**Sommaire**

**Introduction**

**Chapitre 1 : Généralité**

1. **la sécurité qu’est-ce que c’est ?**

1. Définition de la sécurité

2. Les composantes de la sécurité

3. Les acteurs de la sécurité

1. **L’information, qu’est-ce que c’est ?**
2. La définition de l’information
3. Le système d’information
4. **Sécurité de l’information**
5. **Le Système de Management**
6. Le principe des systèmes de management
7. Les principaux systèmes de management
8. L’apport des systèmes de management
9. **Le système de management de la sécurité de l'information**

**Chapitre 2 : Normes Et Methodes**

1. Norme
2. Normalisation
3. L’ISO (Organisation Internationale de Normalisation)
4. Historique des normes en matière de la sécurité de l’information
5. Méthode

**Chapitre 3 : Normes ISO/CEI 27001**

1. Introduction
2. Objectifs de la normes ISO/CEI 27001
3. 3.La structure de la norme ISO/CEI 27001

**CHAPITRE 3 : METHODES ET NORMES D’AUDIT SECURITE DES SYSTEMES D’INFORMATION ........................ 15**

**I- DEFINITIONS ................................................................................................................................ 15**

1- L’ISO (ORGANISATION INTERNATIONALE DE NORMALISATION) .............................................................. 15

2- LES NORMES ............................................................................................................................... 15

3- LES METHODES ............................................................................................................................. 16

4- HISTORIQUE DES NORMES EN MATIERE DE SECURITE DE L’INFORMATION .................................................. 16

**II- LA SUITE DES NORMES ISO 2700X .................................................................................................. 18**

ISO/IEC 27000 .............................................................................................................................. 18

ISO/CEI 27001 .............................................................................................................................. 19

ISO/CEI 27002 .............................................................................................................................. 19

ISO/CEI 27003 .............................................................................................................................. 20

ISO/CEI 27004 .............................................................................................................................. 21

ISO/CEI 27005 .............................................................................................................................. 21

ISO/CEI 27006 .............................................................................................................................. 22

ISO/CEI 27007 .............................................................................................................................. 22

**III-LES SYSTEME DE MANAGEMENT ........................**

**Chapitre 1 : Généralité**

**II- la sécurité qu’est-ce que c’est ?**

**1.Définition de la sécurité**

Le dictionnaire *Le Robert* en donne la définition suivante : « État d’esprit confiant et tranquille

d’une personne qui se croit à l’abri du danger. Situation tranquille qui résulte

de l’absence réelle de danger (absence d’accident). »

Dans toute activité humaine, personnelle ou professionnelle, il existe une

multitude de dangers qui planent sur le cours du temps. Ces dangers

représentent une ou des menace(s) qui risquent d’attaquer notre sécurité

et de l’altérer.

Afin de combattre le sentiment d’insécurité qui va résulter des menaces

et des attaques, il nous appartient de prendre conscience de ces dangers,

d’en identifier les faits générateurs et de trouver des remèdes efficaces pour

les contrer afin de réduire ou de faire disparaître les conséquences néfastes.

**Mesure de sécurité** (§ 2.16) : mesure qui modifie un risque.

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

**2 Les composantes de la sécurité**

Pour décrire la sécurité, deux aspects sont souvent utilisés :

**- La sécurité passive** : cette notion fait appel au domaine de la prévention

(actions préventives). Son rôle consiste à réduire les facteurs de survenance

ou de déclenchement de l’accident.

**- La sécurité active** : cette notion fait appel au domaine de la résolution

(actions correctives). Son rôle consiste à déployer des mesures de

protection à l’encontre des conséquences dommageables lorsque

l’accident survient.

**3 Les acteurs de la sécurité**

La sécurité se situe dans un environnement qui correspond à un échange entre deux ou plusieurs acteurs.

Alors les acteurs de sécurité sont :

- L’organisation (l’organisme)

- Les parties prenantes

- La direction

- Les instances dirigeantes

- Entité de communication des informations sécurisées

**4 Résponsable de la Sécurité**

Pour définir, mettre en oeuvre et suivre la démarche sécurité au sein de l’organisme, il importe de désigner un « Résponsable de la Sécurité ». représentant de la direction ce Résponsable de la Sécurité est investi par la direction de la responsabilité de la gestion de la sécurité.

ses objectifs sont à la fois stratégiques et opérationnels. Le Résponsable de la Sécurité doit être rattaché hiérarchiquement à la direction générale qui lui donne autorité et à laquelle il doit rendre compte de sa mission.

