Gérôme BILLOIS - Responsable du département Sécurité des Systèmes d'Information - Solucom
gerome.billois@solucom.fr - http://www.solucom.fr
Jean-Philippe HUMBERT - Doctorant au Centre de Recherche sur les Médiations (CREM) – Université Paul Verlaine de Metz
jph54@orange.fr
Nicolas MAYER - Ingénieur R&D – Centre de Recherche Public Henri Tudor – Luxembourg
Doctorant à l'Institut d'Informatique de l'Université de Namur - Belgique
nicolas.mayer@tudor.lu – http://nmayer.eu

ISO 2700x : une famille de normes pour la gouvernance sécurité

Les normes sont utilisées dans tous les actes de la vie économique. Elles représentent un langage commun et un lien nécessaire entre les divers acteurs concernés. Aujourd'hui, la normalisation s'intéresse fortement au domaine de la sécurité de l'information en proposant depuis peu un modèle de gouvernance par l'intermédiaire de la norme ISO/IEC 27001 et de la certification associée.

1. Introduction

Pour reprendre M. le Président de l'Association de Normalisation pour la Société de l'Information Luxembourg (ANSIL) : « *Les normes et les standards, ce sont des référentiels que nous côtoyons tous les jours, que ce soit dans le cadre de notre activité professionnelle, mais aussi dans la vie personnelle, dans les produits que nous consommons et les services dont nous bénéficions. Pensez simplement au format de la feuille A4, aux nombreuses camionnettes dont le logo est « affublé » d'une mention « certifié ISO 9001 » mais également au standard SMTP (Simple Mail Transfer Protocol) définissant le cadre unifiant les caractéristiques des messages électroniques* » [1]. Ainsi définies, les normes apportent quotidiennement une aide non négligeable pour tout utilisateur que nous représentons. Nous montrerons que cela est également vrai dans le domaine de la sécurité de l'information.

Cet article est organisé en 3 volets. Le premier est dédié à la normalisation et à l'organisme international ISO. Le deuxième présente les actions en cours au niveau de la sécurité de l'information et en particulier via la famille de norme ISO 2700x. Enfin, le troisième volet détaille la norme ISO 27001[1], aussi bien au niveau de son contenu, que de la possibilité de reconnaissance internationale qu'elle procure par l'intermédiaire de la certification. La conclusion revient sur l'apport de ces normes au quotidien dans une organisation et sur l'intérêt de viser la certification.

2. Concept de normalisation et l'organisme international ISO

"La normalisation a pour objet de fournir des documents de référence comportant des solutions à des problèmes techniques et commerciaux concernant les produits, biens et services qui se posent de façon répétée dans des relations entre partenaires économiques, scientifiques, techniques et sociaux". [2]

La normalisation a permis de déterminer et de dégager des normes, que chacun utilise dans le but de faciliter les échanges, les pratiques, et les significations. Parmi les normes formulées, diffusées et mises en application, nous pouvons distinguer différents types : les normes de base, de portée générale, de terminologie, d'essai, de produit, de processus, de service, d'interface ou encore portant sur des données. Elles peuvent relever de diverses catégories, à savoir : les "Normes internationales", puis les "Normes européennes", enfin, les "Normes nationales", respectivement adoptées par un organisme international, européen, et national de normalisation. L'ensemble produit est toujours disponible auprès des organismes de normalisation.

Une norme est, selon le guide ISO/CEI 2, « *un document de référence couvrant un large intérêt industriel et basé sur un processus volontaire, approuvé par un organisme reconnu, fourni pour des usages communs et répétés, des règles, des lignes directrices ou des caractéristiques, pour des activités, ou leurs résultats, garantissant un niveau d'ordre optimal dans un contexte donné* ». L'élaboration de normes consiste donc à réunir le consensus, c'est-à-dire prendre en compte les points de vue de tous les intéressés, aussi bien public que privé, clients que fournisseurs… La

[1] Pour cet article, nous adopterons la convention suivante : les normes seront citées « ISO XXXXX » en lieu et place de leur dénomination officielle « ISO/IEC XXXXX » et ce sans spécifier la date de parution, nous référant pour chacune à la dernière version.

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

Au niveau mondial, l'ISO [3] a pour missions l'élaboration de normes applicables, la promotion du développement de la standardisation et activités annexes, ainsi que le développement des coopérations dans les sphères d'activités intellectuelles, scientifiques, technologiques et économiques. Cet organisme, plus communément connu sous le label *International Organization for Standardization*, ou encore Organisation Internationale de Normalisation, correspond en fait au terme grec « *Isos* » signifiant « égal ». Sa création remonte à 1947 et il se compose actuellement de 156 membres (organismes nationaux de normalisation). Les résultats principaux de ses travaux se formalisent à travers la publication des standards internationaux : les normes ISO.

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

3. Le sous-comité ISO/JTC1/SC27

Les attributions de l'ISO couvrent de nombreux domaines et champs de compétences. Pour traiter certains d'entre eux, l'ISO a développé une instance conjointe avec le CEI (Commission Electrotechnique Internationale), datant de 1987 et dénommée JTC1 [4] (*Joint Technical Committee*), traitant spécifiquement du domaine des TI (Technologies de l'Information). Le JTC1 est subdivisé en dix-sept sous-comités dont chacun traite un domaine particulier. Le SC 27 est celui qui retient toute notre attention, traitant du champ « *IT Security Techniques* » (ou « Techniques de sécurité des technologies de l'information »).

