Salon Infosecurity 2007 : la norme ISO 27001 gagne du terrain

Comme l'a rappelé Hervé Schauer, consultant spécialisé et animateur de ce Club, « *la norme ISO 27001 permet aux entreprises de démontrer à leurs clients qu'elles ont mis en œuvre de bonnes pratiques en matière de sécurité de l'information*« .

La norme impose la mise en place d'un SMSI (Système de Management de la Sécurité de l'Information). Parmi les témoignages présentés, les trois suivants sont représentatifs d'approches différentes, mais qui se rejoignent dans leurs conclusions. Ces entreprises ont choisi de se faire certifier ou, tout simplement, de suivre la méthode et le référentiel proposé par la norme.

Le **Crédit Mutuel Nord Europe** a choisi de mettre en œuvre un SMSI pour harmoniser les pratiques, adopter un référentiel commun, et pour répondre à la pression réglementaire. L'objectif, a rappelé Luc Petitpré, RSSI, n'était pas la certification. Le projet pilote a concerné deux filiales de la banque. S'appuyant sur des éléments déjà élaborés dans le PCA (Plan de Continuité d'Activité), une analyse des risques a été conduite. Par des mesures simples et concrètes, le niveau de risque a pu être ramené à un « *niveau résiduel*« . Concernant les procédures (auxquelles la norme accorde une place particulièrement importante), la démarche de Luc Petitpré a été de « *faire d'abord, écrire après*« , les procédures les plus difficiles à exprimer étant celles concernant les processus métier de la banque. Le Crédit Mutuel optant volontairement pour une organisation simple et légère, il n'y a pas eu création de « *Comité de Sécurité*« . Au bilan, les apports principaux de ce projet ont été le recensement et la mise en cohérence des mesures existantes, et la pérennisation de la démarche.

On retrouve ces mêmes conclusions chez Gemalto, qui est en revanche allé jusqu'à la certification, et qui lors de la présentation faite au Club 27001 a mis en avant l'avantage compétitif apporté par cette certification. Avantage financier également, car les primes d'assurance ont été revues à la baisse, et le nombre d'audits clients a pu être réduit.

La certification est également un objectif au GIE Systalians, émanation des Caisses de Retraite et de Prévoyance Réunica et Bayard. Emmanuel Garnier, RSSI, a rappelé que le Groupe auquel il appartient ayant une forte culture « *certification et qualité* » (CoBit, Itil, ISO 9001,…) l'adoption de la démarche a été facilitée. Les résultats de la démarche Mehari 2004 ont pu être projetés vers le référentiel de la norme 27002 (qui représente l'ensemble des bonnes pratiques à appliquer pour la 27001). La volonté « *d'aller plus loin* » et de s'aligner sur la norme ISO 27001 en 2009 doit permettre également à Systalians de se démarquer dans le secteur, et de simplifier le dialogue avec les « métiers » internes, avec les fournisseurs, et avec les autres acteurs externes.

Dans la table ronde qui a conclu ces rencontres de RSSI, la question a été posée de savoir si la démarche de mise en conformité avec la norme avait apporté une augmentation effective du niveau de sécurité… Les participants ont tous rapporté que cette démarche avait en tout cas fortement contribué à l'adoption d'un vocabulaire commun et d'un référentiel de travail, et que le « *vrai apport* » de la norme était que celle-ci « *apportait le niveau de sécurité dont l'entreprise a besoin*« , pour reprendre la conclusion de Jean-François Louapre, RSSI d'AG2R. Le traitement du « *risque résiduel* » n'a cependant pas été vraiment abordé par les participants. Réduire le risque, c'est bien,

mais que fait-on de ce risque résiduel ? …. Heureusement, le marché commence à fournir des réponses à cette problématique, à travers les offres d'assurance, et même de « cyber-assurance »…