OPUS 8

APSSIS



« Quand on n'a pas de tête il faut avoir des jambes »

Ma grand-mère paternelle

GUIDE CYBER RÉSILIENCE

L'ISO 27001 PAR ÉTAPE

Par Cédric CARTAU

SOMMAIRE

CYBER RÉSILIENCE

0.8 L'ISO 27001 PAR ÉTAPE

1. RÉSUMÉ P.5
2. INTRODUCTION P.6
3. HISTOIRE DE LA NORME ISO 27001 P.8
   - **3.1 Il était une fois...la BS799**
   - **3.2 Puis vint la norme ISO 27001**
   - **3.3 Le chemin normatif standard**
4. RÉFLEXIONS SUR LA NORME P.10
   - **4.1 Ingénierie versus qualité**
   - **4.2 Ce que cela n'est pas**
   - **4.3 Ce que c'est : vision et tentative de résumé**
   - **4.4 A quoi cela sert et comment le vend-on ?**
     - 4.4.1 En général
     - 4.4.2 Pour la DSI
     - 4.4.3 Pour une Direction Générale

Approche métier : Point de vue du Groupe Evolucare **P.17**

5. LES STRATÉGIES DE DÉPLOIEMENT POSSIBLES P.20
   - **5.1 Les prérequis managériaux**
   - **5.2 Digression utile sur la position du RSSI**
   - **5.3 Y aller, mais comment ?**
6. ETAPE 1 : EN FAIRE SANS LE DIRE, OU L'APPROCHE PAR L'ANNEXE A P.22
   - **6.1 Idée générale**
   - **6.2 Prérequis**
   - **6.3 Périmètre**
   - **6.4 Rôles / Gouvernance**
   - **6.5 Livrables**
   - **6.6 Durée**
   - **6.7 Outillage et moyens**

Approche métier : Point de vue de Stormshield **P.26**

7. ETAPE 2 : METTRE EN PLACE SON SMSI P.29
   - **7.1 Quelques difficultés**
   - **7.2 L'approche à éviter**
   - **7.3 La montée en maturité**
   - **7.4 Une méthode, parmi d'autres**

SOMMAIRE

CYBER RÉSILIENCE

0.8

7.5 Durée

7.6 Outillage et moyens

8. ETAPE 3 : FORMALISER LES PROCESSUS ET ÉTENDRE LE PÉRIMÈTRE P.33

8.1 Idée générale

8.2 Une méthode parmi d'autres

8.3 Durée

8.4 Outillage et moyens

9. COMBIEN CELA COÛTE P.36

10. ET APRÈS... P.37

11. LA QUESTION DE L'OUTILLAGE P.38

Approche métier : Point de vue d'Olfeo P.39

12. LES PROBLÈMES CONNUS P.44

12.1 Confusion entre production documentaire et mise en place d'un SMQ

12.2 Le pipeautage des ESN de conseil / accompagnement

12.3 Les auditeurs de certification

12.4 Points d'attention sur quelques parties de la norme

13. L'AVENIR P.47

13.1 Une obligation pour toutes les DSI

13.2 Les autres normes ou bonnes pratiques en lien avec la 27001

13.2.1 Les autres obligations normatives dans un établissements de santé

13.2.2 La certification des comptes

13.2.3 NIS 1, NIS 2

13.2.4 Les assurances cyber

13.2.5 Le RGPD

Approche métier : Point de vue d'Yves Normand P.49

14. QUELQUES CONSEILS PLUTÔT UTILES P.52

15. ANNEXES P.53

16. RESSOURCES P.54

16.1 Bibliographie

16.2 Sites Web

17. ARTICLES P.55

17.1 Article DSIH, février 2025 : Pourquoi 27001 et NIS ne disparaîtront jamais

17.2 Article DSIH, février 2025 : Match 27001 versus RSSI : 1 à 0

18.1 Article InCyber : Les visions comparées de la 27001

18. ACRONYMES P.60

L'AUTEUR



Cédric CARTAU est RSSI et DPO du CHU de NANTES et du GHT44. Il est vice-président de l'APSSIS et enseigne à l'EHESP, à l'ESIEA et au CNEH. Il est également auteur de plusieurs ouvrages chez Eyrolles ou aux Presses de l'EHESP, sa dernière publication étant « La sécurité du système d'information des établissements de santé », en 2018.

cedric@cartau.net

L'auteur et l'APSSIS remercient ses contributeurs d'avoir accepté le difficile exercice de présenter une approche métier sur une question aussi complexe que la mise en œuvre de l'ISO 27001.

1. RÉSUMÉ

Que l'on parle, comme il y a une décennie, de sécurité des systèmes d'information, ou comme aujourd'hui de « cyber », ces termes et expressions recouvrent un champ large qui va des dispositifs techniques (antivirus, pare-feu, etc.) aux dispositifs organisationnels (constitution de cellule de crise, test d'attaque cyber, etc.), ces derniers adressant aussi bien la Direction des Systèmes d'Information (DSI) que les métiers.

Dans tous les cas, la cyber devient un sujet à part entière, autant que l'ont été les démarches Qualité au début des années 2000 : d'abord « noyée » dans les processus cœur de métier, la Qualité est devenue une préoccupation transversale qui sert d'appui aux démarches des maîtrises d'ouvrage pour faire face à leurs contraintes normatives (HAS entre autres).

La cyber n'est ni un logiciel ni un matériel : elle est une démarche globale, tout comme la Qualité. Et cette démarche doit à la fois piloter l'avancement en maturité des métiers au regard des enjeux modernes (on pense aux nombreuses attaques cyber subies par les hôpitaux tels Dax, Rennes, etc.), et tout autant se structurer elle-même.

Apporter une réponse cyber aux contraintes tels l'assurance en responsabilité civile de l'établissement (pour les dommages causés aux tiers consécutifs à un sinistre cyber), le volet IT de la certification des comptes, la loi sur les OIV ou celle sur NIS 2, les différents plans de financement CaRE ou Hôpital Numérique, le volet IT des autres certifications sectorielles (par exemple celle des plateaux de biologie) implique de factoriser toutes ses réponses sous peine de s'éparpiller, car l'on ne peut courir 15 lièvres, qui seront bientôt 16, puis 17, etc...

La norme ISO 27001 a été conçue pour apporter un cadre méthodologique (un système de management de la qualité, sur la base de la norme ISO 9001) autant que technique (les 93 mesures techniques listées en annexe). Y répondre, s'y conformer et se certifier, c'est avoir l'assurance, pour une Direction Générale, non seulement de factoriser tout ce qui peut l'être et ne pas refaire plusieurs fois le même travail, mais en plus de déployer une méthode de management qui a fait ses preuves, depuis plus de 50 ans, dans des secteurs à hautes contraintes telle l'aviation civile. C'est également l'assurance, pour une Direction Générale, qu'un macro-processus autocorrectif est en œuvre, dont l'objectif est de ne pas laisser traîner des failles sans que personne ne s'en préoccupe.

La norme ISO 27001 est suffisamment souple pour se prêter à une approche en mode big bang autant qu'une approche en mode progressif, c'est tout l'intérêt. Mais une chose est certaine : les entreprises, publiques ou privées, qui prendront du retard sur cette approche normative, devront dépenser beaucoup plus d'énergie humaine ou financière à l'avenir que celles qui auront sauté le pas.

Les certifications sont le sens de l'histoire, et ceci dans tous les secteurs. Les anticiper, c'est garder la maîtrise de son SI face aux enjeux modernes.

2. INTRODUCTION

Il devrait être inutile de repréciser, encore une fois, l'importance qu'a pris la cyber au sein des organisations publiques ou privées depuis environ 10 ans. Mais faisons-le tout de même !

- Première attaque cyber massive d'une grande entreprise française du CAC 40 : Saint-Gobain, 2017.
- Première attaque cyber d'un CHU : CHU de ROUEN, décembre 2019.
- Première attaque massive : CH DAX, avril 2021.

Depuis les noms des gros établissements de santé s'égrènent régulièrement dans la presse spécialisée autant que dans les médias généralistes : CH de CORBEIL, CHU RENNES, CHU BREST, etc. L'ANSSI et le ministère de la santé précisent qu'en moyenne, sur le territoire national, un établissement de santé est attaqué toutes les semaines, et ce chiffre est à notre avis très largement sous-évalué.

La réponse à cette menace récente (récente à l'échelle de l'Histoire d'une nation s'entend) ne peut pas être seulement technique : le meilleur antivirus ne vaut rien s'il n'est pas managé, surveillé, évalué, etc.…, tout comme l'ensemble des dispositifs de sécurité classiques. Et bon nombre de mesures de sécurité ne réclament aucun matériel, aucun logiciel, juste des procédures et une bonne méthode de travail.

Il se trouve que pas mal de personnes ont fait le même constat, et ceci depuis des décennies, et ont commencé à compiler les meilleures pratiques rencontrées çà et là. C'est d'ailleurs comme cela qu'est née l'ITIL[1] : au départ il s'agissait d'un constat, fait par l'administration britannique lors du gouvernement de Margaret Thatcher, que certaines entreprises s'en sortaient mieux que d'autres avec leur informatique, et qu'il fallait compiler les meilleures pratiques mises en place au sein de ces entreprises afin de les diffuser plus largement. ITIL v1 est née en 1989, et depuis plusieurs versions sont sorties, la dernière étant ITIL v4 en février 2019.

La cyber a suivi exactement le même chemin avec quasiment 10 ans de retard, comme nous le verrons au chapitre suivant, et a donné lieu au pendant côté cyber de ce qu'est ITIL côté organisation : la norme ISO 27001. On rencontre cependant souvent des questions, des interrogations, toutes légitimes : A quoi cela sert ? N'est-ce pas surdimensionné pour ma DSI ou mon organisation ? Comment le vendre en interne ? Combien cela coûte ?

Ce guide a pour ambition de répondre à ces questions, et notamment :

- les bénéfices qu'une DSI peut tirer de la norme 27001 ;
- comment « vendre » en interne auprès de sa Direction Générale cette démarche ;
- par quoi commencer ;
- les pièges et chausse-trapes classiques ;
- les étapes de déploiement optimales ;
- ...

Ce guide de cyber résilience, 8ème de la série, s'inscrit dans la suite des précédents : mots de passe (tome 1), les cyber attaques (tome 2), les habilitations métier (tome 3), la protection du Cloud (tome 4), les indicateurs (tome 5), le guide du RSSI (tome 6), la gestion de crise (tome 7) publiées avec le précieux concours de l'APSSIS[2], toujours avec l'ambition de constituer un corpus de référence sur les questions relatives à la sécurité du SI.

1 https://lepapyrus.substack.com/p/lhistoire-de-litil
2 www.apssis.com

Comme pour chaque guide, les contributions en annexe constituent un complément très riche, des points de vue de professionnels du secteur chacun dans sa spécialité. Et comme toujours, les remarques, suggestions d'amélioration sont à envoyer directement à l'auteur pour être prises en compte dans les prochaines versions.

