Université Mohammed V Agdal
Faculté des Sciences Rabat

DEPARTEMENT D'INFORMATIQUE

FILIERE

LICENCE PROFESSIONNELLE

Administration de Systèmes Informatiques

PROJET OFFSHORING MAROC 2010

Mémoire de Projet de Fin d'Etudes

[Audit Sécurité des Systèmes d'Information]

Résumé

L'audit sécurité d'un système d'information est indispensable pour toute organisation qui décide de changements au sein de son système d'information ou de s'assurer de son fonctionnement optimal.

Comme toute démarche qualité, il nécessite une méthodologie rigoureuse et une communication idéale au sein de l'équipe.

Encadré par :

Pr. El Mamoun SOUIDI

Réalisé par :

M. Abbes RHARRAB

Promotion 2011 - 2012

Remerciements

J'exprime toute ma reconnaissance et gratitude à l'ensemble des enseignants de la Licence Professionnelle - Administration des Systèmes Informatiques, de *l'Université Mohammed V Agdal - Faculté des Sciences Rabat* pour leurs efforts à nous fournir une meilleure formation.

Je tiens à remercier mon encadrant Pr. **El Mamoun SOUIDI** de m'avoir permis d'aborder ce thème qui m'a ouvert de nouvelles options en terme de carrière.
Je remercie chaleureusement Mes parents, ma famille, et aussi M.**Mohammed EL HARFAOUI** pour ça précieuse aide, ainsi que tous ceux qui, d'une manière ou d'une autre, ont contribué à la réussite de ce travail et qui n'ont pas pu être cités ici.

Résumé

L'audit de la sécurité d'un système d'information est indispensable pour toute organisation qui décide de changements au sein de son système d'information ou de s'assurer de son fonctionnement optimal.
Comme toute démarche qualité, il nécessite une méthodologie rigoureuse et une communication idéale au sein de l'équipe.

Mots clefs

Audit, Sécurité, Système, information, management, Système d'information, Système de management, Système de Management de la Sécurité de l'Information, SMSI.

Sommaire

Introduction

De nos jours les entreprises sont de plus en plus connectées tant en interne que dans le monde entier, profitant ainsi de l'évolution des réseaux informatiques et la dématérialisation des documents. De ce fait, leur système d'information est accessible de l'extérieur pour leurs fournisseurs, clients, partenaires et administrations. L'accessibilité par l'extérieur entraine la vulnérabilité vis à vis les attaques, mais aussi on peut pas négliger les menaces qui viennent de l'intérieur, ce qui rend l'investissement dans des mesures de protection et de sécurité indispensable, et la mise en œuvre d'un plan de sécurité issu d'un examen méthodique d'une situation liée à la sécurité de l'information en vue de vérifier sa conformité à des objectifs, à des règles, et à des normes ou référentiels, afin de cerner les différentes composantes de la sécurité du Système d'Information, et pour atteindre un niveau de sécurisation répondant aux objectifs organisationnels et techniques.

Chapitre 1 : Généralités

I- Qu'est-ce qu'un Systèmes d'Information ?

1- Qu'est-ce qu'un Systèmes ?

Un système est un ensemble d'éléments en relation les uns les autres et formant un tout. Il représente une unité parfaitement identifiable et évoluant dans un environnement. Il existe donc une limite qui départage le système de son environnement.

2- Qu'est-ce qu'un Système d'Information ?

Un **système d'Information** (noté **SI**) est un ensemble organisé de ressources (matériels, logiciels, personnel, données et procédures) qui représente l'ensemble des éléments participant à la gestion, au traitement, au transport et à la diffusion de l'information au sein de l'entreprise.

A l'origine les systèmes d'informations ont fait leur première apparition dans les domaines de l'informatique et des télécommunications, cependant nous voyons aujourd'hui apparaître le concept dans tous les secteurs, que ce soit des entreprises privées ou publiques.

3- En quoi consiste un Système d'information ?

Un système d'information peut être apparenté au véhicule qui permettra d'établir la communication dans toute l'entreprise. La Structure du système est constituée de l'ensemble des ressources (hommes, matériels, logiciels) qui s'organise pour : collecter, stocker, traiter et communiquer les informations. Le système d'information est le grand coordinateur des activités de l'entreprise et qui joue un rôle crucial dans l'atteinte des objectifs fixer par cette dernière.

Le SI se construit tout autour des processus « métier » et ses interactions. Pas seulement autour des bases de données ou des logiciels informatiques qui le constitue. Le SI doit être en accord avec la stratégie de l'entreprise.

II- La Sécurité de l'Information

1- C'est quoi la « Sécurité de l'information » ?

Pour des soucis d'efficacité et de rentabilité, une entreprise communique aujourd'hui avec ses filiales, ses partenaires et va jusqu'à offrir des services aux particuliers, ce qui induit une ouverture massive à l'information. Par l'ouverture des réseaux, la sécurité devient un facteur décisif du bon fonctionnement de l'entreprise ou de l'organisme.

Il reste qu'une entreprise ou un organisme possède certaines informations qui ne doivent être divulguées qu'à un certain nombre de personnes ou qui ne doivent pas être modifiées ou encore qui doivent être disponibles de manière transparente à l'utilisateur. Ces informations feront l'objet d'une attaque par ce que des menaces existent et que le système abritant ces informations est vulnérable.

Par conséquent on appelle sécurité de l'information, l'ensemble des moyens techniques, organisationnels, juridiques, et humains mis en place pour faire face aux risques identifiés, afin d'assurer la confidentialité, l'intégrité, la disponibilité, et la Traçabilité de l'information traitée:

- La **Confidentialité** : l'information ne doit pas être divulguée à toute personne, entité ou processus non autorisé. En clair, cela signifie que l'information n'est consultable que par ceux qui ont le droit d'y accéder (on dit aussi « besoin d'en connaître »).

- L'**Intégrité** : le caractère correct et complet des actifs doit être préservé. En clair, cela signifie que l'information ne peut être modifiée que par ceux qui en ont le droit.

- La **Disponibilité** : l'information doit être rendue accessible et utilisable sur demande par une entité autorisée. Cela veut dire que l'information doit être disponible dans des conditions convenues à l'avance (soit 24h/24, soit aux heures ouvrables, etc.).

– La **Traçabilité** (ou « *Preuve* ») : garantie que les accès et tentatives d'accès aux éléments considérés sont tracés et que ces traces sont conservées et exploitables.

2- Pourquoi se protéger ?

Parce que on estime que si la perte des informations, va provoquerait :

- Une **perte financière** (exemple : destruction de fichiers client, récupération de contrats par un concurrent,...)

- Une **perte de l'image de marque** (exemple : piratage d'une banque, divulgation d'un numéro de téléphone sur liste rouge,...)

- Une **perte d'efficacité ou de production** (exemple : rendre indisponible un serveur de fichiers sur lequel travaillent les collaborateurs)

3- Qu'est-ce qu'une « politique de sécurité de l'information » ?

Une politique de sécurité de l'information est un ensemble de documents indiquant les directives, procédures, ligne de conduite, règles organisationnelles et techniques à suivre relativement à la sécurité de l'information et à sa gestion. C'est une prise de position et un engagement clair et ferme de protéger l'intégrité, la confidentialité et la disponibilité de l'actif informationnel de l'entreprise.

La politique de sécurité de l'information vous permet de définir, réaliser, entretenir et améliorer la sécurité de l'information au sein de votre entreprise. Elle vous permet aussi de protéger les infrastructures et actifs critiques de votre entreprise.

Chapitre 2 : Mission d'audit sécurité des systèmes d'information

I- Audit sécurité des systèmes d'information

1- Qu'est-ce qu'un Audit ?

En informatique, le terme « **Audit** (une écoute) » est apparu dans les années 70 et a été utilisé de manière relativement aléatoire. Nous considérons par la suite un "audit sécurité de l'information" comme une mission d'évaluation de conformité par rapport à une politique de sécurité ou à défaut par rapport à un ensemble de règles de sécurité.
Une mission d'audit ne peut ainsi être réalisée que si l'on a défini auparavant un référentiel, c'est-à-dire en l'occurrence, un ensemble de règles organisationnelles, procédurales ou/et techniques de référence. Ce référentiel permet au cours de l'audit d'évaluer le niveau de sécurité réel du " ***terrain*** " par rapport à une cible.

Pour évaluer le niveau de conformité, ce référentiel doit être :

- **Complet** (mesurer l'ensemble des caractéristiques : il ne doit pas s'arrêter au niveau système, réseau, télécoms ou applicatif, de manière exclusive, de même, il doit couvrir des points techniques et organisationnels) ;
- **Homogène** : chaque caractéristique mesurée doit présenter un poids cohérent avec le tout ;
- **Pragmatique** : c'est-à-dire, aisé à quantifier (qualifier) et à contrôler. Ce dernier point est souvent négligé.

La mission d'audit consiste à mesurer le niveau d'application de ces règles sur le système d'information par rapport aux règles qui devraient être effectivement appliquées selon les processus édictés. L'audit est avant tout un constat.

