.

✓ Une banque peut diminuer l'immobilisation de ses fonds propres en mettant en place un SMSI.

✓ Une société d'infogérance soumise à de très nombreux audits de la part de ses clients peut espérer alléger cette charge en faisant certifier les activités les plus contrôlées.

✓ Une banque peut diminuer l'immobilisation de ses fonds propres en mettant en place un SMSI.

Exemples

Concrètement, un état des lieux abordera les questions suivantes:

✓**Question 1** : quel est l'état de l'entreprise vis-à-vis des processus de base d'un SMSI ? (gouvernance, documentation, audit interne, formation, indicateurs)

✓**Question 2** : existe-t-il une appréciation des risques?

✓**Question 3** : indépendamment de l'appréciation des risques, quelles sont les mesures de sécurité déjà en place dans l'entreprise?

✓**Question 4**: pour chaque mesure de sécurité déjà en place, quel est son niveau de maturité par rapport au modèle *Plan, Do, Check, Act?*

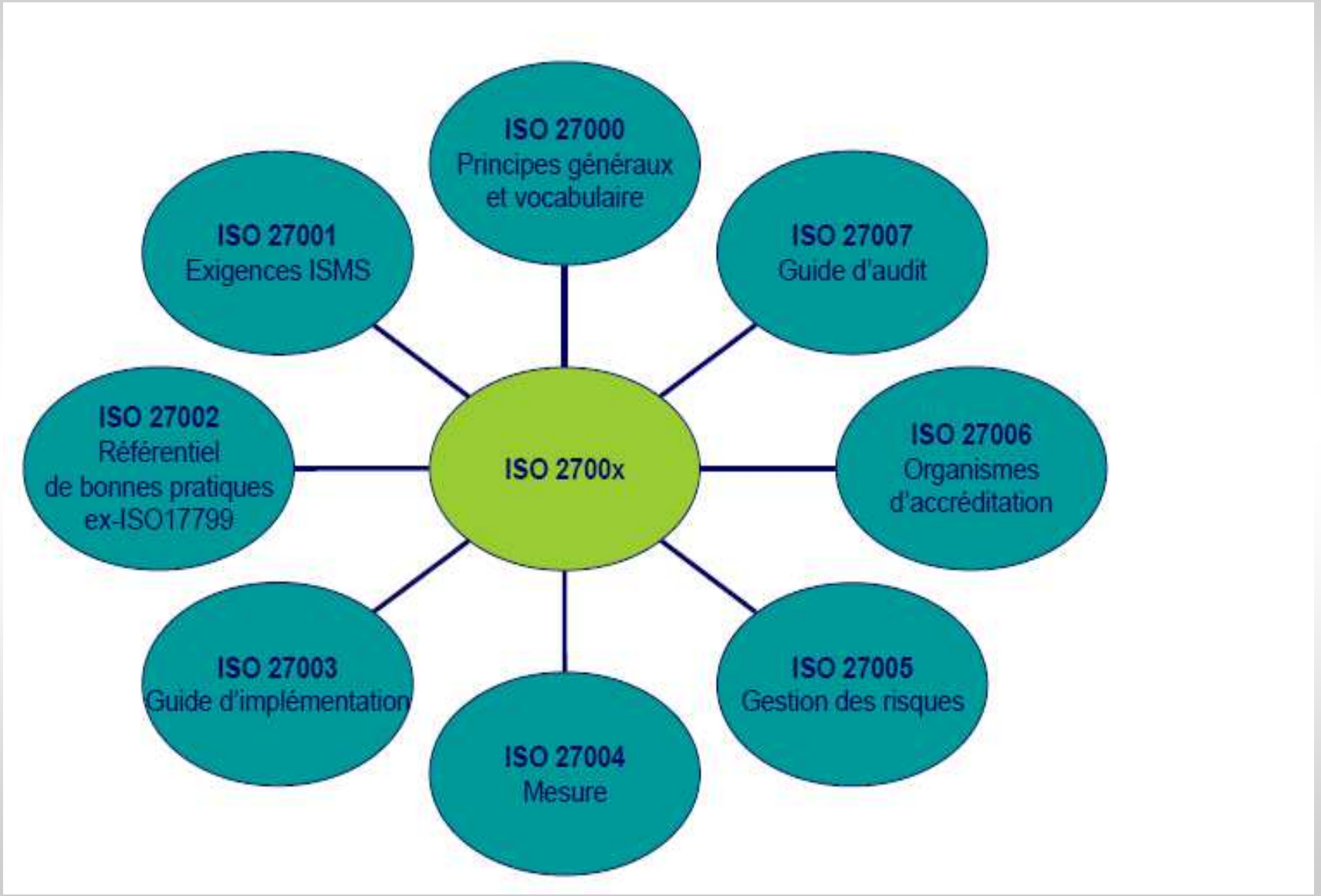
✓**Question 5** : indépendamment de l'appréciation des risques, quelles sont les mesures de sécurité non mises en place?

