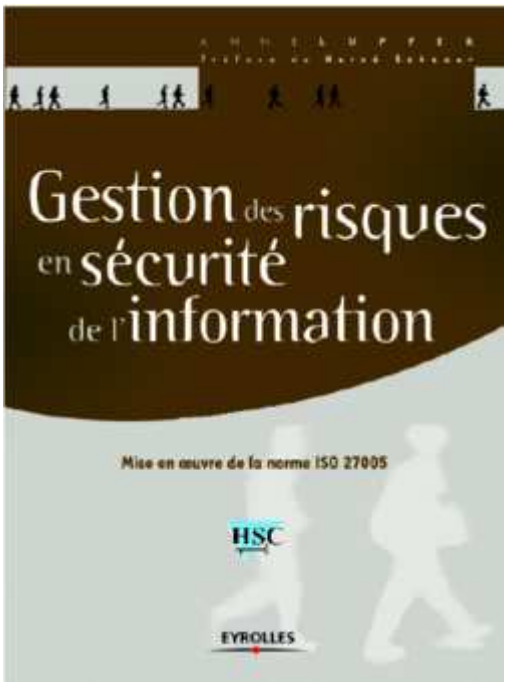
Hervé Schauer Consultants (HSC)
Communiqué de presse

Paris, le 15 septembre 2010



Premier livre français dédié à la norme ISO 27005 : "Gestion des risques en sécurité de l'information, mise en oeuvre de la norme ISO 27005", par Anne Lupfer - 252 pages - 39,90 euros

La gestion des risques a parfois été le parent pauvre de la sécurité de l'information. De nombreux organismes appliquent des mesures de sécurité pour respecter un catalogue de mesures, pour être conforme à un référentiel, ou pour faire comme les autres. Ils ne savent pas nécessairement en quoi ces dispositifs de sécurité réduisent des risques. L'avènement de la norme ISO 27001 qui permet d'organiser sereinement sa sécurité des systèmes d'information sous forme d'un système de management de la sécurité de l'information (SMSI), impose une approche par la gestion des risques.

L'obligation de la réalisation d'une appréciation des risques est une caractéristique fondamentale de l'ISO 27001 en opposition avec les approches conformité comme SoX ou PCI-DSS. La norme ISO 27001 précise en un peu plus d'une page ce que doit obligatoirement comporter une gestion des risques en sécurité de l'information. C'était un peu léger et la norme ISO 27005 est venue combler ce manque avec détail, tout en en allant plus loin, car l'ISO 27005 s'applique non seulement aux SMSI mais à tout type de situation, de manière autonome, comme par exemple la gestion des risques sur un système embarqué.

La norme ISO 27005

La norme ISO 27005 est un guide définissant une méthode d'appréciation des risques en sécurité de l'information. L'ISO 27005 a fait l'objet d'un consensus international et elle permet une meilleure compréhension mutuelle à travers le monde.

L'ISO 27005 apporte une nouveauté fondamentale par rapports aux méthodes qui l'ont précédée comme EBIOS ou Mehari : la gestion des risques dans la durée, dans le temps. Il ne s'agit plus de gérer les risques en y travaillant dur quelques semaines, puis en recommençant son travail quelques années plus tard, mais de gérer les risques en sécurité de l'information au quotidien. Ce changement majeur est imposé par l'approche continue de l'ISO 27001, mais il représente le principal changement par rapport aux méthodes antérieures.

L'ISO 27005 est également la première méthode qui impose à la direction générale d'être parfaitement informée, et lui impose de prendre ses responsabilités en toute connaissance de cause, ce qui clarifie les responsabilités et facilite les arbitrages budgétaires.

Le livre "Gestion des risques en sécurité de l'information"

Cet ouvrage est une aide indispensable à la compréhension et l'application de la méthode ISO 27005. Comme beaucoup de normes, l'ISO 27005 est très structurée mais peu didactique. Comment inventorier et valoriser des actifs ? Comment identifier des menaces, des vulnérabilités, des scénarios d'incidents, des conséquences ? Comment estimer et évaluer des niveaux de risque ? Quels risques doivent être réduits ou transférés ? Comment donner à la direction générale de quoi faire son arbitrage budgétaire ? Au travers d'un schéma de toutes les activités décrites dans la norme, le livre détaille chaque étape, avec des exemples et des scénarios d'incidents réels qui reflètent le savoir-faire de l'auteur.

À qui s'adresse ce livre ?

Cet ouvrage est destiné à tous les responsables sécurité (RSSI) et leurs équipes, et les personnes impliquées dans la mise en oeuvre ou l'audit d'un SMSI. C'est également un livre utile aux DSI, responsables et chefs de projet informatique, et les personnes devant analyser les risques informatiques ou gérer des risques informatiques et en sécurité de l'information dans leur projet. L'ISO 27005 demande à ce que le gestionnaire de risque en sécurité de l'information s'aligne sur les risques opérationnels ou industriels, aussi l'ouvrage est profitable aux gestionnaires de risques désirant approfondir le volet sécurité de l'information. Enfin le livre sera une aide précieuse à ceux qui souhaitent obtenir la certification individuelle "ISO 27005 Risk Manager".

L'auteur Anne Lupfer

Anne Lupfer est entrée chez HSC avec une expérience de gestion des risques dans l'assurance. Elle a créé la formation à la gestion des risques en sécurité chez HSC et et a été une des premières à mettre en œuvre concrètement la méthode ISO 27005 en clientèle.
C'est à la fois son expérience sur le terrain et ses échanges avec les stagiaires que nous avons eu le plaisir de préparer à la certification ISO 27005 Risk Manager que vous retrouverez dans cet ouvrage. Anne Lupfer est ingénieur diplômée de l'ECE, et elle a rejoint un grand groupe pour lequel elle met à profit son expérience acquise en gestion des risques.

Séance de dédicaces le jeudi 7 octobre à 17h00

A l'occasion de la sortie de son livre, Anne Lupfer signera son ouvrage lors d'une séance de dédicaces sur le stand HSC aux Assises de la Sécurité au Grimaldi Forum à Monaco le jeudi 7 octobre à 17h00. Ceux qui auront déjà acquis l'ouvrage sont invités à venir avec leur exemplaire, et à titre exceptionnel le livre sera vendu sur le stand HSC durant le salon.

A propos du livre "Gestion des risques en sécurité de l'information, mise en oeuvre de la norme ISO 27005" :

Auteur : Anne Lupfer
Préface : Hervé Schauer
Editeur : Eyrolles
Code éditeur : G12593
Parution : septembre 2010
Prix : 39,90 euros
ISBN : 978-2-212-12593-1

A propos d'HSC

Fondée en 1989, HSC (Hervé Schauer Consultants), est une société de conseil, d'audit et d'expertise en sécurité des systèmes d'information, pionnière de la mise en oeuvre de la méthode ISO 27005 en France. HSC propose des prestations de conseil et d'accompagnement à l'appréciation des risques et à mise en place de SMSI. HSC est également le n°1 français sur les formations certifiantes aux normes ISO 27001 et ISO 27005, et plus de 1500 professionnels de la SSI ont suivi une formation HSC.