Bonne lecture.

3. HISTOIRE DE LA NORME ISO 27001

3.1 Il était une fois...la BS799

De nombreuses personnes et organisations ont été impliquées à l'origine de la norme ISO 27001.

Initialement en 1993, le Ministère du Commerce et de l'Industrie au Royaume-Uni réunit une équipe pour examiner les pratiques existantes en matière de sécurité de l'information, dans le but de produire un document normatif. Au début de l'année 1993, ce Ministère a décidé de réunir rapidement un groupe de représentants de l'industrie de sept secteurs différents : Shell, BOC Group, BT, Marks & Spencer, Midland Bank, Lloyds Bank, Nationwide et Unilever. C'est ainsi qu'est née l'idée originale d'établir un ensemble de contrôles de sécurité de l'information et de produire un document contenant une liste initiale d'une centaine de contrôles de base dès la fin des années 1980 pour adresser la question de la sécurité de l'information.

Et donc en 1995, le groupe BSI publie la première version de la norme BS 7799-1, basée en partie, sur un manuel de politique de sécurité de l'information élaboré par le groupe Royal Dutch / Shell à la fin des années 1980 et au début des années 1990, et à la démarche de Ministère ci-dessus.

Vint ensuite la BS 7799-2, publiée en 1999, qui introduisit le concept de Système de Management du SI. La version 2002 de cette 7799-2 introduisit quant à elle le schéma d'amélioration continue PDCA (Plan Do Check Act), s'alignant ainsi sur les schémas de la série des normes ISO 9000. BS 7799-2 a été transposée en norme ISO 27001 en 2005.

3.2 Puis vint la norme ISO 27001

La première norme ISO de cette série était donc l'ISO/IEC 17799:2000. Il s'agissait d'une reprise et amélioration de la norme britannique déjà existante : la BS 7799 de 1999. Puis, comme vu ci-dessus, la norme ISO 27001 arriva en 2005 et comprenait donc déjà, dans le « pack de base », les notions de SMSI et d'amélioration continue.

Elle a été révisée en 2013, 2017 et 2022, avec à chaque fois des évolutions majeures quoique pas forcément visibles au premier abord :

- version de 2013 : entre autres, uniformisation du plan de la norme par rapport au standard ISO (la 9001 sera standardisée selon ce même plan un peu plus tard) ;
- version de 2017 : mise à jour des mesures de l'annexe A, introduction de la notion de processus dans le corps de la norme ;
- version de 2022 : refonte totale des mesures de l'annexe A (qui sont répartis en 4 chapitres et non plus en 14 comme par le passé, et nettoyage de certaines mesures ambigües) ; également, généralisation de la notion de processus.

5ème génération

La version de la 27001 que nous avons dans les mains est donc la 5ème génération. Respect. Alors avant de prétendre que la norme est « mal faite », « pas adaptée », merci de bien vous souvenir qu'elle a plus de 30 années d'existence, en est à sa 5ème mouture et représente la somme de travail de milliers de personnes venant de centaines d'entreprises différentes.

3.3 Le chemin normatif standard

Le chemin normatif standard, que l'on soit dans l'IT ou dans l'automobile ou tout autre domaine de l'industrie, est toujours le même :

• d'abord, des bonnes pratiques locales émergent, qui relèvent autant des trucs et astuces que du véritable travail de fond des experts du secteur. C'est ce qui s'est passé avec le manuel de politique de sécurité de l'information élaboré par le groupe Royal Dutch / Shell ;

• ensuite, ces bonnes pratiques locales sont compilées par des groupes de travail, et deviennent une norme de facto, au sens de « communément admise par les experts du domaine », sans forcément qu'il y ait un document normatif ;

• ces bonnes pratiques deviennent ensuite une ou plusieurs normes ;

• enfin, ces normes finissent par devenir des obligations réglementaires. C'est exactement ce qui est en train de se produire avec NIS 1, puis NIS 2 qui est en cours d'élaboration (et qui deviendront ensuite NIS 3) : ces textes législatifs sont très fortement basés sur la norme ISO 27001, on y retrouve peu ou prou les mêmes items.

Non seulement il y a peu de chance que la norme ISO 27001 disparaisse, mais en plus il y a fort à parier qu'elle ira se fondre dans NIS 2 ou ultérieur qui finira par l'absorber.

La poule ou l'œuf

NIS 2 va-t-elle absorber la norme ISO 27001, ou à l'inverse la norme ISO 27001 va-t-elle avaler NIS 2 ? Peu importe, au final, les obligations seront les mêmes, ce qui n'est d'ailleurs pas surprenant.

Dit autrement si l'on considère cette approche par le « chemin normatif », autant se caler rapidement sur la norme ISO 27001 au risque de se faire « rattraper par la patrouille normative » qui finira d'ailleurs par devenir une « patrouille réglementaire ».

4. RÉFLEXIONS SUR LA NORME

4.1 Ingénierie versus qualité

Une « démarche qualité » n'est pas à proprement parler naturelle, y compris - et surtout - pour des informaticiens.

Les études supérieures d'ingénieur tendent à inculquer à tout futur diplômé la volonté de « faire bien et vite ». C'est-à-dire que, confronté à un problème ou en réponse à une demande, l'objectif sera d'apporter une solution jugée optimale dès la première itération, quitte à passer à autre chose (une autre demande, un autre projet) dès que le problème est considéré comme traité. Bien sûr, cette vision est un peu caricaturale, mais pas tant que cela : que l'on songe par exemple aux logiciels à peine sortis de leur boîte et qui sont truffés de bugs informatiques que personne ne corrige (on vit « avec »), aux « machins » mis en place avec 2 bouts de ficelles que l'on « optimisera plus tard » (le plus tard ne venant jamais), etc.

Une démarche qualité est d'une tout autre nature : à la limite, peu importe de faire bien dès le début, l'essentiel est de rentrer dans un processus d'amélioration continue. Il s'agit de la fameuse roue de Deming. Le principe est simple et consiste à rentrer dans une démarche en 4 parties appelées PDCA, ou cycle d'amélioration continue, ou encore roue de Deming :

1. Je dois dire ce que je vais faire **(Plan)**.
2. Je dois faire ce que j'ai dit **(Do)**.
3. Je dois mesurer les écarts entre ce que j'aurais dû faire et ce que j'ai réellement fait **(Check)**.
4. Je dois mettre en place des mesures correctives de ces écarts **(Act)**.

L'expérience montre que cette démarche semble étrange aux informaticiens, mais quelques exemples de leur vie courante suffisent rapidement à leur prouver son intérêt. Qui, parmi ceux qui ne sont pas rentrés dans ce mode de pensée, vérifie régulièrement la liste des comptes admin de domaine, les PC qui ne sont plus protégés par un antivirus, les règles sur le firewall qui devaient être « temporaires » et que personne ne revoit jamais ? Ces simples exemples démontrent bien que laisser en plan un système finit par le voir s'écrouler sous sa propre entropie.

Bizarre tout de même

Être bon en ne faisant « pas tout bien du premier coup ». Dit comme cela, c'est tout de même étrange. Mais parce que la phrase n'est pas terminée : « pas tout bien du premier coup...mais remettre l'ouvrage sur le métier régulièrement ».

L'alchimie qui résulte de la rencontre de ces deux mondes - celui de la DSI et celui de la qualité - est de nature à améliorer fortement la sécurité du SI. Après tout, les démarches qualité ont pénétré bien des domaines avant l'informatique, et jusqu'à preuve du contraire aucune personne sensée aujourd'hui ne viendrait remettre en cause cette approche dans les analyses de laboratoires ou dans le traitement de la septicité des blocs opératoires.

Aussi curieux que cela puisse paraître, une démarche qualité de type PDCA se focalise plus sur la forme (prouver que l'on est dans une démarche d'amélioration continue) que

sur le fond (la résolution de tel ou tel problème technique, le nettoyage des comptes admin de domaine, etc.) et souvent les non-initiés pensent que l'on peut facilement raconter des salades et prétendre avoir fait ce que l'on n'a pas fait. Erreur, les démarches qualité sont d'une redoutable efficacité, on peut certes mentir, mais pas longtemps : 30 ans de maturation des SMSI ont suffi à éliminer assez sûrement toute possibilité de bullshit même à moyen terme dans une DSI.

4.2 Ce que cela n'est pas

La norme ISO 27001 n'est pas une démarche technique : il s'agit d'un Système de Management de la Qualité (SMQ) dans le domaine spécifique de la Sécurité de l'Information (SI), donc un SMSI.

« On peut être absolument nul en cyber, et être certifié ISO 27001 : il « suffit » de s'améliorer constamment » : au regard d'une lecture stricte de la norme ISO 27001, cette phrase pourrait être vraie. Mais la spécificité de la norme ISO 27001 (qui n'existe pas dans la norme 9001) c'est de comporter une annexe (la fameuse annexe A, dont le détail est décrit dans la norme 27002) qui, elle, spécifie des mesures techniques sur lesquelles il est difficile de faire l'impasse.

Par exemple, un auditeur pourrait demander : qu'avez-vous prévu concernant la mesure 5.7 (renseignement sur les menaces) ? Si vous lui répondez : « rien n'est en place mais un plan d'action vise à satisfaire l'exigence sous 3 mois », il pourra se contenter de vous mettre une non-conformité mineure. Mais si vous lui faite la même réponse pour chacune des 93 mesures de l'annexe A, rapidement il va stopper l'audit et vous renvoyer à vos chères études, parce qu'à un moment donné il ne faut pas se moquer du monde. Certes la norme ISO 27001 c'est un SMQ, mais qui vise à améliorer la sécurité du SI, pas à faire de la conformité pour de la conformité.

4 jours c'est long

Un audit de certification dure au moins 3-4 jours - plus selon la taille de la structure à certifier, les durées sont elles-mêmes normées.

Pendant 4 jours, l'auditeur demande ce que l'on a mis en place pour telle partie de la norme, demande des preuves par échantillonnage, analyse les preuves, demande des preuves de traitement des incidents, des traces, etc.

Et 4 jours c'est long, surtout que les auditeurs ont un 6ème sens pour ouvrir les portes qu'il ne faut pas ouvrir et soulever les tapis qui recouvrent la misère.

N'essayez pas de balader un auditeur, c'est une très mauvaise idée.

La norme ISO 27001 n'est donc pas technique : c'est bien un SMQ, mais qui a pour socle la technique. L'histoire de la BS7799 démontre bien qu'à la base, ce type de démarche est issu de la technique : un SMQ vise simplement (si j'ose dire) à encadrer le volet technique afin que les actions soient menées dans les règles de l'art.

4.3 Ce que c'est : vision et tentative de résumé

Lors d'une session du Club 27001 nantais de fin 2024, une table ronde avait été organisée sur le thème : « L'ISO 27001 en résumé, le point de vue d'un consultant, d'un RSSI expérimenté et d'un RSSI récent dans la norme ». Et le moins que l'on puisse dire, c'est que personne n'a donné la même définition.

