REPUBLIQUE TUNISIENNE

MINISTERE DE L'ENSEIGNENMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE

Université Virtuelle de Tunis

Mastère en Optimisation et Modernisation des Entreprises : MOME

Mémoire

Pour l'obtention d'un Diplôme de Mastère Professionnel

(1ère Promotion)

Mise en œuvre d'un système de management de la sécurité de l'information (SMSI) au sein de l'Ambassade du Royaume du Maroc à Tunis

Encadré par : - ***M. Moez Yeddes (UVT)***

- ***M. Mounir Arjdal (Structure d'accueil)***

Réalisé par : Ali Ben Mouloud

Année universitaire : 2010 / 2011

Remerciements

J'exprime toute ma reconnaissance et gratitude à l'administration et à l'ensemble du corps enseignant de l'Université Virtuelle de Tunis pour leurs efforts à nous garantir la continuité et l'aboutissement de ce programme de Master.

Je tiens à remercier aussi et chaleureusement mes encadreurs MM. Moez Yeddes et Mounir Arjdal ainsi que Son Excellence l'Ambassadeur du Roi du Maroc en Tunisie de m'avoir permis de mener ce travail au sein de l'Ambassade malgré la sensibilité du tel sujet dans une structure pareil.

Je remercie enfin 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 / Abstract

Initialement, notre principale motivation était liée à la volonté de se démarquer dans le domaine de la protection des systèmes d'informations par la mise en place d'un premier Système de Management de la Sécurité de l'Information dans le secteur diplomatique.

Aujourd'hui, les bénéfices ne se mesurent pas seulement en termes d'image mais également sur le fonctionnement en interne.

En effet, la mise en œuvre du SMSI a été l'occasion de mettre en avant l'importance de la sécurité du SI, de la faire reconnaître dans les différents services et de donner aux actions un rythme clair et partagé.

Les exigences pour la mise en place du SMSI sont décrites par la norme ISO/CEI 27001.

Cette norme s'adapte à tout type d'entreprise, quelque soit le secteur d'activité, sa structure, sa taille et la complexité de son système d'information.

L'application de cette norme passe par une démarche qualiticienne classique : la roue de Deming (Planifier, Développer, Contrôler, Agir) qui permet de prendre en compte des dysfonctionnements le plus en amont possible et d'amener une amélioration continue du système.

Mots clés : Sécurité de l'information, SMSI, ISO/CEI27001, PDCA,

In the beginning, our main motivation was related to the will of standing out in the field of information systems protection by the installation of a first Information Security Management System in the diplomatic sector.

Today, profits are not appeared only in terms of branding but also on the internal tasks.

Indeed, the implementation of the ISMS was an opportunity to highlight the importance of the information's system security, to make it recognized in the various services and to give to the actions a clear and shared rate.

The requirements for the implementation of the WSIS are described in ISO/ECI 27001. This standard adapts to any type of business, whatever the sector of activity, structure, size and complexity of its information system.

Applying this standard requires a classic approach of quality: the Deming wheel (Plan, Do, Check, Act), which can take into account the failures as early as possible and bring a continuous improvement of the system.

Key words: Information Security, ISMS, ISO/CEI 27001, PDCA.

Table des matières

Listes des figures

Introduction

L'omniprésence des informations croissante soutenue par la révolution numérique des technologies de l'information et de la communication TIC a amplifié le besoin d'assurer l'intégrité, la confidentialité et la disponibilité de l'information.

Malgré des moyens techniques permettant de les contrôler et des compétences pour les mettre en œuvre, la complexité des systèmes d'information exige une planification rigoureuse de la supervision.

Des outils sous forme de « codes de bonnes pratiques » et méthodes d'appréciation des risques permettent aux entreprises de fixer des objectifs, des priorités et coordonner les actions à entreprendre.

Néanmoins ces outils, bien qu'ayant prouvé leur efficacité, souffrent d'un manque de reconnaissance au plan international à cause de leur trop grande diversité.

Pour remédier à l'hétérogénéité des méthodes et pallier le manque de reconnaissance des « codes de bonnes pratiques », l'ISO (Organisation Internationale de Normalisation) a publié en 2005 la norme ISO/CEI 27001.

L'ISO/CEI 27001, clef de voûte d'une famille de normes encore en développement, apporte une dimension supplémentaire à la politique de sécurité de l'information en y intégrant le concept de « système de management ». Cette norme est à la base de notre réflexion pour ce mémoire.

Le travail de la mise en œuvre d'un système de management de la sécurité de l'information (SMSI), présenté dans ce rapport a été effectué dans le cadre de mon projet de fin d'études du Master Optimisation et Modernisation de l'Entreprise à l'Université Virtuelle de Tunis.

Ce travail, réalisé dans les locaux de l'Ambassade du Royaume du Maroc en Tunisie et a pu mené à terme grâce à la collaboration du staff du Ministère des affaires étrangères et de l'Ambassade.

Ce rapport sera organisé comme suit :

Première partie : Etat de l'art des systèmes de management de la sécurité de l'information.

Deuxième partie : La norme ISO/CEI 2700x et principalement ISO/CEI 27001
Son approche en quatre phases (Plan, Do, Check, Act).

Troisième partie : Implémentation et Mise en œuvre de la norme au sein de l'Ambassade.

Première partie

Etat de l'art des systèmes de management de la sécurité de l'information

1. Introduction

L'objectif de cette première partie est de présenter les normes, les concepts, les processus et les acteurs qui ont permis aux organismes d'aboutir à un système de management de la sécurité de l'information.

2. Définitions

2.1- L'ISO (Organisation Internationale de Normalisation)

L'ISO est le fruit d'une collaboration entre différents organismes de normalisation nationaux. Au début du XX^{ème} siècle, L'American Institute of Electrical Engineer[1] 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[2] (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. La figure 1 ci-dessous montre la structure hiérarchique des différents groupes de travail tel que le WG1 issu du JTC1/SC27 de l'ISO/CEI [1].

[1] Aujourd'hui appelé Institute of Electrical and Electronics Engineers ou IEEE avec comme objectif la promotion de la connaissance dans le domaine de l'ingénierie électrique.

[2] CEI est chargée de la normalisation d'équipements électriques. Il est courant de voir ISO/CEI pour nommer une norme élaborée conjointement par les deux organismes.

Figure 1: Structure hiérarchique des groupes de travail et comités de l'ISO/CEI

Créé en 2006, le JTC1/SC27 de l'ISO/CEI a développé un nombre important de normes au sein du WG1[3], celles de la famille ISO/CEI 2700x.

2.2- Les normes

L'ISO et le CEI donnent la définition suivante : «(…) *document établi par consensus et approuvé par un organisme reconnu, qui fournit, 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*[4]». Les documents établis par consensus sont appelés « norme ». On distingue quatre familles de normes :

- Les normes fondamentales concernent les règles qui ont trait à la métrologie.
- Les normes de spécifications, traitent des caractéristiques et des seuils de performance d'un produit ou d'un service.
- Les normes d'analyse et d'essais, renseignent sur les méthodes et moyens pour la réalisation d'un essai sur un produit.
- Les normes d'organisation qui décrivent les fonctions et les relations organisationnelles au sein d'un organisme.

Ces normes peuvent relever de groupes ou d'organismes de normalisation internationaux ou nationaux tels que le CEN qui a pour but l'harmonisation des normes nationales européennes, l'ISO qui publie les normes internationales et L'AFNOR qui s'occupe des normes françaises [2].

3 Le WG1 est le groupe de travail en charge d'organiser et rédiger les normes liées au domaine de la sécurité de l'information.

4 Directives ISO/CEI – partie 2 : Règles de structure et de rédaction des Nomes internationales, cinquième édition, 2004 (§ 3.1).

2.3- La normalisation

Selon le Journal Officiel du gouvernement français, la normalisation «(…) *a pour objet de fournir des documents de référence élaborés de manière consensuelle par toutes les parties intéressées, portant sur des règles, des caractéristiques, des recommandations ou des exemples de bonnes pratiques relatives à des produits, à des services, à des méthodes, à des processus ou à des organisations. Elle vise à encourager le développement économique et l'innovation tout en prenant en compte des objectifs de développement durable* (…) » (Art. 1 du décret du 16 juin 2009)[5]. Les documents de référence élaborés au terme du processus de normalisation sont les «normes ».

2.4- 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[6]» ainsi qu'une mise à jour régulière de la politique.

[5] Le Décret n° 2009-697 du 16 juin 2009 relatif à la normalisation, JO du 17 juin 2009, explicite le fonctionnement du système français de normalisation et rappelle la procédure d'élaboration et d'homologation des projets de normes et les modalités d'application des normes homologuées.

[6] Les points « opérationnel » de la politique de sécurité de l'information peuvent par exemple concerner la politique de sauvegarde, des mots de passe. Les points « stratégiques » concerneront les engagements de la direction vis-à-vis de la sécurité de l'information.

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 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.

La figure 2 ci-dessous résume l'historique des normes traitant de la sécurité de l'information.

Figure 2: Historique des normes liées à la sécurité de l'information

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 SMSI et l'ISO/CEI 27002 qui regroupe un ensemble de bonnes pratiques «best practices» pour la gestion de la sécurité de l'information.

Autour de ces deux normes viennent s'articuler d'autres normes de la même famille, ISO/CEI 2700x, encore en développement pour certaines [3].

Dans la partie qui suit nous présentons les principales propriétés d'un SMSI avant d'aborder les normes de la série ISO/CEI 2700x qui se sont imposées comme références des SMSI.

3. Les SMSI (Systèmes de Management de la Sécurité de l'Information)

3.1- Les systèmes de management

La norme ISO 9000 définit le système de management comme : (…) *un système permettant d'établir une politique, des objectifs et atteindre ces objectifs* (…).

Un système de management peut être interprété comme un ensemble de mesures organisationnelles et techniques ciblant un objectif comme le montre la figure 3 ci-dessous.

Figure 3: Vue d'un système de management

Un système de management se caractérise par un engagement de l'ensemble des collaborateurs de l'organisme ; quel que soit le périmètre du système sur l'activité de l'organisme, il nécessite l'implication de tous les métiers. A cette approche transversale doit s'associer une approche verticale. L'ensemble de la hiérarchie de l'organisme, de la direction jusqu'aux parties intéressées, c'est-à-dire les fournisseurs, partenaires et actionnaires doivent être engagés dans la mise en œuvre du système [4]. Une autre caractéristique des systèmes de management est la formalisation des politiques et procédures de l'organisme afin de pouvoir être audité.

Ces engagements ont un coût en ressources matérielles, humaines et financières.

Comment justifier cet investissement ? Les systèmes de management s'appuient sur des guides de bonnes pratiques, mécanismes d'amélioration continue favorisant la capitalisation sur les retours d'expérience, ce qui a pour effet d'accroitre la fiabilité. En outre, l'audit du système de management par un cabinet d'audit indépendant permet d'établir une relation de confiance entre le client et le fournisseur.

Le fonctionnement du système de management se fait selon le modèle PDCA de l'anglais Plan, Do, Check, Act, en français planifier, faire, contrôler et corriger. Ces quatre phases sont illustrées dans la figure 4 ci-dessous.

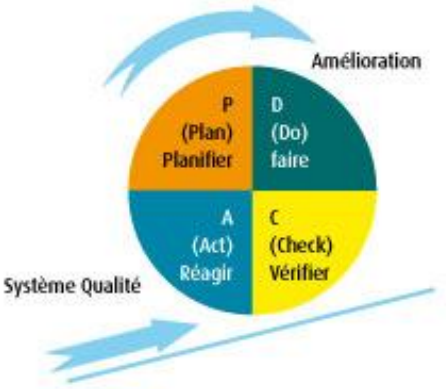

Figure 4: Roue de Deming (PDCA)

- Plan : dire ce que l'on va réaliser dans un domaine particulier.
- Do : faire ce qui a été annoncé.
- Check : vérifier les écarts entre les phases « plan » et «do ».
- Act : ajuster les écarts constatés de la phase « check ».

Une fois que les objectifs fixés par le management sont atteints, il faut s'y tenir dans la durée. La flèche sur la roue Deming, montre qu'un nouveau cycle du processus du système de management doit être entrepris pour y parvenir. Notons que le modèle PDCA s'applique au système de management dans son ensemble ainsi qu'à chacun de ses processus [5].

On retrouve les systèmes de management dans des secteurs d'activités aussi variés que la santé et la sécurité du travail avec la norme OHSAS 18001, l'environnement avec la norme ISO 14001, les services informatiques avec le référentiel ISO/CEI 20000, la sécurité alimentaire avec la norme ISO 22000, la qualité avec la norme ISO 9001 ou encore la sécurité de l'information avec la norme ISO/CEI 27001 que nous allons traiter dans les points suivants.

3.2- Sécurité de l'information

Dans le SMSI, l'information n'est pas restreinte aux systèmes informatiques.

L'information est à prendre au sens large du terme. Elle doit être étudiée sous toutes ses formes indépendamment de son support, humain, papier, logiciel, etc.

Le terme sécurité doit être compris comme l'ensemble des moyens déployés pour se protéger contre les actes de malveillance. La sécurité du SMSI est définie par la norme ISO 13335-1 à travers les notions de confidentialité, d'intégrité et de disponibilité.

- Confidentialité : seuls les entités, personnes et processus autorisés, ont accès à l'information.
- Intégrité : l'information ne peut être modifiée que par ceux qui en ont le droit.
- Disponibilité : l'information doit être accessible à l'entité, la personne ou le processus qui a un droit d'accès.

Ces trois principes de sécurité peuvent être étendus, les SMSI intègrent d'autres notions telles que l'authentification, la traçabilité, la non-répudiation, l'imputabilité qui constituent des mécanismes de sécurité que l'on déploie en fonction des besoins de sécurité de l'organisme [6].

En conclusion 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 un juste dosage, sans exagérations, ni trop de tolérance avec comme finalité la protection des actifs d'information.

Nous avons vu que l'évolution des normes liées à la sécurité de l'information a mené à l'élaboration de SMSI. Dans la partie qui suit nous présentons la famille des normes ISO/CEI 2700x qui font figure de référence en la matière.

4. Les normes de la famille ISO/CEI 2700x

Dans la famille ISO/CEI on trouve deux catégories de normes. Celles qui émettent des exigences : ISO/CEI 27001 et celles qui formulent des recommandations : ISO/CEI 27002. Notons que certaines normes sont encore en cours de rédaction, c'est le cas des normes ISO/CEI 27007 «Audit des SMSI » et ISO/CEI 27008 « Audit des mesures de sécurité ».

Comme représenté sur la figure 5 ci-dessous, la norme ISO/CEI 27001 est le centre de gravité des référentiels du SMSI. La norme ISO/CEI 27001 formule les exigences relatives aux SMSI et fournit une liste de mesures de sécurité pouvant être intégrées au système [7].

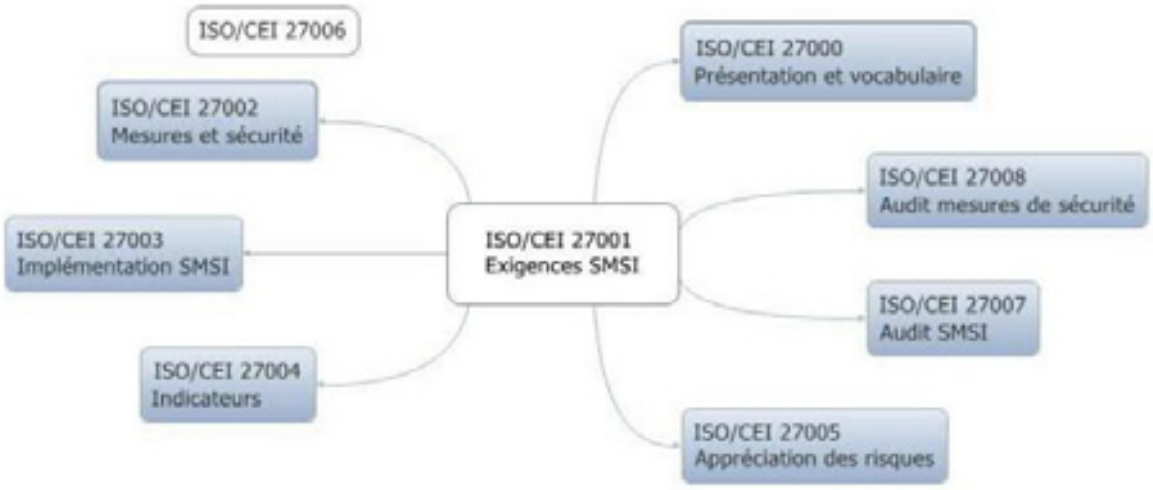

Figure 5: Normes de la famille ISO/CEI 2700x

4.1- L'ISO/CEI 27000

Cette norme a été publiée pour répondre au besoin de définir une terminologie pour les SMSI. Comme nous l'avons vu précédemment, beaucoup de référentiels antérieurs à ISO/CEI 27001 ont été publiés ces dernières années. Ces normes ne fournissent pas de notions, ni de vocabulaire commun, permettant une bonne compréhension des SMSI, c'est ce que propose l'ISO/CEI 27000.

