



ISO/CEI 27001:2005 – l'état de l'art en gestion de sécurité de l'information

par Ted Humphreys



La publication récente de la norme ISO/CEI 27001:2005 *Technologies de l'information – Techniques de sécurité – Systèmes de gestion de sécurité de l'information – Exigences*¹⁾ est un événement important dans le monde de la sécurité de l'information. La norme était attendue avec impatience.

Version révisée et actualisée de la norme britannique BS 7799 Partie 2, qui a connu un grand succès, elle intègre l'approche processus d'ISO 9001:2000 et d'ISO 14001:2004.

Elle spécifie les exigences et les processus qui permettent à une entreprise d'établir, de mettre en œuvre, de revoir et de surveiller, de gérer et d'actualiser

une sécurité de l'information qui soit efficace. Comme ISO 9001, elle est construite sur le modèle du cycle de processus Planifier-Faire-Vérifier-Agir (PDCA) (voir **Figure 1**, page 16) et sur l'exigence d'une amélioration continue.

ISO/CEI 27001:2005 a été élaborée par divers organismes qui ont un intérêt commun – protéger leurs biens d'information, la « sève » de toutes les entreprises. Ces organismes ont élaboré la norme relative au Système de gestion de sécurité de l'information (SGSI) pour leur permettre de créer des solutions rentables en sécurité de l'information et protéger ainsi leurs activités.

Un outil de gestion du risque

La gestion du risque est au cœur de l'approche ISO/CEI 27001 pour réaliser une sécurité efficace de l'information en appliquant en permanence des méthodes d'analyse du risque, incorporées dans le modèle de processus PDCA, afin de surveiller, d'actualiser et d'améliorer cette efficacité. Elle donne un cadre de gestion qui rend possible les meilleures pratiques de contrôle de la norme ISO/CEI 17799:2005, *Technologies de l'information – Techniques de sécurité – Code de bonne pratique pour la gestion de la sécurité de l'information*, à appliquer et gérer dans le cadre

de l'approche générale du risque d'un organisme (voir « La norme ISO/CEI 17799 améliorée ouvre la voie à une nouvelle série sur les systèmes de gestion de la sécurité de l'information », *IMS*, Septembre-Octobre 2005).

1) ISO/CEI 27001:2005 *Technologies de l'information – Techniques de sécurité – Systèmes de gestion de sécurité de l'information – Exigences*, est disponible, au prix de 124 francs suisses, auprès des instituts nationaux membres de l'ISO (dont la liste et les coordonnées sont données sur le site Web de l'ISO : www.iso.org et du Secrétariat central de l'ISO (sales@iso.org).



Ted Humphreys est Animateur du Groupe de travail 1, Exigences, services de sécurité et directives, du Sous-comité 27, Techniques de sécurité des TI, Comité technique mixte ISO/CEI JTC 1, Technologies de l'information. Il est aussi Directeur de XiSEC, société spécialisée dans les systèmes de gestion de sécurité de l'information.

Tél. + 44 1473 626615.

E-mail tedxisec@aol.com

Web www.xisec.com



Figure 1 : Le cycle Planifier-Faire-Vérifier-Agir du Système de gestion de sécurité de l'information (SGSI).

ISO/CEI 27001:2005 donne le moyen de mettre en œuvre une gestion efficace de la sécurité de l'information conformément aux objectifs organisationnels et aux exigences économiques. La norme, une spécification fondée sur l'analyse du risque, est conçue pour prendre en charge les aspects de sécurité de l'information du gouvernement d'entreprise, la protection des biens d'information, les obligations légales et contractuelles, mais aussi le large éventail de menaces qui pèsent sur les systèmes TIC (technologies de l'information et de la communication) d'un organisme et sur ses processus.

Elle renvoie également aux récents Principes de sécurité de l'Organisation de coopération et de développement économiques (OCDE), qui soulignent la nécessité de créer une « culture de la sécurité » au sein d'un organisme. Cet aspect est particulièrement important pour aider l'organisme à assumer ses responsabilités sociales – et pour sa bonne santé générale.

Avantages pour l'entreprise

En affaires, il est essentiel de gagner la confiance des clients. Un organisme peut donner cette assurance aux clients s'il démontre que ses processus et systèmes sont « au point » et répondent à leurs besoins en partageant et en échangeant des informations, en fournissant une gamme de services et en réalisant des transactions en ligne. La sous-traitance, la délocalisation et la fourniture de services gérés s'appuient sur la création et le maintien de la confiance des clients dans les systèmes régissant les activités de l'entreprise. De nombreux organismes ont fait état des effets bénéfiques de l'utilisation de ces normes SGSI pour donner aux clients l'assurance que les services sont fournis d'une manière sûre.

Ils ont également fait état d'effets bénéfiques pour la satisfaction des obligations contractuelles et l'aptitude à en apporter la preuve aux partenaires commerciaux, aux clients et aux autres

parties intéressées. Certains ont aussi affirmé que l'application des normes a contribué à les protéger de nombreux risques économiques tout en sauvegardant des biens essentiels, à la fois tangibles et intangibles, de l'entreprise.