Les nouveaux venus dans l'ISO 27001 sont persuadés qu'il faut produire des tonnes de documents. Ce qui est faux bien entendu, même si certains sont obligatoires. PSSI, manuel du SMSI, analyse des risques, DDA (qui est la réponse à l'Annexe A, par abus de langage on parle souvent de la DDA pour l'Annexe A), etc. : on doit pouvoir commencer avec 10 documents maximum.

Pour certains, surtout dans le secteur concurrentiel, être certifié 27001 c'est avoir un avantage concurrentiel dans les réponses aux appels d'offre, les clients choisissant de plus en plus des prestataires certifiés, vague que l'on a vu apparaître dans l'industrie et qui touche le tertiaire depuis une ou deux décennies - les DSI sont certainement les dernières à être touchées. Certes c'est une lame de fond, mais ce n'est pas que cela.

Autre vision : le respect des bonnes pratiques, qui ont été éprouvées par des années de compilation. Si c'est bien comme cela qu'ont commencé toutes les normes (la BS 7799 incluse, voir plus haut), cette vision passe sous silence l'irruption des SMQ dès 2005 : il s'en est donc passé des choses entre temps.

Enfin c'est la vision de système de management qui arrive à ce stade. Il faut un bon moment pour comprendre véritablement ce qu'est un SMQ - 3 ans au bas mot et je n'exagère pas - et surtout diffuser cette compréhension auprès de tous les acteurs du périmètre. Ma définition - et qui n'engage que moi - est : macro-processus fractal auto-apprenant et auto-nettoyant. Et il me faudrait un tableau blanc et un bon moment pour expliquer chaque terme et le sens général de la phrase. Bon en gros retenez la culture processus.

27001 comme une voiture balai

La 27001 ne garantit pas qu'il n'y aura jamais de problème : elle garantit qu'un dispositif organisationnel est mis en place, qui fait passer la voiture balai, justement pour repérer et nettoyer les scories qui traînent dans les coins.

Certes un SMQ est un macro-processus fractal auto-apprenant et auto-nettoyant, mais il faut rajouter plusieurs dimensions :

- la dimension de rationalisation des méthodes de travail, et là on rejoint aussi l'ITIL ;

- conséquence de cette rationalisation, la sortie « cadrée » de la zone d'humiliation (ce qu'il ne fallait pas faire, que l'on savait qu'il ne fallait pas faire et que l'on faisait quand même, genre les mauvaises pratiques avérées, les trous de sécurité connus mais jamais patchés, etc.) : la norme est un guide qui est là pour que vous n'oubliiez aucune mesure, aucun pan de la sécurité du SI ;

- la dimension de transparence : on dit ce que l'on fait, on fait que ce l'on dit, et rien n'est caché, que ce soit lors de l'audit interne, la revue de direction ou l'audit de certification ; la transparence est un élément essentiel de la confiance qu'induit un SMQ certifié ;

Preuve que la norme est difficile à résumer, les auditeurs ont chacun leur marotte. Pour certains, c'est la gestion documentaire qui en est le pilier, pour d'autre l'appréciation des risques, pour d'autres l'établissement du contexte et la liste des parties intéressées, pour d'autres encore le chapitre 9 (Check), pour d'autre enfin le chapitre 10 (le Act).

Il n'y a pas de cœur, pas de centre : le cycle d'amélioration continue est une roue, la roue de Deming justement, et ni le P, ni le D, ni le C ni le A ne peuvent prétendre en être le centre. Le cycle PDCA n'est pas un état, c'est un mouvement : la roue n'est stable que si elle tourne, et s'il y a un point essentiel, c'est qu'elle doit toujours être en mouvement.

A titre d'illustration du propos et au risque de choquer les puristes, l'appréciation des risques ne vaut pas tant par la méthode retenue (la norme ISO 27001 n'en impose aucune), ni par son résultat (10 risques ou 100), et certainement pas par sa première itération, qui ne sert « que » à déterminer la DDA. L'appréciation des risques vaut par sa mise à jour fréquente, connectée aux événements du SMSI (évolution des menaces, des technologies déployées, etc.) et connectée également aux autres éléments du PDCA : les mesures de la DDA, la validation par la Direction lors de la revue annuelle. La plus belle appréciation des risques figée ne vaut rien, une appréciation des risques qui « vit » avec son SMSI est efficace.

La norme ISO 27001 est un véritable bijou de précision et d'exhaustivité. Des milliers d'heures de travail, par des milliers de gens, des versions toujours plus précises et approchant la perfection : la meilleure preuve est que ceux qui la pratique depuis des années vous disent que tous les 2 ou 3 ans ils en ont une lecture différente, ils l'abordent sous un angle qu'ils n'avaient pas imaginé.

Ne prétendez pas que la norme ISO 27001 est déconnectée de la réalité, qu'elle a été faite en chambre par des technocrates ignorant la réalité du terrain, c'est faux. Si vous ne la comprenez pas, si vous ne savez pas interpréter un paragraphe, le problème n'est pas la norme : c'est juste que l'on ne sait pas la lire. Et certes, une telle densité d'informations dans aussi peu de pages, cela force le respect, mais cela nécessite un investissement en temps pour se l'approprier.

4.4 A quoi cela sert et comment le vend-on ?

4.4.1 En général

Pour les Parties Intéressées (PI) identifiées dans une certification (les pouvoirs publics, les partenaires, les clients, les auditeurs externes, etc.), la certification ISO 27001 a deux intérêts « vendables » :

• l'assurance, pour la PI en question, que la démarche PDCA normative est prise au sérieux dans l'Organisation ; d'ailleurs, un certificat est public, et librement consultable / vérifiable sur le site des organismes certificateurs ;

• éviter de se faire auditer à chaque fois sur les mêmes sujets techniques, par exemple le partenaire qui veut être certain que

vous gérez correctement vos sauvegardes, les mises à jour de votre pare-feu, etc. ; quand on pose une question à un organisme certifié, il répond en envoyant son certificat, le travail a déjà été fait en somme.

D'ailleurs cela marche aussi dans l'autre sens : si vous voulez avoir une idée de la prise en compte de la sécurité informatique chez un de vos fournisseurs (actuel ou potentiel), demandez-lui directement son certificat ISO 27001. Encore une fois, cela ne garantit pas - cela ne garantira jamais - qu'il soit bon, cela garantit qu'il ne prend pas le sujet à la légère.

A quoi reconnaît-on un fournisseur mature sur le plan de la cyber ?

Facile : les commerciaux vous envoient directement par mail le certificat ISO 27001 de leur entreprise à la moindre question sur leur niveau cyber. Cela accélère les discussions.

D'ailleurs, bénéfice collatéral d'une certification ISO 27001 : lorsque d'autres services que la DSI sont certifiés en interne (par exemple avec la norme 15 189 pour les laboratoires), ces normes ont un chapitre consacré à la sécurité informatique du service en question. Fournissez le certificat ISO 27001 à l'auditeur de ce service, il coche directement toutes les cases du chapitre en question et passe au sujet suivant. On factorise les démarches, et au final on économise du temps et de l'argent - imaginez dans un CHU, le nombre d'heures de travail économisées dans toutes les certifications sectorielles en ayant traité une bonne fois pour toute leur chapitre commun sur la cyber !

On économise en fait

Si l'on prend en compte cette dimension de factorisation induite par la certification ISO 27001, pas certain que le « bilan comptable » (incluant les jours de travail autant que les coûts financiers directs) soit débiteur.

4.4.2 Pour la DSI

Pour une DSI, la norme a deux intérêts, au moins.

Pour les ingénieurs et techniciens tout d'abord, l'annexe A leur permet de tout balayer, et de n'oublier aucun aspect du sujet. Combien de fois a-t-on vu un certificat obsolète qui bloque la production en stoppant les échanges sécurisés entre deux serveurs : la norme exige de tenir à jour un registre des actifs, et en particulier de traiter la question des outils de chiffrement. C'est bête, mais pourquoi ne le fait-on pas justement ? L'annexe A peut être vue comme une énorme checklist de points à ne pas oublier.

Ne pas réinventer la roue

C'est exactement le rôle premier de l'annexe A : la norme a fait ce travail de recensement pour vous, inutile de le refaire.

Pour le management de la DSI, la norme sert à dire : on respecte les bonnes pratiques. Cela paraît anodin, mais le jour où un accident de prise en charge médicale imputable à une panne du SI surviendra et où une action judiciaire sera intentée, la DSI sera bien contente de pouvoir disposer de cet argument, en plus de l'éternel « le risque zéro n'existe pas ». Ce n'est pas pour rien que les bonnes pratiques finissent par devenir des normes puis des lois.

Et accessoirement, si ce management n'est pas de culture technique (et même s'il l'est du reste), disposer d'un guide-des-éléments-techniques-à-ne-pas-oublier (l'annexe A) peut être très rassurant.

4.4.3 Pour une Direction Générale

En plus de tous les arguments ci-dessus (respect des bonnes pratiques, confiance des PI, etc.), il en est un qui retient l'attention des DG : le caractère auto-correcteur de la norme.

Une Direction Générale n'a ni le temps ni les moyens d'aller vérifier qu'une DSI fait bien son travail sur la question des antivirus, des règles du pare-feu, des comptes admin, des mots de passe, etc. La norme assure qu'un dispositif managérial éprouvé depuis des lustres (une démarche Qualité) se charge non seulement d'adresser tous ces points, de vérifier que le travail est à un niveau acceptable, de repérer les anomalies et de corriger ce qui doit l'être. C'est extrêmement rassurant pour une DG qui doit faire face, tous les jours, à des sujets tous plus complexes les uns que les autres, de niveau technique très varié dans des domaines très divers.

L'ISO 27001 COMME UN ACCÉLÉRATEUR DE LA MISE EN CONFORMITÉ AVEC LA DIRECTIVE EUROPÉENNE NIS 2

Par Lauranne Peyron, RSSI-DPO du Groupe Evolucare

Approche métier : Point de vue du Groupe Evolucare

NIS 2 - une directive européenne au vaste périmètre

Depuis le début des années 2010[1], la question de la protection des systèmes d'information essentiels au fonctionnement des nations se pose de manière de plus en plus précise, suite à l'essor de la cybercriminalité, et à l'utilisation des capacités de « cyberguerre » dans le cadre de conflits géopolitiques.

En France, ces préoccupations ont été inscrites dans la loi dès 2014, via la Loi de Programmation Militaire 2014-2019, qui définissait des « Organismes d'Importance Vitale » qui devaient se mettre en conformité avec un certain nombre de mesures visant à assurer la sécurité et la résilience de leurs systèmes d'information.

Cette loi a été suivie en 2016 d'une directive européenne, dite « NIS » qui appliquait une logique similaire aux « Opérateurs de Services Essentiels ».

En 2022, sur la base du retour d'expérience de la mise en application de la directive NIS, une nouvelle directive, dite « NIS 2 » a été votée par le Parlement Européen. Elle a pour particularité de définir un cadre plus précis de règles, de manière à encourager l'harmonisation des mesures de sécurité à l'échelle européenne, et surtout, elle étend drastiquement le périmètre d'application en identifiant 11 secteurs d'activités hautement critiques et 7 secteurs d'activité critiques.

