La gestion des risques de la sécurité des systèmes d'information a sa norme internationale : l'ISO 27005.

- Informatique - Sécurité Informatique -

Date de mise en ligne : lundi 9 juin 2008

Hervé Schauer attire notre attention sur la publication de la norme ISO 27005. « Il s'agit de la première norme internationale de gestion de risques en sécurité de l'information. Elle a été publiée le 4 juin 2008 par l'ISO (www.iso.ch), souligne le fondateur du cabinet HSC.

La norme ISO 27005 propose une méthodologie de gestion de risques conforme à la norme ISO 27001, tout en étant utilisable de manière autonome. Elle applique à la gestion de risques le cycle d'amélioration continue PDCA utilisé dans les normes de systèmes de management, comme l'ISO 27001 en sécurité de l'information.

Pour rappel, l'ISO 27001 a été publiée en 2005. Elle définit le Système de Management de la Sécurité de l'Information (ou SMSI). C'est la norme vis-à-vis de laquelle les personnes se certifient, qui définit le processus d'amélioration de la sécurité à mettre en place sous la responsabilité du RSSI.

« L'ISO 27001 exige de réaliser une appréciation des risques. La norme ISO 27005 est le guide expliquant comment faire sa gestion des risques en sécurité de l'information. L'appréciation des risques est un domaine où il a existé dans chaque pays des méthodes locales. En France, par exemple on trouve EBIOS, Mehari, ERSI-CAP, etc. L'ISO 27005 est la synthèse de toutes ces méthodes et reflète le consensus international sur le sujet, estime Hervé Schauer.

L'ISO 27005 est une norme complètement différente de l'ISO 27001 qui la complète pour une des brique les plus complexes : l'appréciation des risques.

"Un des point très nouveau dans l'ISO 27005, c'est le formalisme avec lequel la norme recommande de faire valider le plan de traitement des risques et le risque résiduel qui en découle par la direction générale. Ainsi le RSSI ne prends pas des responsabilités à la place de sa direction générale, c'est à elle de s'engager et prendre ses responsabilités, conclut Hervé Schauer.

Post-scriptum :

http://securite.reseaux-telecoms.ne...