L'ISO/CEI 27000 est structurée en trois parties. La première, définit 46 termes tels que, la confidentialité, l'intégrité, la disponibilité, l'authenticité, tous principalement axés sur l'appréciation et l'analyse des risques, des menaces, de la vulnérabilité, etc. Par exemple,

le mot risque est « la combinaison de la probabilité d'un événement et de ses conséquences ».

La deuxième partie développe la notion de processus avec le modèle PDCA et présente les concepts propres aux SMSI comme par exemple, l'importance de l'engagement de la direction.

La troisième partie, est une présentation de l'ensemble des normes de la famille ISO/CEI 2700x.

4.2- L'ISO/CEI 27002

La norme propose sur onze chapitres, une liste de 133 mesures de sécurité accompagnées chacune de points à aborder pour la mise en place d'un SMSI.

Parmi ces chapitres, on a par exemple, la gestion des actifs, la sécurité physique, la sécurité des ressources humaines, la gestion des incidents, la continuité d'activité, la conformité etc. En résumé, l'ISO/CEI 27002 est un guide de bonnes pratiques, une série de préconisations concrètes, abordant les aspects tant organisationnels que techniques, qui permettent de mener à bien les différentes actions dans la mise en place d'un SMSI [8].

4.3- L'ISO/CEI 27003

Publiée en janvier 2010, ISO 27003 facilite la mise en œuvre du SMSI. Elle est utilisée en complément de la norme ISO 27001. L'ISO 27003 propose cinq étapes pour implémenter le SMSI. Ces étapes concernent l'initialisation du projet, sa politique et son périmètre, l'analyse des exigences en matière de sécurité de l'information, l'appréciation des risques et enfin l'élaboration du SMSI. Chacune de ces étapes est divisée en activités qui font l'objet d'une clause contenant :

- un résumé de l'activité (explication de l'étape en question),
- les entrées (tous les documents à utiliser au cours de l'étape),
- les recommandations (détail des points à aborder),
- les sorties (liste des livrables à produire).

En résumé, ISO 27003 propose un grand nombre de points à aborder et énumère les documents à produire et à consulter. Notons que ISO/CEI 27003 reprend les lignes directrices de la norme ISO/CEI 13335 devenue aujourd'hui obsolète.

4.4- L'ISO/CEI 27004

Cette norme concerne la gestion des indicateurs. L'utilisation d'indicateurs dans le domaine de la sécurité est nouvelle. La norme ISO/CEI 27001 impose leur mise en place dans le SMSI mais sans préciser comment et lesquels utiliser. En utilisant les mesures des indicateurs l'objectif est d'identifier les points du SMSI qui nécessitent une amélioration ou une correction.

4.5- L'ISO/CEI 27005

Une des étapes du PDCA les plus difficiles à mettre en œuvre est « l'appréciation des risques[7] ». L'ISO/CEI 27001 fixe des objectifs à atteindre pour être en conformité avec la norme, mais ne donne aucune indication sur les moyens d'y parvenir. Nous verrons qu'il existe un nombre important de méthodes d'appréciation des risques qui offrent une démarche formelle et pragmatique.

Néanmoins, l'ISO/CEI a souhaité proposer sa propre méthode avec la norme ISO/CEI 27005. L'objectif n'est pas de remplacer ou rendre obsolètes les méthodes existantes mais d'harmoniser le vocabulaire employé. L'ISO/CEI 27005 est constituée de douze chapitres. Les points les plus importants sont traités dans les chapitres sept à douze.

Chap. 7, établissement du contexte

Chap. 8, appréciation du risque

Chap. 9, traitement du risque

Chap. 10, acceptation du risque

Chap. 11, communication du risque

[7] L'appréciation des risques est l'étape 2 de la phase PLAN du PDCA proposé par l'ISO/CEI 27001.

Chap. 12, surveillance et révision du risque

En complément de ces chapitres, viennent s'ajouter six annexes proposant des explications plus détaillées qui présentent des listes de menaces et vulnérabilités types. L'ISO/CEI 27005 peut aussi servir de référence aux organismes qui cherchent à évaluer une méthode d'appréciation des risques [9].

4.6- L'ISO/CEI 27007

Cette norme est à l'état de brouillon « WD[8] ». On peut cependant avancer qu'elle sera le pendant de la norme générique ISO 19011[9] pour les SMSI. L'ISO/CEI 27007 donnera les lignes directrices pour auditer les SMSI.

4.7- L'ISO/CEI 27008

A l'état de WD, l'ISO/CEI 27008 traitera de l'audit des SMSI en proposant un guide qui permettra de contrôler les mesures de sécurité. Elle fournira pour chacune des mesures de sécurité de la 27002, des moyens d'analyse des besoins en contrôle, en tenant compte de l'importance des risques et des actifs. On pourra ainsi déterminer les mesures à contrôler. Ces points sont importants car les auditeurs internes ou externes doivent contrôler des mesures aussi variées que la gestion des mots de passe, la procédure de gestion des incidents et le suivi de législation en vigueur.

4.8- L'ISO/CEI 27006

Cette norme est une reprise enrichie de la norme ISO 17021[10]. Etant destinée aux cabinets d'audit en charge de certifier les organismes, l'ISO/CEI 27006 est moins connue que l'ISO/CEI 27001 qui s'adresse directement aux organismes souhaitant

[8] WD (working draft) est l'état « projet » de la norme avant sa publication.

[9] ISO 19011 fournit des conseils sur les principes de l'audit, le management des programmes d'audit, la réalisation d'audits de systèmes de management. C'est une norme générique qui peut s'appliquer à différents types de systèmes de management.

[10] ISO 17021 spécifie les principes et les exigences relatives à la compétence, à la cohérence et à l'impartialité lors des audits et lors de la certification de systèmes de management de tous types, ISO 27001 pour les SMSI, 9001 pour le management ou 14001 pour l'environnement.

mettre en place un SMSI. L'ISO/CEI 27006 fournit aux organismes de certification les exigences qu'ils doivent faire respecter pour attribuer à leurs clients une certification. Ces exigences sont par exemple : instaurer des mesures pour garantir la confidentialité des données relatives à leurs clients, établir des procédures appropriées pour certifier le SMSI ou encore vérifier régulièrement que les auditeurs soient compétents en matière de sécurité de l'information. Les exigences ne décrivent cependant pas comment l'organisme peut parvenir à la mise en place d'un SMSI. L'organisme doit pour cela procéder à un certain nombre de tâches telles que réaliser un audit des risques, trouver des indicateurs, mettre en œuvre les mesures de sécurité etc. L'organisme a par conséquent besoin d'un guide de bonnes pratiques pour mener à bien son SMSI, et c'est précisément le rôle des normes ISO/CEI 27002 à ISO/CEI 27008.

4.9- Normes ISO/CEI 270xx en préparation

Le tableau 1 ci-dessous donne un aperçu des domaines qui seront couverts par les normes de la famille ISO/CEI 270xx.

PROJET	SECTEUR D'ACTIVITE
ISO/CEI 27010	Gestion de la communication inter secteur
ISO/CEI 27031	Continuité d'activité
ISO/CEI 27032	Cyber sécurité
ISO/CEI 27033	Sécurité réseau
ISO/CEI 27034	Sécurité des applications
ISO/CEI 27035	Gestion des incidents
ISO/CEI 27036	Audit des mesures de sécurité du SMSI
ISO/CEI 27037	Gestion des preuves numériques

Tableau 1 : Normes ISO/CEI 270xx en préparation

Il est à noter que certains secteurs comme les télécommunications ou le domaine médical ont développé des normes plus spécifiques à leur métier, ISO/CEI 27011 et ISO/CEI 27799.

Deuxième partie

La norme ISO/CEI 27001 : Son approche en quatre phases (Plan, Do, Check, Act).

1. Introduction

Pour être en conformité avec la norme ISO/CEI 27001, les SMSI doivent répondre à toutes les exigences comprises entre les chapitres 4 et 8 illustrés dans la figure 6 suivante [10]:

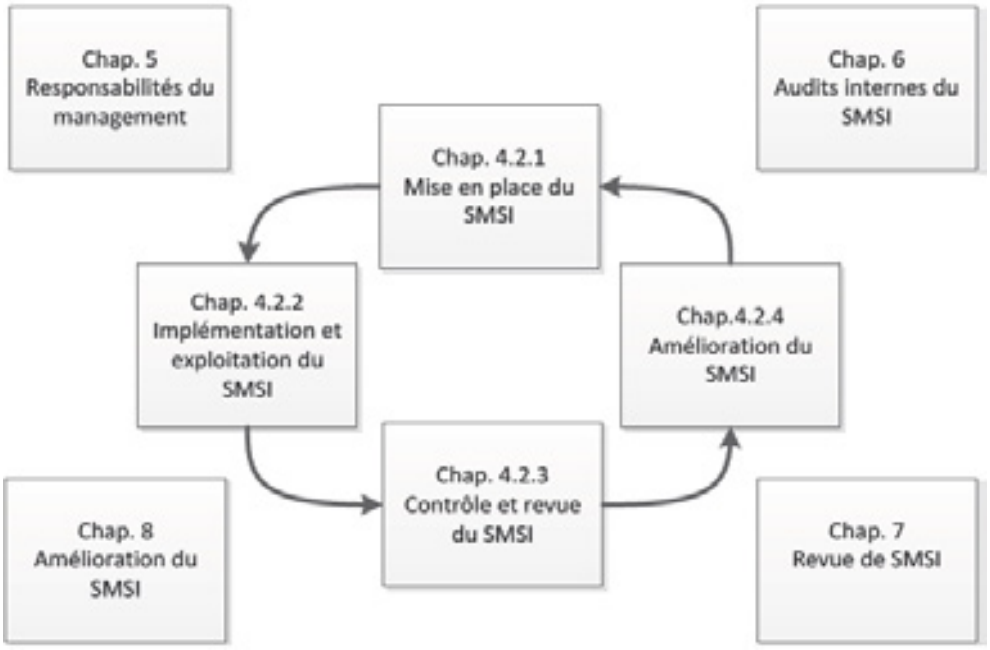

Figure 6: Structure de l'ISO/CEI 27001

- Le chapitre 5 concerne tout ce qui possède un rapport avec les responsabilités du management.
- Le chapitre 6 précise tout ce qui touche aux audits internes.
- Le chapitre 7 développe les aspects relatifs aux revues des différents éléments du SMSI.
- Le chapitre 8 définit les notions d'actions correctives et préventives.
- Le chapitre 4 est au centre de la norme, il regroupe les quatre phases du PDCA (PLAN, DO, CHECK, ACT) de la roue de Deming.

2. Phase « PLAN » du PDCA

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[11] (Statement of Applicability).

Dans la figure 7 ci-dessous, une vue du déroulement de la phase Plan.

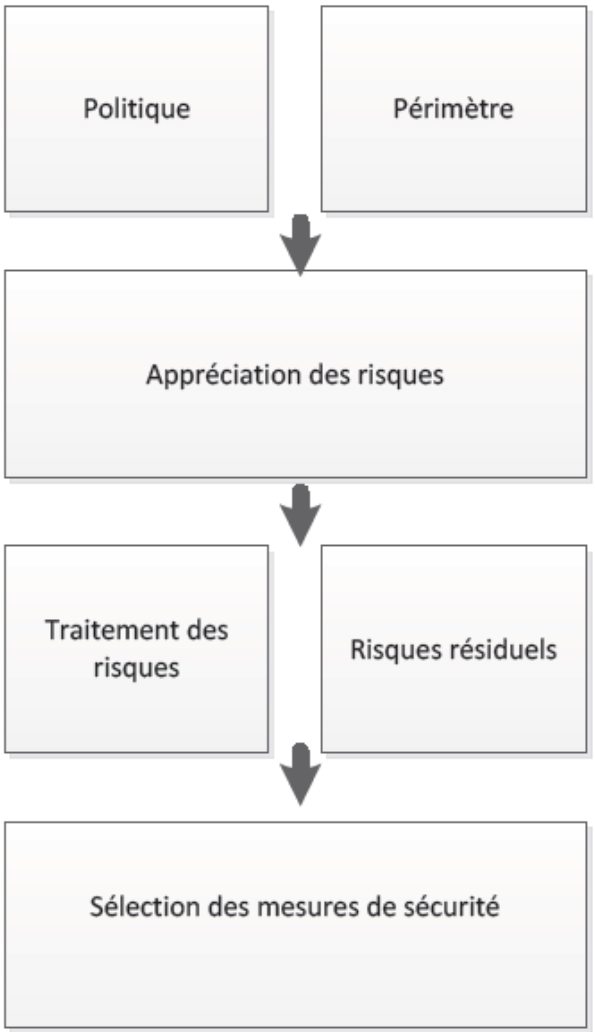

Figure 7 : Etapes de la phase Plan du PDCA

[11] SoA (Statement of Applicability) est un document sous forme de tableau qui énumère les mesures de sécurité du SMSI ainsi que celles non appliquées.

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, mais ne l'impose pas. L'ISO/CEI 27001 ne fait que fixer un cahier des charges spécifiant chacune des étapes clefs de l'appréciation des risques. L'organisme a le libre choix, de développer sa propre méthode en suivant les objectifs fixés par l'ISO/CEI 27001 ou d'en appliquer une déjà éprouvée.

Dans les points suivants nous détaillons le processus d'appréciation des risques avant de donner trois 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 8 ci-dessous.

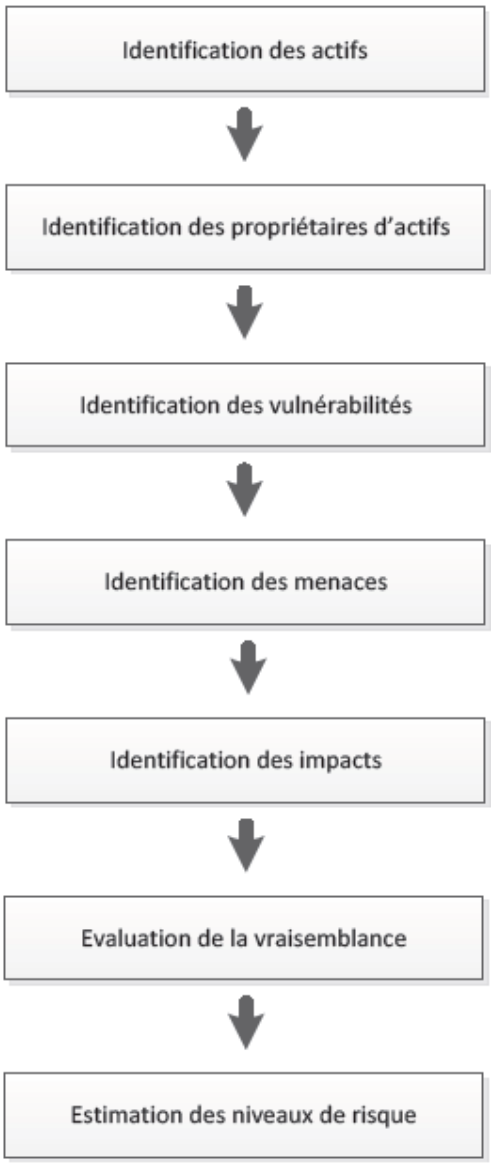

Figure 8: Processus d'appréciation des risqué

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[12], 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[13] 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 [9].

