

# Quelle gouvernance pour la sécurité des Systèmes d'Information ?

**A** l'heure de l'établissement des budgets informatiques pour 2011, il n'est pas toujours aisé pour un Responsable de la Sécurité des Systèmes d'Informations (RSSI) ou pour un Responsable IT d'argumenter pour pouvoir disposer des moyens nécessaires pour mener à bien sa mission sécuritaire. Ce constat est relayé par le CLUSIF (Club de la Sécurité de l'Information Français) qui publie chaque année une étude sur les menaces et les pratiques de sécurité en France. En effet, cette étude a relevé que la part du budget consacré à la Sécurité de l'Information avait malheureusement tendance à stagner entre 2008 et 2010. Cela démontre la nécessité de mieux cibler ce type d'investissements.

Dans le cadre de ses missions de conseil en sécurité des Systèmes d'Information, l'équipe Risk & Resilience d'ebrc est régulièrement sollicitée par les RSSI pour les aider à définir et à mettre en place un cadre "sécurité", nécessaire afin de pouvoir disposer d'un fil conducteur pour leurs projets mais aussi pour obtenir ainsi une meilleure visibilité auprès de leur Direction... Quel cadre utiliser dans "la jungle" existante : COSO, ISO 27001, COBIT, ITIL... ? Les référentiels existants sont trop génériques et ne couvrent pas l'ensemble de la problématique de la Sécurité de l'Information, soit ils ne donnent pas assez d'informations sur la manière de mettre en œuvre ce cadre de contrôle et de gouvernance de la sécurité.

COSO s'intéresse principalement à l'efficacité et l'efficience des opérations, à la fiabilité des informations financières et à la conformité aux lois et aux règlements. Ce cadre global est un référentiel de contrôle interne, ayant pour objectif final la loi de sécurité financière. Il n'aborde pas la mise en œuvre de la Sécurité de l'Information en tant que telle.

COBIT (Objectifs de Contrôle de l'Information et des Technologies Associées) est un guide de bonnes pratiques basées sur des objectifs de contrôles sur l'IT des entreprises. Il s'agit d'un outil de bonne gouvernance essentiellement. Les aspects relatifs à la Sécurité de l'Information y sont brièvement décrits en tant qu'objectifs de contrôles.

ITIL, "Bibliothèque pour l'Infrastructure des Technologies de l'Information" est un ensemble d'ouvrages recensant les bonnes pratiques ("best practices") pour la gestion des Services Informatiques (ITSM), dictées par l'Office Public Britannique du Commerce (OGC). Ce référentiel inscrit la Sécurité de l'Information dans un ensemble complexe de processus et de design des Services Informatiques gérés. ebrc utilise ce référentiel pour organiser le déploiement de ses ser-

vices informatiques internes et auprès de ses clients. ebrc est également en train de mettre en place la norme ISO/IEC 28000:2005 sur cette base en vue d'une certification officielle début 2011.

ISO 9001:2008 fait partie de la série des normes ISO 9000, relatives aux systèmes de gestion de la qualité. Elle dicte les exigences organisationnelles requises pour l'existence d'un système de gestion de la qualité. Les aspects relatifs à la Sécurité de l'Information sont décrits dans une approche documentaire. Ce type de référentiel est régulièrement utilisé par les entreprises. ebrc ne déroge pas à la règle, car l'ISO 9001 est la fondation de la qualité pour les autres normes.

ISO 27001:2005 : pour répondre à la nécessité d'adopter un référentiel complet, cohérent et spécifique à la Sécurité de l'Information au sens large, ebrc, conscient de l'apport de cette norme dans le domaine de la Sécurité des Systèmes d'Information, a développé au cours des trois dernières années les compétences de ses consultants suivant la norme ISO/IEC 27001:2005 (certifications Lead Auditor et Implementer). Afin de contribuer au développement de cette norme sur le territoire luxembourgeois, ebrc a voulu montrer l'exemple en se fixant l'objectif de la certification.

La norme ISO 27001 répond idéalement aux besoins de mettre en place non seulement un système de gestion de la Sécurité de l'Information efficace basé sur une analyse de risques simple et facile à maintenir, mais aussi sur une évaluation, des objectifs et des contrôles structurés.

Depuis le 1<sup>er</sup> septembre 2010, ebrc dispose officiellement de ce certificat et se place troisième société certifiée au Luxembourg et première dans son domaine d'activités. Si l'on connaît le nombre d'entreprises certifiées au total dans le monde (12 934 entreprises recensées dans 117 pays fin 2009, source [www.iso.org](http://www.iso.org)), il est plus difficile de connaître les chiffres exacts par pays. Il y aurait seulement 19 entreprises certifiées en France pour 15 au Benelux et 144 en Allemagne (source [www.iso27001certificates.com](http://www.iso27001certificates.com)). Ces écarts montrent bien que l'intérêt de la certification n'est pas ressenti de la même manière partout dans l'Union Européenne. Cela n'empêche pas ebrc de montrer l'exemple, à l'heure de la confiance numérique accordée au Grand-Duché de Luxembourg.

La norme 27001 représente pourtant des avantages non négligeables sur de nombreux points :

- Au niveau marketing: le peu d'entreprises arborant cette certification au niveau européen représente un critère de différenciation et d'avant-garde pour la société certifiée.
- Au niveau commercial: la certification devient de plus en plus un critère de sélection dans les relations commerciales. Il n'est pas rare qu'elle soit exigée dans les appels d'offres, notamment pour des sociétés outre-Atlantique.
- Au niveau des relations avec les tiers: une certification démontre que des efforts sont faits pour améliorer le management de la Sécurité de

l'information ce qui peut rassurer les différents partenaires: clients, actionnaires, fournisseurs, etc.