2- Rôles et objectifs de l'audit

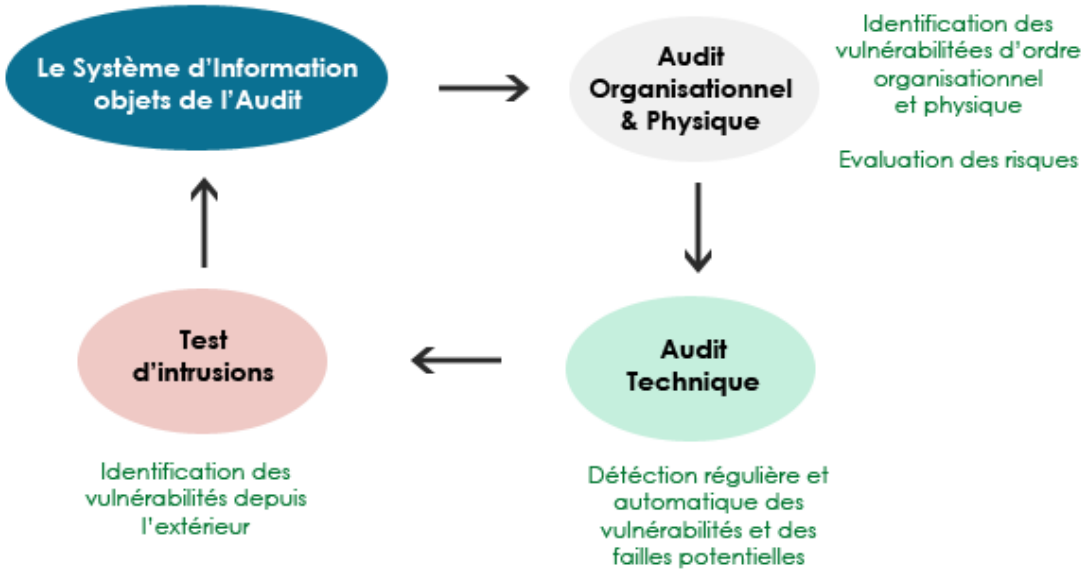
Une mission d'audit vise différents objectifs. En effet nous pouvons énumérer à ce titre :

-La détermination des déviations par rapport aux bonnes pratiques de sécurité.
-La proposition d'actions visant l'amélioration du niveau de sécurité du système d'information.

Egalement, une mission d'audit de sécurité d'un système d'information se présente comme un moyen d'évaluation de la conformité par rapport à une politique de sécurité ou par rapport à un ensemble de règles de sécurité.

3- Cycle de vie d'un audit sécurité des systèmes d'information

Le processus d'audit de sécurité est un processus répétitif et perpétuel. Il décrit un cycle de vie qui est schématisé à l'aide de la figure suivante :



Le cycle de vie d'audit de sécurité

L'audit de sécurité informatique se présente essentiellement suivant deux parties comme le présente le précédent schéma :

- L'audit organisationnel et physique.

- L'audit technique.

Une troisième partie optionnelle peut être également considérée. Il s'agit de l'audit Intrusif (test d'intrusions). Enfin un rapport d'audit est établi à l'issue de ces étapes. Ce rapport présente une synthèse de l'audit. Il présente également les recommandations à mettre en place pour corriger les défaillances organisationnelles ou techniques constatées.

II- Démarche de réalisation d'un audit Sécurité de Système d'Information

Dans la section précédente on a évoqué les principales étapes de l'audit de sécurité des systèmes d'information. Cependant il existe une phase tout aussi importante qui est une phase de préparation.

Nous pouvons schématiser l'ensemble du processus d'audit comme suite :

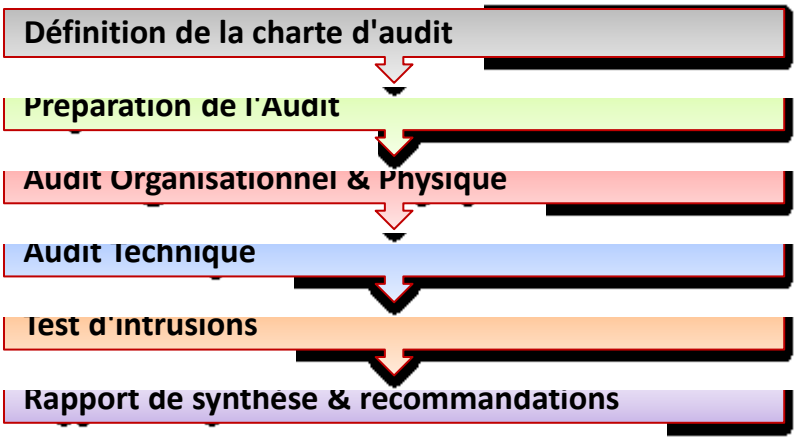


Schéma du processus d'audit

1- Définition de la charte d'audit

Avant de procéder à une mission audit, une chartre d'audit doit être réalisée, elle a pour objet de définir la fonction de l'audit, les limites et modalités de son interventions, ses responsabilités ainsi que les principes régissant les relations entre les auditeurs et les audités. Elle fixe également les qualités professionnelles et morales requises des auditeurs.

2- Préparation de l'audit

Cette phase est aussi appelée phase de pré audit. Elle constitue une phase importante pour la réalisation de l'audit sur terrain. En effet, c'est au cours de cette phase que se dessinent les grands axes qui devront être suivis lors de l'audit sur terrain. Elle se manifeste par des rencontres entre auditeurs et responsables de l'organisme à auditer. Au cours de ces entretiens, les espérances des responsables vis-à-vis de l'audit devront être exprimées. Aussi, le planning de réalisation de la mission de l'audit doit être fixé.

Les personnes qui seront amenées à répondre au questionnaire concernant l'audit organisationnel doivent être également identifiées. L'auditeur (ou les auditeurs) pourrait également solliciter les résultats des précédents audits. Cette phase sera suivie par l'audit organisationnel et physique.

3- Audit organisationnel et physique

a. Objectifs

Dans cette étape, il s'agit de s'intéresser à l'aspect physique et organisationnel de l'organisme cible, à auditer. Nous nous intéressons donc aux aspects de gestion et d'organisation de la sécurité, sur les plans organisationnels, humains et physiques.

L'objectif visé par cette étape est donc d'avoir une vue globale de l´état de sécurité du système d´information et d´identifier les risques potentiels sur le plan organisationnel.

b. Déroulement

Afin de réaliser cette étape de l'audit, ce volet doit suivre une approche méthodologique qui s'appuie sur « une batterie de questions ». Ce questionnaire préétabli devra tenir compte et s'adapter aux réalités de l'organisme à auditer. A l'issu de ce questionnaire, et suivant une métrique, l'auditeur est en mesure d'évaluer les failles et d'apprécier le niveau de maturité en termes de sécurité de l'organisme, ainsi que la conformité de cet organisme par rapport à la norme référentielle de l'audit.

4- Audit technique

a. Objectifs

Cette étape de l'audit sur terrain vient en seconde position après celle de l'audit organisationnel. L'audit technique est réalisé suivant une approche méthodique allant de la découverte et la reconnaissance du réseau audité jusqu'au sondage des services réseaux actifs et vulnérables.

Cette analyse devra faire apparaître les failles et les risques, les conséquences d'intrusions ou de manipulations illicites de données. Au cours de cette phase, l'auditeur pourra également apprécier l'écart avec les réponses obtenues lors des entretiens. Il testera aussi la robustesse de la sécurité du système d'information et sa capacité à préserver les aspects de confidentialité, d'intégrité, de disponibilité et d'autorisation.

Cependant, l'auditeur doit veiller à ce que les tests réalisés ne mettent pas en cause la continuité de service du système audité.

b. Déroulement

Vu les objectifs escomptés lors de cette étape, leurs aboutissements ne sont possibles que par l'utilisation de différents outils. Chaque outil commercial qui devra être utilisé, doit bénéficier d'une licence d'utilisation en bonne et due forme.

Egalement les outils disponibles dans le monde du logiciel libre sont admis. L'ensemble des outils utilisés doit couvrir entièrement ou partiellement la liste non exhaustive des catégories ci-après :

- Outils de sondage et de reconnaissance du réseau.
- Outils de test automatique de vulnérabilités du réseau.
- Outils spécialisés dans l'audit des équipements réseau (routeurs, switchs).
- Outils spécialisés dans l'audit des systèmes d'exploitation.
- Outils d'analyse et d'interception de flux réseaux.
- Outils de test de la solidité des objets d'authentification (fichiers de mots clés)
- Outils de test de la solidité des outils de sécurité réseau (firewalls, IDS, outils d'authentification).
- Outils de scanne d'existence de connexions dial-up dangereuses (wardialing).
- Outils spécialisés dans l'audit des SGBD existants.

Chacun des outils à utiliser devra faire l'objet d'une présentation de leurs caractéristiques et fonctionnalités aux responsables de l'organisme audité pour les assurer de l'utilisation de ces outils.