**III- L’information, qu’est-ce que c’est ?**

**3.1 La définition de l’information**

Le terme « information » vient du latin *informare* qui signifie mettre en forme.

En fait, le même mot désigne à la fois le message (communication, média)

et les symboles codés (signes, alphabet) qui sont contenus dans le message.

La notion d’information est étroitement liée à la relation des individus que nous

sommes avec notre environnement. Ces messages, échangés sous la forme

de signaux, sont véhiculés à notre niveau par nos cinq sens (vision, toucher,

ouïe, goût, odorat). Dans notre civilisation technologique, les moyens de

communication biologiques sont prolongés par des outils qui en accélèrent

la vitesse de transmission et réduisent les limites espace/temps. Il en résulte

que toute perturbation (distorsion, déformation, insuffisance, perte) de la

qualité et de la sécurité de cette information peut avoir de lourdes conséquences

sur nos relations, donc sur notre vie.

**2.3 Le système d’information**

La norme ISO/CEI 27000:2016 définit ainsi le système d’information :

Système d’information (§ 2.39) : applications, services, actifs informationnels ou autres

composants permettant de gérer l’information.

Un système d’information est un ensemble d’éléments qui peuvent être

regroupés selon deux sous-systèmes :

- un sous-système à caractère socio-économique. Il comprend une structure organisationnelle et des moyens humains.

- un sous-système à caractère technique. Il comprend des outils technologiques et des équipements qui sont mis en oeuvre pour assurer

le fonctionnement.

-----------------------------------------------------------------------------------------------

Les 10 clés

pour la sécurité

de l’information

Nouvelle édition

mise à jour et augmentée

ISO/CEI 27001:2013

Claude Pinet

1. **Sécurité de l’information**

la sécurité de l’information c’est la protection de la confidentialité, l’intégrité et disponibilité des informations jugé intéresser de l’entreprise , à travers la mise en œuvre de mesures adaptées, qui regroupent des règles, des processus, des procédures, des structures organisationnelles et des fonctions matérielles et logicielles.

1. **Les Système de Management**

**1- définition des systèmes de management**

Selon La norme ISO 9000 un système de management est un système permettant :

• d’établir une politique ;

• de fixer des objectifs ;

• d’atteindre ces objectifs.

Nous pouvons ainsi dire qu’un système de management est un ensemble de mesures organisationnelles et techniques permettant de mettre en place une politique et visant à atteindre un objectif et, une fois celui-ci atteint, Le système doit être documenté et amélioré sur un périmètre précis.



**Le processus du système de management**

**2- Les principaux systèmes de management**

Les systèmes de management ne se cantonnent pas uniquement à la qualité. Ils concernent des domaines très variés comme l’environnement, les services informatiques, la sécurité de l’information, la sécurité alimentaire ou encore la santé.

Le tableau ci-après donne un aperçu non exhaustif des principaux référentiels de systèmes de management.

|  |  |
| --- | --- |
| **Référentiel** | **Domaine** |
| **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 |

**Principaux référentiels de systèmes de management**

**3- L’apport des systèmes de management**

Les propriétés que nous venons de décrire donnent de bonnes raisons de penser que la mise en place et l’exploitation d’un système de management n’est pas un projet facile à mener. Il faut commencer par fixer des politiques, formaliser les procédures par écrit et mener à bien des audits réguliers. Ces opérations sont loin d’être transparentes. Souvent lourdes à implémenter, leur coût humain et financier n’est pas négligeable. Dans ces conditions, il est légitime de se demander ce qui justifie un tel investissement. Quels bénéfices concrets pouvons-nous en espérer ?

**Premier apport : l’adoption de bonnes pratiques**

Les systèmes de management se basent sur des guides de bonnes pratiques dans le domaine qui les concerne (qualité, sécurité, environnement, etc.). Ainsi, celui qui se lance dans la mise en place d’un système de management est quasiment obligé d’adopter ces bonnes pratiques.

