RECOMMANDATIONS

Brève étude de la norme ISO/IEC 27003

Décembre 2011

CLUB DE LA SECURITE DE L'INFORMATION FRANÇAIS

11, rue de Mogador – 75009 PARIS
Tel : 01 53 25 08 80 – Fax : 01 53 08 81
clusif@clusif.asso.fr - http://www.clusif.asso.fr

La loi du 11 mars 1957 n'autorisant, aux termes des alinéas 2 et 3 de l'article 41, d'une part, que les "copies ou reproductions strictement réservées à l'usage privé du copiste et non destinées à une utilisation collective" et, d'autre part, que les analyses et les courtes citations dans un but d'exemple et d'illustration, "toute représentation ou reproduction intégrale, ou partielle, faite sans le consentement de l'auteur ou de ayants droit ou ayants cause est illicite" (alinéa 1er de l'article 40)

Cette représentation ou reproduction, par quelque procédé que ce soit, constituerait donc une contrefaçon sanctionnée par les articles 425 et suivants du Code Pénal.

Table des matières

1. Remerciements 4
2. Introduction 5
   2.1 A qui s'adresse cette étude de la norme ? 5
   2.2 Objectif de cette étude 5
3. La norme ISO/IEC 27003 6
4. Résumé de l'étude du CLUSIF 7
   4.1 A qui cette norme semble-t-elle destinée ? 7
   4.2 Quelle utilisation peut être faite de la norme ? 7
5. Analyse de la norme ISO/IEC 27003 8
   5.1 Synthèse 8
   5.2 Résumé des chapitres 5 à 9 8
6. Conclusion 16

 © CLUSIF 2011

1. Remerciements

Le CLUSIF tient à mettre ici à l'honneur les personnes qui ont rendu possible la réalisation de ce document, tout particulièrement :

Le responsable du groupe de travail :

Olivier	**ALLAIRE**	*Conix*

Les contributeurs :

Nicolas	**ANDREU**	Devoteam
Régis	**BOURDONNEC**	BNP Paribas
Fabrice	**DUTOURNIER**	Ministère de la Défense
François	**JOLIVET**	Société Générale
Jean-Pierre	**LACOMBE**	Fidens
Laurent	**MARECHAL**	Hapsis
Fred	**MESSIKA**	Sekoia
Paul	**RICHY**	France Telecom
Jean-Louis	**ROULE**	
Hervé	**SCHAUER**	HSC

Ainsi que les membres du comité de relecture.

Avec l'aimable participation de François Zamora ***France Telecom*** *et Alexandre Fernandez-Toro* ***HSC***

2. Introduction

2.1 A qui s'adresse cette étude de la norme ?

Cette étude s'adresse principalement aux personnes en charge de conduire un projet d'implémentation de SMSI (Système de Management de la Sécurité de l'Information), que ce soit dans la phase préliminaire de décision ou dans la phase de définition de projet.

2.2 Objectif de cette étude

Présenter rapidement la norme ISO/IEC 27003 et identifier l'intérêt de celle-ci selon le point de vue de la personne en charge de l'implémentation du SMSI, qu'elle soit expérimentée ou débutante sur le sujet.

Comme tout texte de référence, l'utilité finale de la norme doit être évaluée en fonction du contexte particulier auquel on souhaite se référer.

Note des rédacteurs : ce document utilise de nombreux termes techniques relatifs à la sécurité des systèmes d'information et aux normes de la série 27000. Des définitions de ces termes peuvent être trouvées dans la norme ISO/IEC 27000, disponible gratuitement à l'emplacement suivant : http://standards.iso.org/ittf/PubliclyAvailableStandards/index.html. Des explications et des définitions peuvent également être trouvées dans le document « Les métriques dans le cadre de la série 27000 » issu des travaux du Groupe de travail et disponible gratuitement à l'emplacement suivant http://www.clusif.asso.fr/fr/production/ouvrages/pdf/CLUSIF-Metriques-dans-27000.pdf.

 © CLUSIF 2011

3. La norme ISO/IEC 27003

Cette norme déclare fournir un guide de préparation et d'implémentation de la phase de planification d'un SMSI conforme à la norme ISO/IEC 27001:2005.

