Réunion club 27001 du 18/09/2013

Organisateur de la réunion : Sungard
Auteur du compte-rendu : Olivier Gallais (Devoteam)
Avec les révisions de Béatrice Joucreau (HSC)

Ordre du jour

I. **Comparatif de la nouvelle ISO27001:2013 avec la version 2005 par Béatrice Joucreau (HSC)**
II. **Comparatif de la nouvelle ISO27002:2013 avec la version 2005 par Claire Carré (Solucom)**
III. **Points divers**

I. Comparatif de la nouvelle ISO27001:2013 avec la version 2005

Introduction

Après avoir précisé que la comparaison qui va suivre a été faite à partir de la Final Work Version de l'ISO 27001:2013, **Béatrice Joucreau d'HSC** attaque par les différences les plus visibles au premier abord.

La partie émergée de l'iceberg

La structure de la norme a changé, de nouveaux chapitres et sous chapitres concernant notamment le pilotage du SMSI faisant leur apparition ; on compte ainsi à présent dix chapitres dans ce cru 2013, le chapitre 4 très conséquent de la version 2005 étant maintenant décomposé en 3 chapitres. Autre changement notable, la disparition de la mention explicite à la notion de PDCA et de la roue de Deming au profit d'un cycle assez similaire : Etablir/Implémenter/Maintenir/Améliorer.

En creusant un peu plus…

…on se rend compte qu'il y a des changements de fond également : la prise en compte des parties intéressées est beaucoup plus importante, notamment en ce qui concerne leurs exigences et les exigences LRC (légales, réglementaires et contractuelles). La Politique de Sécurité du SI implique elle désormais un engagement de la Direction.

Le processus SMSI est modifié : l'analyse des risques est moins cadrée au niveau méthodologie mais il est maintenant demandé de prendre en compte les risques et opportunités du projet de SMSI. Par ailleurs, la sensibilisation des contributeurs du projet est mise en avant tandis que la fréquence des revues du SMSI n'est plus précisée.

Le diable est dans le détail

Dans le nouveau chapitre 4, de nouvelles actions sont demandées. En particulier, il faut à présent bien définir en amont le contexte interne et externe autour du projet de SMSI (ce qui est aligné avec l'ISO 31000, chap. 5.3.1). Mais surtout, les parties intéressées deviennent déterminantes : elles doivent être impliquées dans l'audit interne, leurs attentes doivent être prises en compte de même que les LRC et le périmètre du SMSI doit être défini en conséquence.

Dans le chapitre 5, consacré au leadership, on constate que l'on ne parle plus de politique du SMSI mais directement de Politique de Sécurité que la Direction est chargée à présent non plus de valider, mais d'établir. La Politique de Sécurité n'est plus structurante pour le SMSI mais elle représente un engagement de la Direction à satisfaire aux exigences applicables à la sécurité.

Au sein du chapitre 6, un sous-chapitre consacré au pilotage du SMSI fait son apparition en précisant que le projet doit être piloté par les risques, les opportunités et les LRC. Le gros changement de la norme se trouve dans le chapitre suivant : **la méthode d'appréciation des risques** (anciennement basée sur le triptyque actif/vulnérabilité/menace) **n'est plus définie et donc imposée dans la norme**. Il est simplement demandé de définir un processus d'appréciation des risques.

Focus sur la liberté de choix de méthode d'appréciation des risques
Même si d'aucuns y verront l'avantage à présent de pouvoir conserver leur méthode d'analyse de risque habituelle lors de l'implémentation d'un SMSI, ce changement est celui qui a provoqué les réactions les plus nombreuses en séance. Hervé Schauer y voit un certain lobbying des entreprises indiennes et asiatiques visant la certification. Celles-ci ne sont en effet majoritairement pas conformes avec la version 2005 en cela qu'elles n'ont pas d'approche GRC (Governance, Risk Management & Compliance) contrairement aux 3 principaux pays européens consommateurs de 27001. Cette version 2013, moins contraignante, permettrait ainsi à ces entreprises de l'orient une mise en conformité et une ouverture à la certification avec des coûts et des efforts très modérés.

