DNSSI,

Conformité avec le Décret 02-15-712

Apport de la Norme internationale ISO 27001

Livre blanc par ARROUBAT Yahya

AUSIM
beyond digital

Préface

Dans un monde en course folle vers le tout connecté, tout numérisé, etc., la cybercriminalité est désormais un fléau mondialisé. Seulement, le commun des mortels a tendance à oublier que l'erreur est et restera humaine. Les cas d'atteinte à la sécurité de l'information et ce de façon délibérée ou par méconnaissance sont du fait de l'Homme.

Protéger l'information est une responsabilité collective*. Dans un monde interconnecté, les systèmes d'information méritent d'être protégés contre les divers risques encourus.*

Le présent document a pour objectif d'éclairer les acteurs de la sécurité des systèmes d'information qu'au-delà de l'aspect réglementaire, le Décret 02-05-712 et la DNSSI constituent une opportunité à saisir afin d'établir une véritable gestion de la sécurité de l'information, basée sur des Normes internationales. D'autant plus qu'« …*Amener les administrations, les organismes publics et les infrastructures d'importance vitale à se faire auditer en vue d'être certifiés ISO 27001 ou équivalent...* »[1]. Ne peut être que valorisant pour notre pays[2].

Je tiens à adresser au nom de toutes les composantes de l'AUSIM, mes remerciements à M. Yahya ARROUBAT, Responsable de la Sécurité des Systèmes d'Information à la Bourse de Casablanca pour l'effort et l'excellent travail fait pour la production de ce livre blanc.

Je souhaite aux lecteurs de ce livre blanc une bonne lecture et surtout une bonne utilisation.

Mohamed SAAD
CIO Bourse de Casablanca
Président AUSIM

[1] Source : STRATEGIE NATIONALE EN MATIERE DE CYBERSECURITE, page 13
[2] Voir annexe : Palmarès des certifications ISO/IEC 27001 par pays en Afrique

Sommaire

Remerciements

Je tiens à remercier l'Association des Utilisateurs des Systèmes Informations au Maroc (AUSIM[3]) ainsi que son président en exercice M. Mohamed SAAD pour m'avoir donné l'occasion de partager cette modeste contribution, que j'espère utile pour la communauté des utilisateurs des systèmes d'information au Maroc.

L'AUSIM est une association à but non lucratif créée en avril 1993.

Comptant parmi ses adhérents nombre de structures de premier plan aux niveaux organisationnel et managérial (Offices, Banques, Assurances, Entreprises Industrielles, …), l'AUSIM œuvre activement dans l'esprit de développer et de vulgariser l'usage des Technologies de l'Information au Maroc.

A ce titre, elle a pour objectifs :

- L'échange d'expériences et d'informations d'ordre technique, scientifique et culturel entre les adhérents et ce par organisation de rencontres, séminaires et conférences, aussi bien au Maroc qu'à l'étranger.
- L'étude et la sauvegarde, en cas de besoin, des intérêts généraux, à 'caractères techniques, économiques et financiers de ses adhérents.
- La création et entretien des rapports de bonne fraternité entre ses membres et le renforcement des liens avec d'autres associations similaires au Maroc et à l'étranger.
- L'entraide mutuelle au niveau des exploitations des systèmes des logiciels.
- La diffusion des connaissances et d'informations relatives au secteur de l'informatique.
- La participation active aux principales réformes nationales et sectorielles ayant trait aux Technologies de l'Information.

[3] http://www.ausimaroc.com/association/

I. Introduction

Dans un monde en course folle vers le tout connecté, tout numérisé, etc., la cybercriminalité est désormais un fléau mondialisé. Seulement, le commun des mortels a tendance à oublier que l'erreur est et restera humaine. Les cas d'atteinte à la sécurité de l'information et ce de façon délibérée ou par méconnaissance sont du fait de l'Homme.

Protéger l'information n'est pas du ressort que des spécialistes en systèmes d'information, mais c'est une responsabilité collective car « *La valeur de l'information dépasse les mots, les chiffres et les images : la connaissance, les concepts, les idées et les marques sont des exemples de formes d'information immatérielles. Dans un monde interconnecté, l'information et les processus, systèmes et réseaux qui s'y rattachent, ainsi que le personnel impliqué dans son traitement, ses manipulations et sa protection, sont des actifs précieux pour l'activité d'une organisation, au même titre que d'autres actifs d'entreprise importants, et, par conséquent, ils méritent ou nécessitent d'être protégés contre les divers risques encourus.* ». [Extraite de la Norme internationale ISO 27002].

Le présent document a pour objectif d'éclairer les acteurs de la sécurité des systèmes d'information qu'au-delà de l'aspect réglementaire, le Décret 02-05-712 et la DNSSI constituent une opportunité à saisir afin d'établir une véritable gestion de la sécurité de l'information, basée sur des Normes internationales. D'autant plus qu'« …*Amener les administrations, les organismes publics et les infrastructures d'importance vitale à se faire auditer en vue d'être certifiés ISO 27001 ou équivalent...* »[4]. Ne peut être que valorisant pour notre pays[5].

Les termes et abréviations cités dans ce chapitre sont expliqués dans les annexes « Termes et définitions » et « Abréviations ».

[4] Source : STRATEGIE NATIONALE EN MATIERE DE CYBERSECURITE, page 13
[5] Voir annexe : Palmarès des certifications ISO/IEC 27001 par pays en Afrique

II. Quelques concepts

Le présent document cite des concepts en relation avec le management de la sécurité de l'information. Cette section en détaille les plus pertinents.

1. Approche par les risques

Exprimé sous différentes appellations, le management par les risques est à juste titre un des facteurs clé pour la gestion de la sécurité :

L'article 4 du Décret 02-05-712, exige que :

« …Chaque entité établit, sur la base des résultats d'une analyse des risques, un répertoire contenant les listes de ses systèmes d'information sensibles tels que définis à l'article premier…»

La DNSSI, exige que :

« … chaque entité doit…Conduire une analyse de risques pour ses systèmes d'information, et veiller à la définition des mesures de sécurité applicables;…»

La Norme ISO 27001, Indique dans son introduction que :

« … Le système de management de la sécurité de l'information préserve la confidentialité, l'intégrité et la disponibilité de l'information en appliquant un processus de gestion des risques et donne aux parties intéressées l'assurance que les risques sont gérés de manière adéquate…. »[6]

Partant de ce constat, II semblerait judicieux de détailler cette approche et ce avant d'entrer dans le vif du sujet.

L'approche par les risques est essentielle et incontournable que ce soit pour le management de la qualité, les services, la continuité des activités…

En effet et pour un management efficace des risques, il convient qu'un organisme respecte, à tous les niveaux, les principes[7] ci-dessous :

- Le management du risque crée de la valeur et la préserve ;
- Le management du risque est intégré aux processus organisationnels ;

[6] ISO/IEC 27001:2013
[7] Principes ISO 31000:2009

- Le management du risque est intégré au processus de prise de décision ;
- Le management du risque traite explicitement de l'incertitude ;
- Le management du risque est systématique, structuré et utilisé en temps utile ;
- Le management du risque s'appuie sur la meilleure information disponible ;
- Le management du risque est adapté ;
- Le management du risque intègre les facteurs humains et culturels ;
- Le management du risque est transparent et participatif ;
- Le management du risque est dynamique, itératif et réactif au changement ;
- Le management du risque facilite l'amélioration continue de l'organisme.

2. Autres concepts

a. L'amélioration continue[8]

La Norme ISO/IEC 27000:2016, définit l'amélioration continue par une « *activité régulière destinée à améliorer les performances…* »

Et d'ajouter que «…*Le but de l'amélioration continue d'un SMSI est d'augmenter la probabilité de réaliser des objectifs en matière de préservation de la confidentialité, de disponibilité et d'intégrité de l'information. L'amélioration continue est centrée sur la recherche de possibilités d'amélioration, sans partir du principe que les activités de management existantes sont suffisantes, ou aussi appropriées que possible.* ».