Exemples

Le tableau suivant illustre une comparaison de plusieurs options, en mettant en évidence les coûts et les apports escomptés. Naturellement, dans un exemple réel, ces points devront être évalués aussi précisément que possible. La notion de « *coût élevé*.» ou de « *coût moyen* » sera donc remplacée par les évaluations qualitatives ou quantitatives.

Options	Coût défini	Apport escompté
Certification de toutes les activités de l'entreprise	Elevé	Nouveaux clients. Image de marque
Certification des activités de R & D	Moyen	Relations de partenariat favorisés
Certification du service informatique dans un premier temps	Moyen	Amélioration du service rendu aux utilisateurs

Famille ISO 2700x



✓Une société d'infogérance soumise à de très nombreux audits de la part de ses clients peut espérer alléger cette charge en faisant certifier les activités les plus contrôlées.

✓Une banque peut diminuer l'immobilisation de ses fonds propres en mettant en place

✓un SMSI.

✓Un prestataire de services peut espérer gagner des clients en affichant une certification

✓ISO 27001.

Naturellement, chacun de ces arguments doit être quantifié aussi précisément que possible.

Etat des lieux

Concrètement, un état des lieux abordera les questions suivantes:

✓ **Question 1** : quel est l'état de l'entreprise vis-à-vis des processus de base d'un SMSI? (gouvernance, documentation, audit interne, formation, indicateurs)

✓ **Question 2** : existe-t-il une appréciation des risques?

✓ **Question 3** : indépendamment de l'appréciation des risques, quelles sont les mesures de sécurité déjà en place dans l'entreprise?

✓ **Question 4**: pour chaque mesure de sécurité déjà en place, quel est son niveau de maturité par rapport au modèle Plan, Do, Check, Act?

✓ **Question 5** : indépendamment de l'appréciation des risques, quelles sont les mesures de sécurité non mises en place?

Le tableau suivant illustre une comparaison de plusieurs options, en mettant en évidence les coûts et les apports escomptés. Naturellement, dans un exemple réel, ces points devront être évalués aussi précisément que possible. La notion de • coût élevé. ou de • coût moyen. sera donc remplacée par des évaluations qualitatives ou quantitatives.

Options	Coût estimé	Aspects escomptés
Certification de toutes les activités de l'entreprise	Elévé	Niveaux clients. Image de marque
Certification des activités R &D	Moyen	Amélioration de partenariat favorisées
Certification du service informatique dans un premier temps	Moyen	Amélioration du service rendu aux utilisateurs

Deux exemples:

un fabricant de papier spécial et une agence de communication

Considérons une usine fabriquant du papier spécial, destiné à être intégré dans les billets de banque. Il est clair que, pour pénétrer dans cette usine, l'entreprise exigera des visiteurs qu'ils respectent certains processus:

- prendre rendez-vous plusieurs jours avant toute visite sur le site;
- présenter une pièce d'identité, échangée contre un badge;
-' passer par un sas uni personnel pour pénétrer dans les locaux ;
- être accompagnés à tout moment par un membre du personnel.