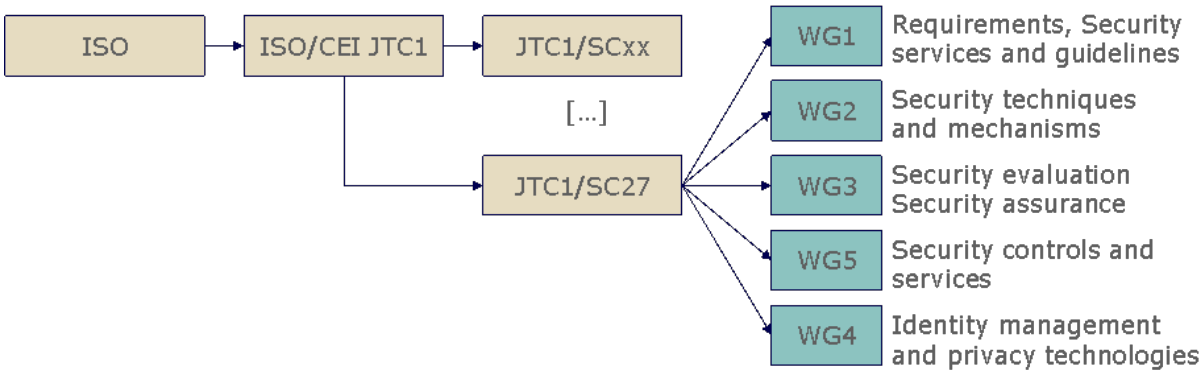

Figure 1 : Comités ISO et Working Groups

Le SC 27, composé de représentants de 47 pays, couvre la normalisation des techniques et des méthodes génériques pour les besoins de sécurité des TI. Dans cette perspective, nous distinguons deux axes forts : l'identification des besoins généraux pour les services de sécurité de l'information et le développement des mécanismes et des techniques associés.

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

- **WG1 - « *Exigences, services de sécurité et directives* »** ayant pour axe de travail le système de gestion de la sécurité de l'information, avec la récente définition de la série 2700x, déclinant une dizaine de normes touchant à la sécurité des systèmes d'information et de communication, dont ISO 17799 (future ISO 27002), ISO 27001, ISO 27005…
- **WG2 - « *Techniques et mécanismes de sécurité* »** traitant de la cryptologie (techniques et algorithmes de chiffrement par exemple).
- **WG3 - « *Critères d'évaluation de la sécurité* »** ayant les Critères Communs (ISO 15408) pour domaine de travail principal (précisant les critères d'évaluation pour la sécurité des TI).
- **WG4 - « *Services et contrôles de sécurité* »** traitant des anciens champs du WG1 ne relevant pas de la nouvelle série 2700x (ISO 18028 sur les architectures de sécurité…).
- **WG5 - « Sécurité biométrique, identité et vie privée »** dédié au domaine de la biométrie et du respect de la vie privée (ISO 24760 par exemple).

Cette déclinaison du SC 27 en cinq WG est très récente (2006), et se met en place progressivement. Depuis, de nombreuses normes se développent rapidement dans chaque WG.

4. WG1 et normes ISO 2700x

Depuis déjà de nombreuses années, la sécurité de l'information est devenue une préoccupation importante au sein des organisations et des entreprises. Le British Standard Institute (BSI) fut, en 1995, le premier organisme à publier une norme dans ce domaine, appelée BS 7799, qui définissait les bonnes pratiques pour la sécurité des systèmes d'information. L'ISO lui a emboîté le pas et a publié de nombreuses normes dans le même domaine, telle que la norme ISO 17799, issue de BS 7799, ou ISO 13335 (lignes directrices pour la gestion de la sécurité). Ces différentes normes visent à assurer la sécurité de l'information, que son support soit de nature électronique ou papier, et que la cause des incidents potentiels soit accidentelle ou délibérée. Cependant, au vu des besoins et de la demande grandissante du marché, l'ISO a depuis peu entrepris une refonte de l'ensemble de ses normes dans l'objectif d'aller au-delà des bonnes pratiques et de proposer un modèle de gouvernance de la sécurité de l'information.

Le WG1 est le groupe de travail chargé de rédiger et d'organiser les différentes normes ayant trait à ce domaine en un ensemble cohérent. Le résultat de cette (r)évolution du monde de la sécurité de l'information est l'émergence de la famille de normes ISO 2700x, définie de manière à devenir le pendant de la sécurité au regard de la série des 900x pour le domaine de la qualité et 1400x pour l'environnement. Le principal point commun entre ces séries de normes est une approche processus, articulée autour de la méthode Plan-Do-Check-Act (PDCA) ou « roue de Deming », afin d'atteindre une amélioration continue.

Au cœur de la famille 2700x se trouve la notion de « Système de Gestion de la Sécurité de l'Information » (SGSI) ou *Information Security Management System* (*ISMS)* en anglais. Un SGSI définit le cadre d'une amélioration continue de la sécurité de l'information, en se basant principalement sur une approche de gestion des risques. Pour le moment, huit normes sont en développement au sein de la série 2700x, dont une seule a déjà été publiée : ISO 27001 définissant les exigences requises pour la certification d'un SGSI. A terme, l'ensemble intégré des normes de la série des 2700x devrait permettre de former un modèle de gouvernance de la sécurité de l'information.