Elle insiste sur l'approbation du projet par la direction de l'organisation, l'attribution de rôles et de responsabilités dans le cadre du projet et la préparation des points importants de cette planification que sont :

- le contenu de la politique de sécurité ;
- l'analyse des exigences de sécurité à partir des enjeux métiers d'affaires appliqués aux actifs ;
- la conduite de l'évaluation et du traitement de risque, particulièrement le choix de la méthode d'analyse de risque à utiliser ;
- l'établissement du contenu et des frontières du SMSI ;
- l'élaboration du plan projet de traitement de risque.

Cette norme, diffusée au début de 2009, a été jugée par un certain nombre d'organismes nationaux de normalisation comme limitative et ainsi devant être améliorée rapidement sur le plan de l'applicabilité et de l'exhaustivité du processus de gestion continue des risques (absence des phases de réalisation, de contrôle et d'amélioration du PDCA). Par exemple la définition du cadre de gestion documentaire arrive après avoir déjà produit de nombreux documents (activité 9.2.2).

Elle développe (en 45 pages) la phase de planification décrite par la norme IS0/IEC 27001.

Cette norme n'existe qu'en version anglaise et il n'est pas prévu à ce jour de version française.

La norme comporte 4 chapitres introductifs, suivis par 5 chapitres en ce qui concerne leur application ainsi que 5 annexes informatives (25 pages).

 © CLUSIF 2011

4. Résumé de l'étude du CLUSIF

4.1 A qui cette norme semble-t-elle destinée ?

Dans la mesure où un SMSI peut être :

- décidé au départ par la direction de l'organisation dans un objectif précis (réduire les risques pour l'organisation ou pour les activités d'une entité, renforcer un élément particulier (ex. continuité d'activité, gestion des accès), obtenir une certification) ;
- ou proposé par le RSSI, le DSI, le "risk manager" ou toute autre partie prenante. Un élément permanent de la norme 27003 est d'obtenir dans ce cas l'approbation de la direction (chapitre 5) puis de consolider cette approbation lors de la réalisation des étapes de la phase Plan.

La norme est plutôt destinée à tout acteur souhaitant initialiser une démarche de mise en place d'un SMSI et devant recueillir l'approbation de la Direction.

4.2 Quelle utilisation peut être faite de la norme ?

L'essentiel de ce que la norme ISO/IEC 27003 apporte est donc utilisable dans une démarche tournée vers l'approbation de la direction jusqu'à la première implémentation de la phase Plan du SMSI.

Il est à noter que bien que la norme ISO/IEC 27001 impose d'utiliser une méthode de gestion de risque, la norme ISO/IEC 27003 fait abstraction de ce que peut apporter une telle méthode, ce qui est paradoxal pour un guide pratique d'implémentation.

Le lecteur pourra utiliser, s'il le souhaite, les différentes méthodes de gestion du risque disponibles actuellement telle que MEHARI la méthode conçue par le CLUSIF et disponible gratuitement.

http://www.clusif.asso.fr/fr/production/mehari/download/

Parmi les documents associés à MEHARI, figure le « guide de la démarche d'analyse et de traitement des risques *» qui reprend la même approche de description pour les étapes de la phase de planification du SMSI que l'ISO/IEC 27003*

5. Analyse de la norme ISO/IEC 27003

5.1 Synthèse

La norme ISO/IEC 27003 est un document de 85 pages comprenant 9 chapitres :

- Introduction (chapitres 1 à 3)
- Le synoptique d'un SMSI (chapitre 4)
- L'approbation du projet SMSI (chapitre 5)
- Le séquencement de la phase PLAN (chapitres 6, 7, 8)
  - Posture de contribution au business et périmètre : « ISMS scope »
  - Objectifs, critères d'appréciation du risque : « ISMS policy »
  - L'analyse de risque brut et net (couverture existante des vulnérabilités.)
  - Instruire les mesures de sécurité (réduction du risque) applicables
  - Décision de traitement du risque et cible de risque résiduel, et la déclaration d'applicabilité
- La préparation de l'implémentation de la phase DO (chapitre 9)

5.2 Résumé des chapitres 5 à 9

Dans cette partie, les chapitres 5 à 9 sont résumés et analysés. Leur utilisation effective est évaluée à partir de l'expérience du groupe de travail du CLUSIF

 © CLUSIF 2011

<u>Chapitre 5</u> : Obtenir l'approbation de la direction pour initialiser un projet SMSI

Ce chapitre traite de l'obtention, auprès de la direction, de l'accord de démarrer un projet SMSI. Cet accord s'appuie sur une proposition structurée et compréhensible. Celle-ci décrira les priorités et les objectifs de mise en œuvre ainsi que la structure organisationnelle du SMSI et le plan du projet initial.