Sont concernées par la directive, de manière variable en fonction de leur secteur d'activité, toutes les entités européennes intervenant dans un des 18 secteurs ciblés, dont le chiffre d'affaires et le bilan annuel dépassent 10 millions d'euros, ou qui emploient au moins 50 personnes.

Un calendrier d'application en France flou, mais de plus en plus proche

NIS 2 étant une directive européenne, elle ne peut s'appliquer dans un état membre que suite à une transposition en droit local. Suite à sa publication au JOUE (Journal Officiel de l'Union Européenne) en décembre 2022, les pays européens avaient jusqu'à mi-octobre 2024 pour voter leurs transpositions.

En France, le projet de loi « Résilience », qui contient ladite transposition, a été déposé au parlement le 14 octobre 2024, voté en

1 2009, création de l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information) en France

première lecture au Sénat le 13 mars 2025 et se trouve à l'heure où j'écris ces lignes en cours d'examen à l'Assemblée Nationale. Suite au vote de la loi, une dernière phase de concertation a été annoncée sur les éléments devant être précisés par décret. La date prévisionnelle d'application de la directive NIS 2 en France reste donc inconnue, mais devrait s'établir courant du 2nd semestre 2025.

La directive européenne elle-même, en tant que texte de loi, émet des objectifs de sécurité plus que des mesures de sécurité concrètes et intelligible pour les structures concernées. Il en sera de même pour le projet de loi français - le détail des exigences sera contenu dans un référentiel de règles qui fera partie du décret d'application.

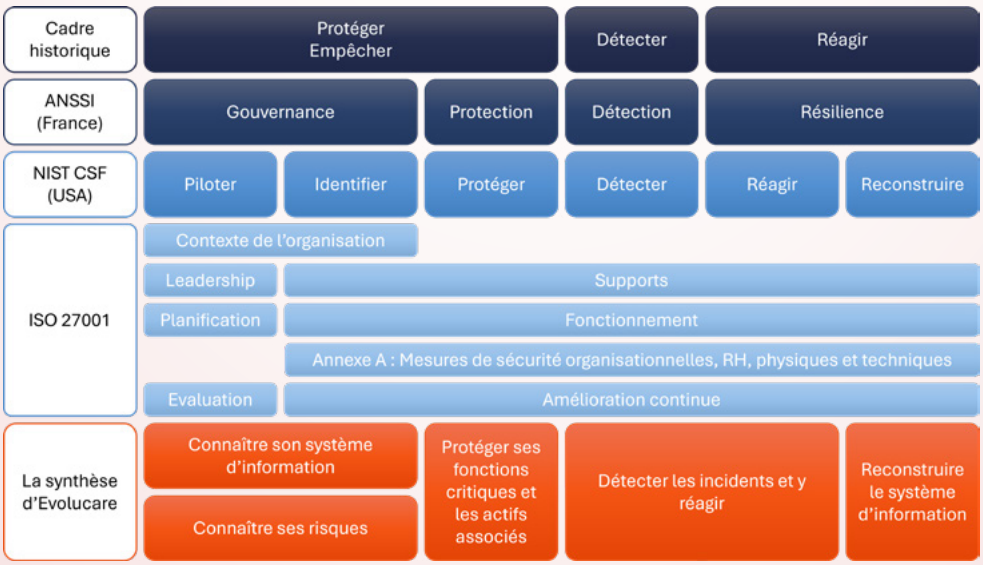
Ce référentiel a été construit par l'ANSSI (Agence nationale de la sécurité des systèmes d'information) en prenant en compte le retour d'expérience de la mise en conformité avec la LPM (Loi de Programmation Militaire) et la première directive NIS, ainsi qu'en menant des concertations successives avec les parties prenantes intéressées : fédérations et associations professionnelles, associations d'élus et de représentants des collectivités territoriales, prestataires de produits et services qualifiés.

Cette co-construction marque la volonté de l'ANSSI de proposer un référentiel de règles qui soit pragmatique et adapté aux organisations qui doivent le mettre en œuvre.

Une harmonisation des structures des différents référentiels

Dès l'émergence de la sécurité informatique - devenue sécurité des systèmes d'information, sécurité de l'information, puis cybersécurité - en tant que domaine spécifique, des référentiels normatifs et des standards ont vu le jour afin de l'aider à se structurer. Au fil des années, même si chaque référentiel conserve ses spécificités propres, ils tendent à se consolider autour des mêmes piliers, ce qui facilite les actions de mise en conformité avec de multiples référentiels.

Ainsi, les futures exigences de sécurité de la transposition française de NIS 2 seront alignées sur le référentiel à 4 piliers de l'ANSSI (Gouvernance, Protection, Détection, Résilience).



Evolucare, certifié ISO 27001 depuis 2023, est confiant dans sa mise en conformité avec NIS 2

À date, nos sources d'information sont le texte de l'article 21 de la directive, les éléments contenus dans le projet de loi « Résilience », ainsi que les éléments partagés par l'ANSSI au cours des phases de concertation sur la construction du référentiel. Ces sources nous permettent de savoir que les entités françaises visées par la directive devront se mettre en conformité avec vingt règles, qui proposeront des modalités différentes en fonction de la catégorisation (importante ou essentielle) de l'entité.

Bien que certains détails restent à préciser, on peut déjà effectuer un croisement entre les thématiques des règles et les exigences ISO 27001:2022, et anticiper sur la future mise en conformité.

Certains éléments sont d'ores et déjà traités par l'existence d'un SMSI : inventaire des systèmes, gouvernance SSI, cartographie des risques, gestion des fournisseurs, ressources humaines, sécurité physique, gestion des incidents de sécurité, audit…

Il restera quelques projets plus lourds, mais le temps gagné grâce à notre SMSI nous permettra d'y consacrer les efforts nécessaires pour assurer une mise en conformité dans les temps.

Conclusion

Le flou qui persiste autour des modalités de transposition de la directive NIS 2 en France peut pousser les organismes à attendre le dernier moment avant de prévoir et de planifier leurs projets de mise en conformité. Il n'est par ailleurs pas exclu que certains organismes n'obtiennent qu'au dernier moment une visibilité sur leur inclusion dans le périmètre de la directive, ou sur leur qualification d'entité importante ou essentielle.

Dans ce contexte, initier un projet de mise en conformité ISO 27001, même sans objectif de certification, ne peut être que bénéfique pour l'organisme. Quel que soit le futur impact de la directive NIS 2 (ou d'autres réglementations), la réflexion orientée par le référentiel ISO 27001 aura permis aux instances dirigeantes de l'entreprise de prendre du recul sur leur système d'information, de considérer les risques auxquels ils doivent pouvoir faire face, et dans l'idéal, d'initier des projets de montée en maturité sécurité.

La protection de nos organisations contre les attaques de plus en plus nombreuses peut souvent paraître comme une montagne insurmontable ; mais petit pas par petit pas, on arrive en haut de l'Everest.

evolucare

www.evolucare.com

SOURCES
1. L'espace mis à disposition des futures entités essentielles et importantes par l'ANSSI : *https://monespacenis2.cyber.gouv.fr/*
2. Le dossier législatif français sur le site de l'Assemblée Nationale : *https://www.assemblee-nationale.fr/dyn/17/dossiers/DLR5L17N50731*
3. La directive NIS 2 : *https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32022L2555*

5. LES STRATÉGIES DE DÉPLOIEMENT POSSIBLES

5.1 Les prérequis managériaux

Il y a deux prérequis à surveiller de près, sans lesquels toute démarche ISO 27001 - et, de façon générale, toute démarche qualité / conformité - est quasi impossible.

Premier point : le soutien de la Direction Générale et de la DSI. Sans cela, tout effort est fait en pure perte.

Non qu'il s'agisse de budgets financiers, mais surtout de priorisation, d'appui de la hiérarchie dans la mise en œuvre des processus et des bonnes pratiques.

Exemple de la checklist de mise en production

Avant toute mise en production, une DSI doit dérouler une checklist : sauvegardes mises en place, documentation produite, tests de restauration effectués, etc. Cela ne réclame aucun budget (c'est une simple feuille, dont le modèle est versionné et évolue dans le temps, et qui comporte juste des cases à cocher), mais sans cette « discipline de travail » et surtout l'appui d'une DSI pour retoquer les mises en production des projets qui n'ont pas rempli cette checklist, point de démarche efficace.

Second point, les informaticiens, qui sont clairement réfractaires à ce genre de démarche. C'est un problème de management et rien d'autre, car l'expérience montre que, lorsque le point de bascule est atteint, ceux qui ont adhéré à cette façon de travailler non seulement ne veulent plus revenir en arrière, mais en plus ne comprennent même pas comment ils ont pu travailler autrement par le passé tellement c'est protecteur des pratiques professionnelles, de la qualité du travail produit et plus généralement des agents.

L'ISO protège, et pas qu'un peu

Un logiciel métier sans matrice d'habilitation ? Pas possible madame / monsieur de la MOA : l'ISO ne le permet pas.

Une ouverture de ports qui met en danger le SI : pas possible, l'ISO ne le permet pas.

Etc., etc., etc.

5.2 Digression utile sur la position du RSSI

Il semble utile de rappeler que le pilotage d'un SMSI est traditionnellement le rôle du RSSI dans une organisation. C'est d'autant plus adéquat que le RSSI est en dehors de la DSI, mais possible même si rattaché à elle (ce qui, on le rappelle encore une fois, est une anomalie).

Attention tout de même à un léger détail, qui est connu des qualiticiens dans la norme ISO 9001 mais que l'on a tendance à oublier dans la norme ISO 27001 : stricto sensu, le pilotage du SMSI échoit au RSMSI : le Responsable du SMSI. Il se trouve que dans tous les hôpitaux (sauf erreur), le rôle du RSMSI est assumé par le RSSI, mais cette situation est essentiellement due à la taille et à la maturité.

Un autre schéma, plus conforme à l'esprit de la norme est de considérer que :

• le rôle de RSMSI est assumé par un qualiticien ;

• le RSSI est un responsable de processus comme un autre.

Ce découpage pose d'autres problèmes, par exemple la dualité du rôle de RSSI qui est à la fois propriétaire d'un processus et principale MOA de la cyber, mais la présente publication ne va pas jusqu'à ce niveau de détails : quand il ne nous (me) restera que ce genre de considération à régler, nous serons à la retraite depuis un bon moment.

5.3 Y aller, mais comment ?

L'idée de prendre la norme (qui fait à peine 11 pages A4), et de dérouler les spécifications ligne à ligne et en séquence, est tout bonnement illusoire. C'est la position d'Alexandre FERNANDEZ-TORO dans son ouvrage sur la norme (voir Annexe), et c'est aussi la mienne : cette idée est à proscrire immédiatement. Il faut donc trouver d'autres méthodes, qui au demeurant font l'objet de la norme ISO 27003, qui curieusement est très peu appliquée et quasiment jamais citée par les consultants.