Il en ira différemment d'une *agence de communication* qui se limitera simplement à leur demander de présenter une pièce d'identité.

Deux exemples:

une **politique exigeante** ou une **politique souple**

Une société peut formuler une politique de SMSI dans laquelle elle s'engage à assurer un niveau très élevé d'**intégrité**, de **confidentialité** et de **disponibilité**. Cette politique l'obligera à **déployer en conséquence un nombre important de mesures de sécurité**.

Une autre peut au contraire formuler une politique de SMSI dans laquelle elle ne s'engage qu'à assurer un niveau correct en matière de disponibilité de l'information. Cela signifie que seules **les mesures relatives à la continuité de service seront déployées**. **Si un incident relatif à la confidentialité des données surgit, aucun reproche ne pourra être formulé quant au fait de ne pas avoir pris de mesures pour se protéger contre un tel incident**

Exemple:

niveau **fin** ou **élevé** de granularité

Si on choisit un niveau **fin de granularité**, on peut considérer qu'un ordinateur portable est un actif ainsi que son système d'exploitation et les fichiers présents sur son disque dur. Ce niveau est **recommandé pour les petits périmètres**, mais il peut très vite s'avérer difficile à gérer dès que le périmètre prend de l'importance.

Dans l'optique d'un niveau **élevé de granularité**, la notion d'actif est au contraire beaucoup plus large. L'importance est donnée à l'information et non à son support, qu'il soit papier ou électronique.

Ainsi, on considérera le ***fichier client*** ou le ***savoir-faire de l'entreprise*** comme des actifs, indépendamment des supports sur lesquels ils reposent. Cette approche est plus appropriée dans les périmètres de taille importante.

Exemple:

Voici plusieurs types d'actifs:

- **matériel:** équipements système, équipements réseau;
- **physique**: entrepôts, bureaux, aires de livraison;
- **logiciel:** systèmes d'exploitation, bases de données, fichiers;
- **humain:** personnel de direction, techniciens, agents d'exploitation, opérateurs;
- **documents:** manuels d'utilisation, documents papier;
- **immatériel:** savoir-faire de l'entreprise.

Exemple:

Considérons une **usine qui fabrique des automobiles**.

Ses *actifs* sont de plusieurs ordres: la *matière première*, les *robots d'assemblage*, etc.

Ses *actifs d'information* sont le réseau qui interconnecte les robots entre eux, les serveurs qui les pilotent, le logiciel d'ERP qui commande les matières premières en flux tendu.

Ces actifs d'information sont importants puisque leur compromission peut entraîner de graves problèmes de production..

Exemple 1:

vol de l'ordinateur portable

L'attitude de l'entreprise peut consister à **accepter le risque de vol des ordinateurs portables**.
Dans ce cas, **aucune mesure de protection particulière ne sera déployée** pour se protéger contre le vol. Si un ordinateur se fait voler, la direction assumera intégralement les conséquences de cet incident (perte et divulgation de données) et achètera un nouvel ordinateur à son employé.

Exemple 2:

piratage de la vitrine web

L'entreprise peut décider de ***ne pas protéger sa vitrine web***. Si jamais la page d'accueil se fait défigurer par un pirate, le site vitrine sera mis hors ligne, le temps de le reconstruire. Ceci veut dire que l'entreprise accepte l'impact en termes d'image d'une défiguration de son site web vitrine.

Exemple 1:

vol de l'ordinateur portable

Une entreprise peut décider que le **vol d'un ordinateur portable est un événement inacceptable**, compte tenu de la sensibilité des informations qui y sont stockées. Dans ce cas, quel est le moyen d'avoir un risque nul de se faire voler des ordinateurs portables ?

Naturellement, **le moyen consiste à ne pas distribuer d'ordinateurs portables aux employés.**

Pas d'ordinateur portable ➔ Pas de vol d'ordinateur portable.

Exemple 2:

accessibilité d'une application web

Une caisse de retraite dispose d'une application permettant de reconstituer la carrière de ses cotisants pour calculer le montant de la retraite à laquelle ils auront droit.

