

LES RELATIONS DE LA FAMILLE ISO 27001 AVEC LES AUTRES FAMILLES ISO

Gestion des risques, qualité de services, exigence de sécurité, tels sont les enjeux actuels des systèmes d'informations. Les entreprises connaissent l'exigence de qualité avec l'ISO 9000 et disposent parfois de certifications ; elles ont aussi travaillé avec ITIL et avec l'ISO 20000. La norme de gouvernance ISO 38500 vient pour sa part d'être publiée au cours de l'été 2008 et la norme de gestion des risques ISO 31000 est en cours d'élaboration. Nous avons ainsi demandé à nos experts de nous apporter leur regard sur ces normes.

GÉRÔME BILLOIS, manager sécurité, constate tout d'abord que les normes ISO 27000, 9000 et 20000 reposent sur le même concept de système de management, elles sont donc faciles à combiner et cela procure même des avantages indéniables en termes de capitalisation et de cohérence. En effet, remarque Matthieu Grall du bureau conseil de la DCSSI, « les démarches qualité, quand elles sont mises en œuvre, allègent considérablement les réflexions de SSI. Le manque de formalisation des processus oblige les acteurs de la SSI à rationaliser le fonctionnement des organismes. Ce travail est non seulement coûteux mais aussi théoriquement hors du spectre de la SSI. Les organismes mettant en œuvre des démarches qualité intègrent donc aisément des approches telles qu'ISO 27001. » Faut-il pour autant rapprocher les RSSI et les directions de la qualité ? La réponse n'est pas aussi claire. « Le RSSI peut être épaulé par la qualité dans la mise en œuvre du système de management, reconnaît Gérôme Billois. Mais la sécurité de l'information reste un domaine à part entière. Pour nous, chaque domaine doit être porté par l'acteur le plus légitime. »

Pour Matthieu Grall, « le bon positionnement du RSSI dépend de la culture et du fonctionnement de l'organisme. » Avant d'ajouter avec un certain sourire : « Et bien souvent du RSSI lui-même ! » Il nous explique ainsi que « la SSI étant une activité de support aux autres activités d'un organisme, au même titre que l'informatique ou la qualité, les acteurs de la SSI, RSSI

ou autres, devraient se positionner en conseillers auprès des responsables métiers et des responsables du patrimoine informationnel qu'ils manipulent. Il serait donc normal que leur positionnement leur permette d'exercer ce rôle. »

De manière pragmatique, Gérôme Billois précise que « la mise en place du système de management est là où la complémentarité est la plus grande. La démarche 27001 profitera alors de l'existant en termes de gestion de la documentation et des enregistrements, des revues de direction ou encore de l'organisation en processus. L'ISO 20000-1 facilitera l'ensemble des démarches relatives au processus ITIL qui sont également référencées dans l'ISO 27002 : gestion des incidents, de la capacité, des changements, inventaire des actifs... » Matthieu Grall va un peu plus loin et indique que « les différentes normes de systèmes de management sont très similaires : ISO 9001 pour la qualité, OHSAS 18001 pour la sécurité des personnes, ISO 14001 pour l'environnement, ISO 27001 pour la sécurité de l'information, entre autres. Elles sont basées sur les mêmes principes, elles sont structurées quasiment à l'identique, elles utilisent une terminologie relativement commune. Elles se distinguent et se complètent par leur objet, à savoir notamment, le produit, l'individu, la communauté environnante, les informations et processus informationnels, et par leur objectif : la satisfaction des clients, la protection en matière d'hygiène, de santé et de sécurité, la protection de l'environnement, la protection du patrimoine informationnel... » Pour nos experts, il n'y a pas d'incompatibilité entre toutes ces normes et les



Gérôme Billois
manager sécurité,
Solucom



Matthieu Grall,
bureau conseil de
la DCSSI - SGDN



Hervé Schauer,
fondateur du
cabinet HSC

entreprises doivent pouvoir faire travailler de concert des équipes très différentes.