Il existe plusieurs approches, qui ont toutes pour point commun de séparer deux phases :

• la phase projet (BUILD) : on met en place certains éléments du SMSI ;

• la phase exploitation (RUN) : une fois que l'on décide que le BUILD a été suffisamment loin on peut passer en mode routine, qui bien entendu va s'inscrire dans un cycle PDCA.

Si l'on revient sur l'histoire de la norme (voir plus haut), on constate que l'on est passé successivement par les phases suivantes :

• la phase « mesures », où la norme concernait uniquement la mise en place de mesures techniques (qui sont devenue les 93 mesures de l'Annexe A) ;

• la phase SMSI, où l'on a inscrit ces mesures dans un SMSI en mode PDCA ;

• la phase actuelle avec une vision processus-centrée.

Sans surprise, ces phases, ou états successifs de maturité, correspondent aux 3 étapes pour la mise en œuvre d'une norme ISO 27001.

6. ETAPE 1 : EN FAIRE SANS LE DIRE, OU L'APPROCHE PAR L'ANNEXE A

6.1 Idée générale

Cela consiste à aller vers de l'ISO 27001, sans forcément que cela soit explicite (bien entendu, la hiérarchie doit avoir validé la méthode).

Dit autrement, cela consiste à aborder par les mesures techniques (c'est bien comme cela que l'ISO a commencé), et donc :

• prendre les 93 mesures de l'annexe A ;

• éliminer rapidement celles qui ne s'appliquent pas au périmètre retenu ; dans les faits, on élimine 2 à 5 mesures, rarement plus ;

• pour chacune, leur attribuer un propriétaire ; comme les mesures sont pour la plupart techniques (chapitres 6, 7 et 8) les propriétaires seront quasiment tous dans les équipes d'infrastructure ; pour le chapitre 5, la plupart des mesures échoient au RSSI lui-même ;

Processus, pas encore

En réalité, les mesures appartiennent à un processus, qui a lui-même un responsable. Mais cette approche arrive trop tôt, l'approche processus implique certains prérequis trop complexes à ce stade.

• pour chacune, demander au propriétaire : et pour cela, tu fais quoi ?

Et pour cela, tu fais quoi ?

6.5, mesures au départ de l'agent : le responsable du processus RH à la DSI doit décrire a minima ce qu'il fait, par exemple pour s'assurer du déprovisionnement des comptes adminsys, restitution des matériels, etc…

7.2, entrées physiques dans les locaux : le responsable des locaux (souvent le responsable infra si l'on parle des datacenters et autres zones sensibles) doit contrôler annuellement (a minima) les habilitations d'accès dans ces locaux et les traces.

8.6, dimensionnement des équipements : le responsable (souvent infra encore) doit démontrer qu'il anticipe a minima la montée en charge (CPU, espace disque, etc.).

• pour chacune de ces réponses, s'assurer qu'il existe un contrôle de vérification de la mesure : le faire une fois c'est bien, s'assurer régulièrement que c'est toujours fait, c'est indispensable ; cela suppose donc un registre des contrôles, chaque contrôle dans le registre appartient au propriétaire de la mesure ;

• mettre en place un calendrier des contrôles, qui doit donc couvrir a minima les 93 mesures (moins celles non retenues, 1 contrôle pouvant couvrir plusieurs mesures, ce qui est même conseillé), chaque contrôle étant bien entendu à la charge du responsable de la mesure.

Le quadriptyque est donc :

Exigence de l'annexe A → réponse attribuée à un responsable → contrôle de la mesure, compilé dans un registre → contrôle exécuté selon un calendrier

La PSSI, pas forcément à ce stade

Les puristes me rétorqueront qu'il manque la PSSI dans l'équation. Certes, ce document est un des fondements de la SSI, mais son statut est un peu étrange dans la norme ISO 27001 : il apparaît comme une mesure (5.1). A ce stade, il y a plusieurs versions : soit la PSSI est une mesure parmi d'autres, soit elle est constituée par l'agrégat des autres mesures, soit enfin la PSSI est le besoin (l'intention) et les autres mesures (au-delà de la 5.1) sont la réponse à ce besoin.

6.2 Prérequis

Aucun si ce n'est la volonté managériale d'engager la DSI dans ce changement de paradigme.

6.3 Périmètre

Il est fortement conseillé, dans un premier temps, de restreindre cette approche à l'infrastructure technique de la DSI : réseau, serveurs, stockage, datacenter et les équipes qui les pilotent, à la fois en RUN et en BUILD.

Il est possible que certaines des 93 mesures soient hors scope dans un premier temps (certaines mesures concernent les accès physiques, d'autres le processus de formation, d'autres enfin des aspects de gouvernance). Ce n'est pas grave à ce stade, l'objectif est la mise en place de ce socle de base.

6.4 Rôles / Gouvernance

Globalement, le RSSI pilote la démarche en lien avec les responsables des équipes qui ont en charge les mesures de l'annexe A (et donc, on le redit, les réponses à ces mesures et les contrôles correspondants).

Le RSSI est donc un facilitateur, un catalyseur, un auditeur, un conseil.

6.5 Livrables

Les livrables sont :

• chaque mesure doit être adressée; attention, toutes les mesures de l'annexe A n'exigent pas que la réponse soit écrite (« documentée » ou « définie » dans la norme, ce qui en fait environ une dizaine), mais a minima que l'on soit en mesure de dire comment on y répond ;

• chaque mesure doit faire l'objet d'un contrôle, lui-même défini (documenté), et qui produit une trace (un enregistrement) ;

La souplesse des contrôles

La norme (chapitre 9.1) est assez souple sur ce sujet, et permet de ne pas couvrir 100 % des mesures par un contrôle, mais il faut évidemment le justifier.

• chaque mesure doit être exécutée selon un calendrier.

Volume documentaire approximatif

On peut estimer les éléments suivants :

• l'annexe A à tenir à jour, pour savoir à qui est attribué chaque mesure ;

• environ 10 mesures à documenter ; pas d'inquiétude, la documentation peut tenir en 1/2 page à chaque fois ;

• un registre des contrôles (1 fichier tableur) ;

• un calendrier des contrôles (également, un fichier tableur),

Soit 3 documents, sans compter bien entendu les traces d'exécution des contrôles.

6.6 Durée

Selon le périmètre retenu, cela peut prendre entre 3 mois et 6 mois, en supposant la volonté managériale, la réservation des ressources, etc.

6.7 Outillage et moyens

Côté outils logiciels, rien, à part un tableur pour suivre le tableau des mesures de l'annexe A, de leurs attributions et le calendrier des contrôles.

Côté moyens externes, le recours à un consultant externe ponctuel peut être nécessaire pour quelques jours de prestations, mais la plupart du temps, l'appel aux copains RSSI du secteur suffira, partant du principe que chaque problème rencontré chez vous l'a déjà été ailleurs, et a déjà été réglé.

Côté journée homme interne, même sur une organisation importante (1500 agents, 25 personnes à la DSI), on peut s'en tirer honorablement avec 1/4 temps de RSSI sur 3 à 6 mois.

DÉPLOIEMENT ET SUIVI DES MESURES TECHNIQUES

Par les équipes de Stormshield

Approche métier : Point de vue de Stormshield

La continuité des soins particulièrement sensible aux ransomwares, l'urgence médicale qui diminue la vigilance numérique et le manque de moyens, exacerbé par la transformation numérique et le déploiement d'objets médicaux connectés, rendent les cliniques et hôpitaux particulièrement sensibles aux cyberattaques. A titre d'exemple, en 2023 l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) recensait plus de 400 attaques contre des établissements de santé. Un chiffre en forte hausse par rapport aux années précédentes.

La mise en place d'un Système de Management de la Sécurité de l'Information (SMSI) va permettre une gestion mesurée des risques et contribuer à l'amélioration de la sécurité du Système d'Information. Véritable bras armé de ce système de management, le déploiement des mesures de sécurité diminue les risques d'une cyberattaque en protégeant notamment les actifs critiques.

Editeur de solutions de cybersécurité, Stormshield propose un ensemble de solutions de cybersécurité permettant de couvrir à la fois les moyens techniques et les points de mesure, et de garantir une homogénéité des mesures de sécurité déployées. Les équipes de sécurité du Système d'Information peuvent ainsi mesurer les écarts à la politique de sécurité et envisager sereinement son évolution.

Les mesures de sécurité techniques

L'Annexe A de la norme ISO/IEC 27001:2022 présente la liste des mesures recommandées pour la gestion des risques dans un SMSI, réparties en quatre catégories (l'organisation, les personnes, la sécurité physique et la technologie). Véritable guide de bonnes pratiques, ces mesures adressent la problématique de la sensibilité des établissements de santé aux cyberattaques et assurent une maitrise des risques induits par la complexité des infrastructures hospitalières, l'hétérogénéité des métiers et des utilisateurs du Système d'Information et la criticité des données patients.

Complexité du SI et ségrégation réseau

Parmi les mesures de l'Annexe A, la catégorie « Mesures technologiques » liste 34 contrôles à appliquer pour protéger les Systèmes d'Information, les données et les infrastructures technologiques.

La ségrégation du réseau est un des points essentiels face à la complexité des Systèmes d'Information des établissements de santé. De la gestion technique des bâtiments en passant par le réseau opérationnel des dispositifs médicaux ou encore le Système

d'Information pour les patients, la complexité globale de l'infrastructure favorise en effet la présence de points de faiblesse pour passer d'un système à l'autre.

Pour exemple, un défaut de segmentation ou de cloisonnement informatique entre un point d'accès wifi pour les patients ou le personnel administratif et une autre partie du Système d'Information facilite le déplacement latéral au sein de l'infrastructure. En exploitant cette porosité entre des réseaux ayant des niveaux de confidentialité différents, un cyber attaquant peut accéder aux actifs critiques et perturber le système opérationnel de soins ou le fonctionnement technique des bâtiments.

Par ailleurs, historiquement hétérogènes et constituées de systèmes vieillissants, les infrastructures des établissements de santé ont dû faire face à une ouverture vers le Cloud et Internet pour le partage de données et la télémaintenance d'équipements critiques (IRM, scanners, automates des laboratoires…). Cette interconnexion des réseaux augmente encore la surface d'attaque et nécessite fortement une segmentation, telle que recommandée par l'Annexe A de la norme ISO/IEC 27001:2022, afin d'isoler les actifs les plus sensibles pour préserver le fonctionnement des établissements.

Diversité des métiers et contrôle d'accès à l'information

Autres points critiques mis en avant par la norme, le contrôle d'accès à l'information et la gestion des privilèges nécessitent une vigilance très fine afin de garantir la confidentialité des données financières, des données à caractères personnelles, des données patients ou encore des informations liées au fonctionnement du système opérationnel des établissements.