- Au niveau de la gestion des risques: maîtriser la confidentialité, l'intégrité et la disponibilité de l'information et identifier les menaces, grâce à une réelle évaluation du risque permet d'évaluer la vulnérabilité de notre système d'information, les probabilités de dysfonctionnements et les impacts potentiels.

- Anticiper les pressions réglementaires présentes et futures: de plus en plus de réglementations locales et européennes sont prévues pour encadrer plus strictement les entreprises sur les domaines de la gestion du risque et de la Sécurité de l'Information. ISO 27001 est une réponse à cette pression réglementaire.

Si beaucoup de sociétés appliquent certaines bonnes pratiques déterminées par cette norme, peu poussent la démarche jusqu'à la certification.

Alors pourquoi les entreprises européennes, et plus particulièrement celles d'Europe de l'Ouest semblent frileuses à l'idée d'aller vers la certification ISO 27001? Une des raisons principales est sans doute que la certification à cette norme est bien souvent appréhendée comme un processus long et coûteux. Aujourd'hui, fort de son expérience personnelle, ebrc peut rassurer les éventuels candidats sur ce point et est à même de les guider dans les différentes étapes menant à la certification. La première étape d'un projet de certification ISO 27001 est d'obtenir l'aval et le support de la Direction, ce qui est crucial pour la survie du projet. Dans le cas d'ebrc, cette étape a été facilitée par le fait que la décision venait de la Direction. Le challenge principal est de formaliser les bonnes pratiques en matière de sécurité acquises au fil des ans et de sensibiliser les employés.

Le processus de certification consiste à mettre en place le système de gestion de la sécurité de l'information (SMSI), basé sur un périmètre de certification (le scope). La certification exige le respect d'une série de clauses que la norme établit, à savoir:

- une politique de gestion de la Sécurité de l'Information;
- une gestion des risques opérationnels basé sur la norme ISO 27005;
- une revue par l'audit interne du système de gestion basé sur l'ISO 27006;
- la mesure de mesures et contrôles mis en place selon la norme ISO 27004;
- la mise en œuvre des contrôles sélectionnés selon le périmètre de la certification basé sur l'ISO 27002;
- la mise en place d'un système de gestion de la Sécurité de l'Information, à la fois efficient, en amélioration continue, communiqué à la direction, selon la norme ISO 27003;
- la mise en place d'un système de gestion documentaire.

Plus spécifiquement, la certification vise à évaluer la maturité d'une entreprise vis-à-vis du respect des objectifs de contrôles des chapitres suivants:

- Chapitre 4: l'appréciation et le traitement des risques opérationnels (incluant les risques infor-

matiques, idéalement selon la norme ISO 27005); (Les objectifs de contrôles issus de la norme ISO 27002)

- Chapitre 5: la mise en place et en œuvre de la Politique de Sécurité de la société;
- Chapitre 6: l'organisation interne et avec les tiers de la Sécurité de l'Information;
- Chapitre 7: la gestion des actifs;
- Chapitre 8: la sécurité liée aux ressources humaines;
- Chapitre 9: la sécurité physique et environnementale;
- Chapitre 10: la gestion de l'exploitation et des télécommunications;
- Chapitre 11: le contrôle d'accès;
- Chapitre 12: l'acquisition, développement et maintenance des systèmes d'information;
- Chapitre 13: la gestion des incidents liés à la Sécurité de l'Information;
- Chapitre 14: la gestion du plan de continuité de l'activité;
- Chapitre 15: la conformité légale, réglementaire et contractuelle.

La certification ne doit pas être une fin en soi. Un des objectifs et surtout l'une des exigences de l'ISO 27001 est l'amélioration continue du système de gestion de la Sécurité de l'Information mis en place selon le cycle Plan - Do - Check - Act, issue de la fameuse Roue de Deming.

- Plan: Préparer, planifier (ce que l'on va réaliser);
- Do: Développer, réaliser, mettre en œuvre;
- Check: Contrôler, vérifier;
- Act (ou Adjust): Agir, ajuster, réagir.

Une fois la certification obtenue, des audits de surveillance ont lieu tous les ans au cours desquels la société certifiée devra alors démontrer sa volonté d'améliorer en continu la sécurité de son système d'information. En conclusion, loin d'être un travail fastidieux et insurmontable en soi, la certification a permis à ebrc, en plus des avantages cités précédemment, d'identifier les objectifs de contrôles qui nécessitent d'être améliorés et ainsi construire un plan directeur de sécurité qui définit clairement les projets et par conséquent les besoins en termes de budget pour les prochaines années.

La Sécurité de l'Information est un souci permanent pour ebrc. Non seulement le système de gestion de la Sécurité de l'Information d'ebrc apporte un niveau élevé de confiance auprès de ses clients, mais il démontre également qu'ebrc a atteint une maturité au niveau technologique mais aussi au niveau de ses processus internes. Fort de ses nombreuses distinctions et certifications, ebrc est devenu un acteur internationalement reconnu et incontournable dans son secteur et peut dès lors se distinguer des acteurs traditionnels sur le marché par son dynamisme et par sa quête d'excellence dans les domaines des Data Centres (Tier IV), ses services d'infogérance, son expérience unique en continuité des opérations, son conseil et la Sécurité de l'Information au sens large.

Olivier ANTOINE & Mark GEISLER  
ebrc Risk and Resilience Advisory



## • 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

