

La gestion de risque pour la série de normes iSO 2700x

L'ensemble des normes iSO 27001 à 27005 entendent bien servir de garantie de prise en compte de la sécurité des systèmes d'informations pour les entreprises. En cela, elles décrivent pas à pas toute le processus «Plan-Do-Check-Act».

La norme ISO 27001 permet aux entreprises et aux administrations d'obtenir une certification qui atteste de la mise en place effective d'un système de management de la sécurité de l'information (SMSI). Elle garantit aux parties prenantes (clients, actionnaires, partenaires, autorités de tutelle, etc.) que la sécurité des systèmes d'information a été pleinement prise en compte et que l'organisme s'est engagé dans un processus d'amélioration continue.

En ce sens, la norme ISO 27001 définit les tâches à respecter pour que ce processus « Plan-Do-Check-Act » ou Roue de Deming soit en place (voir l'encadré Roue de Deming). Elle est complétée par la norme ISO 27006, texte que doivent respecter les organismes de certification. Une série de guides l'accompagne (voir le tableau 1). L'ISO 27005 présente la mise en œuvre de la partie appréciation des risques de la sécurité de l'information de l'ISO 27001. En cela, elle complète les articles 4.2.1 c) à 4.2.1 f), plus le 4.2.3.d) de la norme ISO 27001.

ISO 27005, UNE Norme exhaustive

Une norme est habituellement un consensus entre les acteurs du marché qui représentent le noyau commun sur lequel tout le monde a réussi à

Terminologie

Habituellement, on utilise la terminologie « méthode d'analyse de risque ». Cependant dans les documents anglo-saxons, on emploie « assessment » et « analysis ». Pour éviter toute confusion, on traduira « risk assessment » par « appréciation des risques » ou « appréciation du risque » et « risk analysis » par « analyse de risque ».

s'entendre. Elle ne peut donc être plus exhaustive que les méthodes qui l'ont précédée, comme CRAMM, MEHARI, EBIOS, OCTAVE, etc. Cependant, la norme ISO 27005 est complète, autonome et se positionne donc comme la méthodologie universellement adoptée de par le monde pour l'appréciation des risques en SSI. On y retrouve

les influences des méthodes existantes (voir la figure 1), en premier lieu les rapports techniques de l'ISO sur le sujet développés depuis le début des années 1990 (ISO TR 1335-2 puis ISO TR 1335-3), en second lieu la filière britannique CRAMM (1985), BSI PD3002 (1998), BSI BS7799-3 (2006), mais aussi des influences européennes continentales comme EBIOS (1997), méthode publiée par la DCSSI (Direction centrale à la sécurité des systèmes d'information).

L'ISO 27005 définit un processus de gestion de risque (voir la figure 2), qui s'articule en « Plan-Do-Check-Act » comme le SMSI dans sa globalité, et qui s'applique librement à tout sous-ensemble du SMSI :- Plan... : Identifier, quantifier et analyser les risques et choisir les actions appropriées pour réduire les risques ;

ISO 27002	Mesure de sécurité pour un SMSI, norme connue précédemment sous la référence ISO 17799
ISO 27003	Guide de mise en œuvre d'un SMSI
ISO 27004	Guide de mesurage d'un SMSI, qui explique comment sélectionner des indicateurs
ISO 27005	Gestion de risque pour un SMSI, publiée normalement en 2008.

tableau 1 – Série de guides accompagnant la norme iSO 27001.