Ce document doit permettre aux responsables et collaborateurs de l'organisation de :

- comprendre l'intérêt de mettre en place un SMSI,
- clarifier les rôles et responsabilités propres à l'organisation et nécessaires au projet de SMSI (5.3.2).

Les livrables attendus seront l'accord de la direction pour démarrer la mise en œuvre d'un SMSI et pour la réalisation des actions décrites dans ce document. Ils incluent une proposition structurée décrivant les étapes clefs du plan du projet SMSI.

Les principales étapes consistent à :

- Définir, dans un document, les priorités de l'organisation pour développer un SMSI. Il résumera :
  - (5.2) les objectifs,
  - les priorités de sécurité de l'information,
  - les exigences organisationnelles pour un SMSI.

  Ce document comprendra :
  - une liste des besoins réglementaires, contractuels, et techniques impactant la sécurité de l'information,
  - les caractéristiques principales de l'activité, de l'organisation, de sa localisation, de ses ressources et de sa technologie.
- Définir le périmètre initial du SMSI (5.3.1) en décrivant les rôles et responsabilités et l'organisation nécessaires au succès de la mise en œuvre du SMSI.
- Créer la proposition et le plan projet pour l'approbation de la direction (5.4) en précisant les ressources allouées et les jalons clés tels que l'exécution de l'acceptation de risque, l'implémentation, les audits internes et le suivi du projet par la direction.

Le point de vue du Groupe de travail : Ce chapitre de la norme apporte quelques précisions intéressantes par rapport à l'ISO/IEC 27001, toutefois, il manque des exemples concrets ce qui aurait pu faciliter cette étape.

<u>Chapitre 6</u> : Définir le domaine d'application, les limites et la politique du SMSI

Ce chapitre définit le champ d'application détaillé et élabore la politique du SMSI.

Note : il est prématuré de prendre ces décisions avant d'avoir réalisé l'analyse de risque, car les objectifs et les priorités doivent en résulter normalement.

Les facteurs clé pour une implémentation réussie du SMSI sont :

- la définition détaillée du périmètre et du champ d'application,
- la définition de la politique du SMSI
- l'acceptation et le soutien par la direction.

Les principales étapes consistent à :

- Définir le périmètre organisationnel (6.2) par la description :
  - du champ d'application organisationnel du SMSI, en justifiant l'exclusion de certaines parties ;
  - des fonctions et de la structure des parties de l'organisation incluses dans le champ d'application ;
  - des informations échangées à l'intérieur du champ d'application et de celles échangées à travers les frontières ;
  - des processus organisationnels et des responsabilités pour les ressources informationnelles à l'intérieur et à l'extérieur du champ d'application ;
  - du processus et de la structure de prise de décision de la hiérarchie dans le SMSI.
- Définir le champ d'application des technologies d'information et de communication (TIC) (6.3) par la description :
  - des flux d'informations transitant à l'intérieur du champ d'application et à travers ses frontières ;
  - des frontières des TIC pour le SMSI, en justifiant l'exclusion des TIC liées aux parties qui sont hors du périmètre organisationnel ;
  - des SI et des réseaux de télécommunication en précisant ce qui est dans le champ d'application, y compris les rôles et responsabilités de ces systèmes. Les systèmes exclus seront listés brièvement.
- Définir le périmètre physique et des frontières physiques (6.4) en indiquant les justifications d'exclusion de celles-ci et en indiquant l'organisation et les caractéristiques géographiques correspondant au périmètre.
- Rédiger un document décrivant le périmètre et les frontières du SMSI (6.3) contenant :
  - les caractéristiques clés de l'organisation (fonction, structure, services, ressources et leur champ d'application) ;
  - les processus organisationnels du champ d'application ;
  - les configurations des équipements et réseaux du champ d'application ;
  - une liste initiale des ressources à l'intérieur du champ d'application ;

- une liste des ressources TIC du champ d'application (ex. serveurs) ;
- un plan des sites du périmètre en précisant les frontières physiques du SMSI ;
- les descriptions des rôles et responsabilités à l'intérieur du SMSI et leurs relations avec les structures organisationnelles ;
- le détail et les justifications de toute exclusion du périmètre.