L'amélioration est une activité continue d'actions telles que :

- l'analyse et l'évaluation de la situation existante pour identifier des domaines d'amélioration;
- l'établissement des objectifs d'amélioration;
- la recherche de solutions possibles pour atteindre ces objectifs;
- l'évaluation de ces solutions et la réalisation d'une sélection;

[8] Source : ISO/IEC 27000:2016

- la mise en œuvre de la solution choisie;
- le mesurage, la vérification, l'analyse et l'évaluation des résultats de la mise en œuvre pour déterminer si les objectifs ont été atteints;
- l'officialisation des modifications.

b. L'approche processus[9]

L'« approche processus » peut désigner l'application d'un système de processus au sein d'un organisme, ainsi que l'identification, les interactions et le management de ces processus. Elle se base les énoncés suivants :

- Pour fonctionner de manière efficace et efficiente, les organismes doivent identifier et gérer de nombreuses activités ;
- Toute activité qui utilise des ressources doit être gérée pour permettre la transformation d'éléments d'entrée en éléments de sortie à l'aide d'un ensemble d'activités corrélées ou interactives ;
- Ce type d'activité est également connu sous le nom de « processus » ;
- Les éléments de sortie d'un processus peuvent être utilisés en tant qu'éléments d'entrée d'un autre processus et, généralement, cette transformation s'opère dans des conditions planifiées et maîtrisées.

c. L'audit[10]

L'article 7 du Décret 02-05-712, exige que :

« … les entités … soumettent, conformément au programme des missions d'audit arrêté par l'autorité compétente, leurs systèmes d'information sensibles à un audit …»

L'audit est processus méthodique, indépendant et documenté permettant d'obtenir des preuves d'audit et de les évaluer de manière objective pour déterminer dans quelle mesure les critères d'audit sont satisfaits.

Un audit peut être :

[9] Source : ISO/IEC 27000:2016
[10] Sources : Décret 02-05-712, ISO/IEC 27000:2016

- Interne ou audit de première partie,
- Externe ou audit de seconde ou de tierce partie ou
- Combiné associant deux disciplines ou plus.

III. Les enjeux réglementaires

Au Maroc, la décennie écoulée a connu la profusion de textes de loi relatifs à l'utilisation des technologies de l'information et télécommunication.

Pour plus de précisions, un recueil réglementaire est disponible à l'annexe « recueil réglementaire ».

Dans la suite de ce chapitre nous allons faire un focus sur le décret 02-15-712 ainsi que sur la Directive nationale de la sécurité des systèmes d'information (DNSSI).

A. Le Décret numéro 02-15-712

Le Décret n° 2-15-712 du 22/03/2016 a été publié au Bulletin Officiel n° 6458 du 21/4/2016. Composé de 12 articles et une annexe, il a pour objet de fixer le dispositif de protection des Systèmes d'information sensibles (SIS) des Infrastructures d'importance vitale.

1. Définition[11]

Dans ce document le législateur a défini et clarifié les termes ci-dessous :

- Infrastructures d'importance vitale (Article 1er)
- Secteur d'activités d'importance vitale (Article 1er)
- Information sensible (Article 1er)
- SIS d'une infrastructure d'importance vitale (Article 1er)
- Autorité compétente (Article 1er)
- Entité (Article 2)
- Coordinateur d'un secteur d'importance vitale (Article 3)
- Centre (Article 6)

2. Domaine d'application

Le domaine d'application de ce décret est également défini par les articles 2 et 3 :

- Champ d'application (Article 2)
- Délimitation des secteurs d'activités et des infrastructures d'importance vitale (Article 3)
- Liste des secteurs d'activités d'importance vitale (l'Annexe du décret)
- Liste des coordinateurs pour chaque secteur d'importance vitale (l'Annexe du décret)

3. Les intervenants

Le législateur a également cité les acteurs appelés à intervenir dans le cadre dudit décret :

- DGSSI : L'autorité compétente (Article 1)
- Les « Entités » auxquelles s'applique ce décret (Article 2)
- Le coordinateur d'un secteur d'importance vitale (Article 3 et l'Annexe du décret)
- Le RSSI (Article 4)
- Le Centre : Ma-CERT (Article 6)

[11] Ces termes sont expliqués dans l'annexe de ce document « Termes et définitions ».

- Auditeur (Article 7)
- Le tiers (Article 9)

4. Dates importantes

- Ce décret a été établi le 22/03/2016 et publié au BO le 21/04/2016 (Article 12)
- La liste des SIS doit être communiquée avant le 22/04/2017 (Article 4)

5. Liste des articles du décret

- Article 1 : Définitions
- Article 2 : Champ d'application
- Article 3 : Délimitation des secteurs d'activité et des infrastructures d'importance vitale
- Article 4 : Identification et recensement des SAIV
- Article 5 : Application de la DNSSI et des règles de sécurité sectoriels
- Article 6 : Déclaration et traitement des incidents de sécurité
- Article 7 : Audit de la SSI
- Article 8 : Plan de continuité et de reprise d'activités
- Article 9 : Externalisation des SI
- Article 10 : Prise en compte de la SSI dans les achats et la maintenance
- Article 11 : Accompagnement et assistance des entités
- Article 12 : Publication au Bulletin Officiel

B. La Directive Nationale de la Sécurité des Systèmes d'Information

1. Description de la DNSSI

La directive nationale de la sécurité des systèmes l'information (DNSSI) est un document élaboré par la DGSSI et publié sur son portail. (DNSSI, 2013).

Dans le préambule de la DNSSI, l'auteur explique que « La DNSSI décrit les mesures de sécurité organisationnelles et techniques qui doivent être appliquées par les administrations et organismes publics ainsi que les infrastructures d'importance vitale. »

La DNSSI est composée de deux parties et d'un glossaire dont un extrait est repris en annexe.

2. Partie 1 : Dispositions générales de la DNSSI

La première partie de la DNSSI comporte un ensemble de dispositions dont les extraits ci-dessous :

a) Principes fondamentaux

La DNSSI s'appuie sur les principes directeurs suivants, issus de la Stratégie Nationale de la Cyber sécurité, validée par le CSSSI en date du 05 décembre 2012 :

P1. Structure organisationnelle :

Mettre en place une structure organisationnelle dédiée à la SSI au niveau de chaque entité pour inclure les volets préventifs et réactifs nécessaires à la Cyber sécurité;

P2. Cartographie des systèmes d'information :

Tenir et mettre à jour une cartographie précise des systèmes d'information des entités ;

P3. Budget de la sécurité des systèmes d'information :

Quantifier et planifier le budget consacré à la sécurité des systèmes d'information de chaque entité, tant dans les volets investissements que moyens humains, et son rapport au budget global des systèmes d'information;

P4. Contrôle des administrateurs :

Contrôler et tracer les opérations de gestion et d'administration des systèmes d'information des entités;

P5. Protection de l'information :

Protéger les informations en suivant un ensemble de règles de sécurité précisées dans ce document;

P6. Formation et sensibilisation :

Former et sensibiliser le personnel, notamment les administrateurs systèmes et réseaux et les utilisateurs des systèmes d'information, de leurs droits et devoirs ;

P7. Hébergement national des données sensibles :

Héberger sur le territoire national les informations des entités, qui sont sensibles au regard de leur confidentialité, de leur intégrité ou de leur disponibilité.

b) Domaine d'application

La DNSSI s'applique à tous les systèmes d'information des administrations, des organismes publics et des infrastructures d'importance vitale.

