

L'ISO 27001

Les audits de sécurité techniques permettent de prendre une photo du système d'information ou d'une application, ils délivrent des recommandations fondamentales et sans équivalent. Cependant, ces recommandations ne sont souvent pas prises en compte, ou elles le sont trop tard, pas partout ou pas au bon endroit.

Combien de fois avez-vous recommandé l'application des correctifs de sécurité ? Combien de fois avez-vous trouvé les mêmes problèmes à 2 ou 3 ans d'intervalle ?

La sécurité technique prend sa pleine efficacité avec une bonne organisation de la sécurité, réaliste et pragmatique. C'est ce que permet la norme ISO 27001. Elle définit un *Système de Management de la Sécurité de l'Information (SMSI)*. Sous ce terme barbare, il est simplement suggéré aux *Responsables de la Sécurité des Systèmes d'Information (RSSI)* de s'organiser, pour gérer la sécurité dans le temps et pour améliorer au travers du cercle vertueux *Plan-Do-Check-Act* la manière avec laquelle l'organisme gère la confidentialité, l'intégrité et la disponibilité des informations qui constituent son patrimoine informationnel. Avec le processus imposé par le SMSI de l'ISO27001, l'organisme entre dans une amélioration de sa gestion de la sécurité du système d'information. Il n'est plus possible de sélectionner comme mesure de sécurité la réalisation d'un test d'intrusion ou d'un audit de sécurité sans tenir compte après des recommandations. Il faudra expliquer et justifier pourquoi celles-ci n'ont pas été mises en œuvre. Le SMSI intègre ses propres mécanismes de vérification périodique : audits internes, indicateurs, revue de direction, etc. Qui permettent de garantir que les audits de sécurité techniques servent pour de vrai.

L'ISO 27001 impose aussi de réaliser une appréciation des risques. Celle-ci est pragmatique et accessible à tous, elle peut rester simple, mais elle obligera à réfléchir sur ce qui compte réellement pour la direction. Ainsi, les mesures de sécurité sont

orientées là où elles sont le plus utiles. Le traitement du risque qui suit l'appréciation vous demande d'intégrer vos contraintes dans la sélection de dispositifs de sécurité, comme les réticences des utilisateurs. Là encore, c'est l'équilibre qui est visé.

Les étapes suivantes constituent donc des fondations saines pour une gestion rationalisée, efficace et utile de la sécurité des systèmes d'information ; énoncé des objectifs de l'organisation, analyse de risques, adéquation avec les activités de l'organisation, formalisation des traitements du risque parmi l'évitement, l'acceptation approuvée par la direction, le transfert via des assureurs ou organismes partenaires, et la réduction via une mesure de sécurité, pertinence des mesures de sécurité choisies, ou justification des mesures non-chosies, mesures de l'efficacité des choix effectués : *feed-back* et amélioration continue pour chaque incident détecté.

Ces dernières étapes (choix des traitements du risque, mesures des efficacités, amélioration continue par des mesures préventives et correctives) sont la clé du cercle vertueux *Plan-Do-Check-Act* qui est décliné sur chaque service, chaque processus, chaque mesure de sécurité.

De la panne de papier de l'imprimante à la règle de pare-feu any-any ajoutée puis oubliée par Frédo pour ses propres tests, chaque incident affectant le business de l'organisation sera doublement traité, afin de le corriger sur place, et pour empêcher que l'incident ne se reproduise. Cette méthode peut paraître initialement coûteuse, mais est rentable dès le moyen terme puisqu'elle oblige le niveau de sécurité à toujours aller de l'avant. Le livre d'Alexandre Fernandez-Toro (*Management de la sécurité de l'information* paru aux éditions Eyrolles) explique très clairement comment l'ISO 27001 peut structurer la sécurité tant d'un point de vue technique qu'organisationnel sans pour autant se lancer dans un projet complexe.

L'ISO 27001 s'utilise dans un objectif de certification pour apporter de la confiance aux parties prenantes, mais l'esprit ISO 27001 sans certification permet aussi de développer de bonnes pratiques internes, et d'échanger des idées et des bonnes pratiques entre différents services qui s'auditeront mutuellement. Pensez à l'ISO 27001 pour vous organiser en SSI, c'est simple, adapté à tous les métiers, peu coûteux, pragmatique, et redoutablement efficace.



À propos de l'auteur
Ingénieur de l'École polytechnique et de l'École Nationale Supérieure des Télécommunications (ENST), Raphaël Marichez participe à plusieurs activités associatives, notamment l'association *Polytechnique.org* qu'il a présidée durant deux ans, et l'équipe sécurité de *Gentoo Linux*. Après plusieurs stages, en recherche en cryptographie, et en conseil dans les technologies de l'information, il rejoint l'équipe HSC en 2006 avec une expertise dans les domaines du courrier électronique et de la lutte contre le spam, puis obtient la certification *Lead Auditor ISO 27001* par LSTI en janvier 2007.