- Elaborer la politique du SMSI et obtenir l'approbation de la direction (6.6) dans un document décrivant la politique du SMSI documentée et approuvée par la direction. Il sera validé dans une phase ultérieure du projet dans la mesure où il dépend du résultat de l'évaluation des risques.

Le point de vue du Groupe de travail : C'est probablement, le chapitre le plus utile de la norme, il éclaire sur les clauses 4.2.1a (Define the scope and boundaries of the ISMS) et 4.2.1b (Define an ISMS policy) de l'ISO/IEC 27001 en expliquant clairement comment déterminer un périmètre et fournissant des conseils sur la manière de rédiger la politique du SMSI.

Les actions mentionnées dans les chapitres 6 à 8 sont décrites aussi dans les méthodes récentes d'évaluation de risque.

<u>Chapitre 7</u> : Conduire l'analyse des exigences de sécurité de l'information

L'objectif est de définir les exigences que doit considérer le SMSI à partir de l'identification des actifs et de l'analyse des enjeux à préserver lors d'une atteinte des critères de sécurité (Disponibilité, Intégrité, Confidentialité) qui leur sont rattachés.

Les principales étapes consistent à :

- Définir les exigences de sécurité de l'information intégrées dans le processus de SMSI (7.2)
  - Identification préliminaire des actifs informationnels importants et des exigences essentielles (liées au métier, aux engagements pris et aux obligations légales) ;
  - Identification des visions de la direction, du niveau de sensibilisation des parties prenantes et des besoins en éducation et expertise concernant l'information ;
  - Identification des processus et des éléments utilisés pour traiter, stocker et véhiculer l'information, classification des actifs utilisés et liste des vulnérabilités connues à adresser.
- Identifier les actifs dans le domaine d'application (7.3)
  - Réaliser une cartographie des actifs primordiaux comme de support et les associer aux processus métiers ;
  - Cartographier les applications utilisées et identifier les propriétaires d'actifs ;
  - Classifier l'information, les services nécessaires à son traitement et les exigences de conformité.
- Conduire une évaluation de la sécurité de l'information.
  - Analyser le niveau actuel de la sécurité de l'information au travers des procédures et des mesures de sécurité en place.
    Dans le cas d'une organisation qui a déjà mis en place des mesures de sécurité, il est recommandé de faire une retro appréciation des risques, comme s'il n'y avait aucune mesure de sécurité en place afin de permettre la justification des mesures mises en œuvre et de supprimer celles qui sont inappropriées ;
  - Evaluer les besoins additionnels demandés par l'organisation.
    Il faut noter cependant que cette évaluation doit normalement résulter de l'évaluation de risques effectués dans le chapitre suivant.

Le point de vue du Groupe de travail: Outre les exigences en sécurité de l'information, ce chapitre donne quelques conseils sur la manière d'inventorier les actifs et processus associés, ceux-ci peuvent aider les responsables du SMSI.

Il aborde également les actions préliminaires à l'analyse des risques en expliquant comment réaliser une analyse des exigences en sécurité de l'information.

Sur cet aspect, la norme ISO/IEC 27005 fournit des directives plus complètes pour réaliser l'appréciation des risques

<u>Chapitre 8</u> : Conduire l'appréciation et la planification du traitement des risques

Ce chapitre introduit l'utilisation d'une méthodologie d'évaluation des risques, permettant d'identifier, analyser et évaluer les risques associés à l'information et à sélectionner les options de traitement du risque (réduire, conserver, éviter ou transférer) et planifier les objectifs de sécurité et les mesures appropriées.