La DNSSI s'adresse à l'ensemble du personnel de ces entités ainsi que les tiers (contractants, etc.).

c) Mise en application de la DNSSI

La DNSSI est entrée en vigueur dès sa publication le 31 décembre 2013. A partir de cette date:

- Chaque Entité avait une année pour établir son plan d'actions de mise en conformité;
- Les SI des Entités doivent être en conformité totale dans les 3 ans;

En plus chaque entité doit :

- Désigner un responsable de la sécurité des systèmes d'information (RSSI) ;
- Etablir un inventaire de ses systèmes d'information, et en évaluer la sensibilité;

- Conduire une analyse de risques pour ses systèmes d'information, et veiller à la définition des mesures de sécurité applicables;
- Conduire des actions de sensibilisation et de formation à la sécurité des systèmes d'information et participer aux actions entreprises dans ce sens par la DGSSI ;
- Conduire des actions régulières de contrôle du niveau de sécurité des systèmes d'information et de son périmètre et mettre en œuvre les actions correctives nécessaires;
- Mesurer la résilience de leurs SI par des audits internes et le cas échéant de simulation d'exercices, etc.

Pour le suivi de l'application de la DNSSI :

- La DGSSI met à la disposition de chaque entité un tableau de bord pour le suivi de l'application de la DNSSI ainsi que les guides techniques d'implémentation des différentes règles de sécurité.
- Chaque entité élabore son bilan annuel de mise en application de la DNSSI en se basant sur ledit tableau de bord, et le soumet annuellement à la DGSSI.
- Le bilan annuel constitue une synthèse de l'état d'avancement de l'organisation en sécurité et de l'application des règles édictées par la DNSSI. Ce bilan comprend également un récapitulatif des actions réalisées pour la mise en conformité à la DNSSI, et une synthèse des incidents traités, des éventuels audits diligentés et des exercices menés.

d) Les dérogations à la DNSSI

Il peut être nécessaire, dans certains cas spécifiques, de déroger à des règles énoncées par la DNSSI. Il appartient alors à l'autorité de l'entité concernée de leur substituer formellement des règles particulières.

Pour chacune de ces règles, la dérogation, motivée et justifiée, doit être expressément accordée par le RSSI de l'entité concernée.

La décision de dérogation accompagnée de la justification est tenue à la disposition de la DGSSI.

3. Partie 2 : Objectifs et règles de sécurité de la DNSSI

Dans le préambule de la DNSSI, l'auteur explique que « Pour arrêter les règles de la DNSSI, la DGSSI s'est inspirée de la Norme Marocaine NM ISO/CEI 27002:2009[12] et s'est basée sur les résultats de l'enquête menée au mois de juillet 2013 auprès d'un échantillon représentatif d'administrations et organismes publics et d'opérateurs d'importance vitale »

En effet le quatre cinquième des cinquante-deux pages de la DNSSI est occupé par cette deuxième partie, composée de onze chapitres :

- Chapitre 1 : Politique de sécurité
- Chapitre 2 : Organisation de la sécurité
- Chapitre 3 : Gestion des biens
- Chapitre 4 : Sécurité liée aux ressources Humaines
- Chapitre 5 : Sécurité physique
- Chapitre 6 : Gestion de l'exploitation et des télécommunications
- Chapitre 7 : Contrôle d'accès
- Chapitre 8 : Acquisition, développement et maintenance
- Chapitre 9 : Gestion des incidents
- Chapitre 10 : Gestion du plan de continuité de l'activité
- Chapitre 11 : Conformité

Chaque chapitre est structuré en objectifs, mesures et règles. Soit au total cent quatre règles de sécurité, regroupées en vingt-neuf objectifs de sécurité et trente-deux mesures de sécurité.

A chaque règle est associé un poids allant de 1 à 4 et qui traduit le niveau d'impact croissant de son non-respect sur le SI en termes de disponibilité, d'intégrité, de confidentialité ou de de traçabilité.

Pour chacune de ces règles, sont proposées les fonctions concernées par son application. Telles que : Secrétariat Général ou Direction Générale, Direction SI, RSSI, MOA, MOE, utilisateur…

[12] Norme Marocaine qui reprend intégralement la Norme internationale ISO/CEI 27002:2005

4. Evolution de la DNSSI

Dans le préambule de la DNSSI, l'auteur explique que « Cette directive, appelée à évoluer et à être complétée par des dispositifs d'applications, constitue aujourd'hui la première référence nationale qui fixe les objectifs et les règles de SSI… ».

Et d'ajouter que « Ce socle de règles minimales peut être enrichi pour certains usages. Les mesures complémentaires nécessaires sont définies par les autorités concernées et partagées par la suite avec la DGSSI. »

Dans la première partie de DNSSI, l'auteur annonce que « La DGSSI élabore les évolutions de la DNSSI, en liaison avec les administrations, organismes publics et infrastructures d'importance vitale, en prenant en compte :

- Les résultats d'analyses de risques ;
- Les évolutions des menaces et les retours d'expérience des traitements d'incidents ;
- Les évolutions des contextes organisationnel, juridique, réglementaire et technologique. »

IV. Les Normes de la famille ISO 27000

Partant du fait que la DNSSI est inspirée de la Norme Marocaine NM ISO/CEI 27002:2009[13], il aurait été dommage de ne pas faire profiter les assujettis à cette directive, de l'apport que pourrait être celui des Normes de la famille ISO 27000, à la fois pour la sécurisation des systèmes d'information et surtout pour la gouvernance de la sécurité de l'information.

Après un tour d'horizon de l'univers dans Normes ISO, nous allons nous focaliser sur la Norme internationale ISO 27001.

[13] Norme Marocaine qui reprend intégralement la Norme internationale ISO/CEI 27002:2005

A. Les normes ISO[14]

Les normes ISO sont des accords d'application volontaire, élaborés dans le cadre d'un processus ouvert offrant à toutes les parties prenantes, y compris les consommateurs, la possibilité d'exprimer leurs points de vue et de les voir pris en compte. Ce processus, qui contribue à l'équité et à la pertinence des normes pour le marché, est un gage de confiance quant à leur utilisation.

Les Normes internationales établissent des spécifications de premier ordre pour les produits, les services et les systèmes dans une optique de qualité, de sécurité et d'efficacité. Elles jouent un rôle prépondérant pour faciliter le commerce international.

Jusqu'à présent l'ISO a publié plus de 21571 Normes internationales et publications associées qui couvrent la quasi-totalité des secteurs de l'industrie – des technologies à la sécurité des denrées alimentaires, et de l'agriculture à la santé. Les Normes internationales de l'ISO ont un impact partout, pour tous.

Les publications d'ISO sont protégées par copyright et sauf exception, les Normes ISO sont payantes, à commander auprès de ISO ou l'un des organismes nationaux de normalisation (ONN) sur support papier ou électronique avec possibilité payement en ligne.

Les Normes ISO sont dans un premier temps disponibles en Anglais, avant d'être homologuées par les ONN ou traduites dans différentes langues.

Au Maroc, les normes ISO NM peuvent être disponibles chez IMANOR après homologation et ce en version papier, en anglais ou français.

Une liste de normes marocaines homologuées, est disponible en annexe.

[14] Sources : IMANOR (IMANOR), ISO (ISO)

1. Principes de l'élaboration des Normes à ISO[15]

a. Les normes ISO répondent à un besoin du marché

« Il n'appartient pas à l'ISO de lancer l'élaboration d'une nouvelle norme. L'ISO répond à une demande exprimée par l'industrie ou d'autres parties prenantes comme les associations de consommateurs. En règle générale, un secteur ou un groupe signale l'intérêt d'une norme au membre de l'ISO pour son pays, qui en fait alors part à l'ISO.»

b. Les normes ISO sont fondées sur une expertise mondiale

« Les normes ISO sont élaborées par des groupes d'experts venant du monde entier, qui forment des groupes plus grands : les comités techniques. Les experts négocient les normes dans leurs moindres détails, y compris leur champ d'application, leurs définitions clés et leur contenu.»

c. Les normes ISO sont le fruit d'un processus multipartite

« Les comités techniques sont constitués des experts des industries concernées, mais aussi des représentants d'associations de consommateurs, des milieux universitaires, des ONG et des gouvernements.»

d. Les normes ISO se fondent sur un consensus

« L'élaboration des normes ISO s'inscrit dans une démarche consensuelle et les observations des parties prenantes sont prises en compte.»