Les options de traitement des risques ne sont plus précisées et la Déclaration d'Applicabilité ne doit plus être faite par une sélection exclusive de mesures de l'annexe A. La version 2013 conseille en effet de sélectionner ses mesures dans le catalogue de mesures de son choix et de compléter ensuite si besoin avec des mesures de l'annexe A. En outre, le propriétaire du risque est maintenant défini pour chaque risque et est appelé à valider la plan de traitement des risques et à accepter le risque résiduel, ce qui est plus proche de ce qui se fait dans le monde réel.

Il est précisé fort logiquement que les objectifs de sécurité et les plans d'actions doivent être définis en cohérence avec la PSSI.

Focus sur la nouvelle vision portée par la version 2013
***Pour la version 2005**, on avait la cinématique suivante : Objectifs du SMSI > Politique du SMSI > Appréciation des Risques > Plan de Traitement > Mesures de sécurité.*

***Pour la version 2013**, la vision est moins évidente. Béatrice Joucreau estime que le résultat attendu du SMSI (apporter de la confiance aux parties prenantes) dépend des exigences des parties intéressées et des LRC, ainsi que du contexte et du périmètre choisi. Ces quatre facteurs étant déterminants ensuite pour d'une part définir les objectifs de sécurité et les plans d'actions et de l'autre pour effectuer la phase classique « Appréciation des Risques/Traitement des Risques » (conditionnant eux aussi les objectifs de sécurité) et Déclaration d'Applicabilité. Au final dans la version 2013, l'implémenteur peut donner une coloration plutôt "conformité" à ses objectifs ou bien plutôt "risques", selon le poids des exigences et du contexte ainsi que de l'appréciation des risques et de leur traitement.*

Les chapitres 7, 8, 9 et 10 bousculent quant à eux un peu moins les codes, ils sont globalement plus synthétiques. Les changements dans le chapitre 7, réservé aux processus support (ressources, compétences, sensibilisation, communication et documentation) sont plutôt intéressants car il y apparaît la notion de sanction applicable devant être définie pour les contributeurs ne satisfaisant pas aux exigences du SMSI. Il n'y a rien à signaler de particulier pour le chapitre 8 concernant les actions récurrentes à mener tout au long de la vie du SMSI.

Dans le chapitre 9 consacré à la surveillance du SMSI, l'oratrice relève l'absence toujours cruelle de mention explicite aux indicateurs, d'aiguillage vers la 27004 et de notion d'incidents de sécurité (la gestion des incidents étant supprimée du corps de la norme).

Un point qui a provoqué des réactions d'incompréhension en séance également, est la disparition de la mention précisant que les actions suite à un audit interne doivent être entreprises avec un délai raisonnable (par interprétation, tout type de délai devient donc potentiellement valable face à l'auditeur interne). Par ailleurs, Hervé Schauer relève que la disparition de la fréquence des revues de direction du SMSI (annuelle dans la version 2005) est un alignement avec l'ISO 9001. Enfin le chapitre 10 centré sur la partie amélioration du SMSI a comme particularité qu'on n'y mentionne plus explicitement les notions d' « actions correctives » et « actions préventives », il s'axe ainsi sur l'amélioration continue et la gestion des non-conformités.

Et ma certification dans tout ça ?

Béatrice Joucreau considère que pour une entreprise déjà certifiée, une mise à jour clause par clause sera fastidieuse. En revanche, en alignant ses processus de gestion de la sécurité avec la philosophie de la nouvelle version, le chantier devient plus abordable. LSTI précise que sous 18 mois après la publication officielle de l'ISO 27001:2013, les entreprises déjà certifiées seront auditées lors de leur revue de surveillance selon les exigences de la nouvelle version. Pour les individus, LSTI attendra en revanche que les organismes de formation aient adapté leur contenu pour mettre en conformité également leur examen de certification et leur processus de surveillance.