Par ailleurs, souligne Matthieu Grall, « toutes ces normes reposent sur les lignes directrices pour la justification et l'élaboration de normes de systèmes de management (Guide ISO 72). L'ISO 27001, qui est la plus récente, a été conçue le plus en conformité possible avec ce guide ISO 72. L'ISO a demandé cette année à tous ses comités techniques de se prononcer sur une vision commune des systèmes de management. Le titre et l'ordre des clauses, le contenu et les définitions devront être alignés dans le cadre des prochaines révisions. »

« L'ISO 31000, cadre pour la gestion des risques, et l'ISO 27005, cadre pour la gestion des risques de sécurité de l'information, sont relativement proches, notamment du fait de l'implication de mêmes experts dans la rédaction des deux normes », nous indique Matthieu Grall. « L'ISO 31000 n'apporte pas de solution pour gérer globalement les risques de l'entreprise. Cette norme apporte une structure commune, permettant aux décideurs d'interpréter de la même manière des résultats issus de différents domaines. Une gestion des risques SSI se basant sur l'ISO 27005 peut donc être naturellement intégrée à la gestion globale des risques de l'entreprise. L'objectif de l'ISO 31000 est de décrire le processus de gestion de risques commun à tous les secteurs tels que la finance, la sécurité de l'information, la sûreté de fonctionnement, etc. L'ISO 27005 pour le secteur de la sécurité de l'information est relativement cohérente avec l'ISO 31000. Cela pourrait permettre à la SSI d'être considérée au même titre que les autres secteurs par les risks managers. »

Enfin, indique encore Matthieu Grall, « l'ISO 38500 décrit très brièvement la manière d'appliquer six principes de bonne gouvernance des technologies de l'information : définition de responsabilités, élaboration d'une stratégie, gestion des acquisitions, performance du service, conformité réglementaire et respect du comportement humain ; mais aussi aux tâches génériques des directeurs informatiques, à savoir évaluer, diriger et suivre. Il pourrait être envisagé de s'en inspirer pour « gouverner » la sécurité de l'information. Curieusement, on constate que les principes et tâches mentionnés ne sont pas ceux que l'on trouve dans les référentiels les plus utilisés dans le domaine, par exemple Cobit, Control objectives for information and

related technology, ni même ceux des domaines dans lesquels la notion de gouvernance est largement employée : gouvernance économique, politique, d'entreprise, des projets, etc. ! »

Hervé Schauer, fondateur du cabinet HSC, le rejoint et indique que « la norme ISO 38500 affiche le consensus international sur la notion de gouvernance du système d'information. C'est une norme courte qui pose des grands principes au travers desquels elle répond aux préoccupations des organismes sur la fiabilité et la rentabilité de leur informatique opérationnelle et à la pertinence de leurs nouveaux investissements dans leur infrastructure informatique. Elle donne au DSI les grands principes qu'il doit appliquer dans son métier, un peu dans une forme PDCA. »

Hervé Schauer poursuit : « En matière de sécurité l'ISO 38500 nous dit en 1.4.2 « le DSI peut être considéré responsable des failles de sécurité propres aux ressources IT ». C'est léger mais cela a le mérite d'être écrit. Et en matière de gestion des risques l'ISO 38500 nous dit en 3.3 : « Le DSI doit s'assurer que les ressources IT font l'objet d'une appréciation des risques selon les normes internationales ». L'ISO 38500 nous renvoie là à la future norme ISO 31000, norme de gestion de risques générale à tous les métiers, comme les risques industriels, la santé, et à l'ISO 27005 pour l'appréciation des risques en sécurité de l'information. Nous voyons se dessiner des imbrications, comme le processus "gestion de la sécurité" de l'ISO 20000-1 ou ITIL v3 est une mise en œuvre opérationnelle du SMSI de l'ISO 27001. Les principes posés par l'ISO 38500 aident à évaluer chaque projet d'investissement informatique ainsi que les capacités opérationnelles de son organisme. Une cohérence et un consensus international commencent à se dessiner pour gagner en compréhension mutuelle et en efficacité. Tout un chacun a intérêt à en profiter en commençant par appliquer l'ISO 38500, cela permettra à tous de partager les mêmes principes et d'y voir plus clair. »

Et Matthieu Grall conclut en indiquant que « le RSSI, en tant que conseiller auprès des responsables métiers, devrait mieux comprendre et savoir expliquer davantage comment les différents référentiels se positionnent les uns par rapport aux autres. Dans la mesure du possible, il devrait également assurer la cohérence des référentiels SSI avec les autres afin de faciliter leur appropriation par ceux qui devront les employer et exploiter leurs résultats. » ■