5- Test d'intrusions (Audit intrusif)

a. Objectifs

Cet audit permet d'apprécier le comportement du réseau face à des attaques. Egalement, il permet de sensibiliser les acteurs (management, équipe informatique sur site, les utilisateurs) par des rapports illustrant les failles décelées, les tests qui ont été effectués (scénarios et outils) ainsi que les recommandations pour pallier aux insuffisances identifiées.

b. Déroulement

La phase de déroulement de cet audit doit être réalisée par une équipe de personnes ignorante du système audité avec une définition précise des limites et horaires des tests. Etant donné l'aspect risqué (pour la continuité de services du système d'information) que porte ce type d'audit, l'auditeur doit.

- Bénéficier de grandes compétences.

- Adhérer á une charte déontologique.

- S'engager (***la charte d'audit***) à un non débordement: implication à ne pas provoquer de perturbation du fonctionnement du système, ni de provocation de dommages.

6- Rapport d'audit

A la fin des précédentes phases d'audit sur terrain, l'auditeur est invité à rédiger un rapport de synthèse sur sa mission d'audit.

Cette synthèse doit être révélatrice des défaillances enregistrées. Autant est-il important de déceler un mal, autant il est également important d'y proposer des solutions. Ainsi, l'auditeur est également invité à donner ses recommandations, pour pallier aux défauts qu'il aura constatés.

Ces recommandations doivent tenir compte de l'audit organisationnel et physique, ainsi que de celui technique et intrusif.

Chapitre 3 : Méthodes et Normes d'audit sécurité des systèmes d'information

I- Définitions

Les concepts de méthode de sécurité et de norme de sécurité portent souvent à confusion. Nous allons tenter de définir chacun de ces concepts.

1- 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). 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.

2- Les normes

Une norme est, selon le guide ***ISO/CEI***, « *un document de référence approuvé par un organisme reconnu, et qui 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 entreprises se font certifier pour prouver qu'elles suivent les recommandations de la norme. Pour être certifié, il faut, dans un premier temps acheter la norme. Les normes appliquées à la sécurité des systèmes d'information sont généralement éditées par l'organisme ISO. Ensuite l'entreprise doit mettre en pratique les recommandations décrites dans la norme.

Généralement, une entreprise peut se faire certifier pour trois raisons :

- Pour une **raison commerciale**. Pour certaines entreprises, être certifiées par des normes de qualité par exemple est un gage de qualité pour les clients et est donc un atout commercial.

- Par **obligation**. En industrie aéronautique par exemple, les constructeurs exigent de leurs sous-traitants qu'ils soient certifiés par certaines normes.

- Il y a aussi des entreprises qui se certifient pour elles-mêmes, pour optimiser leur processus en interne.

3- 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…).***

4- Historique des normes en matière de sécurité de l'information

Au cours des vingt dernières années les normes liées à la sécurité de l'information ont évolué ou ont été remplacées. Ces changements rendent difficile une bonne compréhension du sujet. Un rappel historique de l'évolution de ces normes permet de clarifier la situation normative en matière de sécurité de l'information.

Au début des années 90, de grandes entreprises britanniques se concertent pour établir des mesures visant à sécuriser leurs échanges commerciaux en ligne. Le résultat de cette collaboration servit de référence en la matière pour d'autres entreprises qui souhaitaient mettre en œuvre ces mesures. Cette initiative privée fut appuyée par le Département des Transports et de l'Industrie britannique qui supervisa la rédaction au format du BSI, d'une première version de projet de norme de gestion de la sécurité de l'information.

En **1991**, un projet de «best practices» code de bonnes pratiques, préconise la formalisation d'une politique de sécurité de l'information. Cette politique de sécurité doit intégrer au minimum huit points «stratégique et opérationnel» ainsi qu'une mise à jour régulière de la politique.

En **1995**, le BSI publie la norme BS7799 qui intègre dix chapitres réunissant plus de 100 mesures détaillées de sécurité de l'information, potentiellement applicables selon l'organisme concerné.

En **1998**, la norme BS7799 change de numérotation et devient la norme BS7799-1. Elle est complétée par la norme BS7799-2 qui précise les exigences auxquelles doit répondre un organisme pour mettre en place une politique de sécurité de l'information. Cette nouvelle norme est fondée sur une approche de la maîtrise des risques et sur le principe du management de la sécurité de l'information.

En **2000**, la norme BS7799-1, devient la norme de référence internationale pour les organismes souhaitant renforcer leur sécurité de l'information. Après avoir suivi un processus de concertation au niveau international et quelques ajouts, l'ISO lui attribue un nouveau nom, ISO/IEC 17799: 2000.

En **2002**, le BSI fait évoluer la norme BS7799-2 en s'inspirant des normes ISO 9001 :2000 et ISO 14001: 1996. La norme adopte définitivement une approche de management de la sécurité de l'information.

En **2005**, l'ISO/CEI adopte la norme BS7799-2 sous la référence ISO/CEI 27001: 2005 en y apportant quelques modifications pour se rapprocher le plus possible du principe de «système de management » développé par les normes ISO 9001 et ISO14001. L'ISO/IEC 27001: 2005 spécifie les exigences pour la mise en place d'un SMSI (Système de Management de la Sécurité de l'Information).

En **2007**, dans un souci de clarification, l'ISO renomme la norme ISO/IEC 17799 :2005 en changeant sa numérotation pour ISO/IEC 27002. La norme se greffe à la famille des normes ISO/IEC 2700x toujours en développement.

Aujourd'hui les organismes disposent de deux normes qui se sont imposées comme référence des SMSI, l'ISO/CEI 27001 :2005 qui décrit les exigences pour la mise en place d'un Système de Management de la Sécurité de l'Information et l'ISO/CEI 27002 qui regroupe un ensemble de bonnes pratiques «best practices» pour la gestion de la sécurité de l'information.

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

II- La suite des normes ISO 2700x

ISO/IEC 27000 : Systèmes de management de la sécurité de l'information – Vue d'ensemble et vocabulaire

(aussi connue sous le nom de Famille des standards SMSI ou ISO27k) comprend les normes de sécurité de l'information publiées conjointement par l'Organisation internationale de normalisation (ISO) et la Commission électrotechnique internationale (CEI, ou IEC en anglais).

La suite contient des recommandations des meilleures pratiques en management de la sécurité de l'information, pour l'initialisation, l'implémentation ou le maintien de systèmes de management de la sécurité de l'information (**SMSI**, ou **ISMS en anglais**), ainsi qu'un nombre croissant de normes liées au SMSI.

- ***ISO/CEI 27000 :*** Systèmes de management de la sécurité de l'information -- Vue d'ensemble et vocabulaire
- ***ISO/CEI 27001 :*** Systèmes de management de la sécurité de l'information -- Exigences
- ***ISO/CEI 27002 :*** Code de bonne pratique pour le management de la sécurité de l'information
- ***ISO/CEI 27003 :*** Lignes directrices pour la mise en œuvre du système de management de la sécurité de l'information
- ***ISO/CEI 27004 :*** Management de la sécurité de l'information -- Mesurage
- ***ISO/CEI 27005 :*** Gestion des risques liés à la sécurité de l'information
- ***ISO/CEI 27006 :*** Exigences pour les organismes procédant à l'audit et à la certification des systèmes de management de la sécurité de l'information
- ***ISO/CEI 27007 :*** Lignes directrices pour l'audit des systèmes de management de la sécurité de l'information

ISO/CEI 27001 : Systèmes de management de la sécurité de l'information -- Exigences

L'ISO/CEI 27001 est la norme centrale de la famille ISO 2700x, c'est la norme d'exigences qui définit les conditions pour mettre en œuvre et documenter un SMSI, publiée en octobre 2005 par l'ISO.

Objectifs

La norme ISO 27001 publiée en octobre 2005 succède à la norme BS 7799-2 de BSI (British Standards Institution). Elle s'adresse à tous les types d'organismes (entreprises commerciales, administrations, etc…). La norme ISO/CEI 27001 décrit les exigences pour la mise en place d'un Système de Management de la Sécurité de l'Information. Le SMSI est destiné à choisir les mesures de sécurité afin d'assurer la protection des biens sensibles d'une entreprise sur un périmètre défini. C'est le modèle de qualité PDCA (Plan-Do-Check-Act) qui est recommandé pour établir un SMSI afin d'assurer une amélioration continue de la sécurité du système d'information.

La norme dicte également les exigences en matières de mesures de sécurité propres à chaque organisme, c'est-à-dire que la mesure n'est pas la même d'un organisme à l'autre. Les mesures doivent être adéquates et proportionnées à l'organisme pour ne pas être ni trop laxistes ni trop sévères. La norme ISO 27001 intègre aussi le fait que la mise en place d'un SMSI et d'outils de mesures de sécurité aient pour but de garantir la protection des actifs informationnels. L'objectif est de protéger les informations de toute perte ou intrusion. Cela apportera la confiance des parties prenantes.

L'ISO/CEI 27001 définit l'ensemble des contrôles à effectuer pour s'assurer de la pertinence du SMSI, à l'exploiter et à le faire évoluer. Plus précisément, l'annexe A de la norme est composée des 133 mesures de sécurité de la norme ISO/CEI 27002 (anciennement ISO/CEI 17799), classées dans 11 sections. Comme pour les normes ISO 9001 et ISO 14001, il est possible de se faire certifier ISO 27001.