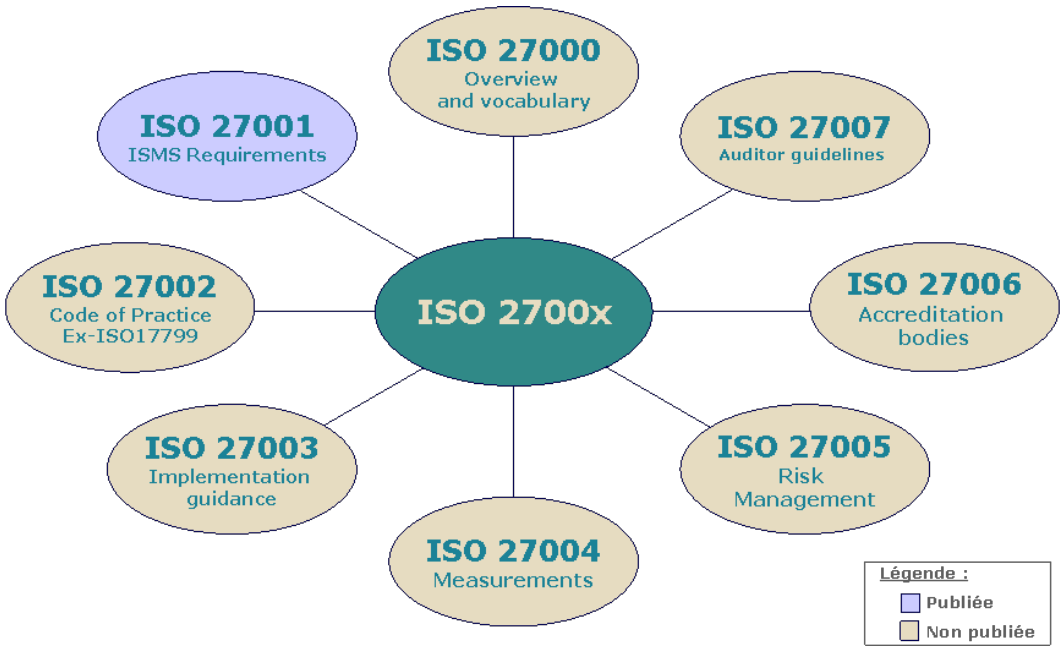

Figure 2 : Les normes de la série ISO2700x

•**ISO/IEC 27000:** ***Overview and vocabulary.*** Cette première norme définit les fondamentaux et le vocabulaire propres à la série. Elle est actuellement à son premier stade de construction, les premiers commentaires de la communauté ISO datant de juin 2006. Dès la sortie de cette norme, la première partie d'ISO 13335, traitant des concepts et modèles relatifs à la gestion de la sécurité

des TI, deviendra obsolète. A noter également que, suite aux résolutions de la dernière réunion plénière du SC27 tenue en Afrique du Sud (novembre 2006), il a été décidé de rendre disponible cette norme à titre gratuit.

- **ISO/IEC 27001:** ***ISMS requirements.*** La norme ISO 27001 correspond à la révision de la norme BS7799-2. Elle a été publiée en octobre 2005 et demeure à ce jour la seule norme de la famille 2700x dans ce cas. Elle est à la base de la certification d'un SGSI à l'instar de ces homologues ISO 9001 pour la qualité et ISO 14001 pour l'environnement. Il faut également noter que depuis sa publication, la norme BS 7799-2, dont la dernière révision datait de 2005, est obsolète.
- **ISO/IEC 27002:** ***Code of practice for information security management*****.** ISO 27002 sera la nouvelle dénomination de la norme ISO 17799 dont la dernière revue date de 2005. Aucune mise à jour sur le fond de la norme ne devrait accompagner la nouvelle numérotation. Sa publication est attendue pour avril 2007.
- **ISO/IEC 27003:** ***ISMS implementation guidance.*** La norme ISO 27003 a pour objectif de fournir un guide d'aide à l'implémentation des exigences d'un SGSI. Cette norme sera plus particulièrement orientée sur l'utilisation du cycle PDCA et des différentes exigences requises à chaque étape du cycle. Sa publication est attendue pour octobre 2008.
- **ISO/IEC 27004:** ***Information security management measurements*****.** Cette norme a pour but d'aider les organisations à mesurer et à rapporter l'efficacité de l'implémentation de leur SGSI. Sa publication est attendue pour fin 2006 – début 2007.
- **ISO/IEC 27005:** ***Information security risk management.*** La norme ISO 27005 est une évolution de la norme ISO 13335. Elle reprendra les parties 3 et 4 de cette dernière, définissant les techniques à mettre en œuvre dans le cadre d'une démarche de gestion des risques. Sa publication est attendue entre 2008 et 2009.
- **ISO/IEC 27006:** ***Requirements for the accreditation of bodies providing certification of ISMS.*** Cette norme, actuellement en cours de validation, a pour but de guider les organismes de certification sur les exigences nécessaires à atteindre pour être accrédités en tant qu'organisme de certification d'un SGSI. Elle devait paraître avant la fin de l'année 2006.
- **ISO/IEC 27007:** ***Auditor guidelines.*** Rentrée très récemment en période d'étude, cette norme va être un guide spécifique pour les audits d'ISMS, notamment en support à l'ISO 27006.

L'ensemble de ces normes constitue des standards internationaux. Elles sont donc destinées à tout type de société, quelle que soit sa taille, son secteur d'activité ou son pays d'origine. Elles ont donc pour but de décrire un objectif à atteindre et non la manière concrète d'y arriver, cette dernière étant généralement dépendante du contexte de l'organisation.

Actuellement, aucun autre numéro de la série 2700x n'est spécifiquement attribué. Cependant, les numéros allant de 27000 à 27010 sont réservés au sein de l'ISO pour la documentation générale d'un SGSI. Il est donc à prévoir que d'autres normes s'ajoutent à celles actuellement en développement. Par ailleurs, la série 27011 à 27019 est d'ores et déjà réservée à des normes dédiées à la spécification d'un SGSI pour des secteurs économiques spécifiques (secteur financier, télécommunication par exemple).