En synthèse

On peut retenir que la version 2013 laisse plus de liberté à l'implémenteur mais c'est à double-tranchant, car un implémenteur un peu isolé se sentira probablement trop peu guidé. Il est à noter aussi que des SMSI qui n'étaient pas conformes avant peuvent à présent devenir certifiables avec cette version 2013 plus flexible.

II. Comparatif de la nouvelle ISO27002:2013 avec la version 2005

Ce qui se conçoit bien s'énonce clairement

Cette version 2013 du catalogue de mesures de sécurité de référence proposé par l'ISO apporte de nombreuses améliorations pour la lisibilité et la cohérence de l'ensemble, mais aussi une actualisation par rapport au contexte technologique et aux nouvelles menaces. Claire Carré note pour commencer que des règles qui étaient beaucoup trop génériques ou difficilement auditables ont été fort judicieusement supprimées, notamment l'ancienne mesure sur la fuite d'information. Autre modification évidente, le nombre de chapitre qui passe de 11 à 14 avec entre autres l'apparition d'un chapitre consacré à la cryptographie et un autre aux relations avec les fournisseurs. Les nombres d'objectifs de sécurité et de mesures ont en revanche eux diminué légèrement, avec plusieurs suppressions mais aussi tout de même quelques ajouts.

Quid de la forme ?

L'ISO a souhaité rendre sa norme plus générique et lisible ; cela se remarque au niveau des objectifs de sécurité qui sont à présent très synthétiques : une phrase suffit à présent à les définir au lieu des paragraphes étoffés de la version de 2005. Les mesures quant à elles, formulées de façon plus générales, imposent à présent moins de contraintes. Par exemple, il n'est plus demandé d'enregistrer de façon détaillée les traces propres à chaque incident de sécurité pour en déterminer l'impact en termes de coût (ce qu'Hervé Schauer regrette pour sa part, car l'évaluation du coût des incidents peut être un levier important pour débloquer les budgets en vue de traiter leur cause profonde).

Dans le fond…ce n'est pas si mal

Claire Carré a noté de nombreux ajouts au sein de chacun des chapitres qui sont les bienvenus. En particulier, le chapitre dédié à la sécurité dans les projets de développement (**SDLC**) précise à présent que des tests de sécurité doivent être réalisés tout au long du développement et demande de mettre -- l'accent sur les applications sensibles et/ou transactionnelles et/ou publiques. En outre, l'aspect sécurité dans les contrats est à présent traité.

Au niveau du chapitre « **continuité** », la norme demande à présent de contrôler la continuité des dispositifs de sécurité et non la continuité business. Ce changement est justifié par la redirection vers les normes 22301, 27031 et 22313 pour tout ce qui a trait au BCP. Hervé Schauer note que ce réaiguillage est un bon point mais déplore que cela n'ait pas été fait partout, notamment dans le chapitre SDLC qui devrait renvoyer vers la 27034 ou le chapitre gestion des incidents qui devrait renvoyer vers la 27035.

Le chapitre « **contrôle d'accès** » quant à lui est plus orienté IAM à présent, les aspects contrôles d'accès réseau, OS et télétravail étant traités dans d'autres chapitres (tel que « **Organisation de la sécurité** » pour le télétravail et les dispositifs mobiles notamment). La norme s'actualise enfin en élargissant les moyens d'authentification au-delà du traditionnel identifiant/mot de passe dans ce chapitre.

La phase de réponse aux incidents est maintenant traitée dans le chapitre, je vous le donne en mille : « **gestion des incidents** ». On note aussi l'ajout approprié de la gestion des vulnérabilités et de la nécessité de faire des audits de sécurité récurrents dans le chapitre « **sécurité des opérations** ». Bien que le chapitre « **relation vers les fournisseurs** » intègre fort justement le report des contrôles de sécurité dans la chaîne de sous-traitance, on regrettera l'absence de report vers les normes 27036 (guide dédié à cet aspect de sécurité dans les relations fournisseurs), 27017 (guide sur la sécurité dans le Cloud) et 27018 (guide sur la sécurité des données nominatives).