ISO/CEI 27002 : Code de bonne pratique pour le management de la sécurité de l'information

La norme ISO/CEI 27002 est une norme internationale concernant la sécurité de l'information, publiée en 2005 par l'ISO, dont le titre en français est Code de bonnes pratiques pour le management de la sécurité de l'information.

L'ISO/CEI 27002 est un ensemble de 133 mesures dites « best practices » (bonnes pratiques en français), destinées à être utilisées par tous ceux qui sont responsables de la mise en place ou du maintien d'un Système de Management de la Sécurité de l'Information.

La sécurité de l'information est définie au sein de la norme comme la « *préservation de la confidentialité, de l'intégrité et de la disponibilité de l'information* ».

Cette norme n'a pas de caractère obligatoire pour les entreprises. Son respect peut toutefois être mentionné dans un contrat : un prestataire de services pourrait ainsi s'engager à respecter les pratiques normalisées dans ses relations avec un client.

Objectifs

ISO/IEC 27002 est plus un code de pratique, qu'une véritable norme ou qu'une spécification formelle telle que l'ISO/IEC 27001. Elle présente une série de contrôles (39 objectifs de contrôle) qui suggèrent de tenir compte des risques de sécurité des informations relatives à la confidentialité, l'intégrité et les aspects de disponibilité. Les entreprises qui adoptent l'ISO/CEI 27002 doivent évaluer leurs propres risques de sécurité de l'information et appliquer les contrôles appropriés, en utilisant la norme pour orienter l'entreprise.

La norme ISO 27002 n'est pas une norme au sens habituel du terme. En effet, ce n'est pas une norme de nature technique, technologique ou orientée produit, ou une méthodologie d'évaluation d'équipement telle que les critères communs CC/ISO 15408. Elle n'a pas de caractère d'obligation, elle n'amène pas de certification, ce domaine étant couvert par la norme ISO/IEC 27001.

ISO/CEI 27003 : Lignes directrices pour la mise en œuvre du système de management de la sécurité de l'information

La norme ISO/CEI 27003 fournit une approche orientée processus pour la réussite de la mise en œuvre d'un SMSI conformément à l'ISO 27001.

Objectifs

Le but de l'ISO / CEI 27003 est de fournir aide et les conseils à mettre en œuvre un Système de Management de la Sécurité de l'Information.

ISO / IEC 27003 guide la conception d'une norme ISO / IEC 27001-SGSI conforme, conduisant à l'ouverture d'un SMSI [la mise en œuvre du projet]. Il décrit le processus du SMSI et la spécification de conception, du début jusqu'à la production des plans d'exécution des projets, couvrant la préparation et la planification des activités préalables à la mise en œuvre effective, et en prenant des éléments clés tels que:

- Approbation de la direction et l'autorisation définitive de procéder à l'exécution des projets;
- Détermination de la portée et la définition des limites en termes de TIC et les lieux physiques;
- L'évaluation des risques sécurité de l'information et de la planification des traitements de risque appropriés, le cas échéant en définissant des exigences de contrôle de sécurité de l'information;

- Conception du SMSI;
- La planification du projet mise en œuvre.

ISO/CEI 27004 : Management de la sécurité de l'information -- Mesurage

ISO / CEI 27004 couvre les mesures de management de sécurité de l'information, généralement connu comme les mesures de sécurité. Élaborée par l'ISO et la Commission électrotechnique internationale (CEI). Son nom complet est la technologie de l'information - Techniques de sécurité - Management de la sécurité de l'information -- Mesurage.

Objectifs

Le but de la norme ISO / IEC 27004 est d'aider les organisations à mesurer, rapporter et donc d'améliorer systématiquement l'efficacité de leurs systèmes de gestion de sécurité de l'information (SGSI).

La norme est destinée à aider les organisations à mesurer, rendre compte et donc d'améliorer systématiquement l'efficacité de leurs systèmes de gestion de l'information de sécurité.

ISO/CEI 27005 : Gestion des risques liés à la sécurité de l'information

La première norme de gestion des risques de la Sécurité des Systèmes d'Information : l'ISO/CEI 27005. Cette norme est un standard international qui décrit le Système de Management des risques liés à la Sécurité de l'information.

Certains expliquent que cette norme est en fait une méthode quasi-applicable en se servant des annexes et en les adaptant à leur contexte. D'ailleurs dans l'enquête 2010 du CLUSIF, 35% des entreprises qui font analyses de risques déclarent le faire en utilisant la norme ISO 27005.

Objectifs

La norme ISO 27005 explique en détail comment conduire l'appréciation des risques et le traitement des risques, dans le cadre de la sécurité de l'information. La norme ISO 27005 propose une méthodologie de gestion des risques en matière d'information dans l'entreprise conforme à la norme ISO/CEI 27001. La nouvelle norme a donc pour but d'aider à mettre en œuvre l'ISO/CEI 27001, la norme relative aux systèmes de management de la sécurité de l'information (SMSI), qui est fondée sur une approche de gestion du risque. Néanmoins, la norme ISO 27005 peut être utilisée de manière autonome dans différentes situations. La norme ISO 27005 applique à la gestion de risques le cycle d'amélioration continue PDCA (Plan, Do, Check, Act) utilisé dans toutes les normes de systèmes de management.

ISO/CEI 27006 : Exigences pour les organismes procédant à l'audit et à la certification des systèmes de management de la sécurité de l'information

ISO/CEI 27006 est un standard de sécurité de l'information publié conjointement par l'ISO et la CEI, afin de fixer les exigences pour les organismes réalisant l'audit et la certification de SMSI.

Objectifs

Son objet est de fournir les prérequis pour les organismes d'audit et de certification à la norme ISO 27001 pour les Systèmes de Management de la Sécurité de l'Information. Cette norme a été remise à jour en 2011 et porte la référence ISO/IEC 27006.

ISO/CEI 27007 : Lignes directrices pour l'audit des systèmes de management de la sécurité de l'information

Cette norme fournit les lignes directrices pour les audits des systèmes de management de la sécurité de l'information, ainsi que des conseils sur la compétence des auditeurs des SMSI. Elle inclue aussi les lignes directrices contenues dans la norme ISO 19011.

III- Les Système de Management

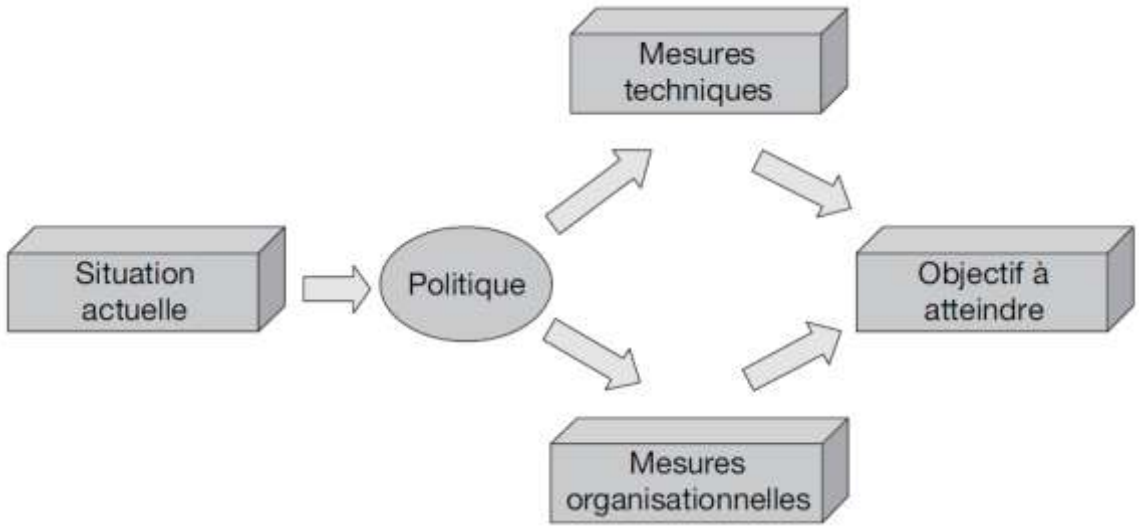
1- Le principe des systèmes de management

Le principe de système de management n'est pas nouveau. Il concerne historiquement le monde de la qualité, surtout dans le domaine des services et de l'industrie. Qui n'a jamais vu un papier à en-tête avec un petit logo « certifié ISO 9001 » ? Qui n'a jamais croisé une camionnette affichant fièrement un autocollant « Société certifiée ISO 9001 » ? La norme ISO 9001 précise les exigences auxquelles il faut répondre pour mettre en place un système de management de la qualité (SMQ).

Comment définir un système de management ? La norme ISO 9000 (à ne pas confondre avec l'ISO 9001 que nous venons d'évoquer) apporte une réponse à cette question en définissant les principes de la qualité. C'est ainsi que dans la rubrique intitulée « Système de management », il est dit qu'un système de management est un système permettant :

- d'établir une politique ;
- d'établir des objectifs ;
- d'atteindre ces objectifs.

Nous pouvons ainsi dire qu'un système de management est un ensemble de mesures organisationnelles et techniques visant à atteindre un objectif et, une fois celui-ci atteint, à s'y tenir, voire à le dépasser.