5. Construire un SGSI : la roue de Deming appliquée à la sécurité

Avant d'aborder le volet de la certification, il nous semble important de détailler le contenu d'ISO 27001 et du concept de SGSI qu'elle propose. Cette norme précise les moyens à mettre en œuvre (aussi bien humain que technique), l'organisation à déployer et la démarche de construction et de pérennisation à suivre. Il s'agit d'une norme de certification comme nous le verrons dans la troisième partie de cet article. La certification peut être un objectif recherché mais il n'est pas le seul avantage à retirer de la norme ISO 27001. En effet une organisation peut décider de suivre les principes avancés sans pour autant viser la certification. Les sections ci-dessous détaillent les concepts présents dans ISO 27001 et abordent des pistes de mise en œuvre.

La mise en œuvre du SGSI se réalise en quatre étapes. Il est important de signaler que la norme vise à la mise en œuvre d'un processus et n'impose pas un niveau de sécurité minimum. Il s'agit principalement de dire ce que l'on va faire (« plan »), de faire ce que l'on a dit (« do »), de contrôler ce que l'on a fait (« check »), de corriger et d'améliorer dans le temps (« act »). Mettre en œuvre un SGSI représente donc un changement important par rapport aux démarches habituellement rencontrées. L'objectif n'est pas d'écrire toutes les règles que l'on souhaite voir implémentées, mais de se concentrer sur les mesures de sécurité à mettre en œuvre à court terme sur un périmètre défini. Ces mesures doivent en particulier répondre à des risques clairement identifiés et documentés. La norme

pose également des principes de base essentiels, tels que l'attribution de ressources (autant financières qu'humaines) dédiées à la sécurité, ainsi qu'un suivi et une approbation régulière du niveau de sécurité au plus haut niveau de l'organisation.

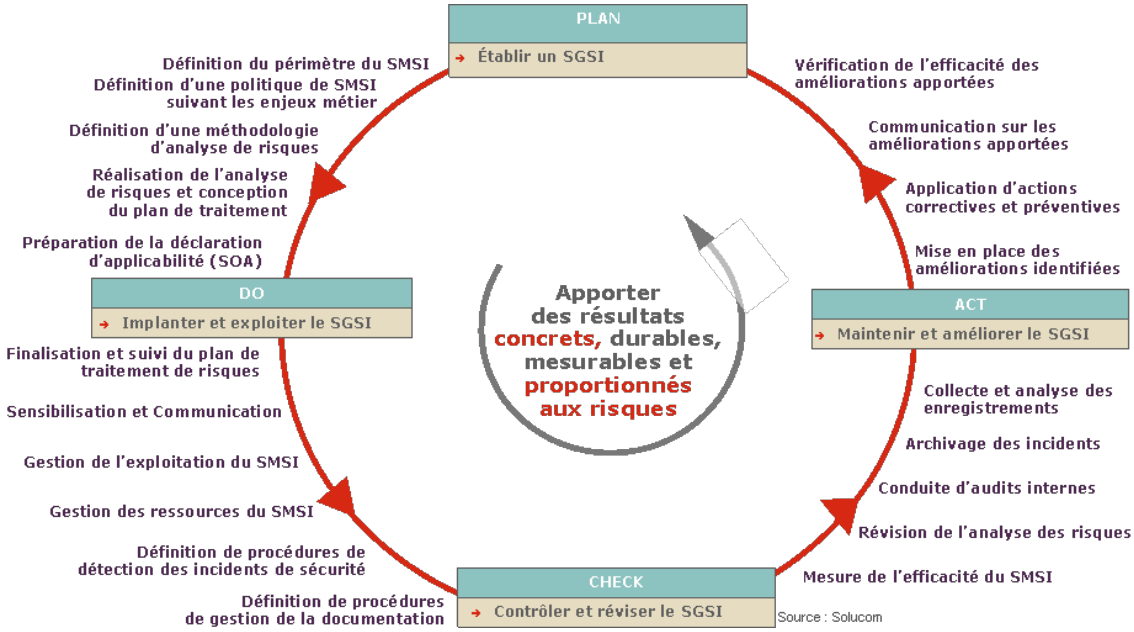

Figure 3 : Le cycle de vie du SGSI

5.1 Planification (Plan)

La phase de planification consiste à établir les bases du SGSI. Il s'agit de définir :

•Le périmètre : un SGSI s'applique à un périmètre précis. Le périmètre doit être clairement délimité et correspondre à une réalité pour l'entreprise (par exemple les processus de la Direction des Systèmes d'Information, un processus métier « visible », un ou plusieurs sites associés à un processus). Celui-ci doit être cohérent par rapport aux enjeux et aux besoins de la société, de plus sa définition doit être claire et précise afin de ne pas créer d'ambiguïté ultérieure. Plus le périmètre du SGSI est vaste, plus il sera difficile à construire et à maintenir dans le temps. Si la certification est visée, cette information peut être communiquée aux partenaires externes le demandant.

> **Exemples de périmètre de sociétés certifiées [5] :**
>
> Samsung Networks (Korea): the information security management system in all activities related with 'SAMSUNG WYZ070' Internet Telephony Service.
>
> AXALTO Barcelona (Spain): Personalization process including data reception from the customer and its processing, smart cards and mailers personalization, packaging and shipment, and key management.
>
> PERN (Poland): Pumping (pipe transporting) and storage of oil and final (refined) products and all the processes connected therewith.

•La politique du SGSI : ce document regroupe les principes fondamentaux du SGSI et identifie les enjeux propres à la société (apports, risques, entités concernés…). La politique résume également les contraintes légales et réglementaires devant être respectées et montre l'engagement de la direction générale dans le projet. Cette validation est un pré-requis de la démarche ISO 27001.