Le contrôle des flux est donc une brique complémentaire à la segmentation réseaux, indispensable pour assurer une étanchéité complète des différents Systèmes d'Information et vérifier l'identité des utilisateurs et leurs niveaux d'accréditation avant de leur donner accès à l'information.

Au-delà de la confidentialité des informations, la fourniture d'un accès Internet aux patients engage également la responsabilité des établissements et les oblige à conserver les données de navigation. Le déploiement d'un système d'authentification fait donc aussi partie des mesures à mettre en place, avec une vigilance accrue pour les données les plus critiques via la mise en place d'une authentification à multiples facteurs.

La nécessaire gestion des incidents de sécurité

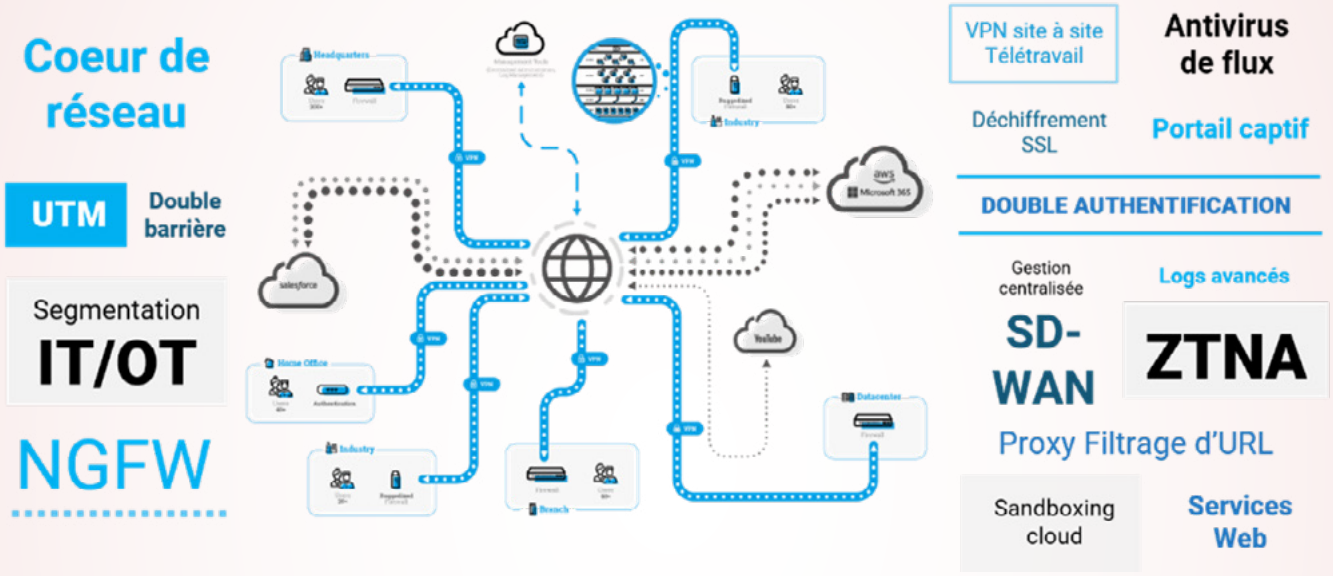
Face à la complexification des attaques cyber, les moyens de prévention actuels ne sont plus suffisants. Les organisations cybercriminelles utilisent de plus en plus des méthodes conçues pour les contourner et rester indétectables avant d'accéder aux systèmes ou aux informations ciblés par leurs attaques. Seuls les indices de compromission permettent alors de détecter la possibilité d'une attaque en cours.

En remontant ces indices dans une solution de gestion des incidents, les équipes de sécurité peuvent effectuer des opérations d'analyses et d'investigations poussées afin de détecter les machines ou systèmes compromis, mettre en place des solutions de remédiation adéquates et suivre dans le temps la résolution des incidents. Les attaques sont ainsi interceptées en amont et endiguées avant qu'elles ne causent des

dégâts dans l'infrastructure.

Stormshield et le suivi des mesures de sécurité

A travers sa solution complète et intégrée « Stormshield Network Security », Stormshield accompagne les établissements de santé dans le déploiement d'un certain nombre de mesures techniques de sécurité identifiées dans le cadre de leur approche de management de la sécurité de l'information, avec également une approche Zero Trust pour la prise en compte des problématiques liées à la mobilité, au télétravail et aux applications et infrastructures hébergées dans le Cloud.



En complément, la solution « Stormshield Log Supervisor » permet aux RSSI de contrôler et de suivre l'implémentation des mesures de sécurité techniques, de mesurer les écarts par rapport à la politique de sécurité et de planifier les corrections et les évolutions de ces mesures, pour une amélioration continue de la sécurité de leur Système d'Information. Cette solution offre également la possibilité de mettre en œuvre un système de gestion des incidents de sécurité complétement intégré.

Choisir Stormshield, c'est faire le choix de solutions de confiance européennes reconnues et de s'assurer d'une intégration parfaite entre le déploiement des mesures de sécurité et le suivi des écarts et de la conformité à la politique de sécurité.



STORMSHIELD

www.stormshield.com

7. ETAPE 2 : METTRE EN PLACE SON SMSI

Ce guide n'a pas pour objectif de décrire la mise en œuvre d'un SMSI : il existe d'excellentes formations pour cela (27001 Lead Implementer notamment, certifiante ou pas) ainsi que d'excellents ouvrages (cf Bibliographie ci-dessous) et des clubs 27001 en France (les deux derniers à avoir vu le jour sont le club 27001 nantais en 2023 et le rennais en 2025).

Le déploiement d'un SMQ en général, et d'un SMSI en particulier (qui est un SMQ parmi d'autres) est très étrange, et cela pour plusieurs raisons.

Fondamentalement, piloter sa sécurité informatique (sujet par essence technique) par un SMSI, c'est demander à la forme de piloter le fond - et le pire c'est que cela fonctionne, et redoutablement bien.

C'est aussi considérer que respecter à la lettre le cycle PDCA produit un résultat très efficace.

C'est enfin accepter de ne pas trop remettre en cause (surtout au début) des concepts qui peuvent paraître surprenants, et de s'en remettre à une intelligence collective qui a accumulé depuis plus de 3 décennies un « objet conceptuel » (le SMQ) parfaitement abouti, le tout en moins de 15 pages A4.

7.1 Quelques difficultés

Certains auditeurs vous expliquent que ce qui est majeur, c'est le descriptif du contexte général (chapitres 4 et 5) et la première itération de l'appréciation des risques (chapitre 6). D'autres, au contraire, mettent le focus sur le contrôle (CHECK, chapitre 9), d'autre enfin sur le ACT (chapitre 10).

La réalité, c'est qu'il va falloir tout faire, et qu'aboutir à un P, un D, un C et un A à peu près présentables à un auditeur de certification demande de l'huile de coude, une certaine humilité et pas mal d'accompagnement et d'échanges avec les pairs.

Pour preuve de la difficulté de l'exercice général, il a fallu à votre serviteur pas mal de temps (je n'ose vous dire combien) pour comprendre la différence entre « contrôler un processus » (chapitre 8) et « mesurer un processus » (chapitre 9). Et presque autant pour savoir où se situaient les « risques et opportunités du SMSI » par rapport à « l'appréciation des risques » (ce n'est pas la même chose).

Pour rentrer dans le cœur d'une démarche ISO / PDCA, on n'évitera pas de devoir « rentrer dans le dur » de la démarche. Le saut culturel que cela implique est important. Pour exemple, le seul document du Manuel SMSI (appelé aussi « Politique du SMSI ») n'est pas trivial et nécessite de nombreuses révisions avant d'aboutir à un document propre. L'appel à des compétences extérieures est indispensable, mais en respectant des règles importantes, évoquées ci-après.

7.2 L'approche à éviter

C'est un grand classique des ESN et des boites de conseil : un accompagnement « full inclusive » avec des centaines de jours homme pour aboutir quasiment clé en main à la certification.

Vous êtes quasiment sûrs d'obtenir le précieux petit papier des organismes certificateurs à la fin de la démarche, et vous êtes quasiment sûrs également de :

• vous retrouver à la tête d'un volume documentaire impressionnant dont vous ne saurez que faire une fois les consultants partis ;

• avoir les plus grandes difficultés à garder ladite certification au-delà du second audit, l'année d'après.

• finir par jeter les 3/4 de la documentation, qui, au final, n'est là que pour faire « habité » dans le SMSI - mais cela vous ne vous en apercevrez justement qu'une fois les consultants partis.

7.3 La montée en maturité

Une certification ISO, ce n'est pas un bout de papier : c'est une démarche de maturité générale de l'Organisation. Et cette maturité ne se décrète pas, encore moins par une tierce partie (l'ESN ci-dessus) : à un moment, l'Organisation doit se prendre en main, quitte à se faire aider bien entendu, mais sans « faire à sa place ».

Marcher, une démarche individuelle

On a tous appris à marcher entre 6 mois et 18 mois. Et le moment où le petit enfant décide de lâcher le bord du canapé pour faire ses premiers pas, il le décide tout seul : nul parent ne peut le décider à sa place. La maturité organisationnelle obéit aux mêmes règles : elle peut être accompagnée, soutenue, mais jamais faite « à la place de ».

7.4 Une méthode, parmi d'autres

Votre serviteur a mis en place un SMSI en laissant quasiment les clés de la maison à un consultant externe pour plus de 200 jours de prestations : je pense avec du recul que cette méthode est vouée à l'échec - et ce n'est que mon avis.

Si cela était à refaire, je ferais appel à un consultant, mais sur un volume de jours beaucoup plus mesuré (environ 50), avec comme mission :

• d'avoir interdiction absolue de « pondre » le moindre document, car c'est un piège abscons ;

• de nous orienter, de nous « donner des devoirs » pour la session suivante, ajuster, contrôler, accompagner, mais certainement pas faire à notre place.

Aller d'abord voir les copains

D'autres RSSI se sont certifiés avant vous : allez les voir ! Perdez une demi-journée à échanger avec eux : non seulement ils n'ont rien à vous vendre, mais ils se feront dans la plupart des cas un plaisir de vous aider à éviter les chausse-trapes dans lesquelles ils sont eux-mêmes tombés.

On est plutôt sur un mode de coaching, qui soit dit en passant est très courant dans des méthodes de type Lean Management ou Six Sigma. Le coach accompagne, guide, corrige les erreurs de trajectoire, mais ne fait rien - ne produit rien - par lui-même.

A vue de nez même pour une organisation de taille conséquente (1500 agents dont 25 à la DSI par exemple), un volume de 50 jours de consultant externe grand maximum doit suffire, s'il est accompagné des formations qui vont bien en amont, des échanges avec les pairs, de quelques participations à des clubs 27001.

Volume documentaire approximatif

En plus de la documentation produite pour la phase précédente, le volume documentaire augmente significativement :

• le manuel du SMSI, qui peut facilement dépasser 20 pages ;

• la Politique du SI, qui ne doit pas dépasser une page ;

• la documentation des processus du SMSI : méthode d'appréciation des risques, surveillance du SMSI, supervision de la performance du SMSI, audit interne, revue de direction, suivi des actions.