[15] Source : https://www.iso.org/fr/developing-standards.html

2. Les normes nationales

L'initiative des normes est prise au niveau national. En règle générale, chaque pays s'est doté d'un organisme national de normalisation (ONN), lequel, dans la plupart des cas, est membre de l'ISO. Les ONN ont les fonctions suivantes :

- Ils publient, et éventuellement rédigent, leurs propres normes nationales
- Ils représentent leur pays dans les enceintes régionales ou internationales qui établissent des normes
- Ils gèrent une bibliothèque de référence des normes nationales, régionales et internationales
- Ils vendent des exemplaires des normes
- Certains ONN offrent également des activités d'évaluation de la conformité, notamment des services d'accréditation, de certification et d'autres prestations commerciales.

Au Maroc, l'ONN est IMANOR. Les normes nationales sont labélisées Norme Marocaine (NM) et sont élaborées selon le procédé suivant :

- Inscription dans le programme général de normalisation ;
- Préparation du projet de norme par les parties concernées ;
- Examen du projet de norme par la commission selon une approche consensuelle ;
- Validation par une large consultation, sous forme d'enquête publique ;
- Homologation par décision du Directeur de l'IMANOR;
- Publication au Bulletin Officiel du Royaume du Maroc.

3. Les normes régionales et internationales

Avec la mondialisation des échanges, les organismes nationaux et régionaux de normalisation adoptent ou utilisent, dans la mesure du possible, des Normes internationales.

Cependant, certains organismes nationaux de normalisation peuvent se regrouper pour établir ensemble des normes régionales. A ce titre d'exemple, les normes européennes servent à étayer la législation paneuropéenne et ceux dans le cadre de leur approche régionales de normalisation[16].

4. Normes et régimes réglementaires

Les normes sont d'application volontaire alors que l'application des lois est obligatoire. Une norme devient d'application volontaire, si elle est référencée dans les textes règlementaires. Ce qui est aussi le cas du Maroc, dont l'article 33 du dahir n° 1-10-15, prévoit que : « […] *toute norme marocaine homologuée[17] peut être rendue obligatoire si une telle mesure est jugée nécessaire par l'autorité gouvernementale compétente. L'acte relatif à cette mesure est publié au "Bulletin Officiel" ».*

A titre d'exemple l'extrait ci-dessous de la liste rendue publique[18], des normes Marocaines d'application obligatoire (NMO).

Norme obligatoire	NM ISO 15875-1 -2009 (Indice de classement : NM 05.6.122)
Désignation	Systèmes de canalisations en plastique pour les installations d'eau chaude et froide - Polyéthylène réticulé (PE-X) - Partie 1 : Généralités ; Rév. 05.6.122
Réf. d'obligation	N° arrêté : 306-13 ; N° BO : 6132 du 07/03/2013

Tableau 1-Exemples de Norme Obligatoire au Maroc (Extrait)

[16] www.newapproach.org (New Approach Standardisation in the Internal Market)
[17] Une liste de Normes Marocaine Homologuées est disponible en annexe.
[18] www.mcinet.gov.ma/~mcinetgov/sites/default/files/11_Liste_des_normes_d_applications_Obligatoires_3-2016.pdf

5. Normes de systèmes de management

Les normes ISO applicables aux systèmes de management fournissent un modèle à suivre pour mettre en place et gérer ce type de systèmes. Elles sont applicables à toutes les organisations, indépendamment de leur taille, du produit ou du service fourni, ou du secteur d'activité. Ci-dessous quelques exemples de normes de systèmes de management :

Norme ISO/IEC	Système de management associé
ISO/IEC 9000	Management de la qualité (SMQ)
ISO/IEC 14000	Management environnemental (SME)
ISO/IEC 27001	Management de la sécurité de l'information (SMSI)
ISO/IEC 22301	Management de la continuité des activités (SMCA)

Tableau 2-Exemples de Normes de Systèmes de Management

a. Les systèmes de managements

Les systèmes de management permettent aux organismes de mettre en œuvre une démarche structurée dans leurs activités afin d'atteindre leurs objectifs.

Dans tout organisme, les employés savent tous comment faire leur travail. Mais il est très utile de disposer de procédures correctement documentées pour s'assurer que chacun connaît bien son rôle. Le système de management vise à systématiser les modes opératoires à suivre. Cette approche offre à l'organisme plusieurs avantages, tels que :

- L'utilisation plus efficace des ressources;
- Une meilleure gestion des risques, et
- La satisfaction accrue des clients, car les services et les produits répondent systématiquement aux attentes.

b. Rôle des audits de systèmes de managements

Les audits sont un élément essentiel de l'approche par systèmes de management, car ils permettent à l'organisation de vérifier si les objectifs fixés sont remplis et si la conformité à la norme est assurée.

Afin de faciliter ces audits, l'ISO a publié la norme ISO 19011:2011[19] qui donne des lignes directrices pour les audits internes et externes des systèmes de management.

c. Certification d'un système de management

Un organisme peut bénéficier des avantages de la mise en œuvre des normes de systèmes de management sans avoir à solliciter une quelconque certification de conformité, tant que ce n'est pas une exigence.

Un organisme qui souhaite obtenir la certification de conformité à une ou à plusieurs normes de système de management, devra s'adresser à un organisme de certification. L'ISO ne fournissant pas de services de certification.

[19] ISO 19011 version 2011.

B. La famille de normes du SMSI[20]

La famille de normes du SMSI a pour objet d'aider les organismes de tous types et de toutes tailles à déployer et à exploiter un SMSI. Elle se compose de plusieurs Normes internationales, regroupées sous le titre général « Technologies de l'information — Techniques de sécurité ».

La description de cette famille de Normes internationales figure dans la Norme ISO/CEI 27000:2016 où nous pouvons lire que :

« *Grâce à l'utilisation de la famille de normes du SMSI, les organismes peuvent élaborer et mettre en œuvre un cadre de référence pour gérer la sécurité de leurs actifs informationnels, y compris les informations financières, la propriété intellectuelle, les informations sur les employés, ou les informations qui leur sont confiées par des clients ou des tiers. Ils peuvent également utiliser ces normes pour se préparer à une évaluation indépendante de leurs SMSI en matière de protection de l'information.* »

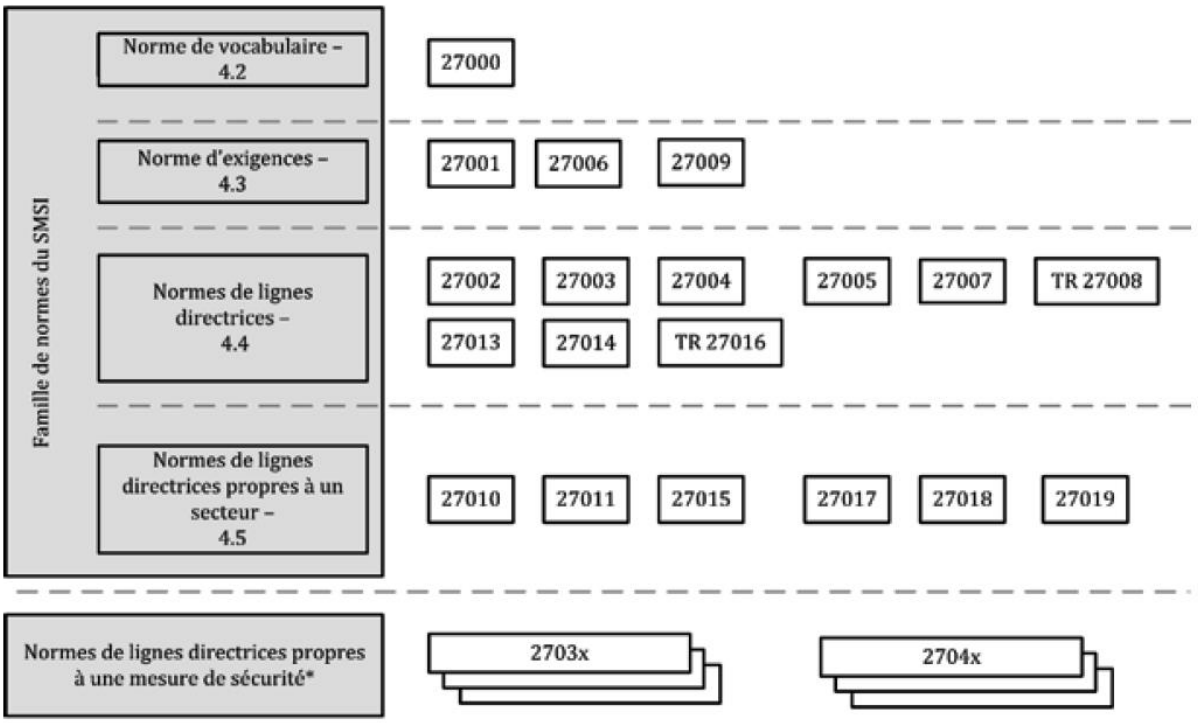

Figure 1-Relations au sein de la famille de normes du SMSI (Extrait)