**Deuxième apport : l’augmentation de la fiabilité**

L’adoption de bonnes pratiques a pour conséquence directe, à court ou moyen terme, l’augmentation de la fiabilité. Ceci est principalement dû au fait que les systèmes de

management imposent la mise en place de mécanismes d’amélioration continue favorisant la capitalisation sur les retours d’expérience.

**Troisième apport : la confiance**

Nous touchons enfin à la raison d’avoir un système de management : il fournit la confiance envers les parties prenantes. Qu’entendons-nous par parties prenantes ? Il s’agit de toute personne, groupe ou instance envers laquelle l’entreprise doit rendre des comptes (*Par exemple : Les actionnaires, Les autorités de tutelle, Les clients, Les fournisseurs, Les partenaires, etc.*).

En fait, nous oublions trop souvent que la confiance est le vecteur qui permet toute relation entre un client et un fournisseur. Autant dire qu’il n’y aurait aucune activité économique sans la confiance.

**4- Les systèmes de management de la sécurité de l'information (SMSI)**

Un SMSI est avant tout est un système de management , c’est évident, concerne la sécurité de l'information , ce qu’il s’agit d’assurer la confidentialité, l’intégrité, la disponibilité et la traçabilité de l’information au sens large .

Alors on peut définir les SMSI comme des ensembles d’éléments interactifs permettant à un organisme de fixer une politique et des objectifs de sécurité de l’information, d’appliquer la politique, d’atteindre ces objectifs, de les contrôler et de les améliorer.

Les objectifs sont fixés sur un périmètre défini et doivent être en adéquation avec les besoins de l’organisme concerné, c’est-à-dire que les mesures de sécurité sont à déployer en fonction du contexte, avec comme finalité la protection des actifs d’information.

1. **La norme**

Iso/cei 27001 :2013

**La norme** est destinée à servir de base dans les relations entre partenaires économiques, scientifiques,

techniques et sociaux.

La norme par nature est d’application volontaire. Référencée dans un contrat, elle s’impose aux parties.

Une réglementation peut rendre d’application obligatoire tout ou partie d’une norme.

**La norme est un document élaboré par consensus** au sein d’un organisme de normalisation par

sollicitation des représentants de toutes les parties intéressées. Son adoption est précédée d’une enquête

publique.

La norme fait l’objet d’un examen régulier pour évaluer sa pertinence dans le temps.

Toute norme est réputée en vigueur à partir de la date présente sur la première page.

<https://openclassrooms.com/fr/courses/1734201-definissez-la-politique-de-securite-de-votre-entreprise/6206511-apprehendez-la-mise-en-place-d-un-smsi>

**Chapitre 2 : Methodes Et Normes**

**Définitions**

**1.les normes**

La norme est, selon le guide ISO/CEI 2, « *un document de référence couvrant un large intérêt*

*industriel et basé sur un processus volontaire, approuvé par un organisme reconnu, fourni pour des*

*usages communs et répétés, des règles, des lignes directrices ou des caractéristiques, pour des*

*activités, ou leurs résultats, garantissant un niveau d’ordre optimal dans un contexte donné* ».

Les normes sont utilisées dans tous les actes de la vie économique. Elles représentent un

langage commun et un lien nécessaire entre les divers acteurs concernés.

L’élaboration de normes consiste donc à réunir le consensus, c’est-à-dire prendre en compte les

points de vue de tous les intéressés, aussi bien public que privé, clients que fournisseurs… La

démarche consiste à développer des solutions globales visant à satisfaire les industries et les clients au niveau mondial. La participation repose sur le principe du volontariat, et une norme « en construction » peut être soumise à enquête publique dans n’importe quel pays.

Parmi les normes formulées, diffusées et mises en application, nous pouvons distinguer différents types : les normes de base, de portée générale, de terminologie, d’essai, de produit, de processus, de service, d’interface ou encore portant sur des données. Elles peuvent relever de diverses catégories, à savoir : les “Normes internationales”, puis les “Normes européennes”, enfin, les “Normes nationales”, respectivement adoptées par un organisme international, européen, et national de normalisation. L’ensemble produit est toujours disponible auprès des organismes de normalisation.