7.5 Durée

Impossible en moins de 12 mois, et encore en y consacrant un temps RSSI ou RSMSI conséquent. Globalement, il faut garder en tête que la phase précédente plus celle-ci sont quasiment impossible à mettre en œuvre en moins de 18 mois. Dans les faits, compter plutôt 2 bonnes années de travail, pas à plein temps, bien entendu.

7.6 Outillage et moyens

Côté outillage, idem que l'étape précédente : quasiment rien à part un tableur, et le consultant évoqué juste ci-dessus.

Côté consultant, 50 jours maximum pas plus.

Côté charge en jour-homme interne, difficile de donner une estimation car c'est très dépendant de la taille de l'organisation, du périmètre certifié, etc. Mais on peut partir sur une base d'1 ETP (réparti sur plusieurs personnes, dont un mi-temps du RSSI) pendant toute la durée des phases 1 et 2.

8. ETAPE 3 : FORMALISER LES PROCESSUS ET ÉTENDRE LE PÉRIMÈTRE

Stricto sensu, les processus doivent avoir été formalisés pour la phase précédente. L'orientation processus est déjà apparue succinctement dans la version 2017 de la norme, elle est omniprésente dans la version 2022.

La comparaison avec les chapitres communs entre la norme ISO 9001 (qui n'a pas évolué depuis 2015) et la norme ISO 27001 est d'ailleurs assez frappante : le mot « processus » apparaît partout dans la seconde. Pour exemple, la norme ISO 9001 précise au tout début du chapitre 9.1 (le CHECK interne qui concerne le SMQ) :

« L'organisme doit déterminer :
a) ce qu'il est nécessaire de surveiller et mesurer ;
b) les méthodes de surveillance, de mesure, d'analyse et d'évaluation nécessaires pour assurer la validité des résultats ;
... »

De son côté, la 27001, au même chapitre, précise quant à elle :

« L'organisation doit évaluer les performances de sécurité de l'information, ainsi que l'efficacité du système de management de la sécurité de l'information.
L'organisation doit déterminer :
a) ce qu'il est nécessaire de surveiller et de mesurer, y compris les processus et les mesures de sécurité de l'information ;
... »

On voit donc arriver à la fois les mots processus et performance.

Démarrer un SMSI par l'angle d'attaque des processus fait débat : certains auditeurs et implémenteurs vous y poussent directement au motif que c'est une exigence de la norme, d'autres argumentent qu'il faut un certain niveau de maturité pour arriver à ce stade.

8.1 Idée générale

Si l'on repart du début de la chaîne dans la 27001, on trouve successivement :

• une cartographie des processus du SMSI ;

• une appréciation des risques, chaque risque portant sur des assets (actifs) et étant affecté à un processus qui en est le propriétaire ; par transitivité, les assets également sont affectés à un processus ;

• des exigences retenues dans l'annexe A (la DDA), et des mesures mises en œuvre pour répondre à ces exigences ; les mesures sont donc rattachées à un risque (au moins), et donc rattachées à un processus qui en est également le propriétaire ;

• et, comme avant, les contrôles pour vérifier la bonne application de chaque mesure, regroupés dans un registre et planifiés selon un calendrier général des contrôles.

Avec les exigences du chapitre 9.1 de la norme, on rajoute une mesure de l'efficacité, ce qui implique que chaque processus définisse des indicateurs de performance en lien avec le triptyque Asset-Risque / DDA / Mesure dont il est le propriétaire.

8.2 Une méthode parmi d'autres

Il s'agit d'abord de définir un pattern (un gabarit ou modèle) de description de fiche processus. On en trouve des tas sur Internet, comme, par exemple, le modèle de tortue de Crosby (voir Annexe) qui peut être pris tel quel ou adapté, ou celui utilisé par votre serviteur, qui dérive de celui de Crosby (voir Annexe).

Ensuite, chaque responsable de processus doit décrire son processus sur la base de ce modèle, dans un document versé au corpus documentaire. Point important : sauf impossibilité (il y en a), il est important de définir des indicateurs de performance du processus permettant de répondre à la question simple : en quoi ce processus contribue-t-il efficacement à la sécurité de l'information ?

Indicateur d'activité ou de performance

Un nombre d'incidents traités par jour ou semaine, c'est un indicateur d'activité : il prouve juste que l'on ne se tourne pas les pouces, pas que l'on est efficace.

Un pourcentage d'incidents de niveau CVE > 9 traités en moins de 48h, c'est un indicateur de performance.

Dans certains cas, les indicateurs de performance sont très difficiles à trouver : par exemple pour une équipe qui attribue les habilitations, on ne pourra quasiment remonter que des indicateurs d'activité. Pas grave, le 9.1 de la norme stipule bien que « L'organisation doit déterminer :

a) ce qu'il est nécessaire de surveiller et de mesurer ».

L'organisation peut donc parfaitement dire que tel processus n'est pas mesuré - il faudra juste le documenter dans le Manuel SMSI.

Une fois pris le « virage processus », on peut dire que la vie change :

- les propriétaires des processus sont responsables de la définition de ceux-ci, de la connaissance de leurs assets, de leurs risques (qui sont liés aux assets), des mesures qui leur sont affectées, des contrôles de ces mesures, des indicateurs ;

- le RSSI peut passer en audit interne de ces processus, par exemple de façon trimestrielle ;

Le RSSI passe en contrôle interne du SMSI

Il est possible de planifier des points trimestriels avec chaque responsable / propriétaire de processus pour vérifier : la mise à jour de la fiche processus, la liste de ses mesures, une vérification de l'application de ces mesures par échantillonnage, une vérification par échantillonnage des contrôles, et une collecte des indicateurs. Il s'agit d'une parfaite illustration de « montée en maturité » : les processus reprennent la main sur leur périmètre.

Il est même possible de développer des contrôles de niveau 2, c'est-à-dire des contrôles de contrôles (ce qui a du sens dans certains cas) ; la responsabilité des contrôles de niveau 2 n'est d'ailleurs pas spécifiée dans la norme, on peut aussi bien considérer que c'est à la charge du RSSI ou des processus eux-mêmes.

8.3 Durée

La question de la durée n'a pas de sens à ce stade, cette étape est supposée avoir été déroulée dans la mise en œuvre du SMSI.

Par contre, toute extension du périmètre du SMSI nécessite d'avoir les idées parfaitement claires sur cette démarche : hors de question de rajouter des équipes ou des métiers de la DSI sans les intégrer directement à la démarche processus, ce qui nécessite une petite formation.

Sensibilisation à l'approche processus
Prévoir 2h à 3h avec l'équipe concernée, pour lui expliquer :
• la démarche générale ;
• la stratégie d'intégration de l'équipe dans cette démarche : approche processus et surtout indicateurs.

8.4 Outillage et moyens

Côté outillage, idem que l'étape précédente : quasiment rien à part un tableur, et le consultant évoqué juste ci-dessus.

A ce stade, la charge de consultant est terminée. A titre personnel, je suis d'avis qu'un RSSI devrait avoir un bon à tirer d'une prestation annuelle de 10 à 15 jours de consultant externe, pour deux sujets :

• la norme évolue et la lecture que l'on en a aussi, il est toujours important de confronter cette lecture à un regard extérieur ; d'ailleurs, on est supposé ne pas garder le même consultant plus de 2 années de suite, car il faut aussi changer ce regard extérieur ;

• les audits internes, qui doivent être réalisés par un expert hors de l'Organisation, donc pas le RSSI ;

Côté charge en jour-homme interne, impossible de répondre puisque cela dépend à la fois de la partie processus qui aura été réglée dans la phase précédente, et des extensions futures.

9. COMBIEN CELA COÛTE

Le déploiement total d'un SMSI dans une DSI peut être évalué de la sorte :

• le temps RSSI ;

• le temps interne dans la DSI ;

• le consulting pendant la phase de mise en œuvre (étapes 1 et 2 précédentes) ;

• la charge d'audit ISO.

De façon (très très très) approximative, cela donne ces ordres de grandeur.

	Etape 1	Etape 2	TOTAL
RSSI	50	100	150
DSI	50	100	150
Consultant externe	50	10	60
Auditeur ISO	N/A	N/A	5

On arrive à un total de 300 jours en interne, 60 jours de consultants sans compter la facture de l'organisme de certification. Réparti sur 2 années, et hors consultant externe, cela fait tout de même 150 jours par an soit environ 3/4 d'ETP.

Si l'on part du principe qu'une démarche qualité ne doit pas consommer plus de 5 % du temps disponible, cela veut dire qu'en dessous de 15 agents dans une DSI, toute démarche ISO 27001 est quasi infaisable.

Ces chiffres constituent des ordres de grandeur : selon le périmètre retenu pour l'ISO 27001, les missions de la DSI, les qualifications des agents et d'autres paramètres qualitatifs impossibles à intégrer dans une équation générale, ces estimations peuvent varier de + /- 20 %.

Les paramètres sur lesquels jouer sont bien entendu :

• la durée de l'étape 1 : plus les agents intégrés au périmètre de certification seront acculturés à la démarche mesure / contrôle / calendrier des contrôles, plus le fait de raccrocher cela à un SMSI sera facilité ;

• la possible parallélisation des étapes 2 et 3.

10. ET APRÈS...

Dans un mode de fonctionnement de type « routine » (si tant est que cela puisse exister pour un SMSI), on a le schéma suivant :

• un évènement de sécurité survient : incident, alerte d'un CERT, résultat d'une veille technologique, évolution d'une menace, etc.

• l'évènement est traité par les équipes en RUN ;

• le problème sous-jacent est analysé (l'incident est conjoncturel, le problème au sens ITIL est structurel) ;

• cela donne lieu à une mise à jour de l'analyse des risques : soit un nouveau risque, soit une cotation revue d'un risque existant ;

• si besoin, cela donne lieu à une mise à jour de la base des assets : nouvel asset affecté à un processus, mise à jour d'un référentiel d'asset existant, etc. ;

• si besoin, cela donne lieu à une modification de processus ;

• si besoin, cela conduit à réviser la DDA (peu probable, les exclusions si elles ont bien été analysées bougent rarement) ;

• cela donne lieu à une mise à jour de la PSSI ;

• cela donne lieu à une nouvelle mesure de sécurité ou mise à jour d'une mesure existante ;

• puis d'un contrôle ;

11. LA QUESTION DE L'OUTILLAGE

Un SMSI ne nécessite pas forcément un outillage logiciel.

La question de la GED

Certes une GED est pratique, elle gère pour vous le cycle documentaire : signature, révisions, etc. Mais rien dans la 27001 n'oblige à ranger les documents du SMSI dans une GED : il est juste exigé de « gérer » la documentation (création, propriétaire, diffusion, etc.), ce qui peut parfaitement être réalisé avec des partages de répertoires et une rigueur dans le cycle de révisions.