Enfin, concernant le chapitre « **Politique de sécurité** », la norme ne demande plus l'établissement d'une unique Politique de Sécurité, mais d'un corpus de Politiques de Sécurité dédiées chacune à une thématique bien précise de la SSI, ce qui se rapproche plus de ce qui est effectué naturellement par les entreprises.

Pros & cons

Si la version 2013 réussit à être plus synthétique, plus lisible et aussi plus « réaliste » que son aînée, avec entre autres des objectifs de sécurité pragmatiques et les mesures de sécurité les plus abstraites à présent supprimées, tout n'est pas encore rose à ce stade. En effet, pour Claire Carré, il subsiste encore certaines mesures abstraites et difficilement auditables. Par ailleurs, le manque de mesures « de base » est assez gênant : quid du durcissement des socles des postes de travail par exemple ? Enfin, l'évolution des technologies et des menaces souffre de ne pas être assez prise en compte, les logiques SIEM, SOC et CERT autour du risque de cybercriminalité n'étant pas abordées. Enfin, l'absence de mesures de sécurité spécifiques aux infrastructures virtualisées dérange un peu en 2013.

ANSSI vs ISO

Le guide de l'hygiène de l'informatique publiée par l'ANSSI n'est pas éclipsé par cette nouvelle version de l'ISO 27002. Au contraire, l'oratrice rapporte que les deux référentiels se complémentent assez biens, celui de l'ANSSI étant plus technique et la 27002 étant plus globale et générique, ce qui lui assurera peut être une plus grande pérennité.

Pour la certification

Les entreprises qui ont un projet de SMSI en cours visant la certification profiteront avec cette version d'une meilleure appropriation des mesures par les acteurs de la DSI. Pour les SMSI déjà certifiés qui doivent se mettre en conformité avec la version 2013, l'impact est limité même si une mise à jour de la

Déclaration d'Applicabilité sera nécessaire et qu'il faudra fournir des efforts plus importants au niveau du Software Development Life Cycle.

Pour conclure

L'ISO 27002 reste avec cette version le guide de référence des mesures de sécurité et conserve une certaine flexibilité puisque les méthodes de mise en œuvre des mesures ne sont pas imposées ni même précisées. En outre, son caractère indépendant des technologies lui permet de se pérenniser.

III. Points divers

Actualité des normes

Hervé Schauer nous précise que la traduction en français des normes 27001 et 27002 de 2013 est terminée et que ces traductions sont passées en relecture publique. Une réunion à l'issue de cette relecture publique est planifiée en octobre afin de finaliser et valider leur version définitive. L'AFNOR pourrait ainsi vraisemblablement publier les versions françaises très peu de temps après la sortie des versions anglaises.

Groupe benchmark outils SMSI

Le groupe **Benchmark outils SMSI** annonce par le biais de Thomas Lebouc que le résultat de leur travail **–un véritable livre blanc des outils d'implémentation/exploitation de SMSI**- sera bien rendu pour la date prévue, le 24 septembre. Il sera ensuite diffusé au sein du club 27001 et probablement au-delà pour faire reconnaitre les initiatives et le travail effectué par le club. Thomas Lebouc précise qu'avec la méthodologie de benchmarking qu'ils ont définie, il est à présent possible de faire évoluer rapidement le livre blanc en incorporant le test de nouveaux outils. Un appel aux bénévoles est fait pour devenir membre du groupe et proposer de tester de nouveaux outils.

Prochaines réunions

La **prochaine conférence annuelle du Club 27001** aura lieu le **18 mars 2014**.

La **prochaine réunion du Club à Paris** est prévue quant à elle le **28 novembre 2013** et l'appel aux sujets et aux présentations pour cette occurrence reste d'actualité, tout autant que l'appel au bénévolat afin de fournir une salle pour accueillir la réunion.

Question

Un participant demande s'il y aura une communication officielle de la part de l'ISO pour détailler les différences entre les anciennes et les prochaines versions. Hervé Schauer répond que cela est très peu probable et qu'il s'agit plutôt d'un travail de consultant, comme cela faisait l'objet de cette séance.

* * *