•L'analyse des risques : l'ensemble de la démarche ISO 27001 est centré sur le concept d'analyse des risques. Celle-ci doit être réalisée régulièrement et permet de réorienter le SGSI en fonction de l'évolution des besoins et des menaces. Pour que ces résultats soient fiables et comparables, une méthode d'analyse des risques doit être choisie. Il est possible d'utiliser des méthodes connues et ayant fait leur preuve (EBIOS par exemple) ou de définir une méthode interne spécifique. La méthode choisie devra respecter les contraintes imposées par la norme ISO

27001, la difficulté résidant principalement dans la définition de critères de risques et la définition du niveau de risque acceptable pour l'organisation.

Cette méthodologie devra être appliquée une première fois pour identifier les actifs et leurs propriétaires, les menaces et les vulnérabilités les concernant, l'impact et la probabilité de réalisation des risques identifiés. Mettre en place une démarche d'analyse des risques systématique et périodique représente un des changements majeurs apportés par la norme ISO 27001.

•Le traitement des risques : Pour chacun des risques identifiés lors de l'analyse initiale, une décision doit être prise et acceptée au plus haut niveau de l'organisation. Les risques peuvent ainsi être:

- ○réduits en appliquant des mesures de sécurité,
- ○transférés (par exemple avec une assurance),
- ○évités (par exemple en arrêtant un service),
- ○acceptés en fonction de critères préalablement définis et s'ils ne remettent pas en jeu l'activité de la société.

•La déclaration d'applicabilité (SOA ou *Statement Of Applicability*) : ce document définit quels contrôles de sécurité seront mis en œuvre dans le périmètre du SGSI. A minima, il s'agit de parcourir l'ensemble des contrôles issus de l'annexe A de la norme ISO27001 (correspondant aux contrôles décrits dans ISO 17799) et d'indiquer si l'on sélectionne ou non le contrôle et pourquoi. Dans le cadre de la certification, ce document peut être communiqué à des partenaires externes.

Réf.	Mesure	Inclus	Commentaire et référence documentaire
A.6.1	**Internal organization** Objective: To manage information security within the organization.		
A.6.1.1	**Management commitment to information security** Control: management shall actively support security within the organization [...]	Oui	Référence: compte-rendu de décision du COMDIR du 31/03/2006, XX-XX-XX-001
A.6.1.2	**Information security co-ordination** Control: Information security activities shall be coordinated by [...]	Oui	Référence: Note d'organisation de la sécurité du SI, NOT-SSI-0002-ORGA, §3.3
[...]			
A.10.9	**Electronic commerce services** Objective: To ensure the security of electronic commerce services, and their secure use.		
A.10.9.1	**Electronic commerce** Objective: Information involved in electronic commerce passing over public networks shall be protected from fraudulent activity, contract dispute, and unauthorized disclosure and modification.	**Non**	Le périmètre du SMSI ne couvre aucune activité de commerce électronique. Note d'organisation du service YYYYYY-XX

Source : Solucom

Figure 4 : Exemple de SOA

L'ensemble de ces décisions doit être validé et approuvé par la direction générale de l'organisation mettant en œuvre le SGSI. Des traces de l'ensemble des étapes de validation doivent être conservées.

Documents liés : périmètre du SGSI, politique du SGSI, méthodologie d'analyse des risques, compte-rendu de l'analyse des risques, pour la certification : déclaration d'applicabilité.

5.2 Déploiement (Do)

Il s'agit de l'étape de mise en œuvre concrète du SGSI. Elle consiste à réaliser les actions suivantes :

•Finalisation du plan de traitement des risques et mise en œuvre des contrôles sélectionnés : il s'agit de décliner opérationnellement les décisions prises lors de l'analyse des risques. Les contrôles sélectionnés dans le SOA et les contre-mesures identifiées doivent être mis en œuvre selon des priorités particulières, avec des ressources définies et approuvées au bon niveau.

Concrètement, il s'agit dans un premier temps de concevoir les différents documents formalisant les processus « sécurité ». Ceux-ci peuvent être des directives techniques, un plan de sensibilisation, un plan de contrôle, des procédures opérationnelles, des guides de sécurisation… Dans un deuxième temps, les opérations techniques de mise en œuvre sont réalisées (nouvelles architectures, nouveaux services de sécurité…).

- Réalisation des actions de sensibilisation et de formation : l'ISO met en avant l'importance de la sensibilisation et de la formation dans le programme sécurité. La mise en œuvre de ces actions doit être large et complète afin de couvrir l'ensemble des personnes ayant des responsabilités formelles dans le fonctionnement du SGSI, mais également tous ceux pouvant être confrontés à la sécurité de l'information (ceci inclut l'ensemble des utilisateurs, mais également les tiers ou les personnes intervenant temporairement dans le périmètre de la société).

- Définition des procédures de gestion et de suivi des incidents : savoir gérer un incident et surtout éviter qu'il ne se reproduise est un élément essentiel d'une démarche sécurité. La norme insiste particulièrement sur cet aspect. La mise en œuvre de cette démarche demande des efforts importants, aussi bien d'un point de vue organisationnel que technique : définition des critères de qualification des incidents, des processus d'alertes, adaptation des processus de gestion des incidents informatiques, mise en place d'une cellule de gestion opérationnelle de la sécurité, analyse des journaux pour identifier les comportements anormaux, déploiement de systèmes techniques pour éviter de nouveaux incidents….

- Définition des indicateurs de suivi du SGSI : les indicateurs doivent donner une vue concrète et fiable de l'efficacité des contrôles mis en œuvre. La norme ISO 27004 donnera des recommandations quant aux indicateurs à sélectionner et la manière de les collecter. Cette démarche doit cependant rester pragmatique et légère en essayant d'automatiser au maximum le processus de collecte, de mise en forme et de publication. Ces indicateurs, même en nombre limité, doivent être positionnés à tous les niveaux, qu'ils soient stratégiques, tactiques ou opérationnels, et doivent couvrir aussi bien le volet technique qu'organisationnel, afin d'offrir une vue cohérente du SGSI.