Les gouvernements dans de nombreuses régions du monde appliquent également des normes SGSI avec profit dans le cadre de leurs stratégies et déploiements de gouvernement électronique.

Applicable à toutes les entreprises

ISO/CEI 27001:2005 est applicable aux petites, moyennes et grandes entreprises. La norme est pratique, assez souple pour s'intégrer aux systèmes de management existants et adaptable à toute approche du risque envisagée par l'entreprise. Ce point de vue est partagé par les organismes qui ont utilisé la norme BS 7799 Partie 2 (devancière d'ISO/CEI 27001) dans le cadre de leur stratégie d'entreprise. Ils

sont d'ailleurs nombreux à être certifiés BS 7799 Partie 2 pour apporter une confirmation indépendante de l'efficacité de leur sécurité de l'information.

La certification du SGSI

La certification BS 7799 Partie 2 a connu une croissance rapide ces dernières années, plus de 2 000 organismes de plus de 50 pays étant certifiés à ce jour. Le Registre international des certifications accréditées (www.ISO27001certificates.com) donne une liste de tous les organismes certifiés par pays. Une nouvelle augmentation est attendue avec la publication d'ISO/CEI 27001:2005, bien que la certification ne soit ni obligatoire, ni mentionnée dans la norme.

Devancière d'ISO/CEI 27001, la norme britannique BS 7799 Partie 2:2002 a montré toute sa valeur pour les nombreux organismes qui, dans le monde, ont été certifiés en utilisant les mêmes processus, lignes directrices et critères pour la certification et l'audit que ceux d'ISO 9001:2000 (par exemple guide ISO/CEI 62:1996, ISO 19011:2002 et EA 7/03²⁾, et qui ont fait état de nombreux avantages réels et tangibles pour l'entreprise.

(Suite page 18)

2) Guide ISO/CEI 62:1996, *Exigences générales relatives aux organismes gérant l'évaluation et la certification/enregistrement des systèmes qualité*; ISO 19011:2002, *Lignes directrices pour l'audit des systèmes de management de la qualité et/ou de management environnemental*; EA 7/03 – (Coopération européenne pour l'accréditation) *Lignes directrices pour l'accréditation des organismes gérant la certification/enregistrement des systèmes de gestion de sécurité de l'information*.

CE QU'EN PENSENT LES UTILISATEURS

Jusqu'à présent, les organismes qui souhaitaient que leur SGSI soit certifié le faisaient en conformité à la norme britannique BS 7799 Partie 2. C'est désormais possible conformément à la Norme internationale ISO/CEI 27001:2005.

Voici certaines observations sur les avantages obtenus par la mise en œuvre et la certification du SGSI dans le monde.

Macquarie Telecom : « Une assurance donnée aux clients »

« La certification BS 7799 donne à nos clients l'assurance, preuve à l'appui, que toutes les ressources, processus et procédures corrects sont en place. Nous observons une prise de conscience accrue de nos clients, qui demandent que les cadres pour la sécurité soient examinés, en particulier du fait que les questions de sécurité et de conformité sont soulevées au niveau des conseils d'administration. BS 7799 est pour nous une des manières de démontrer notre engagement. »

Greg Thompson
Directeur de groupe – Hébergement et sécurité,
Macquarie Telecom, Australie

Tectraxx : « Une grande différence »

« Le fait que nous ayant annoncé notre volonté de mettre en place un système de gestion de la sécurité conforme à BS 7799 Partie 2 a, à lui seul, créé une grande différence par rapport à nos concurrents. Tous nos clients – de Nokia à Siemens – sont très intéressés par le fait que leur fournisseur de services soit conforme à cette norme de sécurité. »

Ernst Wiener
Responsable Sécurité de l'information
et Management de la qualité, Tectraxx,
Wiener Neudorf, Vienne, Autriche

Polaris Software : « Une plus grande confiance des clients »

« La certification BS 7799 Partie 2 a visiblement créé, chez notre personnel et notre direction, une meilleure prise de conscience de la sécurité de l'information, ce qui a conduit à un degré supérieur de conformité, qui a en retour amélioré la confiance de nos clients. »

S. Y. Amarnath
CISO – Groupe Sécurité de l'information,
Polaris Software Lab Limited, Chennai, Inde

Kapsch BusinessCom : « Une reconnaissance internationale »

« Grâce à la vérification indépendante réalisée par CIS, les éventuelles déficiences cachées de notre système de sécurité peuvent être identifiées et éliminées. Toutefois, l'objectif principal de notre certification est d'offrir à nos clients une norme de sécurité bénéficiant d'une reconnaissance internationale. »

Franz Semmerneegg
Directeur général, Kapsch BusinessCom, Vienne, Autriche

SPI Technologies : « Gagner la confiance des clients »

« La norme BS 7799 Partie 2 a montré toute sa valeur pour notre recherche de l'excellence d'entreprise. En ces temps difficiles, où la sécurité de l'information est une priorité absolue, la norme SGSI est devenue l'armure de SPI Technologies. Elle a joué un grand rôle pour obtenir la confiance des clients dans les services et capacités de l'entreprise. Nous sommes convaincus que l'amélioration de la sécurité de l'information au sein de l'organisation met SPI en pointe dans le domaine de l'externalisation des processus, un coup gagnant qui créera la différence par rapport à la concurrence. »

