

Le management de la sécurité des systèmes d'information enfin normalisé par l'Afnor

Isabelle POTTIER

Avocat

Alain Bensoussan – Avocats, Paris

Hervé SCHAUER

Consultant en sécurité informatique

La norme NF ISO/CEI 27001 : 2007-12 homologuée par l'Afnor le 14 novembre 2007 vient de faire l'objet d'une publication pour prendre effet le 14 décembre 2007 (1). Elle spécifie les exigences relatives au management de la sécurité d'un système de management de la sécurité et de l'information (SMSI), composante incontournable de la confiance. Elle permet en effet à toute entreprise d'améliorer la manière avec laquelle elle gère la confidentialité, l'intégrité et la disponibilité des informations qui constituent son patrimoine informationnel. Mieux encore, en obligeant les entreprises à prendre en compte les exigences légales ou réglementaires propres à leurs activités, elle donne à la norme une haute valeur juridique.

I. UNE NORME QUI MET EN PLACE DES FACTEURS D'AMÉLIORATION DE LA SÉCURITÉ

La norme ISO 27001 relative à la définition du management de la sécurité des systèmes d'information au sein d'une entreprise, est l'application pragmatique des principes de la qualité (type ISO 9001) à la sécurité de l'information. Historiquement, elle est issue de la norme BS 7799-2 publiée en 1998 par l'Institut britannique de normalisation (BSI – *British Standard Institute*) et intitulée « Spécification pour les systèmes de management de la sécurité de l'information » (*Specification for Information Security Management Systems*). Cette norme acceptée et reconnue internationalement est appliquée par des législations de plusieurs pays européens (Norvège et Suisse) et aussi par des institutions financières internationales. Elle définit en premier lieu des exigences pour la direction des organisations pour la mise en œuvre du système de management de la sécurité de l'information (SMSI ou ISMS – *Information Security Management System*) et son système de documentation, et impose des actions au niveau organisationnel pour la sécurité informatique, fondées sur une politique de sécurité et une appréciation des risques sur les actifs importants. La norme ISO 27001 est un pilier qui est complété par une série de guides associés qui détaillent son implémentation et son audit (2).

(1) NF ISO/CEI 27001 : 2007-12 (OSP 27001 : 2005).

(2) L'ISO 27002, qui détaille les mesures de sécurité qui sont listées dans l'annexe normative de l'ISO 27001 ; l'ISO 27003, guide de mise en œuvre d'un SMSI dont la publication est prévue en 2009 mais dont la première partie sur la phase « PLAN » est terminée ; l'ISO 27004, guide de mesu-

A – Un champ d'application très large visant toute entreprise

La norme ISO 27001 couvre tous les types d'organismes quels que soient leur taille, leur structure et leur nature, qu'il s'agisse d'entreprises commerciales, d'organismes publics ou d'organismes à but non lucratif. Elle spécifie les exigences relatives à l'établissement, à la mise en œuvre, au fonctionnement, à la surveillance et au réexamen, à la mise à jour et à l'amélioration, d'un SMSI documenté dans le contexte des risques globaux liés à l'activité de toute entreprise. La formalisation des documents sécurité doit couvrir l'intégralité des mesures de sécurité de l'annexe A de la norme ISO 27001 pour montrer qu'aucune bonne pratique de sécurité n'a été oubliée.

La norme ISO 27001 s'appliquant à toutes les tailles d'organismes et à tous les métiers, elle est parfaitement adaptée aux services de confiance, d'archivage, de supervision, d'hébergement et d'infogérance en général qui doivent apporter la confiance auprès de leurs clients en matière de sécurité des systèmes d'information. La norme est conçue pour s'adapter à toutes les échelles ; même une petite société de 15 personnes qui offre une prestation de sauvegarde en ligne sur internet a besoin d'apporter une certaine confiance à ses clients, et la norme ISO 27001 lui est accessible.