[20] Source ISO/CEI 27000:2016 (F) (ISO Freely Available Standards)

A titre d'exemple de normes de cette famille, nous pouvons citer :

Norme ISO/IEC	Objectif de la Norme
27000	Décrit les principes essentiels des systèmes de management de la sécurité de l'information, qui constituent l'objet de la famille de normes du SMSI, et définit les termes qui s'y rapportent.
27001	Fournit des exigences normatives relatives à l'élaboration et à l'exploitation d'un SMSI, y compris un ensemble de mesures de sécurité destinées à la maîtrise et à l'atténuation des risques associés aux actifs informationnels que l'organisme cherche à protéger en mettant en œuvre son SMSI.
27002	Fournit des préconisations pour la mise en œuvre des mesures de sécurité de l'information.
27003	Fournit une approche orientée processus pour la réussite de la mise en œuvre d'un SMSI conformément à l'ISO/IEC 27001.
27004	Fournit un cadre de mesurage qui permet d'apprécier l'efficacité du SMSI à mesurer selon l'ISO/IEC 27001
27005	Fournit des préconisations pour la mise en œuvre d'une approche de gestion des risques orientée processus afin d'aider à la bonne mise en œuvre et à la satisfaction des exigences de gestion des risques liés à la sécurité de l'information de l'ISO/IEC 27001.
27006	Complète l'ISO/IEC 17021 en définissant les exigences permettant aux organismes de certification d'obtenir une accréditation et en les autorisant ainsi à délivrer des certifications de conformité satisfaisant aux exigences stipulées dans l'ISO/IEC 27001.
27007	Fournit des préconisations aux organismes qui doivent effectuer des audits internes ou externes sur un SMSI ou gérer un programme d'audit de SMSI conformément aux exigences spécifiées dans l'ISO/IEC 27001.
27017	Code de bonnes pratiques pour les contrôles de sécurité de l'information fondés sur l'ISO/IEC 27002 pour les services du nuage

Tableau 3-Exemples de normes ISO/IEC 2700x

C. Le SMSI

Afin de vous éclairer sur ce système de management dédié à la sécurité de l'information, un vocabulaire issu de la Normes ISO 27000[21] est disponible en annexe. Ci-dessous nous allons détailler ce système ainsi que son fonctionnement.

1. Qu'est-ce qu'un SMSI ?[22]

Un système de management de la sécurité de l'information (SMSI) se compose des politiques, procédures, lignes directrices et des ressources et activités associées, gérées collectivement par un organisme dans le but de protéger ses actifs informationnels.

2. Pourquoi un SMSI ?

Pour être convaincu de la nécessité d'un système de management de la sécurité de l'information (SMSI), un organisme devra admette les fait ci-dessous :

- Chaque organisme détient et traite de l'information ;
- Ces informations sont exposées à des menaces (fuite, attaques, erreurs, vol, événements naturels, etc.) ;
- Ces informations sont exposées à des vulnérabilités inhérentes à leur utilisation ;
- La sécurité ne se résume pas à mettre en œuvre par moyens techniques sans la gestion appropriée ;
- A sa conception, un système d'information ne tient pas nécessairement compte des exigences de sécurité.

La sécurité de l'information considère que l'information est un actif qui est doté d'une valeur et qui doit bénéficier d'une protection appropriée contre la perte de disponibilité, de confidentialité et d'intégrité.

Adopter un SMSI revient à appliquer des principes tels que :

[21] Ouvrage : ISO 27000:2016
[22] Source : Norme internationale ISO/IEC 27000 Quatrième édition 2016-02-15

- la sensibilisation à la sécurité de l'information;
- l'attribution des responsabilités liées à la sécurité de l'information;
- la prise en compte de l'engagement de la direction et des intérêts des parties prenantes;
- la consolidation des valeurs sociétales;
- les appréciations du risque déterminant les mesures de sécurité appropriées pour arriver à des niveaux de risque acceptables;
- l'intégration de la sécurité comme élément essentiel des systèmes et des réseaux d'information;
- la prévention et la détection actives des incidents liés à la sécurité de l'information;
- l'adoption d'une approche globale du management de la sécurité de l'information;
- le réexamen continu de l'appréciation de la sécurité de l'information et la mise en œuvre de modifications le cas échéant.

3. Fonctionnement d'un SMSI

Le SMSI d'un organisme utilise une approche systématique visant à établir, mettre en œuvre, exploiter, surveiller, réexaminer, maintenir et améliorer la sécurité de l'information d'un organisme afin que celui-ci atteigne ses objectifs métiers :

- Actions à répéter en boucle afin d'identifier les changements qui affectent les risques, les stratégies de l'organisme ou ses objectifs métier:
    - Identifier les actifs informationnels et les exigences de sécurité de l'information associées
    - Apprécier les risques liés à la sécurité de l'information ;
    - Traiter les risques liés à la sécurité de l'information;
    - Sélectionner et mettre en œuvre les mesures de sécurité pertinentes pour gérer les risques inacceptables;
- Surveiller, mettre à jour et améliorer l'efficacité des mesures de sécurité
- Amélioration continue du SMSI.

4. Facteurs critiques de succès d'un SMSI[23]

De nombreux facteurs sont essentiels pour réussir la mise en œuvre d'un SMSI permettant à un organisme de répondre à ses objectifs métiers. Exemples :

- une **politique**, des **objectifs** et des **activités** de sécurité de l'information en phase avec les objectifs de l'organisme;
- une **approche** et un **cadre** pour la conception, la mise en œuvre, la surveillance, le maintien et l'amélioration de la sécurité de l'information, cohérents avec la culture de l'organisme;
- une **adhésion** et un **engagement** visibles à tous les niveaux du management, notamment au niveau de la direction;
- une **compréhension** des exigences de protection des actifs informationnels via l'application de mesures de management du risque lié à la sécurité de l'information (voir ISO/IEC 27005);
- un programme efficace de **sensibilisation**, de formation et d'éducation à la sécurité de l'information, qui informe tous les salariés et autres parties concernées de leurs obligations en matière de sécurité de l'information, telles qu'elles sont détaillées dans les politiques, normes, etc. en matière de sécurité de l'information, et qui les motive à agir en conséquence;
- un processus efficace de **gestion des incidents** liés à la sécurité de l'information;
- une approche efficace de management de la **continuité de l'activité**;
- un système de **mesurage** utilisé pour évaluer la performance du management de la sécurité de l'information et des suggestions d'amélioration issues des retours d'information.

[23] **ISO/IEC 27000:2016(F)**

V. Mise en conformité avec le Décret 02-15-712 et la DNSSI

Pour se conformer avec le Décret 02-15-712 et par conséquent la DNSSI, les tableaux ci-dessous-vous sont proposés.

La précaution d'usage voudrait de préciser que ces informations sont fournies à titre indicatif et qu'elles ne peuvent en aucun cas se substituer ou suppléer le savoir-faire des Entités ni des Tiers fournissant des services d'accompagnement aux Entités.