- Exploitation et gestion du SGSI au quotidien : le système doit fonctionner au quotidien afin de garantir la sécurité dans le temps. Les actions à réaliser ne sont pas forcément limitées aux périmètres informatiques ou sécurité, mais peuvent être liées à l'ensemble des activités métiers, suivant le périmètre définit précédemment. C'est de la phase d'exploitation et de gestion du SGSI que sont issues les informations nécessaires à la réalisation des tableaux de bord et à la gestion des incidents.

La phase de déploiement peut être longue et complexe pour une société décidant de s'aligner sur le modèle proposé par ISO 27001. Elle doit être progressive et surtout réaliste par rapport au contexte de la société en termes de planning et de capacité de contribution des acteurs. Une majorité de société dispose déjà d'un existant pour assurer la sécurité de l'information. Une bonne pratique consiste donc à l'identifier et à réaliser une analyse d'écart lors de la phase de planification, afin d'identifier les domaines où un effort particulier devra être porté.

Il est nécessaire pour ceux qui visent la certification de bien prévoir tous les mécanismes de gestion des documents, des preuves de réalisation des différentes actions et des traces techniques en vue de l'audit de certification.

Documents liés : plan de traitement des risques, plan de sensibilisation, tableaux de bord, toutes procédures relatives au SGSI (gestion des incidents, guide technique, directive…), pour la certification : procédure de gestion des traces et des preuves.

5.3 Contrôle (Check) et Amélioration (Act)

Les phases de contrôle et d'amélioration terminent la boucle de l'amélioration continue et permettent la mise en œuvre d'un système vertueux. Ces étapes, souvent présentes dans les documents de politique de sécurité déjà existants, ne sont aujourd'hui que rarement déclinées dans leur intégralité. La norme ISO 27001 impose la réalisation de nombreux contrôles, un suivi régulier des résultats et la mise en œuvre des améliorations identifiées. Il s'agit d'un des changements majeurs par rapport aux pratiques habituellement rencontrées.

Le processus de contrôle comprend la réalisation d'audits internes, d'audits externes, l'organisation de collectes d'informations auprès des collaborateurs et des acteurs externes à la société. Ces actions de mesure et de contrôle permettent au management de juger de la pertinence des actions et des mesures de sécurité réalisées. Les tableaux de bords vont être le vecteur de la communication.

Dans le même esprit, des actions d'amélioration doivent être menées. En particulier, la réévaluation de l'adéquation du SGSI aux enjeux métier et l'approbation du management doivent être effectuées a minima annuellement. Au-delà de cette action phare, de nombreuses opérations doivent être réalisées : suivi des actions identifiées, démonstration de la réalisation des actions correctives…

Ces deux dernières phases ne s'improvisent pas, elles doivent faire l'objet d'une attention particulière et de moyens dédiés, afin de garantir la pérennité du SGSI dans le temps. Si la certification est visée, une gestion exemplaire des traces et des enregistrements doit être réalisée. La plupart des échecs constatés lors des certifications se joue sur ces aspects à long terme, de contrôle et d'amélioration continue.

Documents liés : plan de contrôle, ensemble des traces relatives aux contrôles, ensemble des traces relatives aux actions d'amélioration, ensemble des décisions d'amélioration prises, approbation régulière du management.

6. Viser la certification

La norme ISO 27001 est une norme de certification au même titre que les normes ISO 9001 ou ISO 14001. La certification garantit de manière indépendante que le SGSI est conforme aux exigences spécifiées, qu'il est capable de réaliser de manière fiable les objectifs déclarés et qu'il est mis en œuvre de manière efficace. Il est important de préciser que la certification vise le processus de gestion de la sécurité. Elle ne garantit donc pas un niveau de sécurité, mais plutôt la capacité d'améliorer dans le temps l'organisation et les processus liés à la sécurité de l'information. L'obtention de la certification permet la délivrance d'un certificat précisant le périmètre du SGSI mis en œuvre. Lorsqu'un organisme met en avant le fait qu'il ait obtenu la certification, il est essentiel d'étudier en détail le certificat et le contenu de la déclaration d'applicabilité (liste des contrôles mis en œuvre) afin de s'assurer que la certification porte bien sur un périmètre clé pour l'organisme et que les moyens mis en œuvre sont pertinents face aux risques encourus. En effet l'organisme visant la certification dispose d'une certaine latitude dans le choix des mesures à mettre en œuvre ce qui peut lui permettre d'obtenir une certification parfois partielle ou incomplète par rapport aux besoins exprimés. Il n'existe pas aujourd'hui de profil type spécifiant les contrôles minimums à mettre en œuvre pour une activité métier particulière (hébergeur, opérateurs, milieu hospitalier…). Il s'agit d'une des prochaines étapes envisageables dans le domaine de la certification ISO 27001.

