La modélisation en support à la certification ISO/IEC 27001:

Un pas de plus vers la confiance

La confiance est actuellement un élément crucial pour les institutions financières. Obtenir la confiance des actionnaires, des clients, des partenaires, des autorités de tutelle est une nécessité: l'ensemble des parties prenantes en est demandeur. Au niveau de la sécurité des SI (Système d'Information), la certification ISO/IEC 27001 se présente, à l'heure actuelle, comme un outil de premier ordre pour apporter cette confiance. Toutefois, ce référentiel étant en phase de développement et d'adoption par le marché européen, de nombreux défis sont encore ouverts afin d'améliorer sa mise en œuvre.

La certification pour augmenter le niveau de confiance de la sécurité des SI

La certification de produits ou de services a prouvé depuis de nombreuses années qu'elle était un outil adapté pour fournir de la confiance aux parties prenantes. Les certifications fondées sur les "systèmes de management" ont largement démontré leur efficacité, et les certifications qualité (ISO 9001) et environnementale (ISO 14001), en sont la parfaite illustration. Leur valeur pour une entreprise et l'intérêt qu'elles suscitent ont poussé la communauté internationale de normalisation en sécurité des SI à produire une norme de système de management sur la sécurité de l'information. Issue en premier lieu d'un standard britannique (BS7799-2), elle est devenue en octobre 2005 une norme internationale: ISO/IEC 27001. La norme ISO/IEC 27001 traite de l'établissement et de la gestion d'un Système de Management de la Sécurité de l'Information (SMSI). Elle s'articule autour du modèle de processus PDCA (Plan-Do-Check-Act) en vue de placer la sécurité du SI de l'entreprise en amélioration continue. Ainsi, quel que soit le niveau réel de sécurité d'une entreprise, ce mode de fonctionnement garantit que ce dernier va s'améliorer jusqu'à tendre vers le niveau optimal de sécurité requis, au regard de ses activités. La pierre angulaire de cette certification reste l'application d'une méthode de gestion des risques de sécurité, dans le but d'aligner les mesures de sécurité mises en œuvre aux besoins de sécurité de l'entreprise et à ses ressources.

La modélisation en support à la certification ISO/IEC 27001

Parmi les nombreux défis que pose l'implémentation d'un SMSI au sein d'une entreprise, deux d'entres eux doivent être soulignés. Tout d'abord, la documentation de l'ensemble du SMSI constitue un travail important. Disposer déjà d'une ossature ISO 9001 permet par exemple de réduire l'ampleur de la tâche, en y appliquant une gestion documentaire identique à celle déjà adoptée. Cependant, la documentation de l'étude des risques et de l'ensemble des mesures de sécurité appliquées sur le SI, afin de diminuer ces risques, reste à faire. Elle est généralement réalisée sous la forme de tableaux, qui d'une part peuvent prendre des proportions importantes et qui, d'autre part, n'offrent pas une vision intuitive des risques et de leur traitement. Ensuite, une fois l'étude des risques réalisée, il est nécessaire de la maintenir à jour durablement en la réactualisant et en tenant compte de l'ensemble des modifications (notamment au niveau de l'architecture du SI) ayant potentiellement un impact sur la sécurité. Sans une vue globale présentant à la fois les composants du SI, les risques les menaçant et les traitements appliqués aux risques, cette mise à jour est généralement difficile, en particulier dans le cas où la personne chargée de mettre à jour l'étude des risques est différente de celle ayant réalisé l'étude initiale.

Le CRP Henri Tudor travaille actuellement sur une approche basée sur la modélisation. Il souhaite ainsi satisfaire aux exigences de la norme et faciliter l'étape d'appréciation des risques. Des premières analyses et expérimentations, il ressort que l'utilisation continue de la modélisation est un plus indéniable à la préparation à la certification. Le modèle, support à la communication, va permettre d'accélérer les phases d'analyses réalisées par les différentes parties tout au long du processus d'établissement du SMSI. De plus, se connecter et s'aligner sur les modélisations des processus business permet de réutiliser un travail souvent déjà existant et validé, afin de démarrer l'appréciation des risques. Au final, une traçabilité complète de la chaîne "actif de l'entreprise – risque – mesure de sécurité" est proposée et sa pertinence, par rapport aux études sous forme de tableaux, est clairement accrue. Actuellement, le principal point d'amélioration de ces travaux reste la partie visuelle du langage de modélisation. Si, d'une part, les aspects conceptuels et méthodologiques semblent aujourd'hui fixés, on constate, d'autre part, que les aspects liés à l'ergonomie des modèles, ainsi que la représentation claire de ces derniers, sont des points qui restent à approfondir.

Nicolas MAYER, ingénieur R&D, CRP Henri Tudor
nicolas.mayer@tudor.lu