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

---

[12] La matrice des risques permet de mettre en rapport les niveaux de risques définis par la direction avec ceux identifiés dans l'appréciation des risques.

[13] VPN (réseau privé virtuel) est vu comme une extension des réseaux locaux et préserve la sécurité logique que l'on peut avoir à l'intérieur d'un réseau local.

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 en avons retenu trois, EBIOS, MEHARI et OCTAVE qui pour l'ENISA (European Network and Information Security Agency) figurent parmi les plus utilisées [11].

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[14] proposent en libre accès sur leur site web toute la documentation[15] ainsi qu'un logiciel libre[16] 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 [12].

EBIOS se compose de cinq modules représentés dans la figure 9 ci-dessous :

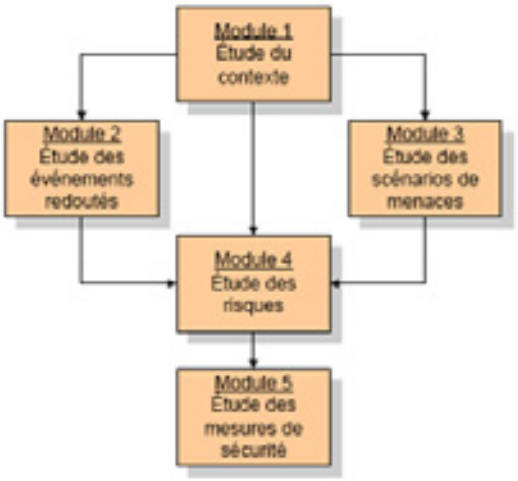

Figure 9: Modules d'EBIOS

[14] Le club EBIOS sur le site : www.club-ebios.org, est une communauté francophone de la gestion des risques basée sur la méthode EBIOS.

[15] La méthode EBIOS est publiée sous la forme d'un guide et de bases de connaissances riches et adaptables (types de biens, d'impacts, de sources de menaces, de menaces, de vulnérabilités et de mesures de sécurité).

[16] Logiciel libre EBIOS, intègre une base de connaissances permettant de saisir les hypothèses et de synthétiser les résultats.

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[17] 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[18] (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.

[17] Terme employé par la méthode pour décrire un constituant de l'organisme.

[18] Critères d'impacts, une liste est fournit par EBIOS.

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.

MEHARI

La méthode MEHARI (Méthode Harmonisée d'Analyse de Risques) a été développée dans les années 1990 par le CLUSIF[19] (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.

MEHARI s'appuie sur deux méthodes anciennes aujourd'hui abandonnées, appelées MARION[20] (Méthode d'Analyse de Risques Informatiques Optimisée par Niveau) et MELISA (Méthode d'évaluation de la Vulnérabilité Résiduelle des Systèmes d'armement).

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,

[19] Club de la Sécurité de l'Information Français, est une association française d'entreprises et de collectivités réunie en groupes de réflexion et d'échanges autour de différents domaines de la sécurité de l'information : gestion des risques, politiques de sécurité, cybercriminalité, intelligence économique.

[20] Marion, méthode d'audit, proposée depuis 1983 par le CLUSIF, visant à évaluer le niveau de sécurité informatique d'une entreprise.

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 [13].

Chaque module peut être utilisé indépendamment ou en combinaison et conduit généralement à un plan d'action, comme le montre la figure 10 ci-dessous.

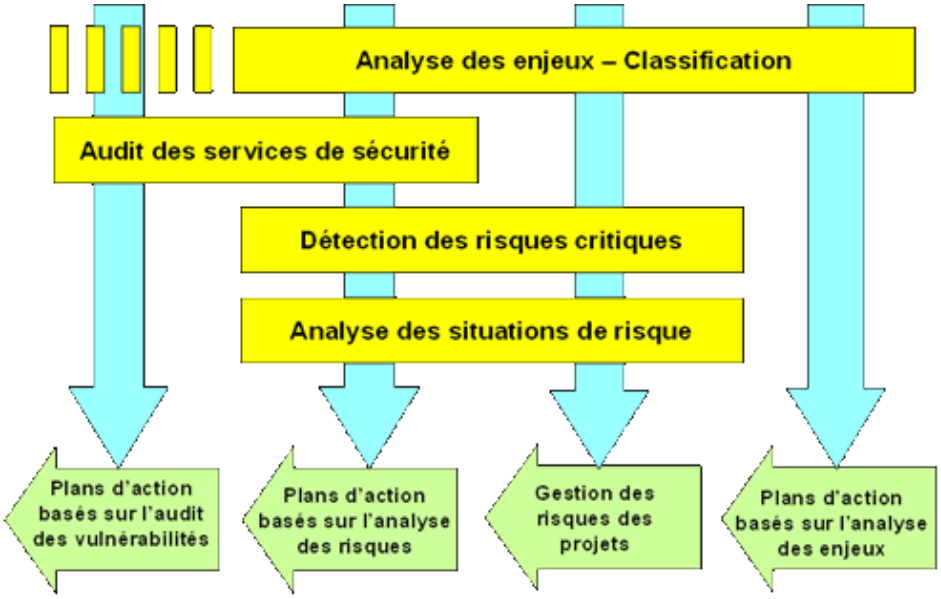

Figure 10: Utilisation des modules de MEHARI

Les modules sont les suivants :

Le module « analyse des enjeux et classification » permet d'identifier et d'analyser les ressources[21] de l'organisation ainsi que les enjeux concernant la sécurité. Ce module s'appuie sur quatre principes.

- Le premier, consiste à présenter les métriques de la méthode (quantification de la potentialité et de l'impact, appréciation des niveaux de risques).
- Le deuxième, vise à dresser une liste des priorités à respecter. Ces objectifs de sécurité, établis par la direction, dépendent des spécificités de l'organisme.
- Le troisième, concerne la classification des ressources de l'entreprise. Les ressources sont identifiées et classées en fonction de leur impact en termes de disponibilité, d'intégrité et de confidentialité.

[21] Ressources peuvent être aussi bien les locaux, qu'un serveur ou un groupe d'employés, la norme ISO/CEI 27001 utilise le terme « actif » pour définir les ressources.

- Le quatrième principe est la mise en œuvre de la charte et de la politique de sécurité de l'organisme.

Le second module concerne les services de sécurité. A l'aide de la base de connaissance des mesures de sécurité de la méthode on corrige les points faibles par des plans d'action, on évalue l'efficacité des mesures mises en œuvre, on prépare l'analyse des risques induits par les faiblesses mises en évidence, et on termine par un audit des vulnérabilités sur la base des normes en usage.

Le troisième module est l'analyse des situations de risque qui permet de faire une synthèse des actions de sécurité préalablement menées. On sélectionne des indicateurs en fonction des objectifs fixés dans le premier module. Ces indicateurs permettent de comparer les résultats obtenus aux objectifs fixés. Cette dernière étape offre un suivi dans le temps du niveau de sécurité de l'information.

En conclusion, la méthode MEHARI, se caractérise par une démarche « descendante », c'est-à-dire une délégation des décisions de la direction vers les entités opérationnelles. Elle convient bien aux organisations multi-environnements. Cette méthode est conforme au cahier des charges imposé par l'ISO/CEI 27001.

OCTAVE

OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) est une méthode d'évaluation du risque développée en 1999 par le Software Engineering Institute de l'Université Carnegie Mellon aux Etats-Unis. La documentation est publique et la dernière version 2.0 date de 2001. Par rapport aux autres méthodes, sa dernière mise à jour est ancienne mais demeure pertinente. Cette méthode se caractérise par une analyse des risques qui peut être réalisée exclusivement à partir des ressources internes. Elle permet, comme les autres méthodes, l'évaluation des menaces et les vulnérabilités des actifs d'information recensés [14]. La méthode est développée autour de trois phases comme le montre la figure 11 ci-dessous.

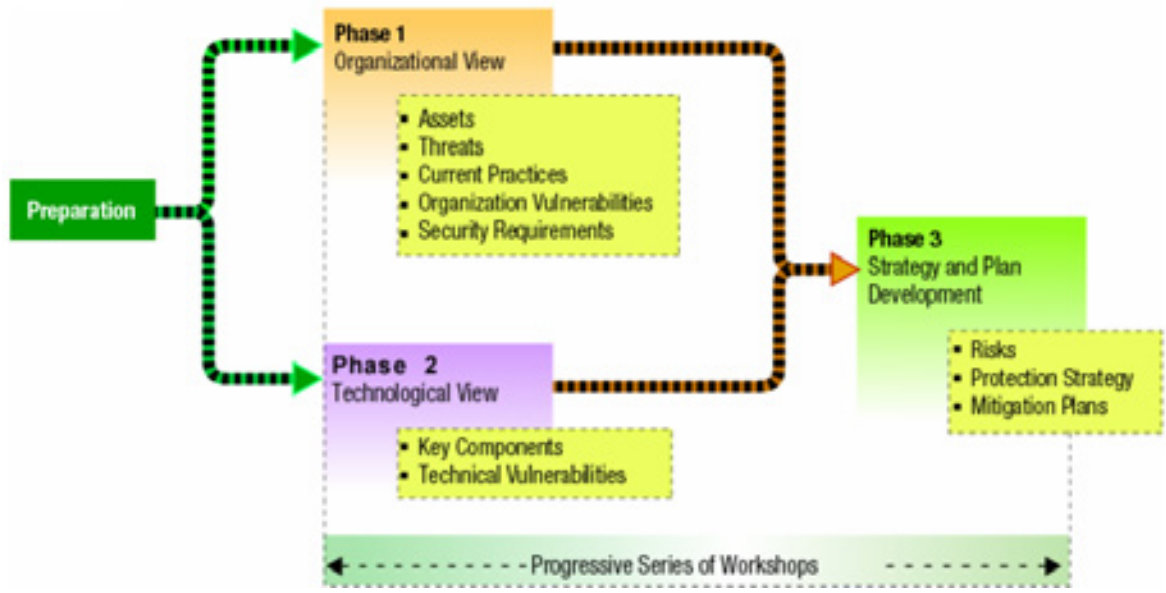

Figure 11: Phases de la méthode OCTAVE

La première phase a pour objectif d'identifier les actifs les plus importants en fonction des menaces et vulnérabilités qui leurs sont associés. On interroge les collaborateurs à tous les niveaux de l'organisme pour rassembler le plus d'informations possibles. Cela permet de dresser des profils de menaces sur les actifs et les besoins en sécurité sur la base de critères tels que la disponibilité, l'intégrité et de confidentialité de l'information.

La deuxième phase a pour but l'identification des vulnérabilités dites techniques. On évalue par exemple, l'infrastructure réseau, on examine les chemins d'accès de chaque actif critique en vue d'obtenir une mesure de la vulnérabilité des infrastructures.

La troisième phase de la méthode décline le développement de la stratégie de la sécurité et sa planification par une analyse de risque et la mise en place des mesures de sécurité.

En conclusion, la méthode OCTAVE offre une « stratégie » de protection pour l'organisationnel et l'opérationnel. Un plan de gestion des risques pour les infrastructures liées à l'information et un plan d'action pour l'ensemble de l'organisation. La méthode vise les administrations et les grands comptes. Il existe aussi une version adaptée pour les PME.

En résumé, l'approche systématique et structurée de ces méthodes, permet d'évaluer les vulnérabilités d'un système d'information, de quantifier les risques et d'aider à la mise en œuvre d'un processus d'appréciation des risques du SMSI.

Cependant, si l'objectif est commun, les termes et expressions employées varient d'une méthode à l'autre. L'ISO/CEI 27001 et 27005 apporte une cohérence à l'ensemble du processus ce qui facilite sa compréhension.

Après avoir étudié en détail l'étape 2 de la phase « Plan » du PDCA, nous allons poursuivre avec l'étape 3 qui concerne le traitement des risques et l'identification des risques résiduels.

2.2.3- 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.

2.2.4- 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, appelé SoA (Statement of Applicability) 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 » du PDCA

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 [10].

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 [7].

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 » du PDCA

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 [10]. 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 » du PDCA

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.

Nous avons présenté la méthode et les exigences de la norme ISO/CEI 27001 pour mettre en œuvre un SMSI. Dans la partie qui suit, nous allons voir comment on a procéder pour implémenter cette norme et la mettre en œuvre au sein de l'Ambassade.

Troisième partie

Implémentation et Mise en œuvre de la norme ISO / CEI 27001

1. Introduction

Dans le cadre de ce travail, on procédera à l'implémentation et mise en œuvre de la norme au sein de l'Ambassade du Royaume du Maroc en Tunisie, les services et les départements sous sa tutelle.

Procéder à un travail pareil au sein de la structure nécessite plusieurs autorisations et vérifications au niveau central au Maroc et un suivi rigoureux de la publication des données résultantes de ce travail aux niveaux académiques et professionnel.

Après plusieurs mois de labeur, je ne suis autorisé de diffuser qu'une partie (présente dans ce rapport) de la totalité du travail effectué vu que les informations traitées au sein de l'Ambassade touchent à la sécurité d'Etat.

Après une présentation de la structure d'accueil, on procédera à une présentation succincte de l'audit effectué et les procédures mise en place lors d'implémentation de la norme.

Seules les parties faisant objet d'une approbation centrale et pour les raisons académiques seront présentes dans ce mémoire de Master.

2. Structure d'accueil

Pour un premier lieu, notre travail sera orienté vers la chancellerie diplomatique et sera généralisé sur l'ensemble des services et départements sous la tutelle de l'ambassade.

La chancellerie diplomatique est formée d'une équipe de diplomates et dirigée par l'Ambassadeur.

Elle assiste l'Ambassadeur, en étroite coordination avec les autres responsables des services de l'Ambassade, dans ses fonctions de représentation du Royaume du Maroc en Tunisie, de mise en œuvre de la politique étrangère marocaine, et de promotion auprès des autorités tunisiennes des prises de position du Maroc sur les grands sujets d'actualité .

La chancellerie contribue à la promotion des relations amicales entre le Maroc et la Tunisie par ses contacts sur place, mais aussi en organisant les visites de personnalités marocaines et en favorisant les échanges de points de vues entre officiels des deux pays.

3. Audit Préalable de l'existant

Comme l'on avait mentionné dans les chapitres précédents, Un SMSI utilise comme élément d'entrée les exigences relatives à la sécurité de l'information et les attentes des parties intéressées, et il produit, par les actions et processus nécessaires, les résultats de sécurité de l'information qui satisfont ces exigences et ces attentes

L'audit mené vise dans ce cadre de travail :

- La détermination de l'existant et des écarts par rapport à la norme ISO/CEI 27001
- La détermination de l'existence ou pas d'un SMSI
- La proposition d'actions correctives pour la mise en conformité du SMSI existant à la norme ISO/CEI 27001 ou la mise en place d'un nouveau SMSI conforme à la norme si aucun SMSI n'est existant à l'Ambassade.

Le processus de l'audit préalable mené au sein de l'Ambassade est conforme aux exigences réglementaires au Maroc gérées par l'Agence Nationale de la Régulation et des Télécommunication [15].