La mise en œuvre des mesures de sécurité préconisées doit être adaptée aux besoins spécifiques de chaque entreprise et notamment des « actifs » qui sont à protéger, c'est-à-dire des éléments représentant de la valeur pour cette dernière. C'est au travers d'un dialogue avec les responsables métier que l'on peut vérifier qu'on a « intuité » les bons actifs à protéger et les procédures à mettre en place. Aussi, pour optimiser l'implémentation de la norme, il est nécessaire que les responsables de la sécurité du système d'information (RSSI) commencent par élaborer des scénarii de vrais risques sur de vrais actifs. Par exemple, la protection de la base de données client de l'ingénieur commercial qui travaille à distance nécessitera de chiffrer le disque

rage du SMSI, qui explique comment mettre en œuvre des indicateurs pour un SMSI, dont la publication est prévue en 2008 ; l'ISO 27005, guide de gestion des risques pour un SMSI, actuellement en cours de vote, dont la publication est donc également prévue pour 2008. Il existe déjà des outils appliquant la norme 27005 et ce guide détaille une partie importante de l'ISO 27001 car l'appréciation des risques doit donner des résultats reproductibles et comparables ; l'ISO 27006, parue en janvier 2007, qui s'adresse aux organismes de certification et qui garantit l'homogénéité des certifications délivrées dans le monde.

dur de son ordinateur portable. Dans certains métiers où les prises de commande se font essentiellement en réseau, la messagerie sera un actif « critique » qu'il faudra à tout prix sécuriser car il peut affecter complètement l'activité de l'entreprise s'il vient à s'arrêter pendant plusieurs heures. En cas d'incident grave survenant, comme le piratage informatique du site Web de commerce en ligne de l'entreprise, celle-ci devra disposer de personnes suffisamment formées aux procédures convenables pour réduire l'impact de cet incident.

Le système de management inclut l'organisation, les politiques, les activités de planification, les responsabilités, les pratiques, les procédures, les processus et les ressources.

B – Une approche "processus"

L'entreprise doit établir, mettre en œuvre, exploiter, surveiller, réexaminer, tenir à jour et améliorer un SMSI documenté dans le contexte de ses activités commerciales d'ensemble et des risques auxquels ses activités sont confrontées. Le processus utilisé est fondé sur le modèle PDCA (« Planifier-Déployer-Contrôler-Agir » ou roue de Deming).

Comme les normes ISO 9001 : 2000 et ISO 14001 : 2004, l'ISO 27001 : 2007 porte moins sur l'efficacité des dispositifs mise en place que sur leur existence et la mise en place de facteurs d'amélioration selon le modèle de processus PDCA. Autrement dit, son objectif n'est pas de garantir un niveau de sécurité, mais de garantir que lorsqu'on l'a atteint, on le garde et on l'améliore ! Elle impose ainsi l'adoption d'une approche « processus » pour l'établissement, la mise en œuvre, le fonctionnement, la surveillance et le réexamen, la mise à jour et l'amélioration d'un SMSI.

Pour fonctionner efficacement, toute entreprise doit identifier et gérer de nombreuses activités. Selon la norme, « toute activité utilisant des ressources et gérée de manière à permettre la transformation d'éléments d'entrée en éléments de sortie, peut être considérée comme un processus ». La mise en place d'un SMSI permet d'entrer dans un processus d'amélioration de la gestion de la sécurité de l'information. Cette gestion porte majoritairement sur ce qui touche à la sécurité du système d'information, c'est-à-dire autour des outils informatiques.

L'adoption du modèle PDCA reflète les principes fixés dans les lignes directrices de l'OCDE en 2002 ⁽³⁾ qui régissent la sécurité des systèmes et des réseaux d'information, à savoir la sensibilisation aux risques tant internes qu'externes, la compréhension des responsabilités, la réactivité et l'esprit de

coopération, la conduite éthique, le respect des valeurs reconnues par les sociétés démocratiques (liberté d'échanger des pensées et des idées, libre circulation de l'information, confidentialité de l'information et des communications, protection adéquate des informations de caractère personnel, etc.), l'évaluation des risques tenant compte des préjudices, l'intégration de la sécurité en tant qu'élément essentiel des systèmes et réseaux d'information, l'approche globale de la gestion de la sécurité, l'examen et la réévaluation de la sécurité des SMSI.