**2. normalisation**

*“La normalisation a pour objet de fournir des documents de référence comportant des solutions à des*

*problèmes techniques et commerciaux concernant les produits, biens et services qui se posent de*

*façon répétée dans des relations entre partenaires économiques, scientifiques, techniques et*

*sociaux”.* [2]

La normalisation a permis de déterminer et de dégager des **normes**, que chacun utilise dans le but de faciliter les échanges, les pratiques, et les significations.

Aujourd’hui, la normalisation s’intéresse fortement au domaine de la sécurité de l’information en proposant depuis peu un modèle de gouvernance par l’intermédiaire de la norme ISO/IEC 27001 et de la certification associée.

**3.L’ISO (Organisation Internationale de Normalisation)**

L’ISO est le fruit d’une collaboration entre différents organismes de normalisation nationaux. Au début du 20ème siècle, L’American Institute of Electrical Engineer (Aujourd’hui appelé Institute of Electrical and Electronics Engineers ou IEEE) invite quatre autres instituts professionnels pour constituer une première organisation nationale, l’AESC (American Engineering Standards Committee) qui aura pour objectif de publier des standards industriels communs avant de prendre le nom d’ASA (American Standards Association) et d’établir des procédures standardisées pour la production militaire pendant la seconde guerre mondiale. En 1947, l’ASA, le BSI (British Standards Institute), l’AFNOR (Association Française de Normalisation) et les organisations de normalisation de 22 autres pays fondent l’Organisation Internationale de Normalisation (ISO).

A ce jour, l’ISO regroupe 157 pays membres, et coopère avec les autres organismes de normalisation comme le CEN (Comité européen de normalisation) ou la Commission Electronique Internationale (CEI).

Au niveau mondial, l’ISO [3] a pour missions l’élaboration de normes applicables, la promotion du développement de la standardisation et activités annexes, ainsi que le développement des

coopérations dans les sphères d’activités intellectuelles, scientifiques, technologiques et économiques. Cet organisme, plus communément connu sous le label International Organization for Standardization, ou encore Organisation Internationale de Normalisation.

Les résultats principaux de ses travaux se formalisent à travers la publication des standards internationaux : les normes ISO.

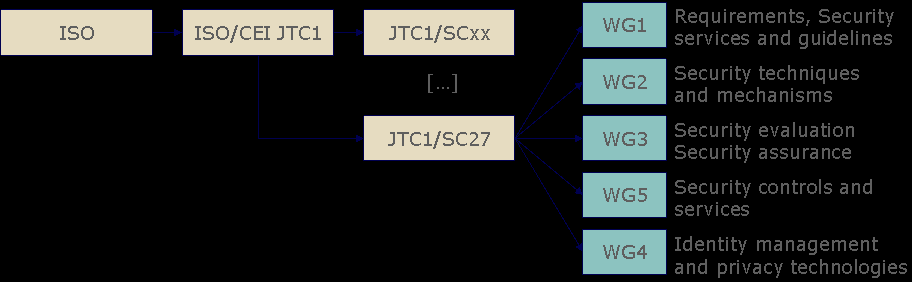
A ce jour, face à la mondialisation des échanges, à l’évolution des besoin métiers et à la diversification des menaces, l’ISO demeure un des organismes de normalisation les plus avancés dans le domaine de la sécurité de l’information.

**Le sous-comité ISO/JTC1/SC27**

En 1987, l’ISO et le ***CEI*** créent le Joint Technical Committee (***JTC1***) pour la normalisation des Technologies de l’Information (TI). Le JTC1 allie les compétences de l’ISO en matière de langage de programmation et codage de l’information avec celles du CEI qui traitent du matériel tel que les microprocesseurs.

Le JTC1 est composé de plusieurs comités techniques (SC) qui traitent de sujets tels que la biométrie, la téléinformatique, les interfaces utilisateurs ou encore les techniques de sécurité de l’information relatives aux normes de la série ISO/CEI 2700x.

La figure 1 ci-dessous montre la structure hiérarchique des différents groupes de travail tel que le WG15 issu du JTC1/SC27 de l‟ISO/CEI [1].



Le SC 27, composé de représentants de 47 pays, couvre la normalisation des techniques et des

méthodes génériques pour les besoins de sécurité des TI. Dans cette perspective, nous distinguons

deux axes forts : l’identification des besoins généraux pour les services de sécurité de l’information et

le développement des mécanismes et des techniques associés.