6.1 Démarche

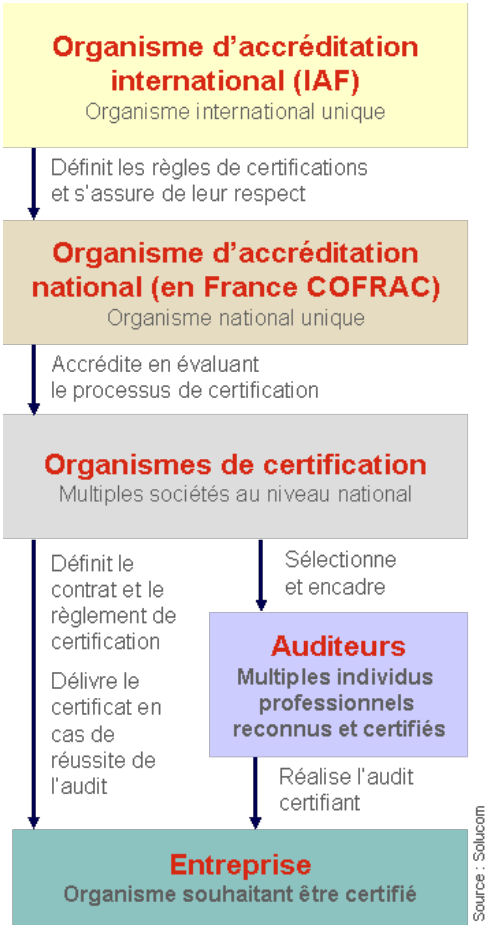

Figure 5 : Les acteurs et les étapes de la certification

Pour obtenir la certification, il est nécessaire de faire auditer son SGSI par un organisme de certification externe. Afin de garantir une légitimité internationale aux certificats émis, les organismes de certification sont contrôlés par un organisme d'accréditation propre à chaque pays (il s'agit, par exemple, du COFRAC [6] en France et de l'OLAS [7] au Grand-Duché de Luxembourg,). Les organismes d'accréditation sont eux-même évalués au niveau de l'IAF (*International Accreditation Forum*) et d'EA (*European co-operation for Accreditation*) afin de garantir l'homogénéité de leurs pratiques d'accréditation. La norme ISO 17021 (qui remplacera officiellement d'ici peu la norme EN 45012) est spécifiquement destinée à l'accréditation des organismes de certification de systèmes de management. Aujourd'hui en France, le seul organisme de certification accrédité pour la certification ISO 27001 est LSTI [8]. Cependant il est possible, dans le cadre d'un contrat international, que d'autres organismes de certification (BVQI, BSI, SGS…) interviennent sur le territoire français.

6.2 Audits

Très concrètement, l'entreprise signe avec un organisme de certification un contrat de trois ans, incluant la réalisation d'audits suivant un rythme défini avec l'entreprise, mais devant au minimum :

- assurer une vérification complète tous les trois ans. Il s'agit de vérifier intégralement le SGSI.
- réaliser des audits de surveillance annuellement. Il est cependant préférable de réaliser ces audits plus fréquemment, afin d'éviter de perdre la certification en cas de problème mineur nécessitant un temps de correction long.

Les audits sont réalisés en respectant les principes de la norme ISO 19011 (lignes directrices pour l'audit des systèmes de management). Une première phase de vérification documentaire devra être validée avant d'enchaîner sur les visites de sites. Lors de cette opération, les auditeurs réaliseront un ensemble de contrôles, techniques et organisationnels, pour vérifier que le SGSI « tourne », que les principes sélectionnés ont bien été mis en œuvre et que le système est pérenne.

Aujourd'hui les guides IAF GD 2: 2005 et EA7/03 définissent les conditions de l'audit (nombre de jours d'intervention, indépendance et qualification des auditeurs…). Cependant, la publication des normes ISO 27006 et 27007 permettra de préciser les conditions de réalisation des audits sur des points très concrets tels que :

- les critères permettant l'adaptation du nombre de jours d'audit en fonction de l'activité de la société et des mécanismes de sécurité mis en œuvre ;
- la typologie des tests techniques à réaliser lors des visites ;
- la cohérence entre l'analyse des risques et les objectifs du SGSI.

Suite à l'audit, les auditeurs feront parvenir leurs recommandations à l'organisme de certification qui approuvera les résultats et délivrera le certificat officiel. En cas de désaccord avec les résultats, il est possible de poser des recours auprès du comité de certification propre à l'organisme de certification, composé de représentants indépendants et spécialistes du domaine.

Lors des audits (initial, de surveillance ou de renouvellement) les auditeurs, s'ils identifient des points litigieux expriment la présence d'un écart. Ceux-ci peuvent, par exemple, être exprimés à trois niveaux différents : un écart majeur (il ne permet pas d'obtenir la certification), un écart mineur (il s'agit d'un problème important mais pouvant être corrigé dans le temps) ou une remarque (il s'agit d'un problème mineur ou d'une appréciation de l'auditeur sur la pertinence du SGSI mis en œuvre). Un écart découvert et non corrigé va voir sa criticité évoluer à chaque visite de surveillance. Si l'organisme ne le corrige pas dans le délai imparti, un écart mineur peut se transformer en écart majeur et entraîner la suppression de la certification.

6.3 Facteurs de risque et de coût

La mise en œuvre d'un SGSI dans l'objectif d'une certification est une opération majeure, qui doit être approuvée au plus haut niveau de la société concernée et faire l'objet d'une réelle demande métier.

Les risques d'échec de la certification viennent en particulier d'une mauvaise gestion des traces et de la difficulté à conserver dans le temps un SGSI conforme. Faire « tourner » le SGSI dans le temps nécessite un effort sans cesse renouvelé. La construction est une étape comparativement plus simple, pouvant être menée en mode projet. Il est donc important de démarrer sur des périmètres de taille raisonnable, où l'intérêt de la certification est prouvé par un besoin métier ou une demande externe forte.

Le coût de la certification est surtout à chercher en interne à l'organisme. Le coût initial de mise en œuvre est dépendant du périmètre, des mesures de sécurités sélectionnées, du degré de maturité en sécurité de l'information, etc. L'effort maximal sera à réaliser sur la mise en place du SGSI dans la structure de la société et en particulier auprès des métiers qui sont concernés (phase de déploiement). Des coûts récurrents sont à prévoir et ne doivent pas être négligés afin d'assurer la pérennité de la démarche et surtout de la certification. Les coûts externes de certification sont relativement limités (quelques jours d'auditeurs à un tarif proche des 1200 €/jours).