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

Nous constatons que la majorité de ces référentiels sont normalisés par l'ISO (Organisation internationale de normalisation). Cependant, d'autres organismes privés ou nationaux peuvent proposer leurs propres référentiels. La dernière ligne de cette liste montre, en effet, que l'ISO n'a pas le monopole des systèmes de management, puisque la norme relative à la sécurité du personnel au travail (OHSAS 18001) n'est pas spécifiée par l'ISO.

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)

Nous avons parlé de la partie SM (système de management) du SMSI. Parlons désormais de la partie SI (sécurité de l'information).

Le principal objectif d'un SMSI est de faire en sorte de préserver la confidentialité, l'intégrité et disponibilité pour les informations les plus sensibles de l'entreprise. La norme ISO 27001 insiste sur ces notions. Ces derniers sont formellement définis dans la norme ISO 13335-1.

Le SMSI est cohérent avec les autres systèmes de management de l'entité, notamment avec les systèmes de management de la qualité, de la sécurité des conditions de travail, et de l'environnement.

Le SMSI inclut donc au minimum :

- Des éléments documentaires (politique, description des objectifs, cartographie des processus impactés, des activités de sécurité, et des mesures),
- La description de la méthode d'analyse des risques utilisée,
- Les processus impliqués dans la mise en œuvre de la sécurité de l'information,
- Les responsabilités relatives à la sécurité de l'information,
- Les ressources nécessaires à sa mise en œuvre,
- Les activités relatives à la sécurité de l'information,
- Les enregistrements issus des activités relatives à la sécurité de l'information,
- Les (relevés de) mesures prises sur les processus,
- Les actions relatives à l'amélioration de la sécurité de l'information.

L'existence d'un SMSI dans l'organisme permet de renforcer la confiance dans le mode de gestion de la sécurité de l'information.

IV- La norme ISO/CEI 27001 (Le modèle PDCA)

1- Définitions (Le modèle PDCA)

Les systèmes de management fonctionnent selon un modèle en quatre temps appelé « PDCA », pour ***Plan***, ***Do***, ***Check***, ***Act***.

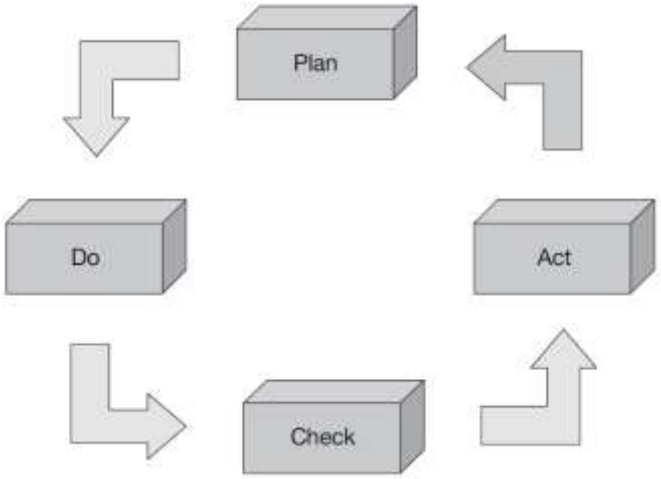
1. Phase Plan : dire ce que l'on va faire dans un domaine particulier (qualité, environnement, sécurité, etc.).

2. Phase Do : faire ce que l'on a dit dans ce domaine.

3. Phase Check : vérifier qu'il n'y a pas d'écart entre ce que l'on a dit et ce que l'on a fait.

4. Phase Act : entreprendre des actions correctives pour régler tout écart qui aurait été constaté précédemment.

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



Le modèle «PDCA »

Ce modèle présente deux propriétés principales : il est cyclique et fractal.

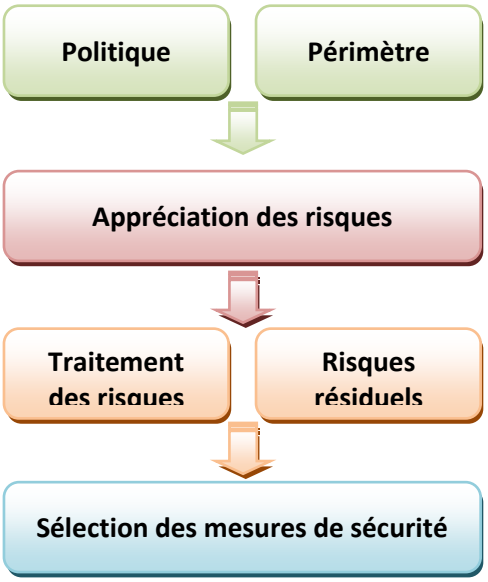
• **Caractère cyclique** – C'est ce cycle Plan, Do, Check, Act qui permet d'atteindre les objectifs (de sécurité, de qualité, d'environnement ou autre) fixés par le management. En revanche, que se passe-t-il une fois que l'objectif a été atteint ? Un nouveau cycle doit être entrepris. C'est pour cela que l'on peut voir une flèche (figure en haut) entre la phase Act et la phase Plan. Cette flèche grisée permet à l'entreprise non seulement d'atteindre ses objectifs, mais aussi de s'y tenir dans la durée. Un système de management est donc un processus qui tourne indéfiniment.

• **Caractère fractal** – Quelle que soit l'échelle à laquelle on observe les systèmes de management, on doit retrouver le modèle Plan, Do, Check, Act.

2- Phase *Plan*

La phase « Plan » du PDCA consiste à fixer les objectifs du SMSI en suivant quatre grandes étapes, la politique et le périmètre du SMSI, l'appréciation des risques, le traitement des risques décidé en tenant en compte des risques résiduels et la sélection des mesures de sécurité présentées dans le ***SoA*** (*Statement of Applicability* : *est un document sous forme de tableau qui énumère les mesures de sécurité du SMSI ainsi que celles non appliquées*).

Dans la figure ci-dessous, une vue du déroulement de la phase Plan.



Processus de déroulement de la phase Plan

2.1- Politique et périmètre du SMSI

La première étape consiste à définir la politique et le périmètre du SMSI. La politique est là pour préciser le niveau de sécurité qui sera appliqué au sein du périmètre du SMSI. La norme ne fixe pas d'exigences sur le périmètre, il peut être restreint ou couvrir l'ensemble des activités de l'organisme. L'objectif est d'y inclure les activités pour lesquelles les parties prenantes exigent un certain niveau de confiance.

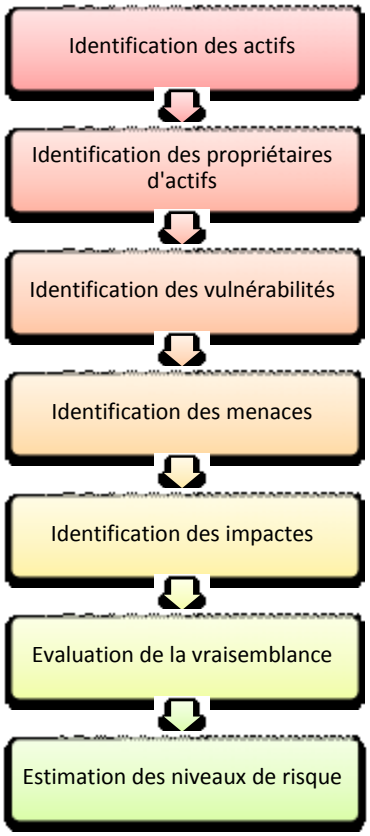
2.2- Appréciation des risques

La deuxième étape concerne un des points les plus importants de l'ISO/CEI 27001, l'appréciation des risques. Le problème de l'appréciation des risques n'est pas nouveau et est traité par de nombreuses méthodes développées dans différents secteurs privés, académiques et agences gouvernementales. Certaines méthodes sont très répandues dans les organismes. En France, les plus connues sont EBIOS et MEHARI, aux Etats- Unis, OCTAVE. L'ISO/CEI propose aussi une méthode, la norme ISO/CEI 27005. Cette norme ne fait que fixer un cahier des charges spécifiant chacune des étapes clefs de l'appréciation des risques.

Dans les points suivants nous détaillons le processus d'appréciation des risques avant de donner deux exemples de méthodes parmi les plus connues.

2.2.1- Processus d'appréciation des risques

Le processus d'appréciation des risques se déroule en sept étapes, illustrées dans figure ci-dessous.



Le processus d'appréciation des risques

La ***première*** étape consiste dresser une liste de tous les actifs qui ont une importance en matière d'information au sein du SMSI. On distingue généralement six catégories d'actifs.

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

La ***deuxième*** étape vise à attribuer pour chaque actif d'information un « propriétaire ». La norme définit le propriétaire comme étant la personne qui connaît le mieux la valeur et les conséquences d'une compromission en termes de disponibilité, d'intégrité et de confidentialité de l'actif.

La ***troisième*** étape est l'identification des vulnérabilités des actifs recensés. La vulnérabilité est la propriété intrinsèque du bien qui l'expose aux menaces. A titre d'exemple, un ordinateur portable est vulnérable au vol mais sa vulnérabilité n'est pas le vol mais sa portabilité. Dans ce cas l'identification de la vulnérabilité est la portabilité.