Ian D. Bellord
Soutien opérationnel mondial, SPI Technologies Inc, Philippines

BAE Systems Bofors : « La certification, une nécessité vitale »

« La certification est une nécessité vitale à la fois pour nous et pour nos clients. Comme nous avons également affaire avec de nombreux contacts internationaux, un certificat mondial de ce type est essentiel. »

Christina Larsson
Responsable Sécurité de l'information, BAE Systems Bofors AB, Suède

Tata Steel : « Des risques réduits en sécurité de l'information »

« En appliquant BS 7799 Partie 2, nous avons pu réduire les risques et menaces sur la sécurité de l'information et donner une assurance à nos parties prenantes. Elle nous a aidés à construire un environnement de prise de conscience de la sécurité de l'information et à définir une approche focalisée et structurée pour la gestion de la sécurité. Nous attendons avec intérêt ISO 27001:2005 qui, nous l'espérons, fournira le cadre pour améliorer les contrôles de sécurité de l'information et leur mise en application. »

Raghavendra Mathur, Chef, Infrastructure TI, Tata Steel, Inde

Siemens : « Un réel atout concurrentiel »

Nous avons recherché la certification parce que cette norme offre un maximum de sécurité. Lorsque nous faisons des offres, nous y joignons le certificat BS 7799 Partie 2. Cela nous évite d'avoir à donner des preuves supplémentaires en matière de sécurité de l'information – un réel atout concurrentiel. »

Albert Felbauer
Directeur général, Siemens Business Services GmbH,
Vienne, Autriche

Biznet Solutions : « Se distinguer dans un marché très actif »

« Depuis l'obtention du certificat BS 7799 en novembre 2004, Biznet Solutions s'est distingué dans un marché très actif. Notre engagement à assurer la sécurité de l'information fournit en permanence une confiance non seulement à nos clients, mais aussi à nos employés et partenaires. La certification a donné à nos systèmes la force et l'intégrité qui nous aident à concurrencer avec succès des entreprises de classe mondiale sur la scène mondiale. »

Gillian Esquivel, Biznet Solutions, Belfast, Irlande du nord

Ces aspects bénéfiques types sont exprimés par plusieurs entreprises certifiées qui sont citées page précédente (voir encadré, « Ce qu'en pensent les utilisateurs »). Des avantages analogues ont été relevés dans la plupart des secteurs commerciaux et industriels, y compris les télécommunications, les finances et les assurances, les services publics, la distribution et la fabrication, les prestataires de services, les soins de santé, les services de police et les services d'urgence, les universités, les départements et agences gouvernementales.

La nouvelle norme devrait devenir **une meilleure vente**

En conséquence, avec la publication d'ISO/CEI 27001:2005, de nombreux organismes ont commencé à se préparer aux processus de mise en œuvre et de certification – dont l'objectif principal est d'obtenir un signe d'approbation reconnu sur le plan international.

La famille ISO/CEI 27000

ISO/CEI 27001:2005 est la première d'une famille de normes SGSI qui seront publiées dans les cinq prochaines années. Il est prévu d'attribuer à ISO/CEI 17799 le nouveau numéro ISO/CEI 27002 en avril 2007, en donnant ainsi aux utilisateurs actuels le temps de se familiariser avec le nouveau système de numérotation.

En cours d'élaboration, la norme ISO/CEI 27003 contiendra des lignes directrices supplémentaires pour la mise en œuvre et la norme ISO/CEI 27004 traitera du sujet important du systè-

me de mesure et des mesurages de la sécurité de l'information. Cela permettra aux organismes de définir des cibles de performance et de procéder à des analyses comparatives pour mesurer l'efficacité de leur sécurité de l'information.

Viendront ensuite les normes ISO/CEI 27000, *Principes et vocabulaire*, comparable à ISO 9000:2000, et ISO/CEI 27005, un ensemble de lignes directrices pour la gestion du risque. Des travaux sont aussi en cours sur un ensemble d'exigences pour les télécoms, en collaboration avec l'UIT-T, l'entité de normalisation de l'Union internationale des télécommunications. Entièrement basées sur ISO/CEI 27001, elles ajoutent des exigences télécoms aux contrôles définis dans ISO/CEI 27002 (ISO/CEI 17799). Le document est actuellement identifié en tant que norme X.1051 de l'UIT-T. Il pourrait s'intégrer à la famille ISO 27000 à l'avenir, par exemple sous référence ISO/CEI 27051.

Meilleure vente

ISO/CEI 27001:2005 inaugurera ainsi une famille de normes internationales SGSI qui devraient apporter de nombreux avantages aux entreprises dans le monde en améliorant la sécurité de l'information dans un environnement aujourd'hui perméable aux risques. La nouvelle norme est destinée à avoir le même succès que sa devancière, la norme BS 7799 Partie 2, et l'on prédit qu'elle deviendra, comme ISO/CEI 17799, une meilleure vente dans des marchés et secteurs très variés. •