7. Tendances et conclusion

Aujourd'hui, il existe des divergences importantes au niveau mondial par rapport à l'adoption d'ISO 27001 et de la certification. Des pays sont très en avance, en particulier le Japon. D'autres (États-Unis, Inde…) sont en train de rattraper leur retard suite à l'internationalisation récente de la norme en octobre 2005 (450 certifications ISO 27001 dans le monde depuis cette date). La figure 6 montre les écarts entre les différents pays [5].

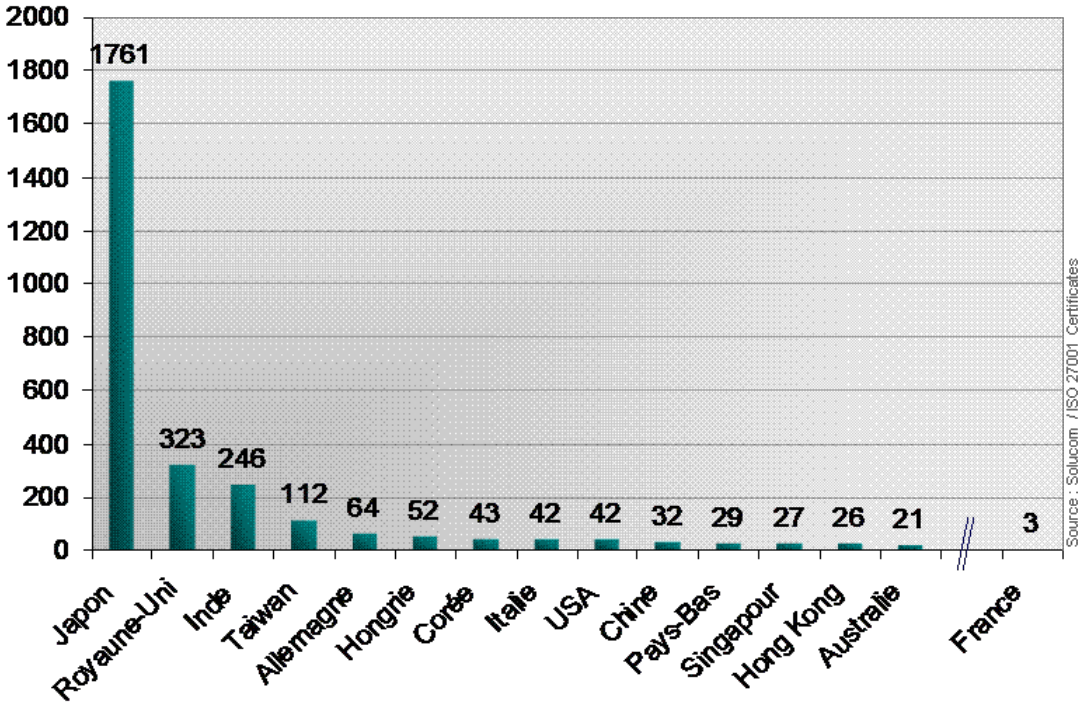

Figure 6 : Nombre de sociétés certifiées par pays

En France, trois certifications ont officiellement été déclarées, il s'agit de Verio Europe (hébergeur web), Gemalto (ex-Axalto, fabricants de carte à puce) et de CMA. Les secteurs d'activité les plus représentés de par le monde sont les sociétés de services informatiques (hébergeurs, fournisseurs d'applications en ligne, infogérants…) même si beaucoup d'autres secteurs d'activité sont actifs au niveau international (banques, organismes médicaux, organismes d'état, opérateurs, groupes industriels…).

En conclusion, il apparaît qu'ISO 27001, et plus généralement la famille ISO 2700x, représente une avancée majeure pour la sécurité de l'information. En effet, ces normes définissent les bases d'un modèle de gouvernance reconnu internationalement, qui permet l'instauration d'une sécurité durable et alignée sur les objectifs métiers d'un organisme. Au-delà de la mise en place de ce système de gestion en interne, les organismes intéressés peuvent viser la certification qui permet :

- Le renforcement de l'image de marque de la société, en particulier dans le domaine de la sécurité de l'information.
- La maîtrise des coûts liés à la sécurité de l'information par l'identification des mesures non efficaces, la rationalisation des processus existants et l'alignement sur les objectifs métiers. Indirectement, la certification entraîne également une baisse du nombre d'audits externes et donc des réductions des coûts nécessaires à leur suivi.
- La facilitation d'autres démarches liées à la sécurité de l'information (en particulier pour les mises en conformité Bâle II ou Sarbanes-Oxley).

La norme est également un outil de communication permettant un dialogue simplifié entre l'ensemble des acteurs du domaine de la sécurité et peut également être vu comme un outil de mobilisation des équipes derrière un objectif commun.

La certification d'un SGSI est une opération pouvant être complexe et longue suivant le périmètre sélectionné. C'est à ce titre qu'il nous semble aujourd'hui opportun d'adopter les principes et le modèle proposés par la norme dans les démarches de sécurité de l'information, sans forcément viser la certification. Celle-ci peut être envisagée sur opportunités et sur des périmètres où un réel besoin métier à été identifié et exprimé.

BIBLIOGRAPHIE

[1] Steichen, P., La normalisation au Luxembourg : un pont entre la qualité et la sécurité, itSMF Magazine Chapitre Luxembourg, septembre 2006

[2] Igalens, J., Penan H., La normalisation, PUF - Que sais-je, 1994.

[3] http://www.iso.ch

[4] http://www.jtc1.org

[5] http://www.iso27001certificates.com

[6] http://www.cofrac.fr

[7] http://www.olas.public.lu/

[8] http://www.lsti.fr