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

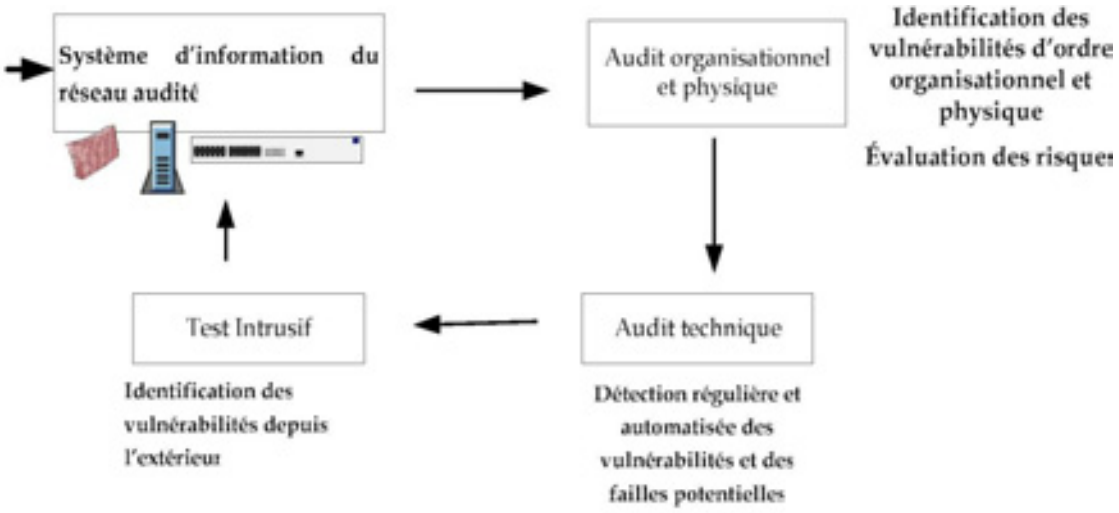

Figure 12: Cycle de l'Audit préalable

A niveau de ce travail, l'audit préalable se présente essentiellement suivant deux parties comme le présente le précédent schéma :

- L'audit organisationnel et physique.
- L'audit technique.

• La troisième partie de l'audit intrusif ne peut être menée qu'à partir des services centraux du Conseil Supérieur de Défense [16] à Rabat (CSD).

Dans ce travail académique et pour des raisons de sécurité, on est autorisé à présenter seulement la démarche de l'audit et les conclusions de ce dernier [16][17].

3.1- Démarche de l'audit préalable

Tel que précédemment évoqué, l'audit préalable d'un SMSI se déroule suivant deux principales étapes. Cependant il existe une phase tout aussi importante qui est une phase de préparation. Nous schématisons l'ensemble du processus d'audit à travers la figure suivante :

Figure 13: Phases de l'audit

3.1.1- 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 auditeur et responsables de l'ambassade. Au cours de ces entretiens, devront être exprimées les espérances des responsables vis-à-vis de l'audit, il doit être fixé l'étendu de l'audit ainsi que les zones et éléments à auditer, de même qu'un planning de réalisation de la mission de l'audit.

Les personnes qui seront amenées à répondre au questionnaire concernant l'audit du

SMSI doivent être également identifiées.

Une fois que les deux parties (auditeur-audité) ont « harmonisé leur registre », l'audit sur terrain peut être entamé. Il débute par l'audit organisationnel et physique.

3.1.2- Audit organisationnel et physique

Dans cette étape, il s'agit de s'intéresser à l'aspect physique et organisationnel de l'Ambassade.

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 SMSI et d´identifier les risques potentiels sur le plan organisationnel.

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 des réalités de l'Ambassade (on n'est pas autorisé à diffuser ce questionnaire).

A l'issu de ce questionnaire, et suivant une métrique, l'auditeur est en mesure d'évaluer les écarts par rapport à la norme et d'apprécier le niveau de maturité en termes de sécurité de l'Ambassade, ainsi que la conformité de cette dernière par rapport à la norme référentielle de l'audit qui est l'ISO/CEI 27001.

Le questionnaire d'audit se compose de 185 questions. Chaque question est affectée d'un coefficient de pondération portant sur l'efficacité de la règle du référentiel sur laquelle porte la question, en matière de réduction de risque.

Après la validation du Questionnaire, les réponses choisies seront introduites dans l'application dédié à cet audit et que nous avons développée sous S.A.S[22] pour permettre l'automatisation du traitement du questionnaire.

Le traitement consiste au calcul d'une moyenne pondérée par les notes obtenues en fonction des réponses choisies et du coefficient d'efficacité. L'on obtient un résultat chiffré (de 0 à 6 ou exprimé en pourcentage) représentant le niveau de sécurité (la

[22] Statistical Analysis System, c'est un langage de programmation de quatrième génération (L4G) édité par le SAS Institute. Il existe depuis plus de trente ans. Depuis 2004, SAS en est à la version 9, ce qui correspond à une évolution majeure dans le logiciel car il intègre une nouvelle brique conceptuelle destinée à s'implanter dans le monde des logiciels d'informatique décisionnelle (Business Intelligence).

maturité) du SMSI audité.

Une fois cette phase réalisée, il est question de passer à l'étape suivante de l'audit ; il s'agit notamment de l'audit technique.

3.1.3- Audit technique

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 des applicatifs, standards téléphoniques, 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 des informations.

Au cours de cette phase, l'auditeur pourra également apprécier l'écart d'avec les réponses obtenues lors des entretiens. Il sera à même de tester 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.

Déroulement

Vu les objectifs escomptés lors de cette étape, leurs aboutissements ne sont possibles que par l'utilisation de différents outils agrées par le Conseil Supérieur de Défense.

Ces outils sont classés et ne peuvent pas être diffusé et leur manipulation m'était impossible avant de bénéficier d'une procédure d'habilitation qui a pris quelques semaines.

3.1.4- Audit intrusif

Cet audit permet d'apprécier le comportement des installations techniques de l'Ambassade face à des attaques. Egalement, il permet de sensibiliser les acteurs (management, équipes 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 palier aux insuffisances identifiées.

Déroulement

La phase de déroulement de cet audit ne peut être utilisée que par le Conseil Supérieur de Défense à Rabat et ses équipes [16].

3.1.5- Synthèse de l'audit préalable :

A la fin des précédentes phases d'audit, nous pouvons formuler les constats suivants :

- Existence de plusieurs SMSI et l'existence d'un SMSI au niveau central à Rabat par rapport à un type d'information bien particulier.
- Le dit SMSI existant touche des informations classées de type très particulier.

Les SMSI existant au sein de l'Ambassade sont :

- système de la messagerie sécurisée
- Système de la messagerie sécurisée spéciale I
- Système de la messagerie sécurisée spéciale II
- Système de messagerie sécurisée spéciale III
- Système de la Gestion Intégrée de la Dépense publique
- Système de Dématérialisation de la commande publique
- Gestion des Ressources
- système fédérateur de services e-finances
- Système de paie publique
- Système d'Emission des Passeports Biométriques et Provisoires
- Système de la Carte Nationale d'identité électronique -
- Infrastructure data sécurisée avec le Ministère de l'Intérieur
- Système de l'Etat Civile
- Système de Identifiant Commun de l'Entreprise
- Application consulaire
- Système du visa sécurisé
- Système du Registre Central du Commerce
- Système de la Propriété Intellectuelle et Industrielle
- Système d'Information et de Réservation des Produits Touristiques au Maroc
- Système de Gestion des Retraites Publiques et Privées
- Système de Gestion des Actifs et des Inventaires des représentations diplomatiques marocaines à l'Etranger
- Système de Gestion du matériel informatique et de télécommunication des Représentations Diplomatiques Marocaines à l'Etranger

3.2- Conclusion de l'audit

Suite aux précédentes synthèses, les SMSI existants sont conformes aux exigences de la norme ISO/CEI 27001 mais ne sont pas regroupés sous un seul SMSI qui pourra assurer l'application de la norme en intégralité.

Le chevauchement des accès aux multiples SMSI existant peut créer des vulnérabilités de sécurité car y a pas un pilotage horizontal de ces SMSI par un SMSI central.

De ce fait, la mise en œuvre de la norme ISO/CEI 27001 au sein de l'ambassade ne peut se faire que par la mise en place d'un SMSI qui regroupe les autres SMSI sous un seul, avec une politique de sécurité et organisation de ce nouveau SMSI. Les autres SMSI existants seront harmonisés pour la conformité à la norme par rapport aux articles correspondants.

Dans le cadre de ce travail académique, l'autorisation de diffusion partielle de ce rapport ne touche que les Articles A.5 et A.6 de la norme ISO/CEI 27001 après modification requise de quelques données par les services compétents à Rabat.

Dans l'annexe sont présentés les articles A.5 à A.15 de ladite norme où on trouve énumérés les objectifs de sécurité et les mesures de sécurité de chaque article, avec des recommandations de mise en œuvre et des lignes directrices afférentes aux meilleures pratiques.

Les listes figurant dans cet annexe ne sont pas exhaustives et un organisme peut considérer nécessaires des objectifs et des mesures de sécurité additionnels.

4. Article « A.5 POLITIQUE DE SECURITE »

4.1- Fondements

La politique de sécurité de l'information se base sur la protection de l'information dite de Sécurité d'Etat.

Toutes les informations traitées au sein de l'Ambassade sont considérées des informations de Sécurité d'Etat [16].

Ces informations constituent une cible majeure pour les services étrangers et les groupements ou les individus isolés ayant pour objectif de déstabiliser l'Etat ou la société.

Les informations de Sécurité d'Etat nécessitent une protection particulière, permettant d'en maîtriser et d'en limiter la diffusion, dans des conditions définies dans la présente politique.

L'atteinte à ces informations est considérée selon la législation marocaine comme acte de haute trahison passible à la peine de mort (Article 181 du Code Pénal)[23] [18].

Il existe trois niveaux de classification : *Très Secret, Secret et Confidentiel.*

Les trois niveaux relèvent du périmètre de la défense nationale vue que ce sont des informations de sécurité d'Etat.

Peuvent faire l'objet de ces classifications les procédés, objets, documents, informations, réseaux informatiques, données informatisées ou fichiers dont la divulgation est de nature à nuire à la défense nationale ou pourrait conduire à la découverte d'un secret de la défense nationale.

Bénéficient également de la protection du secret les lieux qui, en raison des installations ou activités qu'ils abritent, sont classifiés.

L'inobservation des mesures de protection induites par la classification génère la mise en œuvre du dispositif de répression pénale et sera considérée comme un acte de haute trahison. La politique de sécurité vise aussi à rendre responsable, pénalement et

[23] Article 181. 4° Tout Marocain qui livre à une autorité étrangère ou à ses agents, sous quelque forme et par quelque moyen que ce soit, un secret de la défense nationale ou qui s'assure par quelque moyen que ce soit la possession d'un secret de cette nature en vue de le livrer à une autorité étrangère ou à ses agents;

administrativement, toute personne ayant accès à des informations ou supports classifiés.

Une information classifiée est compromise lorsqu'elle est portée à la connaissance du public ou d'une personne non habilitée ou n'ayant pas le besoin d'en connaître.

L'évaluation des risques de compromission des informations ou supports classifiés et des vulnérabilités des personnes ou des systèmes les traitant, au regard des intérêts fondamentaux de la nation, est essentielle afin de garantir la protection de l'information de sécurité d'Etat.

La stricte application des mesures de sécurité définies dans la présente politique contribue à l'efficacité du dispositif et permet de lutter contre des actions malveillantes, souvent facilitées par l'ignorance, l'imprudence, l'inattention ou la négligence.

La protection de l'information de sécurité d'Etat, qu'il s'agisse d'une information, d'un support ou d'un lieu classifié, doit être assurée par les personnes y accédant.

En cas de manquement, même involontaire, ces personnes se rendent coupables de haute trahison.

4.2- Définitions

La mise en place du SMSI central de l'Ambassade ainsi que la présente politique de sécurité emploiera les expressions suivantes :

- **« habilitation »**, pour désigner la décision explicite, délivrée à l'issue d'une procédure spécifique permettant à une personne, en fonction de son besoin d'en connaître, d'avoir accès aux informations ou supports classifiés au niveau précisé dans la décision ainsi qu'au(x) niveau(x) inférieur(s) ;
- **« Informations ou supports classifiés »**, pour désigner les procédés, objets, documents, informations, réseaux informatiques, données informatisées ou fichiers présentant un caractère de secret de la défense nationale ;
- **« Lieux classifiés »**, pour désigner les lieux auxquels il ne peut être accédé sans que, en raison des installations ou des activités qu'ils abritent, cet accès donne par lui-même connaissance d'une information de sécurité d'Etat et ayant fait l'objet d'une décision de classification ;

- **« systèmes d'information »**, pour désigner l'ensemble des moyens informatiques ayant pour finalité d'élaborer, de traiter, de stocker, d'acheminer, de présenter ou de détruire l'information ;
- **« contrat »**, pour désigner tout contrat, toute convention, tout marché quel que soit son régime juridique ou sa dénomination, dans lequel un candidat ou un cocontractant, public ou privé, est amené à l'occasion de la passation du contrat ou de son exécution à connaître et éventuellement à détenir dans ses locaux des informations ou des supports classifiés.

4.3- Champ d'application

Les dispositions de la présente politique sont applicables dans toutes les administrations et services sous l'autorité de l'Ambassade du Royaume du Maroc en Tunisie ainsi qu'à toute personne dépositaire, même à titre provisoire, d'une information relative à l'Ambassade, y compris dans le cadre de la passation et de l'exécution d'un contrat.

4.4- La classification

La décision de classifier au titre du secret de la défense nationale une information ou un support a pour conséquence de le placer sous la protection de dispositions spécifiques du Code Pénal (Article 181) [18].
L'apposition du marquage de classification constitue le seul moyen de conférer cette protection particulière.

Trois niveaux de classification :

- *Très Secret:*

  réservé aux informations et supports qui concernent les priorités gouvernementales en matière de défense et de sécurité nationale et dont la divulgation est de nature à nuire très gravement à la Sécurité d'Etat ;
- *Secret:*

  réservé aux informations et supports dont la divulgation est de nature à nuire gravement à la Sécurité d'Etat ;

- *Confidentiel:*

  réservé aux informations et supports dont la divulgation est de nature à nuire à la Sécurité d'Etat ou pourrait conduire à la découverte d'un secret classifié au niveau

Une information n'ayant pas fait l'objet d'une décision de classification à l'un des trois niveaux définis n'est pas protégé au titre du secret de Sécurité de l'Etat

4.5- Mentions particulières de confidentialité et les Informations Sensibles Non Classées (ISNC)

Certaines informations qu'il n'y a pas lieu de classifier peuvent cependant recevoir, de la part de leur émetteur, une marque de confidentialité destinée à restreindre leur diffusion à un domaine spécifique (précisé par une mention particulière) ou à garantir leur protection (telle que *Diffusion Restreinte*).
Ces mentions, qui ne traduisent pas une classification et ont pour seul objectif la sensibilisation de l'utilisateur à la nécessité de discrétion dont il doit faire preuve dans la manipulation des informations couvertes par cette mention. Ces informations seront considérées des Informations Sensibles Non Classées (ISNC).
Une information sensible est une information dont la compromission, l'altération, le détournement ou la destruction, est de nature à nuire à la Sécurité de l'Etat et à la continuité du fonctionnement des services de l'Etat et de l'exercice du pouvoir de l'Etat.

Il existe trois catégories d'informations Sensibles Non Classées:

- **1ère catégorie** : ISNC sur lesquels une atteinte à la disponibilité, à l'intégrité ou à la confidentialité peut entrainer la **neutralisation** d'une fonction majeure dans le fonctionnement des services de l'Etat et de l'exercice du pouvoir ;

- **2ème catégorie** : ISNC sur lesquels une atteinte à la disponibilité, à l'intégrité ou à la confidentialité peut entrainer une **dégradation** du fonctionnement des services de l'Etat et de l'exercice du pouvoir

- **3ème catégorie** : ISNC sur lesquels une atteinte à la disponibilité, à l'intégrité ou à la confidentialité peut entrainer une **gêne** dans le fonctionnement des services de l'Etat et l'exercice du pouvoir

4.6- L'accès aux informations traitées à l'ambassade (Information de Sécurité d'Etat)

Seules des personnes qualifiées peuvent accéder aux informations classées ou ayant une mention particulière.

La qualification exige la réunion de deux conditions cumulatives :

A. Le besoin de connaître ou d'accéder à une information classifiée est dans la mesure où l'exercice de la fonction ou l'accomplissement de la mission l'exige.

B. La délivrance de l'habilitation correspondant au degré de classification de l'information considérée : la décision d'habilitation est une autorisation explicite, délivrée à l'issue d'une procédure spécifique permettant à une personne, sous réserve du besoin d'en connaître, d'avoir accès aux informations ou supports d'information de sécurité d'Etat au niveau précisé dans la décision ainsi qu'au(x) niveau(x) inférieur(s).