Le SC 27 se compose de cinq « Working Group » (WG) :

**WG1 - « *Exigences, services de sécurité et directives* »** ayant pour axe de travail le système

de gestion de la sécurité de l’information, avec la récente définition de la série 2700x, déclinant

une dizaine de normes touchant à la sécurité des systèmes d’information et de communication,

dont ISO 17799 (future ISO 27002), ISO 27001, ISO 27005…

**WG2 - « *Techniques et mécanismes de sécurité* »** traitant de la cryptologie (techniques et

algorithmes de chiffrement par exemple).

**WG3 - « *Critères d’évaluation de la sécurité* »** ayant les Critères Communs (ISO 15408) pour

domaine de travail principal (précisant les critères d’évaluation pour la sécurité des TI).

**WG4 - « *Services et contrôles de sécurité* »** traitant des anciens champs du WG1 ne relevant

pas de la nouvelle série 2700x (ISO 18028 sur les architectures de sécurité…).

**WG5 - « Sécurité biométrique, identité et vie privée »** dédié au domaine de la biométrie et du

respect de la vie privée (ISO 24760 par exemple).

Cette déclinaison du SC 27 en cinq WG est très récente (2006), et se met en place progressivement.

Depuis, de nombreuses normes se développent rapidement dans chaque WG.

**4- Historique des normes en matière de sécurité de l’information**

Depuis déjà de nombreuses années, la sécurité de l’information est devenue une préoccupation

importante au sein des organisations et des entreprises. Le British Standard Institute (BSI) fut, en

1995, le premier organisme à publier une norme dans ce domaine, appelée BS 7799, qui définissait

les bonnes pratiques pour la sécurité des systèmes d’information. L’ISO lui a emboîté le pas et a

publié de nombreuses normes dans le même domaine, telle que la norme ISO 17799, issue de BS

7799, ou ISO 13335 (lignes directrices pour la gestion de la sécurité). Ces différentes normes visent à

assurer la sécurité de l’information, que son support soit de nature électronique ou papier, et que la

cause des incidents potentiels soit accidentelle ou délibérée. Cependant, au vu des besoins et de la

demande grandissante du marché, l’ISO a depuis peu entrepris une refonte de l’ensemble de ses

normes dans l’objectif d’aller au-delà des bonnes pratiques et de proposer un modèle de gouvernance

de la sécurité de l’information.

Le WG1 est le groupe de travail chargé de rédiger et d’organiser les différentes normes ayant trait à

ce domaine en un ensemble cohérent. Le résultat de cette (r)évolution du monde de la sécurité de

l’information est l’émergence de la famille de normes ISO 2700x, définie de manière à devenir le

pendant de la sécurité au regard de la série des 900x pour le domaine de la qualité et 1400x pour

l’environnement. Le principal point commun entre ces séries de normes est une approche processus,

articulée autour de la méthode Plan-Do-Check-Act (PDCA) ou « roue de Deming », afin d’atteindre

une amélioration continue.

Au coeur de la famille 2700x se trouve la notion de « Système de Gestion de la Sécurité de

l’Information » (SGSI) ou *Information Security Management System* (*ISMS)* en anglais. Un SGSI

définit le cadre d’une amélioration continue de la sécurité de l’information, en se basant

principalement sur une approche de gestion des risques. Pour le moment, huit normes sont en

développement au sein de la série 2700x, dont une seule a déjà été publiée : ISO 27001 définissant

les exigences requises pour la certification d’un SGSI. A terme, l’ensemble intégré des normes de la

série des 2700x devrait permettre de former un modèle de gouvernance de la sécurité de

l’information.

*Figure*



**ISO/IEC 27000: *Overview and vocabulary.*** Cette première norme définit les fondamentaux et le

vocabulaire propres à la série. Elle est actuellement à son premier stade de construction, les

premiers commentaires de la communauté ISO datant de juin 2006. Dès la sortie de cette norme,

la première partie d’ISO 13335, traitant des concepts et modèles relatifs à la gestion de la sécurité

des TI, deviendra obsolète. A noter également que, suite aux résolutions de la dernière réunion

plénière du SC27 tenue en Afrique du Sud (novembre 2006), il a été décidé de rendre disponible

cette norme à titre gratuit.