La ***quatrième*** étape est l'identification des menaces qui pèsent sur les actifs d'information précédemment recensés. Si l'on reprend l'exemple de l'ordinateur portable, la menace est dans ce cas le vol.

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

La ***sixième*** étape demande d'évaluer la vraisemblance des précédentes étapes du processus en plaçant dans leur contexte les actifs. Il s'agit par exemple de considérer les mesures de sécurité déjà en vigueur dans l'organisme. Si l'ordinateur portable possède une clef d'authentification, un cryptage de ses données ou un accès VPN pour travailler, alors la vraisemblance d'observer un impact sur la confidentialité, la disponibilité ou l'intégrité de ses données est limitée.

La ***septième*** étape consiste à attribuer une note finale reflétant les risques pour chacun des actifs d'information. La norme n'impose aucune formule, on peut par exemple utiliser un code couleur (rouge pour un niveau de risque très élevé, orange pour moyen et vert pour faible.

Dans le point suivant, nous présentons deux méthodes connues et largement employées par les organismes pour l'appréciation des risques de leur SMSI.

2.2.2- Méthodes d'appréciation des risques

En 2004, une étude du ***CLUSIF*** (Club de la Sécurité de l'Information Français) dénombrait plus de deux cents méthodes d'appréciation des risques. Nous allons parler des méthodes, ***EBIOS*** et ***MEHARI***.

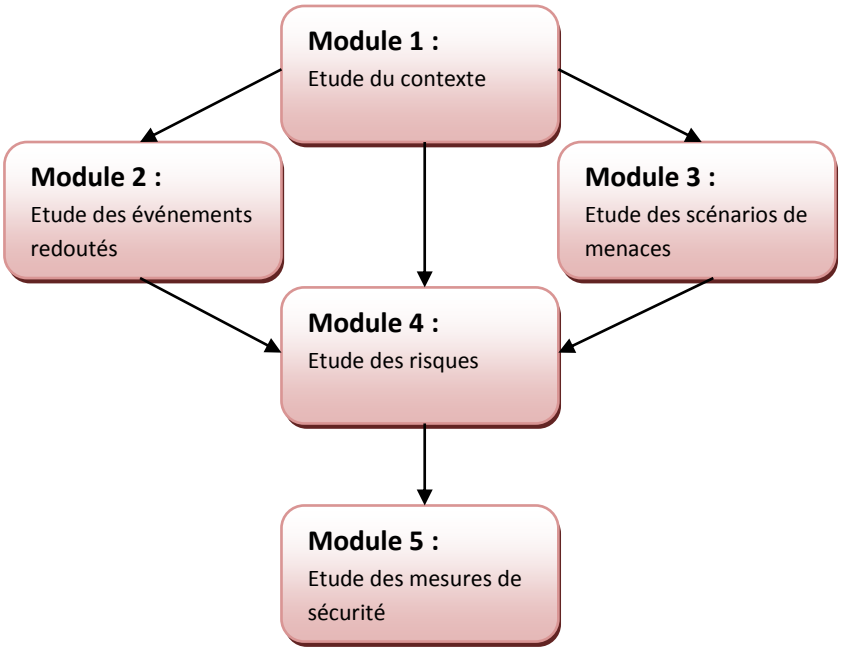
A) La Méthode EBIOS

Développée dans les années 90 sous l'autorité de l'agence française ANSSI (Agence nationale de la sécurité des systèmes d'information), cette méthode est l'«Expression des Besoins et Identification des Objectifs de Sécurité». Elle permet d'apprécier, de traiter et communiquer sur les risques au sein d'un SMSI.

L'ANSSI et le Club EBIOS proposent en libre accès sur leur site web toute la documentation ainsi qu'un logiciel libre facilitant l'utilisation de la méthode.

L'approche de la méthode est itérative, chaque module peut être révisé, amélioré et tenu à jour de manière continue.

EBIOS se compose de cinq modules représentés dans la figure ci-dessous :



Les cinq modules de la méthode EBIOS

Module 1 : il concerne l'étude du contexte. Il s'agit de détailler l'organisation, les missions, les contraintes et les métiers pour rendre applicable et cohérent le choix des objectifs de sécurité. Le point suivant consiste à identifier les fonctions estimées sensibles, la perte, le dysfonctionnement ou la divulgation d'informations qui peuvent avoir des répercussions sur le bon fonctionnement de l'organisme.

Enfin, on répertorie sous forme de matrice les entités techniques propres au SMSI (matériel, logiciels, réseaux) ainsi que les entités organisationnelles (groupes de collaborateurs) pour établir les liens entre les éléments essentiels et les entités.

Module 2 : il concerne l'étude des événements redoutés. Cette étape permet de définir les besoins de sécurité des éléments essentiels précédemment identifiés. On quantifie les besoins sur une échelle de 0 à 4 à l'aide d'un questionnaire que l'on

adresse aux collaborateurs de l'organisme. Les besoins sont sélectionnés sur des critères de sécurité tels que la disponibilité, l'intégrité, la confidentialité et la non-répudiation ainsi que sur des critères d'impacts (interruption de services, dommages matériels).

Module 3 : consiste à étudier les scénarios de menaces. Estimer, évaluer les menaces (incendie, perte d'alimentation électrique, divulgation d'information etc.) et identifier les objectifs de sécurité qu'il faut atteindre pour les traiter. EBIOS fournit une liste de menaces que l'on associe aux éléments essentiels définis dans le module 1. Puis on attribue à chaque élément un niveau de vulnérabilité sur une échelle de 0 à 4.

Module 4 : il vise à étudier les risques. Cette étape permet de dresser une cartographie des risques. Elle explique aussi comment traiter le risque. Estimer, évaluer les risques puis identifier les objectifs de sécurité à atteindre pour les traiter.

Module 5 : il concerne l'étude des mesures de sécurité. Cette dernière étape explique comment appliquer les mesures de sécurité à mettre en œuvre, comment planifier la mise en œuvre de ces mesures et comment valider le traitement des risques résiduels.

En conclusion, la méthode EBIOS par son caractère exhaustif, permet de formaliser tout le SMSI et son environnement. Cette méthode contribue à formuler une politique de sécurité du système d'information. C'est une des méthodes pour mettre en œuvre le cadre défini par l'ISO/CEI 27005. Elle répond aux exigences de l'ISO/CEI 27001 et peut exploiter les mesures de sécurité de l'ISO/CEI 27002.

B) La méthode MEHARI

La méthode ***MEHARI*** (Méthode Harmonisée d'Analyse de Risques) a été développée dans les années 1990 par le ***CLUSIF*** (Club de la Sécurité de l'Information Français). A l'origine, cette méthode ne traitait que de l'analyse des risques. Elle a évolué pour permettre une gestion de la sécurité de l'organisme dans un environnement ouvert et géographiquement réparti.

MEHARI a été adoptée par des milliers d'organismes à travers le monde et reste la méthode la plus utilisée en France, en particulier dans l'industrie. L'utilisation et la distribution de son logiciel sont libres. En outre, certaines bases de connaissances sont disponibles et une étude illustre la méthode pour faciliter son utilisation.

Contrairement à la méthode EBIOS, MEHARI repose sur des scénarios de risques qui permettent d'identifier les risques potentiels au sein de l'organisme. Elle est définie comme une boîte à outils conçue pour la gestion de la sécurité. En fonction des besoins, des choix d'orientation, de politique de l'organisation ou simplement des circonstances, la méthode veille à ce qu'une solution d'appréciation des risques appropriée puisse être élaborée. La méthode est présentée sous la forme d'un ensemble que l'on appelle modules, centrés sur l'évaluation des risques et leur gestion.

1- Principe de fonctionnement

La méthode méhari prend avant tout en compte les informations de l'entreprise afin de développer un plan afin de mieux définir les points à protéger dans l'entreprise.

MEHARI permettra à l'entreprise de définir :

- Un plan stratégique de sécurité
- Un plan opérationnel de sécurité par site ou entité
- Un plan opérationnel d'entreprise
- Le traitement d'une famille de scénarios ou d'un scénario particulier
- Le traitement d'un risque spécifique (Accident, Erreur, Malveillance)
- Le traitement d'un critère de sécurité (Disponibilité, Intégrité, Confidentialité)

MEHARI, conjugue la rigueur d'une analyse des risques liés formellement au niveau de vulnérabilité du système d'information, à l'adaptabilité de la gravité des risques étudiés. En effet, la présence ou l'absence de mesures de sécurité va réduire ou non, soit la potentialité de survenance d'un sinistre, soit son impact. L'interaction de ces types de mesures concoure à réduire la gravité du risque jusqu'au niveau choisi.

Enjeux critiques + Vulnérabilités fortes = Risques inacceptables

Cette expression très simple signifie que le management de la sécurité a pour objectif fondamental d'éviter de se trouver dans une situation telle que des vulnérabilités fortes pourraient être exploitées et conduire à des sinistres très critiques pour l'entreprise ou l'organisation qui en est victime.

