

Sécurité de l'information : une démarche qualité avant tout

Par André OTTAVINO, Business Performance Manager ebrc

De la sécurité informatique à la sécurité de l'information, le "CLUSSIL" perd un "S". En effet, lors de son Assemblée Générale de 2010, le "Club de la Sécurité des Systèmes d'Information Luxembourg" a choisi de changer de dénomination pour devenir le "Club de la Sécurité de l'Information Luxembourg". Au-delà de l'anecdote orthographique, l'évènement reflète une tendance chez les professionnels et responsables en sécurité informatique quant à un recentrage sur la protection des données et à une meilleure maturité de la gestion des risques.

Pourtant, au cours de ces dix dernières années, les responsables en sécurité ont du faire face à de nombreux challenges technologiques: nouveaux modes de communication via internet, évolution

des outils de partage de données ou encore besoin grandissant des utilisateurs et "direction métiers" en Business Intelligence. Face à une telle demande, la réponse la plus fréquente fut une réponse de type opérationnel, avec l'ajout, au sein du système d'information, de solutions de sécurité de plus en plus évoluées telles que firewall, proxy applicatif ou encore anti-virus, pour ne citer que les plus connus. L'activisme des sociétés de solutions de sécurité informatique a contribué à entretenir la confusion entre sécurité IT et gestion des risques. Toutefois, chaque technologie amène intrinsèquement son lot de vulnérabilités et, de facto, une charge additionnelle pour la gestion opérationnelle de la sécurité.

Dans cette course en avant, le perdant est bien souvent la Direction Informatique qui se retrouve confrontée au dilemme suivant: une demande d'augmentation des budgets de sécurité IT opposée à des restrictions budgétaires et à une demande pressante de valorisation de l'IT et de l'alignement de la stratégie IT à la stratégie métier.

Si l'on fait appel au retour d'expérience issue de l'IT governance, une issue possible à ce dilemme serait de placer le débat sur le plan stratégique. La gouvernance

ne nie pas l'importance des solutions de sécurité IT mais les positionne comme réponse à des risques spécifiquement identifiés par tous les acteurs de l'entreprise. La sécurité informatique se place sur un plan tactique et opérationnel, alors que la sécurité de l'information se place sur un plan stratégique.

L'acceptation des normes de la famille ISO 27001 en tant que bonnes pratiques en matière de gestion de la sécurité de l'information en est la preuve. En effet, l'utilisation de ces normes est de plus en plus sponsorisée par les départements de sécurité car elles apportent à la fois:

- Une méthode pragmatique en gestion des risques;
- Un langage commun entre tous les acteurs de la sécurité, de l'utilisateur à l'expert en cryptographie;
- Des principes de gouvernance entre IT et ses métiers qui permettent d'objectiver les exigences métier en termes de protection de l'information et l'adéquation des solutions et contrôles de sécurité qui en découlent.

Conscient de ces enjeux, ebrc, acteur incontournable en matière de Résilience, n'a cessé d'investir en matière de sécurité. Depuis le 1^{er} septembre 2010, ebrc dispose de la certification ISO 27001 et renforce

sa place de leader dans son secteur. La démarche de certification n'est pas une fin en soi, mais permet d'une part de contribuer à pérenniser la relation de confiance qu'ebrc entretient avec ses clients et d'autre part de faire évoluer la maturité de ses processus internes. En effet, l'enjeu principal est bien la montée en maturité des processus IT et opérationnels, garantie d'un service de qualité à la clientèle.

A ce titre, l'une des exigences de la certification est la mise en place d'une démarche d'amélioration continue, soutenue par la Direction Générale, conforme aux principes de la roue de Deming:

- PLAN Planifier ce que l'on veut faire;
- DO: Réaliser ce que l'on a planifié;
- CHECK: Contrôler régulièrement la conformité des réalisations par rapport au plan;
- ACT: Agir et réagir en conséquence.

Cette démarche qualité au sein d'ebrc se poursuivra en 2011 dans le domaine de la gestion des services IT managés ("IT Service management") via la préparation de la certification ISO 20000.

Finalement, sécurité de l'information et IT service Management présentent de nombreux points communs:

- Les supports normatifs qui sont ISO 27000, ISO 20000 ou encore ITIL sont communément reconnus comme des standards de fait en matière de bonnes pratiques;
- Des programmes de certifications pour les entreprises existent pour les deux domaines;
- Le recentrage des discussions sur les aspects stratégiques permet de formaliser les attentes des métiers et de valoriser les solutions IT associées ou à défaut d'objectiver les dépenses IT;
- La recherche d'une adéquation entre le niveau de qualité des services IT et leur coûts replace "le client" au centre de la gouvernance;
- La réflexion sur l'organisation et les rôles clefs de chacun des domaines tels que RSSI versus IT Security manager ou Responsable de production versus IT service Manager, favorise la recherche d'une meilleure maturité des processus IT;
- Et enfin, le besoin commun d'articuler les initiatives d'amélioration en un plan d'amélioration continue.

Ces deux démarches qualité contribuent indéniablement à l'industrialisation des processus IT. N'est-ce pas inconsciemment une étape préliminaire à l'arrivée du cloud computing pour en tirer les bénéfices attendus?

● Your Business Resilience Partner in the heart of Europe

Risk & Resilience Advisory | Business Continuity Services | Agile Managed Services

- Professional of the Financial Sector
- Tier IV-Design certified Data Centres
- ISO 27001 certified
- The largest carrier hotel in Luxembourg

Luxembourg • Paris • Brussels • Frankfurt

ebrc • +352 26 06 1 • www.ebrc.lu • www.ebrc.eu



Business needs Resilience
Agility breeds Success