**ISO/IEC 27001: *ISMS requirements.*** La norme ISO 27001 correspond à la révision de la norme

BS7799-2. Elle a été publiée en octobre 2005 et demeure à ce jour la seule norme de la famille

2700x dans ce cas. Elle est à la base de la certification d’un SGSI à l’instar de ces homologues

ISO 9001 pour la qualité et ISO 14001 pour l’environnement. Il faut également noter que depuis

sa publication, la norme BS 7799-2, dont la dernière révision datait de 2005, est obsolète.

**ISO/IEC 27002: *Code of practice for information security management*.** ISO 27002 sera la

nouvelle dénomination de la norme ISO 17799 dont la dernière revue date de 2005. Aucune mise

à jour sur le fond de la norme ne devrait accompagner la nouvelle numérotation. Sa publication

est attendue pour avril 2007.

**ISO/IEC 27003: *ISMS implementation guidance.*** La norme ISO 27003 a pour objectif de fournir

un guide d’aide à l’implémentation des exigences d’un SGSI. Cette norme sera plus

particulièrement orientée sur l’utilisation du cycle PDCA et des différentes exigences requises à

chaque étape du cycle. Sa publication est attendue pour octobre 2008.

**ISO/IEC 27004: *Information security management measurements*.** Cette norme a pour but

d’aider les organisations à mesurer et à rapporter l’efficacité de l’implémentation de leur SGSI. Sa

publication est attendue pour fin 2006 – début 2007.

**ISO/IEC 27005: *Information security risk management.*** La norme ISO 27005 est une

évolution de la norme ISO 13335. Elle reprendra les parties 3 et 4 de cette dernière, définissant

les techniques à mettre en oeuvre dans le cadre d’une démarche de gestion des risques. Sa

publication est attendue entre 2008 et 2009.

**ISO/IEC 27006: *Requirements for the accreditation of bodies providing certification of***

***ISMS.*** Cette norme, actuellement en cours de validation, a pour but de guider les organismes de

certification sur les exigences nécessaires à atteindre pour être accrédités en tant qu’organisme

de certification d’un SGSI. Elle devait paraître avant la fin de l’année 2006.

**ISO/IEC 27007: *Auditor guidelines.*** Rentrée très récemment en période d’étude, cette norme

va être un guide spécifique pour les audits d’ISMS, notamment en support à l’ISO 27006.

L'ensemble de ces normes constitue des standards internationaux. Elles sont donc destinées à tout

type de société, quelle que soit sa taille, son secteur d'activité ou son pays d’origine. Elles ont donc

pour but de décrire un objectif à atteindre et non la manière concrète d'y arriver, cette dernière étant

généralement dépendante du contexte de l'organisation.

Actuellement, aucun autre numéro de la série 2700x n’est spécifiquement attribué. Cependant, les

numéros allant de 27000 à 27010 sont réservés au sein de l'ISO pour la documentation générale d'un

SGSI. Il est donc à prévoir que d'autres normes s’ajoutent à celles actuellement en développement.

Par ailleurs, la série 27011 à 27019 est d'ores et déjà réservée à des normes dédiées à la

spécification d'un SGSI pour des secteurs économiques spécifiques (secteur financier,

télécommunication par exemple).

Le tableau ci-après reprend cet historique.

|  |  |  |  |
| --- | --- | --- | --- |
| **Année** | **Norme** | **Traite des SMSI** | **Remplace la norme** |
| **1995** | BS 7799:1995 | Non | |
| **1998** | BS 7799-2:1998 | Oui | |
| **2000** | ISO 17799:2000 | Non | BS 7799 :1995 |
| **2002** | BS 7799-2:2002 | Oui | BS 7799-2 :1998 |
| **2005** | ISO 17799:2005 | Non | ISO 17799 :2000 |
| **2005** | ISO 27001:2005 | Oui | BS 7799-2 :2002 |
| **2007** | ISO 27002 | Non | ISO 17799 :2005 |

**Historique des normes en matière de sécurité de l’information**

2- Les méthodes

Une méthode est une démarche, un processus ou un ensemble de principes qui permettent d’appliquer une norme au système d’information de l’entreprise. La méthode sert aussi à faire un audit qui permet de faire, par exemple, un état de la sécurité du système d’information. Une méthode est souvent accompagnée d’outils afin d’appuyer son utilisation. Ils peuvent être disponibles gratuitement auprès des organismes qui les ont produits. Par exemple la méthode **MEHARI**, que nous verrons plus loin, propose un outil (fichier **Microsoft Excel**). Le fichier contient un ensemble de questions et de scénarios. Cette base de connaissance permet de ressortir toutes les vulnérabilités du système d’information et émet des recommandations pour y remédier. La plupart des méthodes sont appliquées par des experts en gestion des ***risques (EBIOS, MEHARI, OCTAVE…).***