Les phases de MEHARI sont les suivantes :

+ Phase 1 : établissement d'un plan stratégique de sécurité (global) qui fournit notamment :

- la définition des métriques des risques et la fixation des objectifs de sécurité,

- la reconnaissance et la détermination des valeurs de l'entreprise,

- l'établissement d'une politique de sécurité entreprise, l'établissement d'une charte de management.

+ Phase 2 : établissement de plans opérationnels de sécurité réalisés par les différentes unités de l'entreprise

+ Phase 3 : consolidation des plans opérationnels (Plan global).

Nous allons détailler ces différentes étapes dans la suite de notre rapport, en étudier les modalités et les moyens à mettre en œuvre.

2- Mise en place de la méthode

MEHARI se présente comme un ensemble cohérent d'outils et de méthodes de management de la sécurité, fondés sur l'analyse des risques. Les deux aspects fondamentaux de MEHARI sont le modèle de risque (qualitatif et quantitatif) et les modèles de management de la sécurité basés sur l'analyse de risque. MEHARI vise à donner des outils et des méthodes pour sélectionner les mesures de sécurité les plus pertinentes pour une entreprise donnée.

Les différentes phases ont pour objectif d'établir le contexte d'entreprise, d'identifier les actifs et les menaces, d'analyser les risques et enfin de définir les mesures de sécurité (traitement du risque).

a- Plan stratégique

C'est le plan qui examinera l'entreprise sur un aspect général. Les aspects qui seront pris en compte lors de cette analyse, sont : la classification des ressources de l'entreprise, l'ensemble des risques existants, et ses objectifs en terme de sécurité.

Première étape : mettre en avant les risques possibles :

Lors de l'audit nous allons donc répertorier les risques pouvant pénaliser l'activité de l'entreprise.

Ensuite pour chacun des risques détectés on définit :

+ Son potentiel :

C'est-à-dire la capacité de destruction. C'est pour cela que l'on mettra en place des tests ou plus précisément des scénarios qui permettent de se mettre en situation et dévaluer ce potentiel.

+ Son impact :

En clair, une fois la catastrophe arrivée concrètement quel seront les dégâts réels.

+ Sa gravité :

Déterminer si vraiment les dégâts son handicapants pour l'entreprise et son fonctionnement.

Deuxième étape : limite d'acceptabilité

De part ces caractéristiques nous allons ensuite mettre en place une échelle pour le degré d'acceptabilité non seulement sur le plan de la gravité mais aussi du temps. Combien de temps l'entreprise pourra être dans cette handicape sans que cela devienne dangereux pour sa survie.

Troisième étape : les ressources de l'entreprise

Lors de cette étape nous définirons en fait les valeurs de l'entreprise, quels services génèrent le plus de chiffre d'affaire, ou sont vital pour le fonctionnement de la société.

Quatrième étape : solution et indicateurs

C'est l'étape finale, c'est lors de celle-ci que l'on mettra en place dans un premier temps les indicateurs afin de prévenir au maximum l'arrivée d'une catastrophe. que l'on regroupera toutes les informations que l'on a pu récupérer et qu'on les analysera

de façon globale afin de pouvoir mettre en œuvre des solutions : règles de sécurité et de responsabilité. Les solutions s'appliquent sur plusieurs niveaux :

Ce découpage permet un regroupement des mesures en six grandes familles :

- Les **mesures structurelles** qui jouent sur la structure même du système d'information, pour éviter certaines agressions ou en limiter la gravité.

- Les **mesures dissuasives** qui permettent, dans le cas d'agresseurs humains, d'éviter qu'ils mettent à exécution la menace potentielle en déclenchant l'agression.

- Les **mesures préventives** : celles qui permettent d'empêcher les détériorations ou d'éviter qu'une agression n'atteigne des ressources du système d'information.

- Les **mesures de protection** qui, sans empêcher les détériorations, permettent tout au moins d'en limiter l'ampleur.

- Les **mesures palliatives** qui agissent une fois les détériorations accomplies, et qui permettent, d'une part d'en limiter les conséquences au niveau de l'entreprise, d'autre part de restaurer les ressources détériorées pour retrouver l'état initial.

- Les **mesures de récupération** qui visent à récupérer une partie du préjudice subi par transfert des pertes sur des tiers, par le biais des assurances ou de dommages et intérêts consécutifs à des actions en justice, dans le cas d'agresseurs humains.

b) Plan opérationnel de sécurité

- Spécifier le domaine et les outils : élaboration des scénarios.
Périmètre et niveau de détail Elaboration des scénarios Validation de la classification

- Auditer le niveau de sécurité : audit des services
Audit des services et sous services Consolidation au niveau cellules

- Evaluer la gravité des scénarios : Potentialité/ Impact/ Gravité
Détermination Potentialité/Impact/gravité

- Exprimer les besoins de sécurité : mesures générales et spécifiques

- Planifier les actions de sécurité : mesures prioritaires
Mesures spécifiques et prioritaires Autres mesures hiérarchisées

c) Plan opérationnel d'entreprise

Dans cette étape il s'agit fondamentalement de mettre en place des scénarii sur les impacts et les conséquences que peuvent avoir ces sinistres sur le bon fonctionnement de l'entreprise. Cette partie conclue la boucle de l'application de la méthode Méhari par la mise en place d'un outil permettant le suivi des opérations à effectuer afin d'améliorer la sécurité de la société.

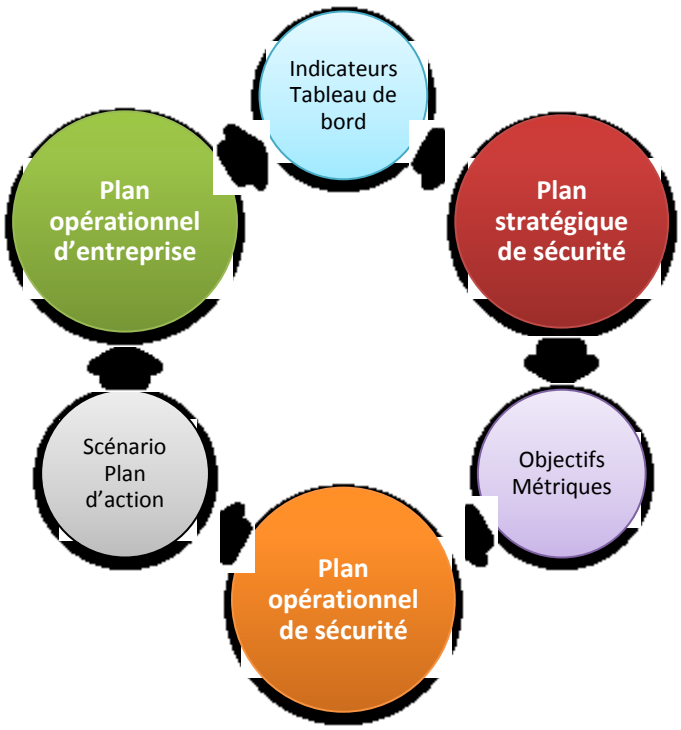
Pour que cette stratégie soit couronnée de succès il est nécessaire de s'assurer que :

- Elle est connue et comprise par la Direction et le personnel de l'entreprise
- Elle est pilotée et sa mise en œuvre est assurée et mesurée
- Elle reste pertinente dans le temps
- Elle se décline en objectifs stratégiques reliés à des objectifs tactiques (ensemble des initiatives, projets, processus et organisation) qui forment un tout cohérent et contribuent pleinement à l'atteinte de la couverture des risques
- Elle est financée et que les budgets sont affectés avec l'assurance de leur meilleure contribution au succès de cette stratégie

Bénéfices :

- Les objectifs poursuivis par la stratégie sécurité sont conformes à ceux de l'entreprise
- Impact sur l'image véhiculée par la SSI
- Pilotage et mesure dans la durée de la stratégie sécurité sur l'ensemble de ses aspects, en privilégiant le caractère stratège du RSSI (Responsable de la Sécurité de Système d'informations)
- Intégration des aspects stratégiques et opérationnels

d) La démarche MEHARI



La démarche MEHARI

2.3- Traitement des risques

La troisième étape concerne le choix du traitement des risques. L'ISO/CEI 27001 a identifié quatre traitements possibles du risque, l'acceptation, l'évitement, le transfert et la réduction.

- « ***Accepter*** » le risque revient à ne déployer aucune mesure de sécurité autre que celles déjà en place. Cette décision peut être justifiée si le vol de données dans un cas précis n'a pas d'impact sur l'organisme.
- « ***Eviter*** » le risque consiste à supprimer par exemple l'activité ou le matériel offrant un risque.
- « ***Transférer*** » un risque par souscription d'une assurance ou par sous-traitance. Ces moyens de transfert du risque sont souvent employés quand L'organisme ne peut ou ne souhaite pas mettre en place les mesures de sécurité qui permettraient de le réduire.
- « ***Réduire*** » le risque consiste à prendre des mesures techniques et organisationnelles pour ramener à un niveau acceptable le risque. C'est le traitement le plus courant.

Il existe d'autres traitements du risque possibles mais pour être en conformité avec la norme, il faut en priorité considérer ceux que nous venons de citer.