A. Démarche proposée

Partant d'un cas réel, la proposition de démarche de mise en conformité avec ce décret :

Etape	Actions
Compréhension du texte réglementaire	Constituer un groupe de travail
	Atelier de relecture et analyse des écarts
Planification des actions	Lister les actions à effectuer
	Planifier en groupe, les actions à réaliser
Réalisation des actions de mise à jour	Recueil réglementaire
	Procédures (si nécessaire)
Réalisation des actions sensibilisation	Diffuser les documents modifiés
	Sensibiliser le personnel

Tableau 4-Liste des étapes de la démarche

B. Actions proposées

Ci-dessous des exemples d'actions concrètes à dérouler selon les articles du décret 02-15-712 et basées sur ISO 27001 :

Art.	Actions	Remarques
1-3	Mise à jour documentaire	Surtout : Référence au décret et Nouvelles parties prenantes (ma-CERT, DGSSI)
4	Analyser les risques liés à la sécurité de l'information	Un inventaire à jour
		Une démarche formalisée s'impose, basée sur ISO 27005
		La DGSSI propose un guide
	Renseigner la liste des SI sensibles et le communiquer à la DGSSI	Canevas proposé par la DGSSI
		Notifier DGSSI si changement des SI sensibles
	Désigner un RSSI, point de contact vis-à-vis de la DGSSI	Formaliser un plan de communication de la sécurité et y inclure ce canal
5	Etude des écarts avec la DNSSI et plan d'actions correctives	Veiller à ce que les SI sensibles soient conformes aux règles prescrites par la DNSSI
		Se conformer aux standards de sécurité édictés par la DGSSI
6	Mettre en place les moyens nécessaires à la supervision et détection des Cyberattaques	Attention au coût et au délai de mise en place
	Mettre en place une procédure pour communiquer avec maCERT	Le délai pour notifier maCERT est de 48h
		Ils peuvent exiger des informations complémentaires (fichiers logs)
7	Mettre à jour la procédure d'audit, le cas échéant	Planifier, réaliser et faire le suivi des audits de la sécurité des systèmes d'information
8	Mettre à jour les procédures de continuité des et de reprise d'activités activités, le cas échéant	En profiter pour adopter la Norme ISO 22301:2012
	Planifier les tests de continuité des activités	
9	Règles internes et sensibilisation des salariés concernés	Ne pas oublier d'actualiser les modèles des contrats et cahiers des charges
10		

Tableau 5-Liste des actions

VI. Annexes

A. Acronymes

ADM	: Administration de la Défense Nationale.
CEI	: Commission électrotechnique internationale (www.iec.ch)
CSSSI	: Comité Stratégique de la SSI
CT	: Comité technique (ISO, ISO en pratique, 2016)
DGSSI	: Direction générale de la SSI, rattachée à l'ADM. (www.dgsssi.ma)
DIS	: Projet de Norme internationale
DNSSI	: Directive Nationale de la SSI.
FDIS	: Projet de Norme internationale
IIV	: Infrastructures d'importance vitale
IMANOR	: Institut Marocain de Normalisation. (www.imanor.gov.ma)
ISO	: Organisation Internationale de Normalisation (www.iso.org)
JTC	: Join technical committee
Ma-CERT	: Moroccan Computer Emergency Response Team (ou MaCERT).
NM	: Norme Marocaine
OCDE	: Organisation de coopération et de développement économiques
OMC	: Organisation mondiale du commerce
ONG	: Organisation non gouvernementale
ONN	: Organisme national de normalisation
RSSI	: Responsable de la Sécurité des Systèmes d'Information
SI	: Système(s) d'information.
SIS	: Système(s) d'information sensible(s)
SMCA	: Système de management de la continuité des activités
SMQ	: Système de management de la qualité
SMSI	: Système de management de la sécurité de l'information
SSI	: Sécurité des SI.
TIC	: Technologies de l'information et des communications
UIT	: Union internationale des télécommunications (www.itu.int)

B. Termes et définitions

1. Termes issus du Décret 02-15-712

Autorité compétente

Autorité gouvernementale chargée de l'administration de la défense nationale (DGSSI).

Centre (Voir Ma-CERT)

Infrastructures d'importance vitale (IIV)

Installations, ouvrages et systèmes qui sont indispensables au maintien des fonctions vitales de la société, de la sante, de la sureté, de la sécurité et du bien-être économique ou social, et dont le dommage ou l'indisponibilité ou la destruction aurait un impact induisant la défaillance de ces fonctions.

Information sensible

Information dont la compromission, l'altération, le détournement ou la destruction est de nature à nuire à la continuité du fonctionnement ou mettant en danger le patrimoine informationnel de l'infrastructure d'importance vitale.

Ma-CERT

Centre de veille, de détection et de réponse aux attaques informatiques, au Maroc, relevant de la DGSSI.

Secteur d'activités d'importance vitale

Secteur constitué d'activités qui fournissent des biens et service indispensables difficilement substituables ou remplaçables, ou qui peuvent présenter un danger grave pour la population :

- pour la vie des populations, ou
- à l'exercice des prérogatives de l'Etat, ou
- au fonctionnement de l'économie, ou
- au maintien des capacités de sécurité du pays.

SI sensible d'une infrastructure d'importance vitale

SI traitant des informations sur lesquelles une atteinte à la confidentialité, à l'intégrité ou à leur disponibilité porterait préjudice à la continuité de fonctionnement de l'infrastructure d'importance vitale.

Entité

Administrations, établissements et entreprises publics et organismes disposant d'un agrément ou d'une licence de l'Etat pour exercer une activité règlementée, considérés comme des infrastructures d'importance vitale et disposant de SI sensibles.

Coordinateur d'un secteur d'activité d'importance vitale

Autorité gouvernementale ou établissement public ou personne morale de droit public assurant la coordination d'un secteur d'activités d'importance vitale.

2. Termes issus de la DNSSI[24]

Analyse des risques

Utilisation systématique d'informations pour identifier les sources et pour estimer le risque.

Audit

Activité périodique (ou ponctuelle) permettant d'évaluer la sécurité d'un système ou de détecter les traces d'une activité malveillante.

Confidentialité

Objectif de sécurité permettant de s'assurer que les informations transmises ou stockés ne sont accessibles qu'aux personnes autorisées à en prendre connaissance.

Cyber sécurité

Situation recherchée pour un système d'information lui permettant de résister à des événements issus du cyberespace susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises.

Cyberespace

Ensemble de données numérisées constituant un univers d'information et un milieu de communication, lié à l'interconnexion mondiale des ordinateurs.

Disponibilité

Objectif de sécurité qui consiste à assurer un accès permanent à l'information et aux services offerts par le système d'information. C'est une garantie de la continuité de service et de performances des applications, du matériel et de l'environnement organisationnel.

Incident de sécurité

Un ou plusieurs évènements liés à la sécurité de l'information indésirables ou inattendus d'origine accidentelle ou malveillante, impactant l'un ou plusieurs objectifs de sécurité (Confidentialité, Intégrité, Disponibilité), et présentant une probabilité forte de compromettre les activités de l'organisme et de menacer la sécurité de l'information (Fuites de données, Déni de service, Intrusion informatique ou physique, inondation…).

Intégrité

Objectif de sécurité qui consiste à empêcher, ou tout du moins à détecter, toute altération non autorisée de données. Par altération on entend toute modification, suppression partielle ou insertion d'information. Cet objectif peut être assuré par la signature électronique.

[24] Source : DNSSI - Glossaire

Mesure

Moyen de gérer un risque, et pouvant être de nature administrative, technique, gestionnaire ou juridique.

Non répudiation

Objectif de sécurité qui permet de garantir qu'une transaction ne peut être niée.

Normes

Document de référence contenant des spécifications techniques précises destiné à être utilisé comme règles ou lignes directrices.