**Chapitre 3 : Normes ISO/CEI 27001**

**1.Introduction**

L'ISO/CEI 27001 est une norme internationale de sécurité des systèmes 'information de l'ISO et la CEI. Publiée en octobre 2005 et révisée en 2013, son titre est "Technologies de l'information - Techniques de sécurité - Systèmes de gestion de sécurité de l'information - Exigences". Elle fait partie de la suite ISO/CEI 27000 et permet de certifier des organisations

**2.Objectifs de la normes ISO/CEI 27001**

La norme ISO/CEI 27001, publiée en octobre 2005 et révisée en 2013, succède à la norme BS 7799-2 de BSI (British Standards Institution)[1]. Elle s’adresse à tous les types d’organismes (entreprises commerciales, ONG, administrations…) et définit les exigences pour la mise en place d'un système de management de la sécurité de l'information (SMSI). Le SMSI recense les mesures de sécurité, dans un périmètre défini, afin de garantir la protection des actifs de l'organisme. L’objectif est de protéger les fonctions et informations de toute perte, vol ou altération, et les systèmes informatiques de toute intrusion et sinistre informatique. Cela apportera la confiance des parties prenantes.

La norme précise que les exigences en matière de mesures de sécurité doivent être adéquates et proportionnées aux risques encourus donc n'être ni trop laxistes ni trop sévères.

L'ISO/CEI 27001 énumère un ensemble de points de contrôles à respecter pour s'assurer de la pertinence du SMSI, permettre de l'exploiter et de le faire évoluer. Plus précisément, l'annexe A de la norme est composée des 114 mesures de sécurité de la norme ISO/CEI 27002 (anciennement ISO/CEI 17799), classées dans 14 sections. Comme pour les normes ISO 9001 et ISO 14001, il est possible de faire certifier un organisme ISO/CEI 27001.

Des points ont disparu par rapport à la norme BS 7799-2 : l’ISO 27001 n’incorpore plus l’amélioration de la compétitivité, des cash flow, de la profitabilité, le respect de la réglementation et l’image de marque.

**3.La structure de la norme ISO/CEI 27001**

Dans sa version 2013, la norme est conforme à la nouvelle structure commune des normes de management de l'ISO, l'HLS [2]. Elle ne fait plus explicitement allusion au PDCA ou roue de Deming mais utilise à la place la formulation « établir, implémenter, maintenir, améliorer »[3].

La norme 27001 comporte 10 chapitres et une annexe ; les exigences qu'ils contiennent doivent être respectées pour obtenir une certification.

**Phase d'établissement (Plan)**

On y détermine les objectifs du SMSI. Cette phase d'établissement du SMSI comprend 4 étapes :

**Étape 1 : Définir la politique et le périmètre du SMSI**

**Périmètre** : domaine d’application du SMSI. Son choix est libre, mais il est essentiel, car il figure ensuite le périmètre de certification. Il doit comprendre tous les actifs métiers (actifs primordiaux au sens de la norme ISO/CEI 27005) et les actifs support à ces activités qui sont impliquées dans le SMSI.

**Politique** : niveau de sécurité (intégrité, confidentialité, disponibilité de l’information) qui sera pratiqué au sein de l’entreprise. La norme n’impose pas de niveau minimum de sécurité à atteindre dans le SMSI. Son niveau devant être proportionné aux risques évalués.

Le choix du périmètre et de la politique étant libre, ces deux éléments sont des « leviers de souveraineté » pour l’entreprise. Ainsi, une entreprise peut être certifiée ISO 27001 tout en définissant un périmètre très réduit et une politique de sécurité peu stricte et sans répondre aux exigences de ses clients en matière de sécurité.