   La décision d'habilitation est assortie d'un engagement de respecter, après en avoir dûment pris connaissance, les obligations et les responsabilités liées à la protection des informations ou supports classifiés.

4.7- Lieux abritant des informations de sécurité d'Etat

Les lieux abritant des éléments couverts par une classification sont les locaux dans lesquels sont détenus des informations ou supports classifiés, quel qu'en soit le niveau, par des personnes par ailleurs habilitées au niveau requis.

Les « lieux classifiés » sont ceux auxquels il ne peut être accédé sans que, en raison des installations ou des activités qu'ils abritent, cet accès donne par lui-même connaissance d'une information de sécurité d'Etat et qui ont fait l'objet d'une décision de classification.

L'accès à ces lieux, pour motif de service, est encadré par les dispositions relatives au droit du travail, aux contrats de prestation de service, au droit pénal, à la procédure pénale ou issues de conventions internationales.

4.8- Contrôles et inspections

Des contrôles et des inspections sont organisés périodiquement pour vérifier l'application des instructions et des directives relatives à la protection de l'information de sécurité d'Etat.

Les inspections et les contrôles sont assurés par la cellule de sécurité de l'Information crée par la dite politique. Cette cellule propose toutes mesures propres à améliorer les conditions générales de sécurité de l'information et le maintien du SMSI central de l'Ambassade.

Les inspections et les contrôles sont organisés en liaison avec les autres services et départements sous tutelle de l'ambassade du royaume du Maroc en Tunisie

En cas d'anomalies constatées, la cellule Sécurité de l'Information peut saisir, par l'intermédiaire de l'ambassadeur de Sa Majesté, les services qui concourent à la répression des crimes et délits.

Les rapports de synthèse incluant les mesures préconisées pour rectifier les déficiences constatées et leur planification sont adressés aux autorités centrales responsables des services est département représenté au sein de l'Ambassade.

5. Article « A.6 ORGANISATION DE LA SECURITE DE L'INFORMATION »

5.1- Principe

Nul n'est qualifié pour connaître des informations de Sécurité d'Etat ou supports s'il n'est habilité au niveau requis et s'il n'a le besoin de les connaître.

5.2- Implication de la direction

a. Le Conseil Supérieur de Défense à Rabat [16] : *Partie non diffusée / Contenu Confidentiel*

b. L'Ambassadeur de Sa Majesté le Roi [17]:

- Pour le niveau *Très Secret* :
  - Détermine les critères et les modalités d'organisation de la protection et définit des classifications spéciales correspondant aux différentes priorités gouvernementales au sein de l'ambassade et le pays de représentation ;
  - fixe les conditions dans lesquelles chaque cadre ou agent et département dont il a la charge détermine les informations et supports qu'il y a lieu de classifier à ce niveau ;
- Pour les niveaux *Secret* et *Confidentiel* :
  - Fixe les conditions dans lesquelles chaque ministre, pour le département dont il a la charge, détermine les informations et supports qu'il y a lieu de classifier et les modalités de leur protection;
- Pour les habilitations :
  - Définit la procédure préalable à la décision d'habilitation ;
  - Prend la décision d'habilitation pour le niveau Très Secret et indique les classifications spéciales auxquelles la personne habilitée peut accéder.

Pour l'exercice de ces compétences, l'Ambassadeur est assisté par le conseiller en sécurité, l'attaché militaire et la cellule Sécurité de l'Information.

5.3- Elaboration du Catalogues des Fonctions des Informations de Sécurité d'Etat de l'Ambassade (CFISE)

L'Ambassadeur de Sa Majesté Le Roi assisté par le conseiller en sécurité, l'attaché militaire et la cellule de sécurité de l'Information élaborent les instructions nécessaires pour faire établir au sein de chaque service de l'ambassade et pour chaque niveau de classification, la liste des fonctions nécessitant l'accès à des informations ou supports classifiés. Ces listes sont désignées «Catalogues des Fonctions des Informations de Sécurité d'Etat ».

C'est en référence aux CFISE que les demandes d'habilitation sont établies. Lorsqu'une demande d'habilitation parvient, le secrétariat particulier de l'Ambassadeur vérifie l'inscription de la fonction concernée dans le catalogue des fonctions ISE correspondant. Il examine, à titre exceptionnel, le bien-fondé de la demande lorsque l'emploi ne figure pas au catalogue.

Ces catalogues peuvent être établis par direction, par service ou au niveau des services représentés. Ils sont mis à jour au moins une fois par an, notamment à l'occasion d'une réorganisation de service.

Afin de faciliter l'actualisation, il est vérifié auprès des titulaires des postes répertoriés s'ils ont effectivement eu accès à des informations classifiées pour le niveau concerné.

L'habilitation ne permet pas d'accéder sans limite à toute information ou à tout support classifié au niveau correspondant.

Une personne habilitée n'accède à une information ou à un support classifié que si son autorité hiérarchique estime que cet accès est nécessaire à l'exercice de sa fonction ou à l'accomplissement de sa mission.

L'autorité hiérarchique apprécie de façon rigoureuse et mesurée le besoin de connaître des informations classifiées.

5.4- Candidats à l'habilitation et gestion de l'habilitation

Lors de leur demande d'habilitation, les candidats sont informés, par les mentions portées sur la notice individuelle qui leur est remise, des obligations induites par l'habilitation ainsi que des dispositions relatives à leur responsabilité pénale en cas de compromission.

A la notification d'une décision d'habilitation favorable par l'officier de sécurité suite à la décision de l'Ambassadeur, l'information initiale est complétée par une séance de sensibilisation aux risques de compromission puis, par la suite, par des rappels périodiques de la réglementation en vigueur.

Une sensibilisation aux menaces d'investigations ou d'approches par des individus ou des organisations étrangères est obligatoire et des règles de prudence élémentaire sont rappelées.

L'autorité hiérarchique doit veiller à l'habilitation du personnel placé sous sa responsabilité et, à ce titre, initier, par la constitution d'un dossier, la procédure d'habilitation au niveau requis par le catalogue des fonctions ISE de l'Ambassade.

La demande d'habilitation déclenche une procédure destinée à vérifier qu'une personne peut, sans risque pour la sécurité nationale ou pour sa propre sécurité, connaître des informations ou supports classifiés dans l'exercice de ses fonctions. La procédure comprend une enquête de sécurité permettant à l'autorité d'habilitation de prendre sa décision en toute connaissance de cause.

Les informations ou supports classifiés ne peuvent être portés à la connaissance de personnes non habilitées.

Aussi, toute personne visant ou occupant un poste pour lequel le besoin d'une habilitation est avéré et qui refuserait de se soumettre à la procédure d'habilitation devra être écartée du poste considéré.

5.5- Procédure d'habilitation

La procédure préalable à la décision d'habilitation est une opération coûteuse en temps et en personnel.

Lorsqu'un poste à pourvoir exige une habilitation au niveau *Secret* ou *Confidentiel,* la procédure n'est engagée qu'au seul profit de la personne effectivement nommée dans l'emploi, sauf cas particulier.

Anticiper la prise de poste en engageant la procédure d'habilitation sans attendre la prise effective de fonction peut être une mesure de bonne gestion, qui permet à la personne nouvellement affectée de prendre connaissance des informations classifiées sans perdre de temps.

Il convient toutefois d'éviter toute surcharge inutile des services chargés de cette mission en limitant autant que possible le nombre de demandes d'habilitation.
Lorsque l'habilitation requise est du niveau *Très Secret*, il revient au Conseil Supérieur de Défense à Rabat d'apprécier l'opportunité d'une enquête portant sur chacun des candidats au poste concerné.

5.5.1- Constitution du dossier

Le dossier d'habilitation a pour objet de réunir les éléments qui seront vérifiés lors de l'enquête de sécurité. Il est en format papier et constitué de :

- La demande d'habilitation formulée par le chef du service employeur attestant le besoin de connaître des informations ou supports classifiés à un niveau donné, pour une personne nommément désignée ;
- La notice individuelle de sécurité, renseignée intégralement par l'intéressé et vérifiée par l'officier de sécurité de l'ambassade. Elle est établie en trois exemplaires (un original et deux photocopies, datées et revêtues de la signature originale du candidat) ;
- Trois photographies d'identité originales, identiques et récentes.

5.5.2- Instruction du dossier

Les enquêtes de sécurité menées dans le cadre de la procédure d'habilitation sont des enquêtes administratives et d'environnement permettant de déceler chez le candidat d'éventuelles vulnérabilités.
Elles sont diligentées par le Conseil Supérieur de Défense, le service enquêteur du ministère de l'intérieur et le service enquêteur de l'administration de la défense [16].
Les enquêtes sont fondées sur des critères objectifs permettant de déterminer si l'intéressé, par son comportement ou par son environnement proche, présente une vulnérabilité, soit parce qu'il constitue lui-même une menace pour la sécurité, soit parce qu'il se trouve exposé à un risque de chantage ou de pressions pouvant mettre en péril les intérêts de l'Etat, chantage ou pressions exercés par un service étranger de renseignement, un groupe terroriste, une organisation ou une personne se livrant à des activités subversives.

5.5.3- Clôture de l'instruction et avis de sécurité, durée d'habilitation et conclusions

Les enquêtes menées dans le cadre de l'habilitation s'achèvent par l'émission d'un avis de sécurité, par lequel les services enquêteurs font connaître les conclusions techniques à l'Ambassadeur pour prendre la décision d'habilitation.

Cet avis est une évaluation des vulnérabilités éventuellement détectées lors des enquêtes et permettent à l'Ambassadeur d'apprécier l'opportunité de l'habilitation de l'intéressé, au regard des éléments communiqués et des garanties qu'il présente pour le niveau d'habilitation requis.

Les conclusions de l'avis de sécurité sont de trois types :

- «avis sans objection», lorsque l'instruction n'a révélé aucun élément de vulnérabilité de nature à constituer un risque pour la sécurité des informations ou supports classifiés ni pour celle de l'intéressé ;

- « avis restrictif », lorsque l'intéressé présente certaines vulnérabilités constituant des risques directs ou indirects pour la sécurité des informations ou supports classifiés auxquels il aurait accès, mais que des mesures de sécurité spécifiques prises par l'officier de sécurité permettraient de maîtriser ;

- «avis défavorable», lorsque des informations précises font apparaître que l'intéressé présente des vulnérabilités faisant peser sur le secret des risques tels qu'aucune mesure de sécurité ne semble suffisante à les neutraliser.

L'avis de sécurité est émis pour un niveau donné d'habilitation. L'avis « sans objection » est valable pour le niveau précisé ainsi que pour le(s) niveau(x) inférieur(s).

Pour les avis restrictifs ou défavorables, les services enquêteurs se prononcent, au cas par cas, sur l'opportunité d'accorder une habilitation pour le(s) niveau(x) inférieur(s).

Les avis restrictifs ou défavorables sont classifiés au niveau *Confidentiel*.

Les avis restrictifs et défavorables sont assortis d'une fiche confidentielle indiquant les motifs de l'avis. Cette fiche est composée de deux parties distinctes, permettant de séparer les éléments, non classifiés, qui peuvent être communiqués au candidat, de ceux, le cas échéant classifiés, qui ne peuvent être portés qu'à la connaissance de l'Ambassadeur.

Ne pouvant être reproduite, la fiche confidentielle est retournée après communication et sans délai au service enquêteur qui l'a émise, aux fins de conservation.

La durée de validité de l'avis de sécurité est fonction du niveau d'habilitation demandé. Elle ne peut excéder :

- Cinq ans pour le niveau *Très Secret*;
- Sept ans pour le niveau *Secret*;
- Dix ans pour le niveau *Confidentiel*.

L'avis de sécurité ne constitue en soi ni une autorisation ni un refus, et ne lie pas l'Ambassadeur, qui prend sa décision après avoir apprécié les différents éléments recueillis pendant l'instruction du dossier.

5.6- La décision d'habilitation

La décision d'habilitation ou de refus d'habilitation est prononcée par l'Ambassadeur au regard des conclusions du service enquêteur. Quel que soit le sens de l'avis de sécurité, auquel il n'est d'ailleurs fait aucune référence dans la décision, l'Ambassadeur peut admettre ou rejeter une demande d'habilitation.

L'Ambassadeur peut décider, lorsque l'enquête a mis en valeur des éléments de vulnérabilité, de n'accorder l'habilitation qu'après avoir pris des précautions particulières déclenchées par une procédure de mise en garde.

5.6.1- La décision d'habilitation

La décision d'habilitation est l'autorisation donnée à une personne, en fonction de son besoin d'en connaître, d'accéder aux informations ou supports classifiés au niveau précisé dans la décision, ainsi qu'au(x) niveau(x) inférieur(s).

Pour le niveau *Très Secret*, la décision précise la classification spéciale concernée. Lorsqu'une personne doit avoir accès de façon régulière à des informations relevant de plusieurs classifications spéciales, une décision d'habilitation doit être émise pour chacune de ces classifications. Aussi une personne peut-elle être visée par plusieurs décisions d'habilitation.

5.6.2- La mise en garde

Lorsqu'un avis de sécurité est restrictif ou défavorable, l'Ambassadeur peut néanmoins décider d'accorder l'habilitation tout en mettant en garde l'officier de sécurité compétent.

Cette procédure permet à celui-ci de mettre en œuvre des mesures de sécurité ou de prendre des précautions particulières à l'égard de l'intéressé, si nécessaire avec le conseil supérieur de défense ou du service enquêteur. Le service enquêteur, en liaison avec le Conseil Supérieur de défense, apprécie, parmi les éléments révélés par l'enquête, ce qu'il convient de communiquer à l'officier de sécurité et, le cas échéant, aux chefs de services.

A l'issue de l'entretien de mise en garde, une attestation particulière est signée par l'officier de sécurité de l'ambassade.

La décision d'habilitation n'est rendue qu'à l'issue de la procédure. L'attestation est conservée par l'Ambassadeur.

Au niveau *Très Secret*, la procédure de mise en garde est menée par le Conseil Supérieur de Défense, qui conserve l'attestation.

5.6.3- La mise en éveil

Lorsque l'Ambassadeur décide d'accorder l'habilitation sur la base d'un avis de sécurité restrictif ou en dépit d'un avis de sécurité défavorable, il peut choisir de demander la mise en éveil de l'intéressé, qui consiste à sensibiliser ce dernier sur les éléments communicables de vulnérabilité révélés par l'enquête.

La mise en éveil est menée par l'ambassadeur, en présence de l'officier de sécurité. L'ambassadeur définit les modalités de la mise en éveil en liaison avec le service enquêteur et peut, au cas par cas, solliciter sa présence lors de l'entretien avec l'intéressé. Le cas échéant, l'officier de sécurité étudie avec ce service les mesures de sécurité

complémentaires à mettre en œuvre au regard de la situation.
A l'issue de l'entretien de mise en éveil, une attestation particulière est signée par le représentant de l'ambassadeur, par l'officier de sécurité et par l'intéressé.
La décision d'habilitation n'est rendue qu'à l'issue de la procédure. L'attestation est conservée par l'ambassadeur.
Au niveau *Très Secret*, la mise en éveil est menée par le Conseil Supérieur de Défense, qui conserve l'attestation.

5.6.4- Le refus d'habilitation

L'intéressé est informé de la décision défavorable prise à son endroit. Un refus d'habilitation n'a pas à être motivé lorsqu'il repose sur des informations qui ont été classifiées.

5.7- La notification de la décision

La décision prise par l'ambassadeur est transmise à l'officier de sécurité. A réception, ce dernier notifie au candidat à l'habilitation la décision individuelle prise à son endroit, qu'elle soit favorable ou non.