Cette application est utilisée par les services internes de la caisse.

Considérons **qu'il est question de rendre cette application accessible à tous depuis Internet**

Malgré les nombreuses mesures de protection qui seront déployées (cloisonnement de réseaux, sécurisation des serveurs, protection contre le Cross *Site Scripting et l'injection* SQL), **il demeure un risque limité qu'une personne malveillante puisse accéder à la carrière d'une autre personne**.

Ce risque peut être jugé inacceptable par la caisse de retraite, qui préférera ne pas mettre en ligne l'application, afin d'être certaine que personne n'accédera frauduleusement à la carrière des autres.

Exemple 1:

assurance

L'exemple typique du risque qui ne peut être évité est **l'incendie**. C'est pour cela que tous les organismes sont assurés contre ce genre de sinistre.

L'assurance n'empêche pas l'occurrence du sinistre, mais *elle en transfère les conséquences financières vers un prestataire* solvable, c'est-à-dire l'assureur (qui a mutualisé le risque sur l'ensemble de ses clients).

Exemple 2:

sous-traitance

La plupart des centres de production informatiques ont besoin de **stocker une copie de leurs sauvegardes à l'extérieur du site**. Ainsi, si un sinistre détruit le centre, une copie des informations est toujours disponible. Il est alors **possible de reconstruire le centre de production** en restaurant les sauvegardes qui étaient stockées hors site.

Ce stockage hors site est souvent confié à des prestataires. C'est un exemple classique de transfert de risque, puisque c'est **un prestataire qui se charge** de mettre en place les mesures de sécurité nécessaires: **transport en camion blindé, stockage en lieu sûr, procédures d'authentification pour accéder aux sauvegardes, etc**.

Exemple 1:

ordinateur portable

Attacher l'ordinateur portable à la table grâce à un câble, verrouillé par un cadenas, réduit le risque de vol, donc d'indisponibilité

Chiffrer les données présentes dans le disque dur, en utilisant un algorithme approprié avec une clé de bonne qualité, réduit le risque de perte de confidentialité de l'information

Exemple 2:

un autre traitement, le financement du risque

Il existe un traitement appelé ***financement du risque*** qui n'est pas spécifié dans la norme. Ce type de traitement consiste à provisionner les moyens financiers pour couvrir les frais induits suite à l'occurrence d'un sinistre.

C'est une sorte ***d'auto-assurance***, mélange *d'acceptation* et de *transfert*.

Ce traitement est très utilisé par les banques dans le cadre de la gestion des risques opérationnels imposée par les accords de Bâle II.

Exemple:

risque résiduel non acceptable

Le **risque de se faire voler un ordinateur portable est moindre** lorsque ce dernier est *attaché à la table par un cadenas*.
Pourtant, le *risque résiduel demeure très élevé*, puisqu'il est très **simple de forcer la serrure de ces petits cadenas** (le Web regorge de démonstrations étonnantes à ce sujet).
Ce traitement est très utilisé par les banques dans le cadre de la gestion des risques opérationnels imposée par les accords de Bâle II.

Exemple:

ordinateur portable

Attacher l'ordinateur portable à la table grâce à un câble, verrouillé par un cadenas, **réduit le risque de vol, donc d'indisponibilité**.

Chiffrer les données présentes dans le disque dur, en utilisant un algorithme approprié avec une clé de bonne qualité, **réduit le risque de perte de confidentialité de l'information**.

Exemple:

risque résiduel acceptable

Le fait de chiffrer les données dans le disque dur réduit considérablement le risque de perte de confidentialité, pour peu que l'algorithme, la longueur et la qualité de la clé soient bien choisis.

Le risque résiduel est souvent accepté, sauf dans les très rares cas où les données à protéger intéressent une entité prête à mettre les moyens pour casser la clé (typiquement, un État).

Exemple:

Exclusion bien fondée

Une usine fabriquant des véhicules livre ses produits à son réseau de concessionnaires, qui se chargent de la vente. Le **SMSI de l'usine** n'est donc pas concerné par le commerce électronique. En conséquence, la mesure «Commerce électronique. » ne sera pas sélectionnée. La justification « Pas de commerce électronique dans l'entreprise » est parfaitement recevable.