La norme ISO 27001 participe ainsi à ce qu'une prise de conscience s'effectue quant aux risques encourus du fait de la connectivité croissante des systèmes et réseaux d'information qui les expose à un nombre grandissant et à un éventail de plus en plus large de menaces et de vulnérabilités. Or cette prise de conscience ne pourra se faire qu'avec une meilleure compréhension des questions de sécurité, propre à développer une « culture de la sécurité ».

À ce titre, la norme porte sur la mise en œuvre de facteurs d'amélioration selon le modèle PDCA comme par exemple, des audits internes, procédures de gestion des incidents et mesures de sécurité (y compris pré techniques) pertinentes selon le type d'actifs à protéger. C'est au travers d'un dialogue avec les responsables métier que l'on peut vérifier qu'on a « intuité » les bons actifs à protéger et les procédures à mettre en place. La norme applique les principes de la qualité à la sécurité de l'information et constitue un référentiel précis et auditable permettant d'apporter la confiance nécessaire au développement d'une activité en ligne.

C – Une décision stratégique

La mise en œuvre d'un système de management de la sécurité de l'information (SMSI) basé sur l'ISO 27001 est une décision stratégique : l'engagement de la direction générale, sans laquelle rien n'est possible, est incontournable. Une fois la décision prise, les principes sont de décider d'un périmètre, rédiger une politique de sécurité ou politique du SMSI qui exprime la vision de la direction en SSI, établir la liste des actifs importants de l'entreprise, appliquer une appréciation des risques sur ces actifs, en déduire des mesures de sécurité (en s'appuyant sur celles proposées par la norme ISO 27002) qui vont permettre de réduire les risques à un niveau acceptable pour la direction générale, mettre en œuvre les mesures de sécurité choisies, vérifier la mise en œuvre et l'efficacité des mesures et, bien sûr, « reboucler » pour s'améliorer.

L'expérience montre que la mise en œuvre de la norme ISO 27001 impose généralement au RSSI (responsable de la sécurité des systèmes d'informa-

(3) Lignes directrices de l'OCDE régissant la sécurité des systèmes et réseaux d'information, vers une culture de la sécurité, Paris, OCDE, juillet 2002, <http://www.oecd.org/dataoecd/58/63/1946938.doc>

tion) un travail sur les aspects suivants imposés par la norme : la mise en place d'une sensibilisation à la sécurité de l'information auprès de tout le personnel, c'est-à-dire allant au-delà du périmètre du SMSI, la mise en place un processus d'audit interne du SMSI et la conservation des enregistrements de ce qui a été fait.

Le responsable sécurité doit construire une gestion de risques qui s'inscrit, elle aussi, dans un cycle d'amélioration continue. Il doit redévelopper une appréciation des risques périodiquement, en revalidant avec les propriétaires des processus métiers, afin de bien concentrer la mise en œuvre des mesures de sécurité sur ce qui compte réellement le plus pour l'organisme et donc réduire les risques les plus importants. Même si cette appréciation des risques (qui s'appelait dans le monde de la sécurité des systèmes d'information « analyse de risque ») était déjà une des bases de la sécurité des systèmes informatiques, le fait de l'intégrer dans un processus cyclique est nouveau.

La norme ISO 27001 n'impose pas une méthode d'appréciation des risques particuliers mais donne un cahier des charges très précis de ce que doit faire au minimum une telle méthode. Le guide ISO 27005 qui sera publié en 2008 fournira une synthèse de tous les travaux tant en France (4) qu'à l'étranger et détaillera de manière pragmatique la manière de dérouler son processus d'appréciation des risques, en les identifiant, les estimant et les évaluant.