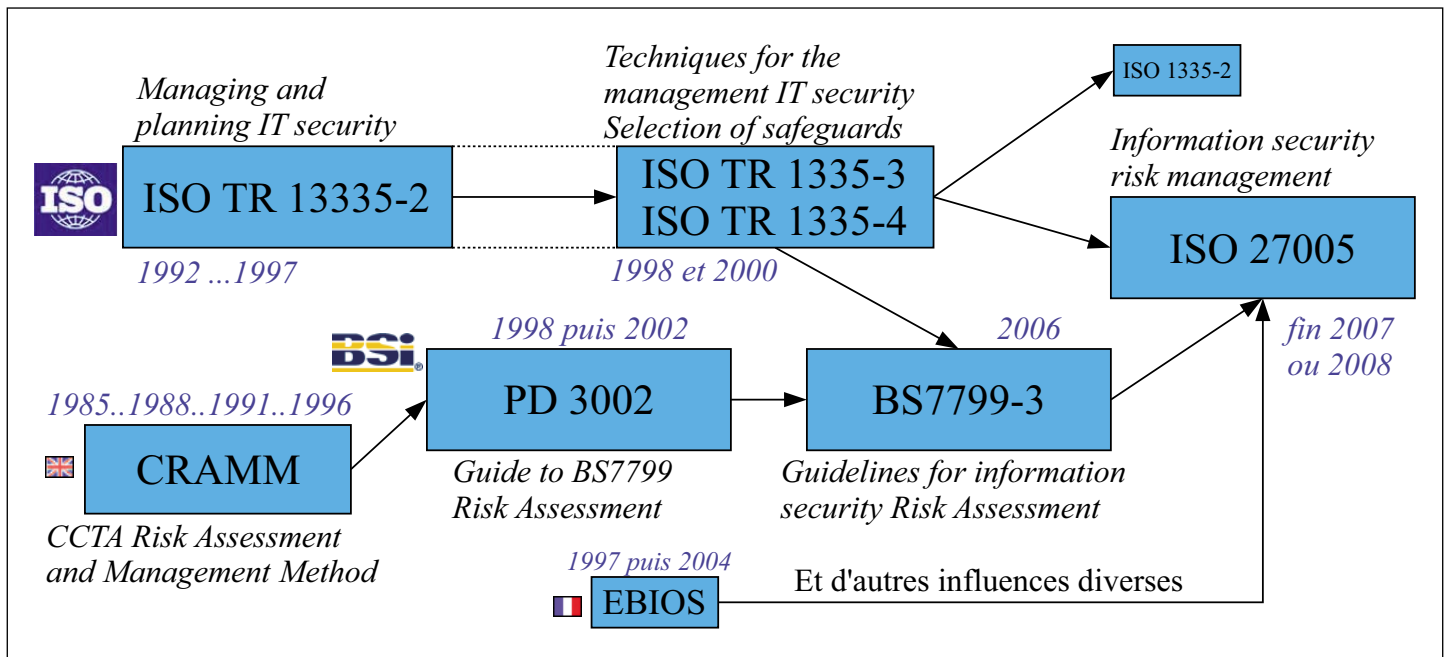


Figure 1 – Historique de l'ISO 27005.

- Do..... : Implémenter les actions pour réduire les risques et éduquer la direction et le personnel sur les risques ;
- Check... : Surveiller et réexaminer les résultats, l'efficacité et l'efficacité du processus de gestion de risque ;
- Act.... : Rectifier le traitement du risque et améliorer le processus de gestion du risque.

ETABLIR LE CONTEXTE

Avant toute chose, le premier processus est l'établissement du contexte, à savoir la délimitation du processus de gestion de risque, les contraintes qui pèsent sur l'organisme et la définition des critères de base :

- critères d'évaluation des risques, qui doivent être cohérents avec l'évaluation des actifs faite dans l'activité suivante ;
- critères d'impact, car un incident peut affecter tout ou partie d'un actif ou plusieurs actifs ;
- critères d'acceptation des risques, permettant de voir quel est le seuil au-delà duquel la direction n'acceptera pas de conserver un risque.

L'APPROCHE ITÉRATIVE DE LA GESTION DU RISQUE

Le processus de gestion du risque (voir la figure 3) est décomposé en deux activités séquentielles et itératives : l'appréciation et le traitement du risque. L'approche itérative est conçue pour s'adapter

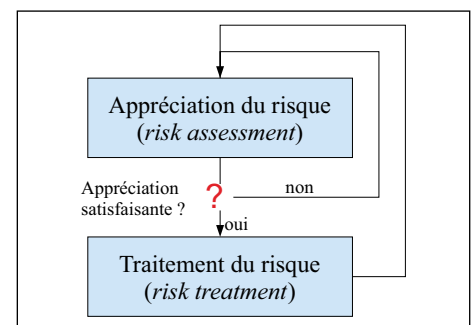


Figure 2 – Gestion du risque.

ter aux réalités des entreprises où il faut faire, dans un premier temps, les choses rapidement et de manière un peu grossière, avant d'affiner l'analyse lors d'itérations ultérieures. Cela garantit une appréciation des risques élevés en minimisant le temps et l'effort consenti dans l'identification des mesures de sécurité : le processus avance en dépit d'informations manquantes ou d'interlocuteurs clés peu bavards...

L'appréciation du risque se découpe en deux activités : l'analyse de risque, elle-même segmentée en deux sous-activités (l'identification et l'estimation des risques) et l'évaluation du risque.

En premier lieu, l'identification des risques définit les actifs : ceux primaires, c'est-à-dire les activités métier et l'information, et ceux secondaires, comme un serveur, avec pour chacun son propriétaire et sa valeur selon une échelle commune. Ensuite, on recherche pour chaque actif étudié les menaces, les vulnérabilités et les conséquences, c'est-à-dire les dommages possibles quand une menace exploite une vulnérabilité sur cet actif. Enfin, on liste les mesures de sécurité existantes. L'estimation des risques

ROUE DE DEMING

Scientifique américain, William Edwards Deming (1900-1993) [1] a inventé les principes de la qualité, et les a appliqués à partir de 1950 pour la reconstruction du Japon avec le succès que nous connaissons. Il appelait lui-même sa roue « roue de Shewhart », l'ayant reprise en 1922 au statisticien Walter Andrew Shewhart [2], et ayant surtout développé au-delà tous les principes de qualité qui ont abouti aux normes ISO 9000.