Exclusion infondée

Considérons une société qui s'est engagée, dans sa politique de SMSI, à assurer un niveau élevé de continuité de service. Si dans son *SoA, elle n'a pas retenu les mesures* A.14.1.1 à A.14.1.5 (qui traitent pourtant du plan de continuité d'activité) et que la justification se limite à « il n'y a pas de plan de continuité d'activité ", l'exclusion des points A.14.1.1 à A.14.1.5 est infondée, car en contradiction directe avec la politique du SMSI.

Exemple:

usine de billets de banque et société d'assurances

Dans une **usine qui imprime des billets de banque**, des palettes de billets en cours de fabrication sont amenées à passer d'un atelier à l'autre. Pour éviter toute fraude (vol de papier), une **fiche de suivi accompagne chaque palette**. À l'entrée de chaque atelier, les liasses de papier imprimé sont comptées par **un employé** qui en écrit le nombre dans la fiche de suivi avant de la signer. À la sortie de l'atelier, un **autre employé** renouvelle l'opération. **Ainsi, chaque palette est contrôlée pendant tout le processus de fabrication, à l'entrée comme à la sortie de chaque atelier.**

Pour contrôler la bonne application de cette procédure, le contrôleur interne se placera sans prévenir entre deux ateliers et attendra la sortie d'une palette pour vérifier que les comptes sont bien tenus dans la fiche de suivi.

Une fiche de constat sera rédigée en cas de non-conformité.

Exemple:

Dans une **société d'assurances**, le contrôleur interne choisit au hasard trois collaborateurs et **contrôle les logiciels qui sont installés** sur leur poste de travail.
Si des logiciels **illicites ou sans licence sont détectés**, une fiche de constat est rédigée.
Ceci permettra de régulariser la situation, soit en **désinstallant** les logiciels illicites, soit en **achetant** la licence si l'utilisateur en a réellement besoin pour faire son travail.

Exemple:

procédure de contrôle d'accès physique

Considérons une **procédure de contrôle d'accès physique** aux locaux stipulant qu'en zone rouge, seules les personnes portant un badge de couleur rouge ont le droit d'entrer.

La présence en zone rouge d'une personne sans badge est donc un écart par rapport à la procédure.

Le **premier volet de l'action corrective** consistera à vérifier que la personne en question est bien autorisée à entrer en zone rouge. **Si c'est le cas, on lui fera porter son badge. Dans le cas contraire**, **elle sera reconduite à l'extérieur. C'est l'action sur les effets.**

Le **second volet de l'action** corrective consistera à **lancer une campagne de sensibilisation du personnel en rappelant l'importance de ce point de la procédure, quitte à prévenir que toute récidive pourra entraîner des sanctions disciplinaires**.

On évite ainsi que l'écart ne se reproduise. C'est l'action sur les causes.

Exemple:

accès à une salle machine

La salle machine d'une société de distribution de consommables pour les stations service est située au rez-de-chaussée. Une porte blindée avec contrôle par badge protège l'accès à la. salle.

Pourtant, la personne chargée de l'appréciation des risques ne s'est pas rendue compte- qu'il suffit à une personne malveillante de briser la vitre de la salle machine depuis l'extérieur pour y pénétrer.

Mais, à ce jour, aucune effraction n'a encore eu lieu.

L’action préventive consiste à protéger les fenêtres par des barreaux.

Exemple:

procédure d'intégration des nouveaux collaborateurs

La **procédure d'intégration** des nouveaux collaborateurs d'une société de courtage impose à tout nouvel arrivant de passer d'abord par le service du personnel pour présenter son extrait de casier judiciaire. Il passe ensuite aux services généraux pour obtenir un badge d'accès, puis demande au service informatique un accès au réseau.