Après avoir sélectionné le traitement et mis en place les mesures de sécurité, un risque peut persister. Il convient de traiter ce risque comme les autres c'est-à-dire, l'accepter, l'éviter, le transférer ou le réduire.

2.4- Sélection des mesures de sécurité

L'étape 4 est la dernière étape de la phase « Plan » du PDCA, elle consiste à sélectionner les mesures de sécurité. La norme ISO/CEI 27001 propose dans son annexe A, 133 mesures de sécurité réparties sur onze chapitres. A ce stade, le travail consiste à dresser un tableau ***SoA*** dans lequel figurent les 133 mesures qu'il faut déclarer applicables ou non applicables, pour réduire les risques du SMSI.

Notons que les 133 mesures proposées par l'ISO/CEI 27001 répertorient presque tout ce qui peut être entrepris en matière de sécurité de l'information cependant, cette liste ne comporte pas d'exemples ni d'explications sur le déploiement des mesures à entreprendre. L'ISO/CEI 27002 répond en partie à ce besoin en fournissant une série de préconisations et d'exemples techniques et organisationnels qui couvrent la liste de l'ISO/CEI 27001.

Une fois choisie la politique et le périmètre du SMSI, appréciés et traités les risques, et sélectionnées les 133 mesures de sécurité dans le tableau SoA, il faut mettre en œuvre les objectifs fixés de la phase « Plan » du PDCA. Il s'agit de la phase « ***Do*** » du PDCA.

3- Phase *Do*

Cette phase consiste à décrire la mise en œuvre des mesures de sécurité sélectionnées dans le SoA à travers quatre étapes.

3.1- Plan de traitement

Il faut premièrement gérer l'interdépendance des actions à entreprendre. Certaines mesures sont partiellement ou déjà en place, d'autres doivent être intégralement déployées ou nécessitent la mise en œuvre d'une autre action avant de pouvoir être lancées. Ce travail revient à établir un plan de traitement qui peut être assimilé à de la gestion de projet. Une fois ce travail effectué, il faut déployer les mesures de sécurité en suivant le plan de traitement.

Par la suite, le responsable de projet doit définir des « mesures d'efficacité » pour contrôler le bon fonctionnement du SMSI.

3.2- Choix des indicateurs

Ce point consiste à mettre en place des indicateurs de performance pour vérifier l'efficacité des mesures de sécurité ainsi que des indicateurs de conformité pour contrôler la conformité du SMSI. Trouver de bons indicateurs n'est pas une tâche facile.

La norme ne préconise pas d'indicateurs précis à utiliser mais l'ISO/CEI 27004 propose une démarche qui peut aider à les sélectionner.

L'étape suivante concerne la sensibilisation des collaborateurs aux principes de la sécurité de l'information.

3.3- Formation et sensibilisation des collaborateurs

Nous avons vu que les mesures de sécurité couvrent de nombreux domaines allant de la sécurité organisationnelle à la sécurité physique, en passant par la sécurité des systèmes réseaux etc. Les collaborateurs doivent maîtriser les outils de sécurité déployés dans les domaines très variés. Une formation du personnel peut s'avérer nécessaire.

La sensibilisation à la sécurité du système d'information concerne tous les collaborateurs. Elle peut débuter par un rappel des engagements de leur entreprise en matière de sécurité et se poursuivre par une liste de conseils tels que le respect de certaines règles de sécurité pour les mots de passe et l'environnement de travail.

3.4- Maintenance du SMSI

La maintenance consiste à garantir le bon fonctionnement de chacun des processus du SMSI et vérifier que leur documentation est à jour. Cela permet à l'auditeur

externe de contrôler la gestion du SMSI. Il est à noter que tous les systèmes de management ISO sont concernés par la maintenance.

A ce stade de l'avancement du SMSI, les mesures identifiées du SoA fonctionnent, les indicateurs sont implémentés et les collaborateurs de l'organisme formés et sensibilisés à la sécurité du SMSI, nous pouvons poursuivre avec la phase « ***Check*** » du PDCA.

4- Phase *Check*

La phase « Check » du PDCA concerne les moyens de contrôle à mettre en place pour assurer «l'efficacité » du SMSI et sa « conformité » au cahier des charges de la norme ISO/CEI 27001. Pour répondre à ces deux exigences de la norme, les organismes emploient le contrôle et les audits internes ainsi que les revues de direction.

4.1- Les audits internes

L'audit interne peut s'organiser avec le personnel de l'organisme ou être sous-traité à un cabinet conseil. Si l'audit est confié à un collaborateur, il ne faut pas que ce dernier puisse auditer un processus dans lequel il est impliqué au niveau de sa mise en œuvre ou de son exploitation. L'audit a pour but de contrôler la conformité et l'efficacité du SMSI en recherchant les écarts entre la documentation du système (enregistrement, procédures, etc.) et les activités de l'organisme. La norme exige que la méthode utilisée pour l'audit soit documentée dans une procédure et que les rapports soient enregistrés pour être utilisés lors des revues de direction.

4.2- Les contrôles internes

L'objectif du contrôle interne est de s'assurer au quotidien que les collaborateurs appliquent correctement leurs procédures. Contrairement à l'audit interne qui est planifié longtemps à l'avance, les contrôles internes sont inopinés.

4.3- Revues de direction

La revue est une réunion annuelle qui permet aux dirigeants de l'organisme d'analyser les événements qui se sont déroulés sur l'année en cours. Les points passés en revue sont généralement :

- les résultats des audits,
- le retour des parties prenantes,
- l'état des lieux sur les actions préventives et correctives,
- les menaces mal appréhendées lors de l'appréciation des risques,
- l'interprétation des indicateurs et les changements survenus dans l'organisme.

A partir de ces informations la direction peut fixer de nouveaux objectifs et allouer de nouvelles ressources (financières, humaines et matérielles).

Les contrôles de la phase « Check » peuvent faire apparaître des dysfonctionnements du SMSI. Cela peut être un écart entre les exigences de la norme et le système de management ou des mesures de sécurité inefficaces.

C'est dans la phase « ***Act*** » du PDCA que l'on réduit les dysfonctionnements par des actions correctives, préventives ou d'améliorations.

5- Phase *Act*

5.1- Actions correctives

On intervient de manière « corrective » lorsqu'un dysfonctionnement ou un écart est constaté. On agit premièrement sur les effets pour corriger cet écart ou dysfonctionnement, puis sur les causes pour éviter qu'ils ne se répètent.

5.2- Actions préventives

On emploie les actions préventives quand une situation à risque est détectée. On agit sur les causes avant que l'écart ou le dysfonctionnement ne se produisent.

5.3- Actions d'améliorations

Les actions d'améliorations ont pour objectif l'amélioration de la performance du SMSI.

Les résultats des différentes actions doivent être enregistrés et communiqués aux parties prenantes. Ces actions contribuent à rendre plus efficace et performant le SMSI.

Conclusion

Une démarche d'audit de la sécurité des systèmes d'information doit être le fruit d'une réflexion en amont afin d'envisager les meilleurs solutions possibles. Prenant en compte les besoins particuliers de l'organisation, tant organisationnelles que techniques.

De nos jours la sécurité des systèmes d'information, ce n'est pas seulement le fait d'avoir une bonne gestion des risques, mais elle s'étend de plus en plus à une gouvernance de la sécurité des système d'information.

Références

Bibliographie

Management de la sécurité de l'information [Mise en place d'un SMSI et audit de certification - Implémentation ISO 27001 et ISO 27002] de ***Alexandre Fernandez - Toro***

Webographie

CLUSIF, Présentation de MEHARI. Sur : http://www.clusif.asso.fr

Information security management systems (ISMS - ISO). Sur : http://www.iso.org

YSOSECURE est un cabinet de conseil indépendant. Sur : http://www.ysosecure.com

Méthode de gestion des risques. Sur: http://www.ssi.gouv.fr

Acronymes

AESC: American Engineering Standards Committee

AFNOR : Association Française de Normalisation

ANSSI : Agence Nationale de la Sécurité des Systèmes d'Information

ASA: American Standards Association

BSI: British Standards Institute

CEI : Commission Electronique Internationale

CEN : Comité Européen de Normalisation

CFISE : Catalogue des Fonctions des Informations de Sécurité d'Etat

CLUSIF : Club de la Sécurité de l'Information Français

CSD : Conseil Supérieur de Défense

EBIOS : Etude des Besoins et Identification des Objectifs de Sécurité

ENISA: European Network and Information Security Agency

ISO : Organisation Internationale de Normalisation

JTC : Joint Technical Committee

MARION : Méthode d'Analyse de Risques Informatiques Optimisée par Niveau

MEHARI : Méthode Harmonisée d'Analyse des Risques

MELISA : Méthode d'Evaluation de la Vulnérabilité Résiduelle des Systèmes d'Armement

OCTAVE: Operationally Critical Threat, Asset, and Vulnerability Evaluation

PDCA : Plan, Do, Check, Act

PME : Petites et Moyennes Entreprises

SAS : Statistical Analysis System

SMI : Système de Management de l'Information

SMSI : Système de Management de la Sécurité de l'Information

SoA : Statement of Applicability

TI : Technologies de l'Information

TIC : Technologies de l'Information et de la Communication