Plan de Continuité d'Activité (PCA)

Vise à assurer et maintenir la continuité de l'activité à plein régime ou en mode dégradé, en cas de désastre ou panne informatique majeure touchant le SI. Il permet de garantir la survie de l'organisme en préparant à l'avance la continuité des activités désignées comme stratégiques. Au contraire du PRA, le PCA n'autorise pas de coupure intégrale du service : la continuité, au moins partielle doit être assurée. Ce plan traite essentiellement des activités "métier", le secours de moyens informatique ne constitue que l'un de ces aspects.

Sécurité des Systèmes d'Information (SSI)

l'ensemble des mesures techniques et non techniques (organisationnelles et humaines) de protection permettant à un système d'information de résister à des évènements susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises.

Système d'information (SI)

Est un ensemble organisé de ressources (matériels, logiciels, personnel, données et procédures) qui permet de regrouper, de classifier, de traiter et de diffuser de l'information sur un environnement donné.

Tiers

Personne ou organisme reconnu(e) comme indépendant(e) des parties concernées.

3. Termes issus de ISO 27000[25]

Information

L'information est un actif qui, comme tous les autres actifs importants de l'organisme, est essentiel à son fonctionnement et qui, par conséquent, requiert une protection adéquate. Elle peut être stockée sous différentes formes, notamment numérique (par exemple: des fichiers de données stockés sur un support électronique ou optique), matérielle (par exemple: sur papier) ou en tant qu'information intangible (par exemple: les connaissances des salariés). L'information peut être transmise par différents moyens, notamment par courrier ou dans le cadre de communications électroniques ou verbales. Quel que soit la forme que prend l'information ou quel que soit son vecteur de transmission, elle requiert une protection appropriée.

Dans de nombreux organismes, l'information dépend des technologies de l'information et des communications. Ces technologies représentent souvent un élément essentiel dans l'organisme et elles facilitent la création, le traitement, le stockage, la transmission, la protection et la destruction de l'information.

Management

Le management implique des activités de pilotage, de contrôle et d'amélioration continue de l'organisme dans des structures appropriées. Les activités de management incluent les actions, la manière ou les pratiques instaurées pour organiser, prendre en charge, diriger, superviser et contrôler les ressources. Les structures de management peuvent aller d'une personne dans un petit organisme à des hiérarchies de management composées d'un grand nombre de personnes dans les grands organismes.

Au sens d'un SMSI, le management implique la supervision et la prise de décisions nécessaires à l'atteinte des objectifs métiers par le biais de la protection des actifs informationnels de l'organisme. Le management de la sécurité de l'information s'exprime au travers de la formulation et de l'utilisation de politiques, de procédures et de lignes directrices relatives à la sécurité de l'information, qui sont ensuite appliquées à tous les niveaux de l'organisme par toutes les personnes qui y sont associées.

Management du risque

Activités coordonnées visant à diriger et contrôler un organisme vis-à-vis du risque.

Organisme

Personne ou groupe de personnes qui exerce ses propres fonctions associées aux responsabilités, pouvoirs et relations nécessaires pour atteindre ses objectifs.

[25] Source ISO/CEI 27000:2016 (F) (ISO Freely Available Standards)

Risque

Effet de l'incertitude sur l'atteinte des objectifs.

Sécurité de l'information

La sécurité de l'information garantit la confidentialité, la disponibilité et l'intégrité de l'information. Afin de contribuer au succès de l'organisme et à sa pérennité, et de réduire le plus possible l'impact des incidents liés à la sécurité de l'information, la sécurité de l'information implique l'application et le management de mesures de sécurité appropriées, ce qui sous-entend la prise en compte d'un vaste éventail de menaces.

La sécurité de l'information s'obtient par la mise en œuvre d'un ensemble de mesures de sécurité applicables, sélectionnées au moyen d'un processus déterminé de management du risque et gérées à l'aide d'un SMSI contenant les politiques, processus, procédures, structures organisationnelles, logiciels et matériels permettant de protéger les actifs informationnels identifiés. Ces mesures doivent être spécifiées, mises en œuvre, surveillées, réexaminées et améliorées, si nécessaire, pour s'assurer qu'elles répondent aux objectifs métiers et sécurité de l'information spécifiques de l'organisme. Il est attendu que les mesures pertinentes de sécurité de l'information s'intègrent parfaitement aux processus métier de l'organisme.

Système de management

Un système de management utilise un cadre de référence permettant à un organisme d'atteindre ses objectifs. Il comprend la structure organisationnelle, les politiques, les activités de planification, les responsabilités, les pratiques, les procédures, les processus et les ressources.

En termes de sécurité de l'information, un système de management permet à un organisme:

- de satisfaire aux exigences en matière de sécurité de l'information des clients et des autres parties prenantes;
- d'améliorer les plans et les activités d'un organisme;
- de répondre aux objectifs de sécurité de l'information de l'organisme;
- de se conformer aux réglementations, à la législation et aux autorités sectorielles; et
- de gérer les actifs informationnels d'une manière organisée qui facilite l'amélioration et l'ajustement continus aux objectifs actuels de l'organisme.

4. Autres termes

Certification

Attestation (c'est-à-dire fourniture d'une affirmation) réalisée par une tierce partie, démontrant que des exigences spécifiées relatives à des produits, des processus, des systèmes ou des personnes sont respectées (définition adaptée d'ISO/CEI 17000:2004, définitions 5.2 et 5.5).

IMANOR (www.imanor.gov.ma)

L'institut Marocain de Normalisation, est créé par la loi n°02-06[26] relative à la normalisation, la certification et l'accréditation. Il représentation le Maroc auprès des organisations internationales et régionales de normalisation.

Information

L'information est un bien essentiel au fonctionnement des organismes et par conséquent, requiert une protection adéquate.

L'information peut être stockée sur support électronique, optique, papier ou mémorisée par les individus. Elle peut être transmise oralement, par courrier ou par voie électronique.

Généralement, l'information dépend des TIC, souvent essentielles car elles facilitent sa création, son traitement, son stockage, sa transmission, sa protection et sa destruction.

ISO (www.iso.org)

L'ISO (Organisation internationale de normalisation) est une fédération mondiale d'organismes nationaux de normalisation (comités membres de l'ISO). L'ISO collabore étroitement avec la Commission électrotechnique internationale (IEC) en ce qui concerne la normalisation électrotechnique.

L'ISO est composée de 163 membres (dont IMANOR) et a publié plus de 21578 Normes internationales, depuis 1947.

Normes internationales

Les Normes internationales sont des documents qui définissent des exigences, des spécifications, des lignes directrices ou des caractéristiques à utiliser systématiquement pour assurer l'aptitude à l'emploi des matériaux, produits, processus et services, dans une optique de qualité, de sécurité et d'efficacité. Elles jouent un rôle prépondérant pour faciliter le commerce international.

[26] Source : Ministère de la Justice (Maroc)

Management

Le management implique des activités de pilotage, de contrôle et d'amélioration continue de l'organisme dans des structures appropriées. Les activités de management incluent les actions, la manière ou les pratiques instaurées pour organiser, prendre en charge, diriger, superviser et contrôler les ressources. Les structures de management peuvent aller d'une personne dans un petit organisme à des hiérarchies de management composées d'un grand nombre de personnes dans les grands organismes.

Organisme/Organisation

Personne ou groupe de personnes qui exerce ses propres fonctions associées aux responsabilités, pouvoirs et relations nécessaires pour atteindre ses objectifs. Ce concept inclut, sans s'y limiter, les travailleurs indépendants, compagnies, sociétés, firmes, entreprises, autorités, partenariats, œuvres de bienfaisance ou institutions, ou toute partie

Partie prenante

Individu ou groupe d'individus dont les intérêts peuvent influer sur l'organisation ou être soumis à son influence (extrait d'ISO 26000: 2010, définition 2.20).

Produit

Résultat d'un processus, c'est-à-dire d'un ensemble d'activités corrélées ou interactives qui transforme des éléments d'entrée en éléments de sortie, les quatre catégories génériques de produits étant les services, les «softwares», les produits matériels, les produits issus de processus à caractère continu (définition adaptée d'ISO 9000:2005, définitions 3.4.1 et 3.4.2).