**Étape 2 : Identifier et évaluer les risques liés à la sécurité et élaborer la politique de sécurité**

La norme ISO 27001 ne donne pas de directives sur la méthode d’appréciation des risques à adopter. Les entreprises peuvent donc en inventer une en veillant à bien respecter le cahier des charges ou en choisir une parmi les plus courantes notamment la méthode EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité) mise en place en France par l'ANSSI (Agence Nationale de la Sécurité des Systèmes d’Information).

Le cahier des charges relatif à l’appréciation des risques se développe en 7 points :

1. Identifier les actifs ;

2. Identifier les personnes responsables ;

3. Identifier les vulnérabilités ;

4. Identifier les menaces ;

5. Identifier leurs impacts sur les actifs à défendre ;

6. Évaluer la vraisemblance ou potentialité du risque ;

7. Estimer les niveaux de risque, fonction de leur potentialité et de leur impact.

**Étape 3 : Traiter le risque et identifier le risque résiduel par un plan de gestion**

Il existe quatre traitements possibles de chacun des risques identifiés, présentés par ordre décroissant d'intérêt pour l'organisme :

1. **L’évitement** : politique mise en place si l’incident est jugé inacceptable ou si les mesures sont aisément accessibles. Il s'agit de réorganiser le système d'information à protéger de façon à éliminer totalement la potentialité du risque.

2. **La réduction** : on ramène la potentialité et/ou l'impact du risque à un niveau acceptable par la mise en oeuvre de mesures techniques et organisationnelles. C'est la solution la plus utilisée.

3. **Le transfert** (ou partage) : la part de risque qui ne peut pas être évitée ou réduite est dénommée **risque résiduel**. L'organisme peut transférer la responsabilité technique de tout ou partie de ce risque résiduel en recourant à une solution d'externalisation de sécurité. Il peut aussi souscrire une assurance pour diminuer l'impact financier du risque.

4. **L’acceptation** (ou maintien) : ne mettre en place aucune mesure de sécurité

supplémentaire car les conséquences du risque résiduel non transférable sont

acceptables. Par exemple, le vol d’un ordinateur portable ne comportant pas de

données primordiales pour l’entreprise est sans grand impact. Cette solution peut n'être que ponctuelle.

Lorsque la décision de traitement du risque est prise, l’entreprise doit identifier les risques résiduels c’est-à-dire ceux qui persistent après la mise en place des mesures de sécurité. S'ils sont jugés inacceptables, il faut définir des mesures de sécurité supplémentaires. Cette phase d'acceptation formelle des risques résiduels s'inscrit souvent dans un processus d'homologation. Le système étant homologué en tenant compte de ces risques résiduels.

**Étape 4 : Choisir les mesures de sécurité à mettre en place**

La norme ISO 27001 contient une annexe A qui propose 114 mesures de sécurité classées en 14 catégories (politique de sécurité, sécurité du personnel, contrôle des accès…) Cette annexe normative, n'est qu’une liste qui ne donne aucun conseil de mise en oeuvre au sein de l’entreprise. Les mesures sont présentées dans la norme ISO 27002.

**Phase d'implémentation (Do)**

Met en place les objectifs. Elle comporte plusieurs étapes :

1. Établir un plan de traitement des risques

2. Déployer les mesures de sécurité

3. Générer des indicateurs De performance pour savoir si les mesures de sécurité sont efficaces De conformité qui permettent de savoir si le SMSI est conforme à ses

spécifications

4. Former et sensibiliser le personnel

**Phase de maintien (Check)**

Consiste à gérer le SMSI au quotidien et à détecter les incidents en permanence pour y réagir rapidement. Trois outils peuvent être mis en place pour détecter ces incidents :

1. Le contrôle interne qui consiste à s’assurer en permanence que les processus

fonctionnent normalement.

2. Les audits internes qui vérifient la conformité et l’efficacité du système de management.

Ces audits sont ponctuels et planifiés.

3. Les revues (ou réexamens) qui garantissent périodiquement l’adéquation du SMSI avec son environnement.

**Phase d'amélioration (Act)**

Mettre en place des actions correctives, préventives ou d’amélioration pour les incidents et écarts constatés lors de la phase Check Actions correctives : agir sur les effets pour corriger les écarts puis sur les causes pour éviter que les incidents ne se reproduisent Actions préventives : agir sur les causes avant que l’incident ne se produise Actions d’amélioration : améliorer la performance d’un processus du SMSI.