La conformité de cette méthodologie aux directives données par la norme ISO/IEC 27005:2008 est mentionnée à cette occasion.

Les principales étapes consistent donc à :

- Réaliser l'évaluation des risques (8.2), c'est à dire :
  - Identifier les menaces et les vulnérabilités qu'elles peuvent exploiter ;
  - Identifier les impacts d'une atteinte aux actifs et les conséquences sur les affaires ;
  - Evaluer la vraisemblance des scénarios d'incidents et les niveaux de risque associés, puis les classifier.
- • Sélectionner les objectifs de sécurité et les mesures à prendre (8.3)
  - Il importe de justifier la relation entre les risques et les options choisies pour les traiter ;
  - En particulier, il faut indiquer comment les mesures de sécurité choisies dans le plan de traitement pourront réduire les risques ;
  - Lors de cette appréciation, l'audit des mesures déjà en place doit permettre de faciliter les mesures additionnelles nécessaires ;
  - L'attention doit être portée sur la confidentialité des actions effectuées et planifiées.
- Obtenir l'approbation de la direction pour réaliser un SMSI (8.4)
  - Documenter les résultats de l'évaluation des risques ;
  - Réaffirmer l'intérêt du SMSI pour les affaires et préparer un plan projet ;
  - Collecter et documenter la politique du SMSI et les frontières.

Le point de vue du Groupe de travail : Comme pour le chapitre précédent, la norme ISO/IEC 27005 fournit des directives plus complètes pour réaliser l'évaluation des risques.

Les méthodes d'évaluation et de traitement des risques capables de proposer les mesures de sécurité (organisationnelles et techniques) répondent à ce chapitre. C'est le cas de MEHARI avec sa base de connaissance.

<u>Chapitre 9</u> : Concevoir le SMSI

Le chapitre 9 explicite la démarche à suivre pour élaborer un plan projet détaillé portant sur la mise en place du SMSI (Système de Management de la Sécurité de l'Information) et rappelle les pré requis :

- l'engagement de la direction ;
- l'identification des actifs ;
- l'analyse du niveau de sécurité informatique actuel et le plan de gestion des risques.

Les principales étapes consistent à :

- Définir l'organisation en charge de la sécurité informatique (9.2.1) par la définition des fonctions dans l'organisation, les responsables et les processus nécessaires au SMSI.
- Définir la gestion documentaire (9.2.2) en détaillant la documentation et les enregistrements nécessaires au SMSI. La gestion documentaire comprend :
  - le format de la documentation et des enregistrements
  - les processus pour les obtenir et les présenter à la direction
- Elaborer la politique de sécurité de l'information (9.2.3) en détaillant la présentation des orientations stratégiques de la direction pour la sécurité de l'information. La norme donne une approche pragmatique pour la création de la politique de sécurité informatique. Elle insiste sur son importance pour la motivation des acteurs du SMSI.
- Elaborer les référentiels et les procédures de sécurité de l'information (9.2.4) par la sollicitation des acteurs de l'organisme qui ont un rôle dans la sécurité informatique pour un travail d'équipe en vue de créer les standards et les procédures de sécurité informatique. Ils s'appuieront notamment sur les normes ISO/IEC 27001 et ISO/IEC 27002 pour leur production de documents. Le fruit de ce travail donne les mesures de sécurité à mettre en place dans l'organisation.
- Créer des mesures de sécurité pour la protection physique et l'exploitation Informatique et Télécom (9.3) en précisant les mesures techniques détaillées de sécurité informatique en faisant le lien avec la sensibilisation à la sécurité informatique et en mettant aussi l'accent sur l'intégration des mesures de sécurité dans les processus existants de l'organisme.
- Planifier les revues de direction (9.4.1) pour obtenir le soutien de la direction et pour vérifier l'adéquation du SMSI au besoin métier de l'organisme. La norme donne une approche pratique pour ces revues de direction. Elle fait le lien avec le besoin de tableaux de bords et d'audits internes du SMSI.
- Définir les actions de sensibilisation et de formation à la sécurité informatique (9.4.2) en détaillant les formations indispensables aux acteurs du SMSI. Elles doivent aider à obtenir leur adhésion et leur faire acquérir les compétences pour mettre en œuvre les mesures de sécurité. La norme détaille les thèmes à aborder, insiste sur le besoin de mettre à jour les formations et de contrôler la participation des utilisateurs.
- Produire le plan projet final pour le déploiement du SMSI (9.5) en précisant les acteurs, les outils, les méthodes et les tâches planifiées qui permettront une mise en place réussie du SMSI.