5.7.1- Décision favorable et engagement de responsabilité

La décision d'habilitation est notifiée par l'officier de sécurité compétent à l'intéressé, qui signe un engagement de responsabilité.
Par cet acte, le candidat reconnaît avoir eu connaissance des obligations particulières imposées par l'accès à une information ou à un support classifié, ainsi que des sanctions prévues en cas d'inobservation, délibérée ou non, de la réglementation protégeant l'information de sécurité d'Etat.
Il est également notifié à l'intéressé qu'il est tenu d'informer au plus vite, pendant toute la durée de son habilitation, l'officier de sécurité de tout changement affectant sa vie personnelle (mariage, divorce, établissement ou rupture d'une vie commune…), relations professionnelles ou son lieu de résidence.
Il lui est signifié qu'il devra l'informer de toute relation suivie et fréquente, dépassant le

strict cadre professionnel, avec un ou plusieurs citoyens étrangers.
L'officier de sécurité devra alors lui faire remplir, afin de mettre à jour les informations, une notice individuelle et la transmettre à l'ambassadeur.
Ce changement de situation pourra justifier un réexamen du dossier d'habilitation et, le cas échéant, la saisie du service enquêteur en vue de l'émission d'un nouvel avis.
Le second volet de cet engagement est signé par l'intéressé à la cessation de ses fonctions ou au retrait de l'habilitation, et précise que les obligations relatives à la protection des informations classifiées auxquelles il a pu être donné accès, perdurent au-delà du terme mis à ses fonctions ou à son habilitation. Une fois signé, ce second volet est retourné à l'ambassadeur.

5.7.2- Refus d'habilitation

La décision de refus d'habilitation est notifiée à l'intéressé par l'officier de sécurité. L'intéressé contresigne la décision, attestant ainsi en avoir pris connaissance.
Si le candidat sollicite, par l'exercice d'un recours, une explication du rejet de la demande d'habilitation, il obtient communication des motifs lorsqu'ils ne sont pas classifiés.
Lorsqu'ils le sont, le candidat se voit opposer les règles applicables aux informations classées.

5.8- Habilitation et changement d'affectation

Lorsqu'une personne habilitée change d'affectation, son habilitation prend fin et une autre décision peut être prise, si la nouvelle affectation l'exige, sur la base de l'avis de sécurité en cours.
Si l'ambassadeur change, l'officier de sécurité de l'ambassade renvoie la décision d'habilitation et l'engagement de responsabilité à l'ambassadeur sortant.
Afin d'informer le nouvel ambassadeur qu'un avis de sécurité est en cours de validité, l'officier de sécurité de l'ambassade lui transmet un certificat de sécurité.
Si l'avis est restrictif ou défavorable, le nouvel ambassadeur peut, pour prendre sa décision, demander à connaître les motifs qui l'ont justifié.
Pour le niveau *Très Secret*, lorsque l'habilitation est devenue sans objet en raison du changement d'affectation de son titulaire, l'ambassadeur en avise le Conseil Supérieur de

Défense et lui renvoie sans délai la décision d'habilitation ainsi que l'engagement de responsabilité (volet 2), dûment signé.

5.9- Conservation des décisions

Pendant leur durée de validité, les décisions d'habilitation sont conservées par l'officier de sécurité. Ces documents, qui portent une mention de protection, ne sont en aucun cas remis aux intéressés ni reproduits.
En cas de nécessité, il peut être remis aux intéressés, par l'ambassadeur, un certificat de sécurité délivré pour une mission déterminée et une période limitée. La délivrance de ces certificats peut être déléguée à l'officier de sécurité. Ce certificat est restitué à l'officier de sécurité dès le retour de mission.

5.10- Répertoire des habilitations

Il est tenu, pour chacun des trois niveaux de classification, un répertoire :

- Des dossiers d'habilitation en cours d'instruction ;
- Des habilitations en cours de validité.

Le Conseil Supérieur de Défense tient à jour le répertoire central des habilitations au niveau *Très Secret*.
Un rapport de suivi trimestriel des personnes habilitées est adressé au Conseil Supérieur de Défense.

5.11- Fin de l'habilitation

L'habilitation prend fin de trois manières : soit lorsque l'intéressé quitte le poste qui a motivé son habilitation, soit lorsque la validité de l'habilitation expire, soit parce que l'habilitation est retirée.

5.11.1- Cessation des fonctions

L'habilitation liée à l'occupation d'un poste ou à l'exercice d'une fonction déterminée expire lorsque son titulaire change d'affectation ou cesse ses fonctions. En quittant l'emploi précisé dans la décision d'habilitation, le titulaire signe, le second volet de l'engagement de responsabilité.

5.11.2- Expiration de validité et renouvellement

Le titulaire d'une habilitation dont le terme fixé dans la décision arrive à échéance signe, le second volet de son engagement de responsabilité.

Seule une demande de renouvellement, engagée dans les formes et les délais requis, permet de proroger provisoirement la validité de l'habilitation, afin d'éviter une interruption inopportune des conditions d'emploi, de fonction ou de la mission du titulaire.

La demande de renouvellement doit être effectuée dans le délai de six mois et, au plus tard, un mois avant la date d'expiration de l'habilitation en cours.

Elle doit comprendre une nouvelle demande d'habilitation et trois exemplaires, mis à jour et signés, de la notice individuelle, accompagnés de trois photographies datant de moins d'un an.

La validité de la décision initiale d'habilitation est prorogée d'une durée maximale de douze mois après péremption de l'avis de sécurité, lorsque le besoin de connaître des informations classifiées subsiste au-delà de la durée de validité de cet avis, et à la condition impérative qu'une demande de renouvellement ait été régulièrement engagée, dans l'attente des conclusions de l'instruction du nouveau dossier.

Cette prorogation est autorisée dans les mêmes conditions lorsqu'une demande, à un niveau supérieur, est formulée dans le délai de six à un mois (au plus tard) précédant la date d'expiration de l'habilitation en cours.

5.11.3- Retrait d'habilitation

La décision d'habilitation ne confère pas à son bénéficiaire de droit acquis à son maintien. L'habilitation peut être retirée en cours de validité ou à l'occasion d'une

demande de renouvellement si l'intéressé ne remplit plus les conditions nécessaires à sa délivrance, ce qui peut être le cas lorsque des éléments de vulnérabilité apparaissent, signalés par exemple par :

- Le service enquêteur ;
- Le supérieur hiérarchique ou l'officier de sécurité, à la suite d'un changement de situation ou de comportement révélant un risque pour la sécurité nationale.

La décision de retrait est notifiée à l'intéressé dans les mêmes formes que le refus d'habilitation, sans que les motifs lui soient communiqués s'ils sont classifiés.
L'intéressé est informé des voies de recours et des délais qui lui sont ouverts pour contester cette décision.

6. Conclusion

L'intégralité de notre travail de mise en place d'un SMSI central conformément à la norme ISO/CEI 27001 au sein de l'Ambassade du Royaume du Maroc en Tunisie a été validée et félicitée par les Services Centraux au Maroc et le Conseil Supérieur de Défense.

A l'issue de ce travail, une perspective de généralisation de cette mise en place sur l'ensemble des représentations diplomatiques marocaines à l'étranger est envisagée par le Ministère des Affaires Etrangères pour l'année 2012. L'objectif futur est d'aboutir à une certification du réseau diplomatique marocain par un organisme accrédité par l'ISO d'où une nouvelle mission que je serai amené à chapoter.

L'obstacle principal rencontré lors de ce travail est sur le volet de diffusion partielle du contenu de ce rapport pour les raisons académiques. Apres deux mois d'attente, il m'est autorisé de diffuser que les parties contenues dans ce rapport.

Grâce au programme poursuivit au sein de ce master, j'ai pu contribuer au développement et à l'optimisation du fonctionnement de l'Ambassade du Royaume du Maroc en Tunisie par la réussite de la mise en place d'un SMSI central conforme à la norme ISO/CEI 27001.

Références

Bibliographie

[3] Alan Calder, The case for ISO 27001. Ed. IT Governance Publishing 2006.

[6] Alan Calder, Information Security Based on ISO 27001/ISO 27002 A Management Guide Editeur : van Haren Publishing; Édition : 2nd edition (31 juillet 2009).

[14] C. Alberts, A. Dorofee, J. Stevens. Introduction to the OCTAVE® Approach. Networked Systems Survivability Program. Carnegie Mellon Software Engineering Institute Pittsburgh, 2003.

[4] Jean-Louis Le Moigne, La Théorie du système général : Théorie de la modélisation. Presses Universitaires de France, Paris, 1977.

Webographie

[15] ANRT, Agence Nationale de la Regulation et des Telecommunication. Disponible sur : http://www.anrt.net.ma

[2] CEN. About us. Disponible sur : http://www.cen.eu/cen/pages/default.aspx

[13] CLUSIF, Présentation de MEHARI. Disponible sur : http://www.clusif.asso.fr

[18] CODE PENAL MAROCAIN. Disponible sur : http://adala.justice.gov.ma

[11] ENISA Inventory of Risk Management / Risk Assessment Methods and Tools. Disponible sur : http://www.enisa.europa.eu

[1] ISO. Discover ISO. Disponible sur : http://www.iso.org/iso/home.htm

[7] ISO. Information security management systems. Disponible sur: http://www.iso.org

Notes Directives

[5] ISO 9001. Quality management systems: Requirements. International Organization for Standardization, Geneva, 2000.

[8] ISO/IEC 27002. Information technology - Security techniques - Code of practice for information security management. International Organization for Standardization, Geneva, 2005.

[9] ISO/IEC 27005. Information technology - Security techniques – Information security risk management. International Organization for Standardization, Geneva, 2008.

[10] ISO/IEC 27001. Information technology - Security techniques – Information security management systems - Requirements. International Organization for Standardization, Geneva, 2005.

[12] EBIOS, Méthode de gestion des risques, ANSSI, Version du 25 janvier 2010.

[17] Note Circulaire du Ministère des Affaires Etrangères et de la Coopération.

[16] Note Directive du Conseil Supérieur de Défense Marocain.

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

ISNC : Information Sensible Non Classée

ISE : Information de Sécurité d'Etat

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

VPN : Virtual Private Network

WD : Working Draft

WG : Working Group

Tables des indexes

Annexe

(normative)

Objectifs de sécurité et mesures de sécurité

Les objectifs de sécurité et les mesures de sécurité énumérés dans le Tableau A.1 proviennent directement et sont alignés sur les objectifs de sécurité et les mesures de sécurité énumérés dans l'ISO/CEI 27001: 2005, Articles 5 à 15. Les listes figurant dans ces tableaux ne sont pas exhaustives et un organisme peut considérer nécessaires des objectifs de sécurité et des mesures de sécurité additionnels. Les objectifs de sécurité et les mesures de sécurité mentionnés dans ces tableaux doivent être sélectionnés comme partie intégrante du processus d'application du SMSI spécifié en 4.2.1.

Les Articles 5 à 15 de l'ISO/CEI 27001: 2005 fournissent des recommandations de mise en œuvre et des lignes directrices afférentes aux meilleures pratiques, venant à l'appui des mesures spécifiées aux paragraphes A.5 à A.15.

Tableau A.1 — Objectifs de sécurité et mesures de sécurité

A.5 Politique de sécurité		
A.5.1 Politique de sécurité de l'information *Objectif:* Apporter à la sécurité de l'information une orientation et un soutien de la part de la direction, conformément aux exigences métier et aux lois et règlements en vigueur.		
A.5.1.1	Document de politique de sécurité de l'information	*Mesure* Un document de politique de sécurité de l'information doit être approuvé par la direction, puis publié et diffusé auprès de l'ensemble des salariés et des tiers concernés.
A.5.1.2	Réexamen de la politique de sécurité de l'information	*Mesure* Pour garantir la pertinence, l'adéquation et l'efficacité de la politique de sécurité de l'information, la politique doit être réexaminée à intervalles fixés préalablement ou en cas de changements majeurs.
A.6 Organisation de la sécurité de l'information		
A.6.1 Organisation interne *Objectif:* Gérer la sécurité de l'information au sein de l'organisme.		
A.6.1.1	Implication de la direction vis-à-vis de la sécurité de l'information	*Mesure* La direction doit soutenir activement la politique de sécurité au sein de l'organisme au moyen de directives claires, d'un engagement démontré, d'attribution de fonctions explicites et d'une reconnaissance des responsabilités liées à la sécurité de l'information.
A.6.1.2	Coordination de la sécurité de l'information	*Mesure* Les activités relatives à la sécurité de l'information doivent être coordonnées par des intervenants ayant des fonctions et des rôles appropriés représentatifs des différentes parties de l'organisme.
A.6.1.3	Attribution des responsabilités en matière de sécurité de l'information	*Mesure* Toutes les responsabilités en matière de sécurité de l'information doivent être définies clairement.
A.6.1.4	Système d'autorisation concernant les moyens de traitement de l'information	*Mesure* Un système de gestion des autorisations doit être défini et mis en œuvre pour chaque nouveau moyen de traitement de l'information.

A.6.1.5	Engagements de confidentialité	*Mesure* Les exigences en matière d'engagements de confidentialité ou de non-divulgation, conformément aux besoins de l'organisme, doivent être identifiées et réexaminées régulièrement.
A.6.1.6	Relations avec les autorités	*Mesure* Des relations appropriées doivent être mises en place avec les autorités compétentes.
A.6.1.7	Relations avec des groupes de spécialistes	*Mesure* Des contacts appropriés doivent être entretenus avec des groupes de spécialistes, des forums spécialisés dans la sécurité et des associations professionnelles.
A.6.1.8	Réexamen indépendant de la sécurité de l'information	*Mesure* Des réexamens réguliers et indépendants de l'approche retenue par l'organisme pour gérer et mettre en œuvre sa sécurité (c'est-à-dire le suivi des objectifs de sécurité, les politiques, les procédures et les processus relatifs à la sécurité de l'information) doivent être effectués ; de tels réexamens sont également nécessaires lorsque des changements importants sont intervenus dans la mise en œuvre de la sécurité.
A.6.2 Tiers *Objectif:* Assurer la sécurité de l'information et des moyens de traitement de l'information appartenant à l'organisme et consultés, traités, communiqués ou gérés par des tiers.		
A.6.2.1	Identification des risques provenant des tiers	*Mesure* Les risques pesant sur l'information et les moyens de traitement de l'organisme qui découlent d'activités impliquant des tiers doivent être identifiés, et des mesures appropriées doivent être mises en œuvre avant d'accorder des accès.
A.6.2.2	La sécurité et les clients	*Mesure* Tous les besoins de sécurité doivent être traités avant d'accorder aux clients l'accès à l'information ou aux actifs de l'organisme.
A.6.2.3	La sécurité dans les accords conclus avec des tiers	*Mesure* Les accords conclus avec des tiers qui portent sur l'accès, le traitement, la communication ou la gestion de l'information, ou des moyens de traitement de l'information de l'organisme, ou qui portent sur l'ajout de produits ou de services aux moyens de traitement de l'information, doivent couvrir l'ensemble des exigences applicables en matière de sécurité.

A.7 Gestion des actifs		
A.7.1 Responsabilités relatives aux actifs *Objectif:* Mettre en place et maintenir une protection appropriée des actifs de l'organisme.		
A.7.1.1	Inventaire des actifs	*Mesure* Tous les actifs doivent être clairement identifiés et un inventaire de tous les actifs importants doit être réalisé et géré.
A.7.1.2	Propriété des actifs	*Mesure* La propriété de chaque information et des moyens de traitement de l'information doit être 'attribuée[3)]' à une partie définie de l'organisme.
A.7.1.3	Utilisation correcte des actifs	*Mesure* Des règles permettant l'utilisation correcte de l'information et des actifs associés aux moyens de traitement de l'information doivent être identifiées, documentées et mises en œuvre.
A.7.2 Classification des informations *Objectif:* Garantir un niveau de protection approprié aux informations.		
A.7.2.1	Lignes directrices pour la classification	*Mesure* Les informations doivent être classées en termes de valeur, d'exigences légales, de sensibilité et de criticité.
A.7.2.2	Marquage et manipulation de l'information	*Mesure* Un ensemble approprié de procédures pour le marquage et la manipulation de l'information doit être élaboré et mis en œuvre conformément au plan de classification adopté par l'organisme.

3) Explication: Le terme "propriétaire" identifie une personne ou une entité ayant accepté la responsabilité du contrôle de la production, de la mise au point, de la maintenance, de l'utilisation et de la protection des actifs. Ce terme ne signifie pas que la personne jouit à proprement parler de droits de propriété sur l'actif.