Par ailleurs, la norme ISO 27001 formalise l'engagement de la direction générale sur le plan de traitement des risques et les coûts associés.

Mais ce qui fait tout l'intérêt de la norme, c'est que les objectifs de sécurité et les mesures de sécurité sont sélectionnés sur les résultats et les conclusions du processus d'appréciation du risque et de traitement du risque, ainsi que sur les exigences légales ou réglementaires et les obligations contractuelles, et les exigences métier de l'organisme, relatives à la sécurité de l'information.

II. UNE NORME À HAUTE VALEUR JURIDIQUE

Être certifié ISO 27001 présente de nombreux avantages et notamment celui de la compétitivité, l'amélioration de la maîtrise de sa sécurité des systèmes d'information et des coûts liés aux mesures de sécurité, l'augmentation du niveau de sécurité dans

(4) Parmi les outils méthodologiques pour la sécurité des systèmes d'information, citons la méthode EBIOS (Expression des besoins et identification des objectifs de sécurité) développée par Direction centrale de la sécurité des systèmes d'information (DCSSI) qui permet d'apprécier et de traiter les risques relatifs à la sécurité des systèmes d'information (SSI). Elle permet aussi de communiquer à leur sujet au sein de l'organisme et vis-à-vis de ses partenaires afin de contribuer au processus de gestion des risques SSI, site de la DCSSI, <http://www.ssi.gouv.fr/fr/conflance/ebiospresentation.html>

le temps, etc. Mais s'il en est un auquel on ne saurait rester insensible, c'est celui de sa valeur légale incontestable.

A – La prise en compte des exigences légales ou réglementaires et des obligations de sécurité contractuelles

La norme ISO 27001 définit en effet une politique de sécurité qui tient compte des exigences légales et confère donc au SI une présomption de fiabilité aux yeux des tribunaux. En cas de litige avec un client ou un partenaire, elle permet de constituer des dossiers de preuve et de préjudice plus facilement et de rendre leur contestation beaucoup plus difficile.

La norme prévoit en effet l'obligation pour l'entreprise de tenir compte non seulement des exigences liées à son activité mais également « des exigences légales ou réglementaires, ainsi que des obligations de sécurité contractuelles » (v. 4.2.1b).

Pour cela, l'entreprise doit « identifier une méthodologie d'appréciation du risque adaptée à son SMSI, ainsi qu'à la sécurité de l'information identifiée et aux exigences légales et réglementaires » (v. 4.2.1c). Ensuite, les objectifs de sécurité et les mesures de sécurité proprement dites doivent être sélectionnés et mis en œuvre pour répondre aux exigences identifiées par le processus d'appréciation du risque et de traitement du risque. « Cette sélection doit tenir compte des critères d'acceptation des risques ainsi que des exigences légales, réglementaires et contractuelles » (v. 4.2.1g).

La certification s'obtient par un organisme de certification qui diligente une équipe d'audit et permet la publication d'un certificat ISO 27001. Pour les prestataires de service de confiance, le certificat de conformité tierce partie vaut présomption de conformité à la réglementation en cas de litige porté devant les tribunaux. Ainsi, dans l'affrontement après sinistre ou incident majeur, l'entreprise certifiée conforme à la norme aura un avantage certain par rapport à celle qui ne l'est pas, ne serait-ce que parce qu'elle aura l'ensemble des preuves et enregistrements de sécurité exigés par la norme. La norme décrit en effet des procédures de preuve et d'enregistrements formels permettant de faciliter la constitution des dossiers de preuves et de préjudice.

