Les PME et la certification ISO/IEC 27001

Le Centre de Recherche Public Henri Tudor s'engage pour la sécurité de l'information.

Quelle entreprise luxembourgeoise peut se targuer de ne pas être concernée par la loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel ? Données clients, renseignements sur les fournisseurs, coordonnées et salaires des employés sont autant d'exemples d'informations relatives à la vie privée des personnes physiques pour lesquelles la loi impose une sécurité de traitement. Cependant, nul n'ignore aujourd'hui que la sécurité des informations est un problème complexe, en perpétuelle évolution et que le risque zéro n'existe pas. Comment donc respecter les contraintes réglementaires et être conforme à cette loi ? Si l'on se penche de plus près sur l'article 23 de celle-ci, le législateur impose d'être à l'état de l'art en termes de sécurité, tout en tenant compte des risques et des coûts liés à la mise en œuvre des mesures. Une solution s'impose donc de fait : la mise en place d'un Système de Management de la Sécurité de l'Information (SMSI).

La norme ISO/IEC 27001 décrit les exigences à respecter afin d'établir un SMSI. L'objectif est d'obtenir un cycle d'amélioration continue pour la sécurité de l'information. Ce cycle s'articule principalement autour d'une appréciation des risques, ayant pour but de définir au plus juste les mesures de sécurité à mettre en place au regard des risques encourus. Cependant, le constat réalisé conjointement par le ministère de l'Economie et le CRP Henri Tudor est clair : la complexité et le coût de la démarche sont un frein évident à l'adoption de la norme ISO/IEC 27001. Cet état de fait est renforcé par la nature du tissu économique local, composé de plus de 90 % de PME aux moyens et ressources par nature limités.

> « Une solution s'impose de fait : la mise en place d'un Système de Management de la Sécurité de l'Information (SMSI) »

Un modèle en grappe

Pour répondre à cette problématique, le ministère de l'Economie et du Commerce extérieur a commandité et cofinancé le projet *Information Security Management System pour PME* (ISMS-PME) mené par le CRP Henri Tudor. Deux résultats principaux sont attendus. Le premier est un guide d'implémentation d'un SMSI. Sur base de l'expérience du CRP Henri Tudor et de la connaissance d'experts luxembourgeois du domaine, ce guide décrit une démarche simple et efficace à suivre pour les PME. En support à ce guide, le second résultat du projet est un ensemble de modèles et d'outils logiciels permettant d'accélérer la démarche. Les expérimentations réalisées ont clairement montré l'apport d'une telle base de travail, pouvant être réutilisée et adaptée au contexte ou servir de source d'inspiration pour les différentes procédures nécessaires au respect de la norme. Ce guide et ses outils supports ont aujourd'hui été expérimentés dans plusieurs organismes luxembourgeois et s'apprêtent à être transférés aux professionnels du domaine.

Conscient qu'un tel projet, bien que fondamental, n'est pas une fin en soi en vue d'augmenter la pénétration de l'ISO/IEC 27001 au Luxembourg, une nouvelle initiative est actuellement à l'étude au CRP Henri Tudor. Elle proposera un modèle en grappe de préparation à la certification ISO/IEC 27001. Par modèle en grappe, on entend la création d'un groupe de 3 à 5 entreprises mutualisant les coûts et leur expérience dans la mise en place d'un SMSI. Ce modèle s'articulera d'une part, autour de formations communes et, d'autre part, autour d'un coaching personnalisé à la mise en place du SMSI dans chaque entreprise. Cette initiative aura notamment pour objectif de démontrer la réalisabilité pour une PME d'une telle certification à un coût acceptable. Ce projet devrait démarrer en janvier 2010 et l'étude des entreprises potentielles est actuellement en cours. En effet, dans ce type de démarche commune, l'implication et la disponibilité des ressources allouées par l'entreprise est fondamentale pour garantir un avancement efficace et synchrone de la grappe.

Nicolas Mayer
Product manager
Security & Continuity Management
CRP Henri Tudor
nicolas.mayer@tudor.lu