A.8 Sécurité liée aux ressources humaines		
A.8.1 Avant le recrutement[4)] *Objectif:* Garantir que les salariés, contractants et utilisateurs tiers connaissent leurs responsabilités et qu'ils conviennent pour les fonctions qui leur sont attribuées et réduire le risque de vol, de fraude ou de mauvais usage des équipements.		
A.8.1.1	Rôles et responsabilités	*Mesure* Les rôles et responsabilités en matière de sécurité des salariés, contractants et utilisateurs tiers doivent être définis et documentés conformément à la politique de sécurité de l'information de l'organisme.
A.8.1.2	Sélection	*Mesure* Qu'il s'agisse de postulants, de contractants ou d'utilisateurs tiers, les vérifications des informations concernant tous les candidats doivent être réalisées conformément aux lois, aux règlements et à l'étique et doivent être proportionnelles aux exigences métier, à la classification des informations accessibles et aux risques identifiés.
A.8.1.3	Conditions d'embauche	*Mesure* Dans le cadre de leurs obligations contractuelles, les salariés, contractants et utilisateurs tiers doivent se mettre d'accord sur les modalités du contrat d'embauche les liant et le signer. Ce contrat doit définir leurs responsabilités et celles de l'organisme quant à la sécurité de l'information.
A.8.2 Pendant la durée du contrat *Objectif:* Veiller à ce que tous les salariés, contractants et utilisateurs tiers soient conscients des menaces pesant sur la sécurité de l'information, de leurs responsabilités financières ou autres, et disposent des éléments requis pour prendre en charge la politique de sécurité de l'organisme dans le cadre de leur activité normale et réduire le risque d'erreur humaine.		
A.8.2.1	Responsabilités de la direction	*Mesure* La direction doit demander aux salariés, contractants et utilisateurs tiers d'appliquer les règles de sécurité conformément aux politiques et procédures établies de l'organisme.
A.8.2.2	Sensibilisation, qualification et formations en matière de sécurité de l'information	*Mesure* L'ensemble des salariés d'un organisme et, le cas échant, les contractants et utilisateurs tiers doivent suivre une formation adaptée sur la sensibilisation et doivent recevoir régulièrement les mises à jour des politiques et procédures de l'organisme, pertinentes pour leurs fonctions.
A.8.2.3	Processus disciplinaire	*Mesure* Un processus disciplinaire formel doit être élaboré pour les salariés ayant enfreint les règles de sécurité.

4) Explication: Le terme "recrutement" défini ici couvre toutes les différentes situations suivantes: recrutement de personnes (durée provisoire ou plus longue durée), affectation de domaines d'activité, modification de domaines d'activité, cession de contrats et résiliation de l'un de ces contrats.

A.8.3 Fin ou modification du contrat		
Objectif: Veiller à ce que les salariés, contractants et utilisateurs tiers quittent un organisme ou changent de poste selon une procédure définie.		
A.8.3.1	Responsabilités en fin de contrat	*Mesure* Les responsabilités relatives aux fins ou aux modifications de contrats doivent être clairement définies et attribuées.
A.8.3.2	Restitution des actifs	*Mesure* Tous les salariés, contractants et utilisateurs tiers doivent restituer la totalité des actifs de l'organisme qu'ils ont en leur possession à la fin de leur période d'emploi, contrat ou accord.
A.8.3.3	Retrait des droits d'accès	*Mesure* Les droits d'accès de l'ensemble des salariés, contractants et utilisateurs tiers à l'information et aux moyens de traitement de l'information doivent être supprimés à la fin de leur période d'emploi, ou modifiés en cas de modification du contrat ou de l'accord.
A.9 Sécurité physique et environnementale		
A.9.1 Zones sécurisées		
Objectif: Empêcher tout accès physique non autorisé, tout dommage ou intrusion dans les locaux ou portant sur les informations de l'organisme.		
A.9.1.1	Périmètre de sécurité physique	*Mesure* Les zones contenant des informations et des moyens de traitement de l'information doivent être protégées par des périmètres de sécurité (obstacles tels que des murs, des portes avec un contrôle d'accès par cartes, ou des bureaux de réception avec personnel d'accueil).
A.9.1.2	Contrôles physiques des accès	*Mesure* Les zones sécurisées doivent être protégées par des contrôles à l'entrée adéquats pour s'assurer que seul le personnel habilité est admis.
A.9.1.3	Sécurisation des bureaux, des salles et des équipements	*Mesure* Des mesures de sécurité physique doivent être conçues et appliquées pour les bureaux, les salles et les équipements.
A.9.1.4	Protection contre les menaces extérieures et environnementales	*Mesure* Des mesures de protection physique contre les dommages causés par les incendies, les inondations, les tremblements de terre, les explosions, les troubles civils et autres formes de catastrophes naturelles ou de sinistres provoqués par l'homme, doivent être conçues et appliquées.
A.9.1.5	Travail dans les zones sécurisées	*Mesure* Des mesures de protection physique et des directives pour le travail en zone sécurisée doivent être conçues et appliquées.
A.9.1.6	Zones d'accès public, de livraison et de chargement	*Mesure* Les points d'accès tels que les zones de livraison/chargement et les autres points par lesquels des personnes non habilitées peuvent pénétrer dans les locaux doivent être contrôlés. Les points d'accès doivent également, si possible, être isolés des moyens de traitement de l'information, de façon à éviter les accès non autorisés.

A.9.2 Sécurité du matériel		
Objectif: Empêcher la perte, l'endommagement, le vol ou la compromission des actifs et l'interruption des activités de l'organisme.		
A.9.2.1	Choix de l'emplacement et protection du matériel	*Mesure* Le matériel doit être situé et protégé de manière à réduire les risques de menaces et de dangers environnementaux et les possibilités d'accès non autorisé.
A.9.2.2	Services généraux	*Mesure* Le matériel doit être protégé des coupures de courant et autres perturbations dues à une défaillance des services généraux.
A.9.2.3	Sécurité du câblage	*Mesure* Les câbles électriques ou de télécommunications transportant des données doivent être protégés contre toute interception d'information ou dommage.
A.9.2.4	Maintenance du matériel	*Mesure* Le matériel doit être entretenu correctement pour garantir sa disponibilité permanente et son intégrité.
A.9.2.5	Sécurité du matériel hors des locaux	*Mesure* La sécurité doit être appliquée au matériel utilisé hors des locaux de l'organisme en tenant compte des différents risques associés au travail hors site.
A.9.2.6	Mise au rebut ou recyclage sécurisé(e) du matériel	*Mesure* Tout le matériel contenant des supports de stockage doit être vérifié pour s'assurer que toute donnée sensible a bien été supprimée et que tout logiciel sous licence a bien été désinstallé ou écrasé de façon sécurisée, avant sa mise au rebut.
A.9.2.7	Sortie d'un actif	*Mesure* Un matériel, des informations ou des logiciels ne doivent pas être sortis des locaux de l'organisme sans autorisation préalable.
A.10 Gestion de l'exploitation et des télécommunications		
A.10.1 Procédures et responsabilités liées à l'exploitation		
Objectif: Assurer l'exploitation correcte et sécurisée des moyens de traitement de l'information.		
A.10.1.1	Procédures d'exploitation documentées	*Mesure* Les procédures d'exploitation doivent être documentées, tenues à jour et disponibles pour tous les utilisateurs concernés.
A.10.1.2	Management des modifications	*Mesure* Les changements apportés aux systèmes et moyens de traitement de l'information doivent être contrôlés.
A.10.1.3	Séparation des tâches	*Mesure* Les tâches et les domaines de responsabilité doivent être séparés pour réduire les occasions de modification ou de mauvais usage non autorisé(e) ou involontaire des actifs de l'organisme.
A.10.1.4	Séparation des équipements de développement, d'essai et d'exploitation	*Mesure* Les équipements de développement, d'essai et d'exploitation doivent être séparés pour réduire les risques d'accès ou de changements non autorisés dans le système d'information en exploitation.

A.10.2 Gestion de la prestation de service conclus avec un tiers		
Objectif: Mettre en œuvre et maintenir un niveau de sécurité de l'information et de service adéquat et conforme aux accords de prestation de service conclus avec un tiers.		
A.10.2.1	Prestation de service	*Mesure* Il doit être assuré que les mesures de sécurité, les définitions du service et les niveaux de prestation prévus dans l'accord de prestation de service tiers sont mis en œuvre, appliqués et tenus à jour par le tiers.
A.10.2.2	Surveillance et examen des services tiers	*Mesure* Les services, rapports et enregistrements fournis par les tiers doivent être régulièrement contrôlés et réexaminés, et des audits doivent être régulièrement réalisés.
A.10.2.3	Gestion des modifications dans les services tiers	*Mesure* Les changements effectués dans la prestation de service, comprenant le maintien et l'amélioration des politiques, procédures et mesures existant en matière de sécurité de l'information, doivent être gérés en tenant compte de la criticité des systèmes et processus de gestion concernés et de la réévaluation du risque.
A.10.3 Planification et acceptation du système		
Objectif: Réduire le plus possible le risque de pannes du système.		
A.10.3.1	Dimensionnement	*Mesure* L'utilisation des ressources doit être surveillée et ajustée au plus près, et des projections doivent être faites sur les dimensionnements futurs pour assurer les performances requises par le système.
A.10.3.2	Acceptation du système	*Mesure* Les critères d'acceptation doivent être fixés pour les nouveaux systèmes d'information, les nouvelles versions et les mises à niveau, et les tests adaptés du (des) système(s) doivent être réalisés au moment du développement et préalablement à leur acceptation.
A.10.4 Protection contre les codes malveillant et mobile		
Objectif: Protéger l'intégrité des logiciels et de l'information.		
A.10.4.1	Mesures contre les codes malveillants	*Mesure* Des mesures de détection, de prévention et de recouvrement pour se protéger des codes malveillants ainsi que des procédures appropriées de sensibilisation des utilisateurs doivent être mises en œuvre.
A.10.4.2	Mesures contre le code mobile	*Mesure* Lorsque l'utilisation de code mobile est autorisée, la configuration doit garantir que le code mobile fonctionne selon une politique de sécurité clairement définie et tout code mobile non autorisé doit être bloqué.
A.10.5 Sauvegarde		
Objectif: Maintenir l'intégrité et la disponibilité des informations et des moyens de traitement de l'information.		
A.10.5.1	Sauvegarde des informations	*Mesure* Des copies de sauvegarde des informations et logiciels doivent être réalisées et soumises régulièrement à essai conformément à la politique de sauvegarde convenue.

A.10.6 Gestion de la sécurité des réseaux *Objectif:* Assurer la protection des informations sur les réseaux et la protection de l'infrastructure sur laquelle elles s'appuient.		
A.10.6.1	Mesures sur les réseaux	*Mesure* Les réseaux doivent être gérés et contrôlés de manière adéquate pour qu'ils soient protégés des menaces et pour maintenir la sécurité des systèmes et des applications utilisant le réseau, notamment les informations en transit.
A.10.6.2	Sécurité des services réseau	*Mesure* Pour tous les services réseau, les fonctions réseau, les niveaux de service et les exigences de gestion doivent être identifiés et intégrés dans tout accord sur les services réseau, qu'ils soient fournis en interne ou en externe.
A.10.7 Manipulation des supports *Objectif:* Empêcher la divulgation, la modification, le retrait ou la destruction non autorisé(e) d'actifs et l'interruption des activités de l'organisme.		
A.10.7.1	Gestion des supports amovibles	*Mesure* Des procédures doivent être mises en place pour la gestion des supports amovibles.
A.10.7.2	Mise au rebut des supports	*Mesure* Les supports qui ne servent plus doivent être mis au rebut de façon sûre, en suivant des procédures formelles.
A.10.7.3	Procédures de manipulation des informations	*Mesure* Des procédures de manipulation et de stockage des informations doivent être établies pour protéger ces informations d'une divulgation non autorisée ou d'un mauvais usage.
A.10.7.4	Sécurité de la documentation système	*Mesure* La documentation système doit être protégée contre les accès non autorisés.

A.10.8 Echange des informations		
Objectif: Maintenir la sécurité des informations et des logiciels échangés au sein de l'organisme et avec une entité extérieure.		
A.10.8.1	Politiques et procédures d'échange des informations	*Mesure* Des politiques, procédures et mesures d'échange formelles doivent être mises en place pour protéger les échanges d'informations liées à tous types d'équipements de télécommunication.
A.10.8.2	Accords d'échange	*Mesure* Des accords doivent être conclus pour l'échange d'informations et de logiciels entre l'organisme et la partie externe.
A.10.8.3	Supports physiques en transit	*Mesure* Les supports contenant des informations doivent être protégés contre les accès non autorisés, le mauvais usage ou l'altération lors du transport hors des limites physiques de l'organisme.
A.10.8.4	Messagerie électronique	*Mesure* Les informations liées à la messagerie électronique doivent être protégées de manière adéquate.
A.10.8.5	Systèmes d'information d'entreprise	*Mesure* Des politiques et procédures doivent être élaborées et mises en œuvre pour protéger l'information liée à l'interconnexion de systèmes d'informations d'entreprise.
A.10.9 Services de commerce électronique		
Objectif: Assurer la sécurité des services de commerce électronique, ainsi que leur utilisation sécurisée.		
A.10.9.1	Commerce électronique	*Mesure* Les informations liées au commerce électronique transmises sur les réseaux publics doivent être protégées contre les activités frauduleuses, les litiges sur les contrats et la divulgation et la modification non autorisées.
A.10.9.2	Transactions en ligne	*Mesure* Les informations liées aux transactions en ligne doivent être protégées pour empêcher la transmission incomplète, les erreurs d'acheminement, la modification non autorisée, la divulgation non autorisée, la duplication non autorisée du message ou la réémission.
A.10.9.3	Informations à disposition du public	*Mesure* L'intégrité des informations mises à disposition sur un système accessible au public doit être protégée pour empêcher toute modification non autorisée.
A.10.10 Surveillance		
Objectif: Détecter les traitements non autorisés de l'information.		
A.10.10.1	Journaux d'audit	*Mesure* Les journaux d'audit, qui enregistrent les activités des utilisateurs, les exceptions et les événements liés à la sécurité doivent être produits et conservés pendant une période préalablement définie afin de faciliter les investigations ultérieures et la surveillance du contrôle d'accès.
A.10.10.2	Surveillance de l'exploitation du système	*Mesure* Des procédures permettant de surveiller l'utilisation des moyens de traitement de l'information doivent être établies et les résultats des activités de surveillance doivent être réexaminés périodiquement.

A.10.10.3	Protection des informations journalisées	*Mesure* Les équipements de journalisation et les informations journalisées doivent être protégés contre le sabotage et les accès non autorisés.
A.10.10.4	Journal administrateur et journal des opérations	*Mesure* Les activités de l'administrateur système et de l'opérateur système doivent être journalisées.
A.10.10.5	Rapports d'anomalies	*Mesure* Les éventuels défauts doivent être journalisés et analysés et les mesures appropriées doivent être prises.
A.10.10.6	Synchronisation des horloges	*Mesure* Les horloges des différents systèmes de traitement de l'information d'un organisme ou d'un domaine de sécurité doivent être synchronisées à l'aide d'une source de temps précise et préalablement définie.
A.11 Contrôle d'accès		
A.11.1 Exigences métier relatives au contrôle d'accès *Objectif:* Maîtriser l'accès à l'information.		
A.11.1.1	Politique de contrôle d'accès	*Mesure* Une politique de contrôle d'accès doit être établie, documentée et réexaminée sur la base des exigences métier et de sécurité.
A.11.2 Gestion des accès des utilisateurs *Objectif:* Contrôler l'accès des utilisateurs autorisés et empêcher les accès non autorisés aux systèmes d'information.		
A.11.2.1	Enregistrement des utilisateurs	*Mesure* Une procédure formelle d'inscription et désinscription des utilisateurs destinée à accorder et à supprimer l'accès à tous les systèmes et services d'information doit être définie.
A.11.2.2	Gestion des privilèges	*Mesure* L'attribution et l'utilisation des privilèges doivent être restreintes et contrôlées.
A.11.2.3	Gestion du mot de passe utilisateur	*Mesure* L'attribution de mots de passe doit être réalisée dans le cadre d'un processus formel.
A.11.2.4	Réexamen des droits d'accès utilisateurs	*Mesure* La direction doit réexaminer les droits d'accès utilisateurs à intervalles réguliers par le biais d'un processus formel.