Sécurité de l'information

La sécurité de l'information garantit la confidentialité, la disponibilité et l'intégrité de l'information. Elle implique l'application et le management de mesures de sécurité appropriées, par la prise en compte d'un vaste éventail de menaces.

Service

Résultat d'au moins une activité nécessairement réalisée à l'interface entre le fournisseur et le client, et généralement immatériel (voir ISO 9000:2005, définition 3.4.2, Note 2).

Système de management

Un système de management utilise un cadre de référence permettant à un organisme d'atteindre ses objectifs. Il comprend la structure organisationnelle, les politiques, les activités de planification, les responsabilités, les pratiques, les procédures, les processus et les ressources.

C. Recueil réglementaire

Loi 07-03

Complétant le code pénal en ce qui concerne les infractions relatives aux systèmes de traitement automatisé des données, cette loi permet de sanctionner toutes les intrusions non autorisées dans un système de traitement automatisé de données.

Loi 53-05

Relative à l'échange électronique de données juridiques, cette loi fixe le régime applicable aux données juridiques échangées par voie électronique (cryptographie) et à la signature électronique.

Loi 09-08

Relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel, cette loi vise à assurer une protection efficace des particuliers contre les abus d'utilisation des données de nature à porter atteinte à leur vie privée et d'harmoniser le système marocain de protection des données personnelles.

Loi n°31-08

Loi édictant des mesures de protection du consommateur, y compris la protection du consommateur en ligne. Se fixe pour principal objectif le renforcement et la protection des droits des consommateurs, et ce, en leur garantissant une meilleure information, en les protégeant contre les clauses abusives et certaines pratiques.

Loi n°24-96

Loi consolidée relative à la poste et aux télécommunications, telle qu'elle a été modifiée et complétée. L'objet de cette loi est de définir le cadre juridique précisant le nouveau paysage du secteur de la poste et des télécommunications, notamment celui des réseaux des Télécommunications.

Dahir n° 1-10-15

Dahir du 11/02/2010, portant promulgation de la loi n° 12-06 relative à la normalisation, à la certification et à l'accréditation.

Décret n° 2-15-712

Décret du 22/03/2016 fixant le dispositif de protection des systèmes d'information sensibles des infrastructures d'importance vitale.

Décret n° 2-08-518

Décret du 21/05/2009, pris pour l'application des articles 13, 14, 15, 21 et 23 de la loi n° 53-05 relative à l'échange électronique des données juridiques.

Décret n° 2-11-508

Décret du 21/09/2011, portant création du comité stratégique de la sécurité des systèmes d'information.

Décret n° 2-11-509

Décret du 21/09/2011 complétant le décret n° 2-82-673, relatif à l'organisation de l'administration de la défense nationale et portant création de la direction générale de la sécurité.

Décret n° 2-09-165

Décret du 21/05/2009 pris pour l'application de la loi n° 09-08 relative à la protection des personnes physiques à l'égard des traitements des données à caractère personnel

Circulaire et Arrêtés :

- Circulaire du chef du gouvernement n° 3/2014 du 10 mars 2014 pour l'application de la Directive Nationale de la SSI
- Arrêté n° 3-90-13 du 20/01/2015 fixant le modèle du cahier des charges devant accompagner la demande d'agrément de prestataire de services de certification électronique.
- Arrêté n° 3-89-13 du 20/01/2015 fixant le modèle du cahier des charges devant accompagner la demande que doivent déposer les personnes ne disposant pas de l'agrément de prestataires.
- Arrêté n° 3-88-13 du 20/01/2015 fixant la forme et le contenu de la demande d'autorisation préalable d'importation, d'exportation, de fourniture, d'exploitation ou d'utilisation de moyens ou de prestations...
- Arrêté n° 3-87-13 du 20/01/2015 fixant la forme de la déclaration préalable d'importation, d'exportation, de fourniture, d'exploitation ou d'utilisation de moyens ou de prestations de cryptographie...
- Arrêté n° 3-74-11 fixant l'organisation de la direction générale de la sécurité des systèmes d'information.

D. Bibliographie

(s.d.). Récupéré sur New Approach Standardisation in the Internal Market: www.NewApproach.org

DGSSI. (s.d.). www.dgssi.gov.ma. Récupéré sur http://www.dgssi.gov.ma

DNSSI. (2013). Directive Nationale de la Sécurité des Systèmes d'information. Récupéré sur http://www.dgssi.gov.ma

IMANOR. (s.d.). ISO | IMANOR. Récupéré sur http://www.imanor.gov.ma/participation-a-la-normalisation-internationale-et-regionale/

ISO. (s.d.). Récupéré sur www.iso.org

ISO. (2016). ISO en pratique.

ISO Freely Available Standards. (s.d.). Freely Available Standards. Récupéré sur http://standards.iso.org: http://standards.iso.org/ittf/PubliclyAvailableStandards/index.html

Maroc, M. d. (s.d.). http://adala.justice.gov.ma/production/html/Fr/liens/..%5C161932.htm. Récupéré sur ADALA MAROC Portail Juridique et Judiciaire du Ministère de la Justice et des Libertés du Maroc: http://adala.justice.gov.ma

ISO/CEI 27001:2013, Technologies de l'information – Techniques de sécurité – Systèmes de management de la sécurité de l'information – Exigences.

ISO/IEC 27000:2016, Technologies de l'information -- Techniques de sécurité -- Systèmes de gestion de sécurité de l'information -- Vue d'ensemble et vocabulaire

ISO/IEC 9001:2015, Systèmes de management de la qualité — Exigences

Stratégie nationale en matière de cyber sécurité

Le Comité Stratégique de la SSI

Direction Générale de la SSI (DGSSI)

Moroccan Computer Emergency Response Team (maCERT)

Décret n° 2-15-712 du 22/03/2016 (BO n° 6458 du 21/4/2016)

Directive Nationale de la Sécurité des Systèmes d'Information

Guide de gestion des risques de la sécurité des systèmes d'information

Guide d'audit de la sécurité des systèmes d'information

E. Exemples de Normes Marocaines Homologuées

Technologies de l'information - Techniques de sécurité :

Code	Titre	Année	Indice de classement
NM ISO/CEI 27000	Systèmes de management de la sécurité de l'information Vue d'ensemble et vocabulaire	2014	00.5.700
NM ISO/CEI 27001	Systèmes de management de la sécurité de l'information – Exigences	2014	00.5.701
NM ISO/CEI 27002	Code de bonne pratique pour le management de la sécurité de l'information	2014	00.5.702
NM ISO/CEI 27003	Lignes directrices pour la mise en œuvre du système de management de la sécurité de l'information.	2014	00.5.703
NM ISO/CEI 27004	Management de la sécurité de l'information - Mesurage	2013	00.5.715
NM ISO/CEI 27005	Gestion des risques liés à la sécurité de l'information	2013	00.5.716
NM ISO/CEI 27006	Exigences pour les organismes procédant à l'audit et à la certification des systèmes de management de la sécurité de l'information	2013	00.5.717
NM ISO/CEI 27007	Lignes directrices pour l'audit des systèmes de management de la sécurité de l'information	2013	00.5.718
NM ISO/CEI TR 27008	Lignes directrices pour les auditeurs des contrôles de sécurité de l'information	2013	00.5.710

F. Palmarès des certifications ISO/IEC 27001 par pays en Afrique[27]

Pays / Année	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015
Nigeria						5	9	12	16	39
Morocco			2	2	1	5	7	9	5	18
South Africa	5	8	10	14	14	14	22	35	22	18
Kenya				1	1				4	12
Mauritius			1	2	3	4	8	11	9	8
Tunisia				2		1	2	8	5	8
Egypt	1	2	3	7	8	6	11	17	11	7
Ghana				3	1	3		3		6

[27] ISO Survey of certifications to management system standards - Full results. Source: http://isotc.iso.org/livelink/livelink?func=ll&objId=18808772&objAction=browse&viewType=1