Le principe de la roue de Deming est de définir les objectifs, les moyens à mettre en œuvre pour les atteindre et la vérification de la conformité et de la stabilité du résultat obtenu, procéder à une amélioration, et recommencer.

Ce cycle vertueux garantit l'amélioration continue et par conséquent minimise la détérioration. Cette situation est très courante en sécurité des systèmes d'information : si au premier jour tout a été fait dans les règles de l'art, chaque modification, nouvelle version ou fonctionnalité remet en question la sécurité. Ce principe d'itération est donc important et prioritaire en sécurité de l'information, car rien ne sert d'analyser les risques s'il n'y a pas aussi un processus d'amélioration continue en place dans l'organisme.

Pour aller plus loin

[1] http://en.wikipedia.org/wiki/William_Edwards_Deming

[2] http://en.wikipedia.org/wiki/Walter_A._Shewhart

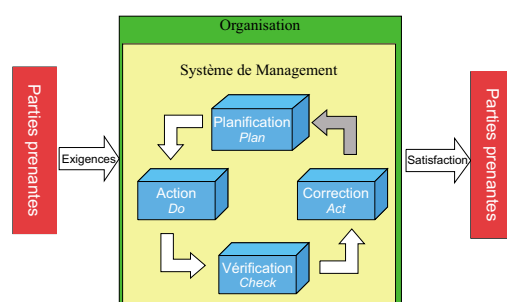


Figure a – Roue de Deming.

consiste à évaluer les conséquences et les probabilités d'occurrence des menaces, analyser les vulnérabilités, afin d'estimer les niveaux de risques. Sur ce point, la norme ISO 27005 n'impose aucune formule reliant le qualitatif et le quantitatif, mais propose trois possibilités de calcul en annexe à titre informatif. C'est sans doute dans cette phase de calcul où les possibilités de développement pour des méthodes propriétaire demeurent possibles.

Ensuite, l'évaluation du risque correspond à la prise de décision par comparaison des niveaux de risque.

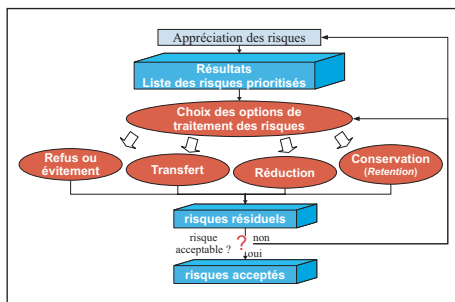


Figure 3 – t traitement du risque.

Le Tra IT eme NT e L'a C Ce P Ta TI o N DU r ISQU e

A la suite de ces deux étapes itératives vient le traitement du risque (voir la figure 4) qui réside en quatre choix classiques, la solution intégrant les coûts, et leur mise en œuvre dans la réalité :

- refuser ou éviter le risque ;
- transférer le risque ;
- réduire le risque par l'application de mesures de sécurité ;
- conserver le risque.

Dernier processus : l'acceptation du risque, c'est-à-dire l'approbation par la direction des choix effectués lors du traitement du risque. Deux activités complètent la gestion de risque : la communication du risque et le réexamen du processus de gestion de risques.

Chacune des phases du processus de l'ISO 27005 que nous venons de voir est détaillée dans la norme avec les données d'entrées, le traitement à réaliser et les résultats en sortie, comme c'est le cas dans EBIOS. Les annexes de l'ISO 27005 sont suffisamment exhaustives pour mener à bien l'appréciation des risques dans un SMSI.

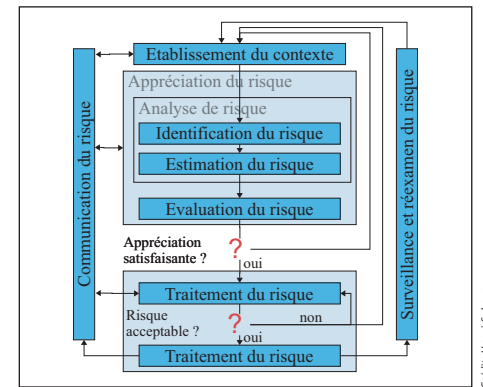


Figure 4 – Activités du processus de gestion de risque.

Cette méthodologie, accessible à tous et pragmatique, satisfera le plus grand nombre et homogénéisera la manière de faire d'un pays à l'autre. Le seul manque à court terme est l'outillage afin de faciliter le travail, comme des tableaux ou les logiciels, modules présents dans les méthodologies existantes.

Herve SCHAUE r
Consultant sécurité
www.hsc.fr