Ce chapitre éclaire les activités nécessaires pour aboutir à une mise en place réussie de la phase de déploiement du SMSI.

Les annexes donnent au lecteur des informations pour aller dans le détail de ces activités.

Le point de vue du Groupe de travail : Ce chapitre apporte une aide intéressante pour la définition de la politique de sécurité du SMSI. Toutefois, au niveau des exigences de rédaction de la documentation associée à la mise en place du SMSI, elle se contente de paraphraser l'ISO/IEC 27001.

6. Conclusion

C'est par l'appropriation de la méthode mise en œuvre et de ses résultats, en l'intégrant dans un vrai processus d'amélioration continue, que la norme ISO/IEC 27001 apporte une nouveauté (en obligeant à en faire des utilisations plus formalisées : savoir-faire). Elle propose également une validation externe (la certification, faire savoir) permettant d'établir la motivation au sein de l'organisation comme la confiance auprès de ses partenaires.

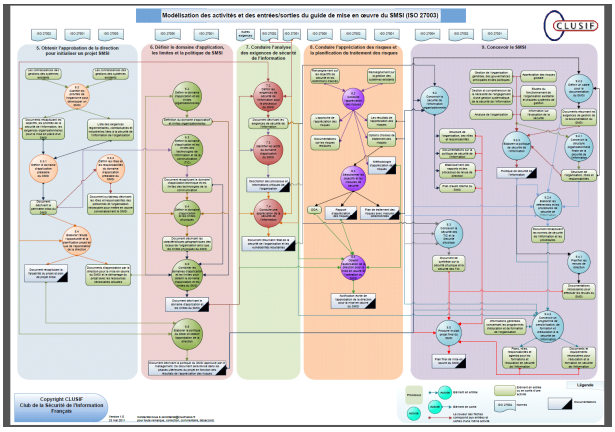
ISO/IEC 27003 est un guide d'implémentation pour un SMSI. Cette norme est centrée sur la réalisation d'un plan pour implémenter le SMSI et insiste sur la démarche d'approbation de la direction de l'organisation. Il s'agit d'une approche certes limitée essentiellement à la phase PLAN mais qui facilite l'obtention des investissements initiaux, tout en risquant d'entraîner un retard dans la réalisation du SMSI lui-même.

Cette approche n'est pas développée dans la norme ISO/IEC 27001, qui mentionne l'engagement de la direction comme étant précédemment acquis, et qui se focalise sur les phases de la démarche PDCA (Planifier, Développer, Contrôler, Améliorer) comme si elles étaient « naturelles » dans l'esprit des responsables. Le concept d'amélioration continue formalisé par ISO/IEC 27001 étant novateur, ISO/IEC 27003 peut être utile pour en préparer la réalisation et en obtenir le financement sur le long terme.

Une des difficultés de compréhension de la norme ISO/IEC 27003 est que celle-ci est ambiguë car elle peut être comprise comme une aide à l'étape préalable à la mise en place du SMSI, consistant à obtenir l'approbation du management pour le projet alors qu'elle se veut être une aide à la mise en place une fois cette décision prise.

Un schéma, modélisant les activités et entrées/sorties décrites dans la norme ISO/IEC 27003, a été réalisé par le groupe de travail, et est disponible en téléchargement à l'adresse ci-dessous.

.



http://www.clusif.asso.fr/fr/production/ouvrages/pdf/CLUSIF-2011-Modelisation-ISO-27003.pdf

L'ESPRIT DE L'ÉCHANGE

CLUB DE LA SÉCURITÉ DE L'INFORMATION FRANÇAIS

11, rue de Mogador
75009 Paris
✆ 01 53 25 08 80
clusif@clusif.asso.fr

Téléchargez les productions du CLUSIF sur

www.clusif.asso.fr