Ces **trois étapes sont jugées coûteuses** car elles impliquent à chaque fois trois services de l'entreprise. **L'action d'amélioration consiste** à faire en sorte que ce soit **le service du personnel, seul, qui reçoive l'extrait de casier judiciaire, fournisse le badge à l'employé et fasse le nécessaire pour lui ouvrir un compte sur le réseau.**

Cela n'augmente pas forcément la conformité du SMSI ou la sécurité du système d'information, mais cela contribue à simplifier le processus.

Exemple:

Objet: l'objet de la présente politique est de se prémunir contre toutes les menaces, qu'elles soient internes ou externes, délibérées ou accidentelles, et protéger les actifs d'information de la société X.
Responsabilités: il est de la responsabilité de **X** de s'assurer que l'information est protégée contre les accès non autorisés, que la confidentialité de l'information est préservée et qu'elle n'est pas dévoilée à des personnes non autorisées par le moyen d'actions délibérées ou involontaires.
Portée: tout le personnel de **X** est responsable de la mise en place de cette politique de sécurité et aura le soutien de la direction.
Les responsabilités sont réparties de la façon suivante:

- l'encadrement de **X** crée et réévalue la présente politique.
- Le responsable sécurité met en place cette politique par le moyen des démarches et procédures applicables.
- Tout le personnel ainsi que les prestataires suivent les procédures relatives à la sécurité.
- Tout le personnel a la responsabilité de rapporter les incidents de sécurité ainsi que toute vulnérabilité identifiée.
- Tout acte délibéré menaçant la sécurité des informations de **X** est sujet à des poursuites disciplinaires et/ou judiciaires.

Exemple:

Considérons une société dont la direction générale décide de mettre en ligne sur Internet une application qui, à l'origine, n'a pas été conçue pour cela.

Voici les propos que risque de tenir l'ingénieur sécurité en s'adressant à son directeur (DSI) : " Soit, j'entends bien vos préoccupations en termes de politique de sécurité et de procédure de sauvegarde, mais mon problème à moi est ailleurs: la direction me demande de mettre en ligne sur Internet une application qui n'a pas été conçue pour cela. Alors voici les questions auxquelles il me faut une réponse:

quelle ligne de mon fichier *httpd.conf dois-je changer* dans mon relais inverse?

Dans quelle DMZ dois-je placer ce relais inverse?

Quels protocoles dois-je filtrer?

Quels ports dois-je laisser passer?

Sur quel pare-feu dois-je implémenter les règles de filtrage?

Et les réponses à ces questions, il me les faut maintenant, car la direction veut que ça soit en ligne dès la semaine prochaine! »

Exemple:

Voici un extrait de l'ISO 27002. Il s'agit de la mesure de sécurité 11.2,4 de la norme. (Citation extraite de l'ISO/CEl 27002, 1" édition du 15/06/2005.)

11.2.4 Réexamen des droits d'accès utilisateurs

Mesure: il convient que la direction revoie les droits d'accès utilisateurs â intervalles réguliers par le biais d'un processus formel.

Préconisations de mise en oeuvre: il convient que le réexamen des droits d'accès utilisateurs tienne compte des lignes directrices suivantes:

a) il convient de réexaminer les droits d'accès utilisateurs â intervalles réguliers, par exemple tous les 6 mois, et après tout changement, tel qu'une promotion, une rétrogradation ou le départ d'un salarié (voir 11.2.1) ;

b) il convient de réexaminer et de réattribuer les droits d'accès utilisateurs en cas de changement de fonction au sein de l'organisme;

c) il convient de réexaminer les autorisations accordées pour les droits d'accès utilisateurs dotés de privilèges spéciaux (voir 11.2.2) â une plus grande fréquence, par exemple, tous les 3 mois;

d) il convient de vérifier l'attribution de privilèges â intervalles réguliers pour s'assurer qu'aucun privilège non autorisé n'a été accordé;

e) il convient de journaliser les modifications apportées aux comptes dotés de privilèges pour les besoins du réexamen périodique.

Informations supplémentaires: il est nécessaire de réexaminer â intervalles réguliers les droits d'accès utilisateurs afin de conserver un contrôle sur l'accès aux données et aux services d'information.