B – Quand la sécurité tend à être une obligation légale... la boucle est bouclée

Les données contenues dans le système d'information d'une entreprise justifient à elles seules la mise en place d'une politique de sécurité destinée à éliminer les risques de piratage, d'erreurs ou de malveillances. Cette nécessité tend de plus en plus à être imposée par la loi. Tel est le cas des données

considérées comme « sensibles » et qui bénéficient pour cette raison d'un régime spécifique prévu par la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifiée en 2004. Compte tenu de leur nature, ces informations susceptibles de venir à la connaissance d'un prestataire sous-traitant doivent faire l'objet de précautions de sa part (5). La violation de cette obligation de sécurité est assortie de sanctions pénales : 5 ans d'emprisonnement et 300.000 € d'amende (6). Il est donc nécessaire pour l'entreprise de connaître avec précision l'ensemble des lois et règlements qui s'appliquent aux informations qu'elle manipule dans son secteur d'activité (aéronautique, santé, finance...).

Or, depuis la fin 2001, les lois dont le sujet est la sécurité ne se comptent plus, qu'il s'agisse de la loi sur la sécurité quotidienne, celle pour la sécurité intérieure, la sécurité financière, ou encore la cybercriminalité, si l'on ne tient compte que des réglementations nationales. À celles-ci s'ajoutent les obligations imposées par Sarbanes-Oxley (la « SOX »), Outre-Atlantique, pour toute entreprise cotée (7) et par Bâle II, en Europe, pour les établissements financiers. L'article 404 de la loi SOX exige, pour les entreprises cotées aux États-Unis (y compris à leurs filiales françaises et sous-traitants), la mise en place d'un contrôle interne efficace sur le reporting financier. Ces dispositions de la loi obligent l'auto-évaluation des contrôles internes, la mise en place de procédures de reporting financier, la traçabilité de tous les mouvements financiers. Cette nécessité d'un contrôle interne efficace du reporting financier impose donc de contrôler également le système d'information de l'entreprise. Les obligations de la SOX ont, en effet, un impact sur tous les processus informatiques partagés dans la mesure où la loi impose aussi une obligation de stocker tous les documents numériques pendant trois ans, et notamment les e-mails.

Le coût de la certification ISO 27001 peut être considérablement réduit pour les entreprises déjà soumises à des audits internes de type Sarbanes-Oxley (SOX) puisque les structures internes utilisées sont les mêmes. Mieux encore, avec la multiplication des référentiels d'exigences spécialisés contenant un volet sécurité tels la SOX ou ce que vérifient la Commission bancaire et la Cour des comptes, les organismes certifiés ISO 27001 vont avoir l'opportunité de réduire le nombre des audits de conformités qu'ils doivent subir régulièrement. En outre, les nombreuses entreprises qui utilisent la norme CobiT (*Control Objectives for Business*

and related Technology) (8) pour l'audit de leur système d'information, trouveront un grand intérêt à se tourner vers la création d'un SMSI certifié !

La norme 27001 ne doit pas être vue comme une contrainte mais bien comme un moyen de structuration. Une démarche ISO 27001 apporte l'amélioration continue de la sécurité de l'information, l'universalité et la complétude des pratiques, une approche axée sur les processus et le développement du dialogue et de la communication au sein de l'entreprise sur les problématiques sécurité, en même temps qu'une forte présomption de conformité à la réglementation. Ses objectifs sont de faire adopter de bonnes pratiques, de définir une organisation générale de la sécurité et de produire un modèle reproductible. La démarche ISO 27001 est partie intégrante de la gouvernance d'entreprise, d'une approche globale de la sécurité et facteur d'amélioration continue.

(5) Articles 34 et 35 de la loi du 6 janvier 1978 modifiée.

(6) Article 226-17 du Code pénal.

(7) La « SOX » intitulée « Management assessment of internal control » a été adoptée le 30 juillet 2002 par le Congrès américain pour répondre aux scandales Enron et Worldcom et rétablir la confiance des investisseurs dans les sociétés cotées. Plus d'information sur le site <http://www.sarbanes-oxley.com>

(8) La première édition de cette norme date de 1996 et a été créée par l'association ISACA (Information Systems Audit and Control Association). Pour de plus amples renseignements sur cette norme, consulter le site <http://www.isg.org/>