A.11.3 Responsabilités de l'utilisateur		
Objectif: Empêcher l'accès d'utilisateurs non habilités et la compromission ou le vol d'informations et de moyens de traitement de l'information.		
A.11.3.1	Utilisation du mot de passe	*Mesure* Il doit être demandé aux utilisateurs de respecter les bonnes pratiques de sécurité lors de la sélection et de l'utilisation de mots de passe.
A.11.3.2	Matériel utilisateur laissé sans surveillance	*Mesure* Les utilisateurs doivent s'assurer que tout matériel laissé sans surveillance est doté d'une protection appropriée.
A.11.3.3	Politique du bureau propre et de l'écran vide	*Mesure* Une politique du bureau propre doit être adoptée pour les documents papier et les supports de stockage amovibles, et une politique de l'écran vide doit également être adoptée pour les moyens de traitement de l'information.
A.11.4 Contrôle d'accès réseau		
Objectif: Empêcher les accès non autorisés aux services disponibles sur le réseau.		
A.11.4.1	Politique relative à l'utilisation des services en réseau	*Mesure* Les utilisateurs doivent avoir uniquement accès aux services pour lesquels ils ont spécifiquement reçu une autorisation.
A.11.4.2	Authentification de l'utilisateur pour les connexions externes	*Mesure* Des méthodes d'authentification appropriées doivent être utilisées pour contrôler l'accès des utilisateurs distants.
A.11.4.3	Identification des matériels en réseaux	*Mesure* L'identification automatique de matériels doit être considérée comme un moyen d'authentification des connexions à partir de lieux et matériels spécifiques.
A.11.4.4	Protection des ports de diagnostic et de configuration à distance	*Mesure* L'accès physique et logique aux ports de diagnostic et de configuration à distance doit être contrôlé.
A.11.4.5	Cloisonnement des réseaux	*Mesure* Les groupes de services d'information, d'utilisateurs et de systèmes d'information doivent être séparés sur le réseau.
A.11.4.6	Mesure relative à la connexion réseau	*Mesure* Pour les réseaux partagés, en particulier les réseaux qui s'étendent au-delà des limites de l'organisme, la capacité de connexion réseau des utilisateurs doit être restreinte, conformément à la politique de contrôle d'accès et aux exigences relatives aux applications métier (voir 11.1)
A.11.4.7	Contrôle du routage réseau	*Mesure* Des mesures du routage des réseaux doivent être mises en œuvre afin d'éviter que les connexions réseau et les flux d'informations ne portent atteinte à la politique de contrôle d'accès des applications métier.

A.11.5 Contrôle d'accès au système d'exploitation		
Objectif: Empêcher les accès non autorisés aux systèmes d'exploitation.		
A.11.5.1	Ouverture de sessions sécurisées	*Mesure* L'accès aux systèmes d'exploitation doit être soumis à une procédure sécurisée d'ouverture de session.
A.11.5.2	Identification et authentification de l'utilisateur	*Mesure* Un identifiant unique et exclusif doit être attribué à chaque utilisateur et une technique d'authentification doit être choisie, permettant de vérifier l'identité déclarée par l'utilisateur.
A.11.5.3	Système de gestion des mots de passe	*Mesure* Les systèmes qui gèrent les mots de passe doivent être interactifs et doivent fournir des mots de passe de qualité.
A.11.5.4	Emploi des utilitaires système	*Mesure* L'emploi des programmes utilitaires permettant de contourner les mesures d'un système ou d'une application doit être limité et contrôlé étroitement.
A.11.5.5	Déconnexion automatique des sessions inactives	*Mesure* Les sessions inactives doivent être déconnectées après une période d'inactivité définie.
A.11.5.6	Limitation du temps de connexion	*Mesure* Les temps de connexion doivent être restreints afin d'apporter un niveau de sécurité supplémentaire aux applications à haut risque.
A.11.6 Contrôle d'accès aux applications et à l'information		
Objectif: Empêcher les accès non autorisés aux informations stockées dans les applications.		
A.11.6.1	Restriction d'accès à l'information	*Mesure* Pour les utilisateurs et le personnel chargé de l'assistance technique, l'accès aux informations et aux fonctions applicatives doit être restreint conformément à la politique de contrôle d'accès.
A.11.6.2	Isolement des systèmes sensibles	*Mesure* Les systèmes sensibles doivent disposer d'un environnement informatique dédié (isolé).
A.11.7 Informatique mobile et télétravail		
Objectif: Garantir la sécurité de l'information lors de l'utilisation d'appareils informatiques mobiles et d'équipements de télétravail.		
A.11.7.1	Informatique et communications mobiles	*Mesure* Une procédure formelle et des mesures de sécurité appropriées doivent être mises en place pour assurer une protection contre le risque lié à l'utilisation d'appareils informatiques et de communication mobiles.
A.11.7.2	Télétravail	*Mesure* Une politique, des procédures et des programmes opérationnels spécifiques au télétravail doivent être élaborés et mis en œuvre.

A.12 Acquisition, développement et maintenance des systèmes d'information		
A.12.1 Exigences de sécurité applicables aux systèmes d'information *Objectif:* Veiller à ce que la sécurité fasse partie intégrante des systèmes d'information.		
A.12.1.1	Analyse et spécification des exigences de sécurité	*Mesure* Les exigences métier relatives aux nouveaux systèmes d'information ou les améliorations apportées aux systèmes d'information existants doivent spécifier les exigences de sécurité.
A.12.2 Bon fonctionnement des applications *Objectif:* Empêcher toute erreur, perte, modification non autorisée ou tout mauvais usage des informations dans les applications.		
A.12.2.1	Validation des données en entrée	*Mesure* Les données entrées dans les applications doivent être validées afin de vérifier si elles sont correctes et appropriées.
A.12.2.2	Mesure relative au traitement interne	*Mesure* Des contrôles de validation doivent être inclus dans les applications afin de détecter les éventuelles altérations de l'information dues à des erreurs de traitement ou des actes délibérés.
A.12.2.3	Intégrité des messages	*Mesure* Les exigences permettant d'assurer l'authentification et la protection de l'intégrité des messages dans les applications doivent être identifiées, et des mesures appropriées doivent être identifiées et mises en œuvre.
A.12.2.4	Validation des données en sortie	*Mesure* Les données de sortie d'une application doivent être validées pour assurer que le traitement des informations stockées est correct et adapté aux circonstances.
A.12.3 Mesures cryptographiques *Objectif:* Protéger la confidentialité, l'authenticité ou l'intégrité de l'information par des moyens cryptographiques.		
A.12.3.1	Politique d'utilisation des mesures cryptographiques	*Mesure* Une politique d'utilisation des mesures cryptographiques en vue de protéger l'information doit être élaborée et mise en œuvre.
A.12.3.2	Gestion des clés	*Mesure* Une procédure de gestion des clés doit favoriser l'utilisation par l'organisme de techniques cryptographiques.
A.12.4 Sécurité des fichiers système *Objectif:* Garantir la sécurité des fichiers système.		
A.12.4.1	Mesure relative aux logiciels en exploitation	*Mesure* Des procédures doivent être mises en place pour contrôler l'installation du logiciel sur les systèmes en exploitation.
A.12.4.2	Protection des données système d'essai	*Mesure* Les données d'essai doivent être sélectionnées avec soin, protégées et contrôlées.
A.12.4.3	Contrôle d'accès au code source du programme	*Mesure* L'accès au code source du programme doit être restreint.

A.12.5 Sécurité en matière de développement et d'assistance technique		
Objectif: Garantir la sécurité du logiciel et des informations d'application.		
A.12.5.1	Procédures de contrôle des modifications	*Mesure* La mise en œuvre des modifications doit être contrôlée par le biais de procédures formelles.
A.12.5.2	Réexamen technique des applications après modification du système d'exploitation	*Mesure* Lorsque des modifications sont apportées aux systèmes d'exploitation, les applications critiques métier doivent être réexaminées et testées afin de vérifier l'absence de tout effet indésirable sur l'activité ou sur la sécurité.
A.12.5.3	Restrictions relatives à la modification des progiciels	*Mesure* La modification des progiciels ne doit pas être encouragée, et doit être limitée aux changements nécessaires. Un contrôle strict doit également être exercé sur ces modifications.
A.12.5.4	Fuite d'informations	*Mesure* Toute possibilité de fuite d'informations doit être empêchée.
A.12.5.5	Externalisation du développement logiciel	*Mesure* Le développement logiciel externalisé doit être encadré et contrôlé par l'organisme.
A.12.6 Gestion des vulnérabilités techniques		
Objectif: Réduire les risques liés à l'exploitation des vulnérabilités techniques ayant fait l'objet d'une publication.		
A.12.6.1	Mesure relative aux vulnérabilités techniques	*Mesure* Toute information concernant toute vulnérabilité technique des systèmes d'information en exploitation doit être obtenue à temps, l'exposition de l'organisme aux dites vulnérabilités doit être évaluée et les actions appropriées doivent être entreprises pour traiter le risque associé.
A.13 Gestion des incidents liés à la sécurité de l'information		
A.13.1 Remontée des événements et des failles liés à la sécurité de l'information		
Objectif: Garantir que le mode de notification des événements et failles liés à la sécurité de l'information permet la mise en œuvre d'une action corrective, dans les meilleurs délais.		
A.13.1.1	Remontée des événements liés à la sécurité de l'information	*Mesure* Les événements liés à la sécurité de l'information doivent être signalés, dans les meilleurs délais, par les voies hiérarchiques appropriées.
A.13.1.2	Remontée des failles de sécurité	*Mesure* Il doit être demandé à tous les salariés, contractants et utilisateurs tiers des systèmes et services d'information de noter et de signaler toute faille de sécurité observée ou soupçonnée dans les systèmes ou services.

A.13.2 Gestion des incidents liés à la sécurité de l'information et des améliorations		
Objectif: Garantir la mise en place d'une approche cohérente et efficace pour la gestion des incidents liés à la sécurité de l'information.		
A.13.2.1	Responsabilités et procédures	*Mesure* Des responsabilités et des procédures doivent être établies, permettant de garantir une réponse rapide, efficace et pertinente en cas d'incident lié à la sécurité de l'information.
A.13.2.2	Exploitation des incidents liés à la sécurité de l'information déjà survenus	*Mesure* Des mécanismes doivent être mis en place, permettant de quantifier et surveiller les différents types d'incidents liés à la sécurité de l'information ainsi que leur volume et les coûts associés.
A.13.2.3	Collecte de preuves	*Mesure* Lorsqu'une action en justice civile ou pénale est engagée contre une personne physique ou un organisme, à la suite d'un incident lié à la sécurité de l'information, les éléments de preuve doivent être recueillis, conservés et présentés conformément aux dispositions légales relatives à la présentation de preuves régissant la ou les juridiction(s) compétente(s).
A.14 Gestion de la continuité de l'activité		
A.14.1 Gestion de la continuité de l'activité d'un point de vue aspects de la sécurité de l'information		
Objectif: Empêcher les interruptions des activités de l'organisme, protéger les processus métier cruciaux des effets causés par les défaillances majeures des systèmes d'information ou par des sinistres et garantir une reprise de ces processus dans les meilleurs délais.		
A.14.1.1	Intégration de la sécurité de l'information dans le processus de gestion du plan de continuité de l'activité	*Mesure* Un processus de continuité de l'activité dans l'ensemble de l'organisme doit être élaboré et géré, qui satisfait aux exigences en matière de sécurité de l'information requises pour la continuité de l'activité de l'organisme.
A.14.1.2	Continuité de l'activité et appréciation du risque	*Mesure* Les événements pouvant être à l'origine d'interruptions des processus métier doivent être identifiés, tout comme la probabilité et l'impact de telles interruptions et leurs conséquences pour la sécurité de l'information.
A.14.1.3	Élaboration et mise en œuvre des plans de continuité intégrant la sécurité de l'information	*Mesure* Des plans doivent être élaborés et mis en œuvre pour maintenir ou restaurer l'exploitation et assurer la disponibilité des informations au niveau et dans les délais requis suite à une interruption ou une panne affectant les processus métier cruciaux.
A.14.1.4	Cadre de la planification de la continuité de l'activité	*Mesure* Un cadre unique pour les plans de continuité de l'activité doit être géré afin de garantir la cohérence de l'ensemble des plans, de satisfaire de manière constante aux exigences en matière de sécurité de l'information et d'identifier les priorités en matière de mise à l'essai et de maintenance.
A.14.1.5	Mise à l'essai, gestion et réévaluation constante des plans de continuité de l'activité	*Mesure* Les plans de continuité de l'activité doivent être testés et mis à jour régulièrement afin de s'assurer qu'ils sont actualisés et efficaces.

A.15 Conformité		
A.15.1 Conformité aux exigences légales		
Objectif: Eviter toute violation des obligations légales, statutaires, réglementaires ou contractuelles et des exigences de sécurité.		
A.15.1.1	Identification de la législation en vigueur	*Mesure* Pour chaque système d'information et pour l'organisme, toutes les exigences légales, réglementaires et contractuelles en vigueur doivent être définies, documentées et mises à jour, ainsi que la procédure utilisée par l'organisme pour satisfaire à ces exigences.
A.15.1.2	Droits de propriété intellectuelle (DPI)	*Mesure* Des procédures appropriées doivent être mises en œuvre, visant à garantir la conformité avec les exigences légales, réglementaires et contractuelles concernant l'utilisation du matériel pouvant être soumis à des droits de propriété intellectuelle et l'utilisation des logiciels propriétaires.
A.15.1.3	Protection des enregistrements de l'organisme	*Mesure* Les enregistrements importants doivent être protégés contre la perte, destruction et falsification conformément aux exigences légales, réglementaires et aux exigences métier.
A.15.1.4	Protection des données et confidentialité des informations relatives à la vie privée	*Mesure* La protection et la confidentialité des données doivent être garanties, telles que l'exigent la législation ou les réglementations applicables, et les clauses contractuelles le cas échéant.
A.15.1.5	Mesure préventive à l'égard du mauvais usage des moyens de traitement de l'information	*Mesure* Les utilisateurs doivent être dissuadés de toute utilisation de moyens de traitement de l'information à des fins illégales.
A.15.1.6	Réglementation relative aux mesures cryptographiques	*Mesure* Des mesures cryptographiques doivent être prises conformément aux accords, lois et réglementations applicables.
A.15.2 Conformité avec les politiques et normes de sécurité et conformité technique		
Objectif: S'assurer de la conformité des systèmes avec les politiques et normes de sécurité de l'organisme.		
A.15.2.1	Conformité avec les politiques et les normes de sécurité	*Mesure* Les responsables doivent s'assurer de l'exécution correcte de l'ensemble des procédures de sécurité placées sous leur responsabilité en vue de garantir leur conformité avec les politiques et normes de sécurité.
A.15.2.2	Vérification de la conformité technique	*Mesure* La conformité des systèmes d'information avec les normes relatives à la mise en œuvre de la sécurité doit être vérifiée régulièrement.

A.15.3 Prises en compte de l'audit du système d'information *Objectif:* Optimiser l'efficacité et réduire le plus possible l'interférence avec le/du processus d'audit du système d'information.		
A.15.3.1	Contrôles de l'audit du système d'information	*Mesure* Les exigences d'audit et les activités impliquant des contrôles des systèmes en exploitation doivent être planifiées de manière précise et doivent être le résultat d'un accord afin de réduire le plus possible le risque de perturbations des processus métier.
A.15.3.2	Protection des outils d'audit du système d'information	*Mesure* L'accès aux outils d'audit du système d'information doit être protégé afin d'empêcher tous mauvais usage ou compromission éventuels.