Pour l'ensemble du corpus documentaire, un tableur et un traitement de texte suffisent, avec le bon marquage et le bon cartouche qualité.
Il existe cependant des situations pour lesquelles un outillage est souhaitable :

• un SMSI très étendu, sur une Organisation de plusieurs centaines de personnes, avec des dizaines de processus, des centaines de mesures et de contrôles ;

• un SMSI géographiquement éclaté avec des nombreux sites ; c'est le cas des entreprises avec siège et filiales multiples, y compris à l'étranger ;

• de très fortes obligations réglementaires dans des secteurs précis : aéronautique, banque, défense, etc. ;

• la nécessité opérationnelle de ranger plusieurs normes dans un seul outil, lorsque l'entreprise commence à vouloir faire converger les certifications multiples : 9001, 27001, DORA, NIS, etc.

• une volonté de pousser certaines appréciations des risques, par exemple du fait de contraintes assurantielles ;

Attention cependant à la charge de travail nécessaire pour prendre la main sur ces outils : on constate que les organisations qui les adoptent ont souvent des équipes cyber conséquentes, avec un RSSI et son assistant, une personne spécifiquement dédiée à la gestion documentaire, etc.

SHADOW IT ET SAAS HOSPITALIERS : REPRENDRE LE CONTRÔLE POUR UNE CONFORMITÉ ISO 27001 RENFORCÉE

Par les équipes d'Olfeo

Approche métier : Point de vue d'Olfeo

Le cloud et le SaaS : catalyseurs de transformation mais angles morts de la sécurité hospitalière

Ce n'est un secret pour personne, les applications SaaS se multiplient à un rythme soutenu et les RSSI sont confrontés à un défi majeur : maîtriser les usages numériques qui échappent au périmètre traditionnel du système d'information. C'est précisément là que se situe l'apport stratégique des solutions CASB (Cloud Access Security Broker). Au-delà de leur fonction technologique, elles s'inscrivent aujourd'hui comme un levier fort de mise en conformité avec la norme ISO/IEC 27001:2022, notamment pour les organisations qui doivent encadrer des usages cloud en forte croissance sans renoncer à la sécurité ni à la fluidité des métiers.

Enjeu critique : la perte de visibilité et de contrôle sur les usages cloud métiers

Dans le secteur hospitalier, ces risques se traduisent par :

- Des fuites accidentelles de dossiers patients via des plateformes non sécurisées.
- Des collaborateurs qui utilisent des outils de partage cloud grand public sans chiffrement ni authentification forte.
- Des échanges de données santé via des messageries instantanées non souveraines et non conformes (WhatsApp, Slack...).
- Une incapacité des RSSI à détecter ou tracer ces usages hors SIH traditionnel.

Les conséquences peuvent être graves :

- Non-conformité potentielle vis-à-vis du RGPD, des exigences HDS ou de la doctrine du numérique en santé.
- Risque juridique en cas de fuite de données (amendes, signalements à l'ANS).
- Surface d'attaque élargie et difficilement contrôlable (Shadow IT, Shadow Cloud, Shadow RH…)
- Risques de sécurité avec réutilisation des login/mot de passe d'une application à une autre, voir même la réutilisation d'accès d'une application métier interne, permettant à un criminel qui aura profité d'une fuite de données d'une application SaaS tiers, d'accéder au SI d'un hôpital.

CASB : une approche pragmatique pour reprendre la main sans freiner les usages métiers

Le CASB (Cloud Access Security Broker), intégré dans les architectures SSE (Security Service Edge), est aujourd'hui une réponse éprouvée et graduellement adoptée par des RSSI santé en Europe (ex : CHU, groupements hospitaliers, GHT). Se basant sur les fonctions de proxy et de filtrage d'URL, la solution est capable d'identifier les accès à des URLs, domaines ou IPs correspondant à des applications SaaS.

Fonctions clés activables en contexte santé :

1. Shadow IT Discovery

• Découverte automatisée de toutes les applications cloud utilisées par les collaborateurs, internes ou externes.

• Identification des services à risques non conformes RGPD (HDS à venir)

• Cartographie dynamique des usages métiers réels.

2. Évaluation de risque adaptée santé

• Scoring de risque basé sur des critères santé (localisation des données, fuites documentées, indicateurs tiers)

• Visualisation claire pour la DSI et les métiers des écarts par rapport aux exigences du SIH.

3. Mise en place de politiques granulaires

• Blocage ou limitation d'usage des applications non validées.

• Autorisation conditionnelle avec restrictions (accès en lecture seule...)

• Redirection vers des solutions internes validées (portail cloud privé, plateformes HDS).

L'utilisation du CASB dans une démarche ISO 27001

Pour comprendre la valeur du CASB dans une démarche ISO 27001, il faut revenir à l'objectif fondamental de la norme : garantir la confidentialité, l'intégrité et la disponibilité des actifs informationnels en s'appuyant sur une gestion systématique des risques. Or, dans les environnements numériques modernes, les services cloud et les applications SaaS, malgré leur bénéfices indéniables, représentent une extension critique du périmètre du SI, mais aussi l'un de ses angles morts les plus fréquents, au niveau des usages et de la gestion d'accès.

La norme ISO/IEC 27001, dans sa version 2022, aborde explicitement cette problématique avec le contrôle A.5.36, qui impose aux organisations de définir des règles précises d'utilisation des services cloud notamment. Ce contrôle appelle à une gouvernance proactive des usages SaaS, à travers des politiques claires, des responsabilités établies, et une surveillance continue avec traçabilité des utilisations.

Le CASB répond précisément à cette exigence.

Il permet non seulement de détecter l'usage d'applications cloud non référencées, mais

aussi d'en évaluer automatiquement le niveau de risque, leur conformité avec les politiques internes et leur compatibilité avec les réglementations (comme le RGPD ou les exigences de localisation des données).

La norme insiste également sur la nécessité d'une surveillance active des services (contrôle A.8.16) et de la mise en place de contrôles d'accès granulaires (A.5.20). Sur ces deux points, le CASB joue un rôle essentiel. Il permet par exemple de définir des politiques d'accès conditionnel aux services cloud, en fonction de l'identité de l'utilisateur, de son appareil ou de sa localisation, assurant ainsi que les droits d'usage sont en adéquation avec le principe du moindre privilège. En parallèle, les capacités de journalisation et d'alerte du CASB permettent de détecter les comportements anormaux ou les activités suspectes, facilitant la mise en œuvre des contrôles A.5.15 (journalisation et surveillance) et A.5.27 (réponse aux incidents).

Pourquoi le CASB intégré au SSE est plus adapté que des solutions CASB seules ?

Les solutions CASB en mode stand-alone ont montré leurs limites dans les environnements hospitaliers :

• Complexité d'intégration avec les proxies et SIH existants.

• Difficultés à gérer les usages en mobilité ou en accès direct Internet (médecins sur smartphone personnel).

• Peu de lien avec les politiques DLP et ZTNA potentielles de l'hôpital.

L'approche SSE/SASE permet d'intégrer nativement le CASB avec :

• DLP unifié, pour prévenir les fuites de données DPI même en mode SaaS.

• Zero Trust Internet Access, pour contrôler finement les accès cloud en fonction de l'identité et du domaine de destination.

• Politiques centralisées et homogènes, déployées sur tous les usages (web, cloud, applications métiers).

• L'appui sur l'agent SSE déjà déployé pour avoir l'option CASB disponible en un clic.

De plus, dans un contexte de conformité avec la norme ISO 27001, cette convergence technologique permet de couvrir d'autres exigences de la norme, telles que la protection des accès distants (A.5.22), la gestion des actifs logiciels (A.8.9), ou encore la sensibilisation à la sécurité de l'information (A.6.4), en fournissant aux utilisateurs des messages pédagogiques en contexte lorsqu'un usage risqué est détecté.

Levier de gouvernance et d'accélération numérique

Au-delà de la sécurité pure, le CASB SSE devient un levier de gouvernance cloud pour les RSSI et DSI santé :

• Dialogue constructif avec les métiers : accompagner les usages plutôt que les bloquer.

• Rationalisation des applications utilisées et maîtrise budgétaire (cloud sprawl).

• Alignement rapide avec les exigences du référentiel SecNumCloud, HDS et doctrine du numérique en santé.

Enfin, il convient de souligner que l'intégration d'un CASB dans un SMSI bien structuré facilite l'approche par amélioration continue exigée par l'ISO 27001. Grâce aux tableaux de bord, aux journaux d'événements et aux rapports de conformité qu'il génère, le CASB alimente directement les processus de revue de direction, d'audit interne, et de gestion des non-conformités. Il devient alors un outil au service de la gouvernance de la sécurité, et non une simple brique technologique isolée.

Comment réussir le déploiement d'une solution CASB dans un établissement de santé ?

Avant toute chose, il faut savoir ce que l'on veut sécuriser. La cartographie des usages cloud est une étape essentielle. Il faut identifier :

• Les applications SaaS officielles (Office 365, Teams, DPI en cloud…)

• Les usages non officiels (shadow IT : Google Drive perso, WhatsApp, Dropbox…)

• Les flux de données sensibles vers l'extérieur.

Comment ?

• En analysant les logs proxy/firewall.

• En utilisant la fonction discovery du CASB.

• En impliquant les métiers : quelles applis cloud utilisent-ils vraiment ?

Conseil santé : beaucoup d'applications shadow IT apparaissent dans les services médicaux pour des raisons pratiques (partage de fichiers, mobilité). Il faut les comprendre, pas juste les bloquer.

Définir des politiques d'usage adaptées au secteur santé

La réglementation impose certaines obligations :

• Hébergement des données de santé chez des hébergeurs HDS.

• Respect du RGPD, traçabilité, limitation des usages.

Les politiques d'usage du CASB doivent donc :

• Autoriser uniquement les applications conformes.

• Contrôler les accès selon les profils (médecins, soignants, IT…).

• Mettre en place des règles DLP (Data Loss Prevention) adaptées : exfiltration de dossiers patients, partage non sécurisé, etc.

Focus métier : il ne s'agit pas de tout interdire, mais d'encadrer les usages pour éviter la fuite de données sensibles.

Choisir le bon mode de déploiement : API, Proxy ou Agent ?

Les CASB proposent plusieurs modes d'intégration :

• API : visibilité et contrôle sur les applis SaaS officielles (OneDrive, Teams, Salesforce…).

• Proxy : inspection en temps réel du trafic web et cloud.

• Agent : visibilité sur les terminaux.

Dans le secteur santé :

• Le mode proxy est souvent le plus pertinent (contrôle du Shadow IT, protection des postes internes et nomades).

• Le mode API est indispensable pour sécuriser les SaaS institutionnels.

• L'agent est également recommandé, en complémentarité aux devices qui ne peuvent pas héberger un agent (IOT, Serveurs, BYOD)

Impliquer les utilisateurs et communiquer

Un CASB peut être perçu comme un frein si mal expliqué.

Il faut accompagner le changement :

• Expliquer les risques (fuite de données de santé = sanctions, image, responsabilité pénale).

• Montrer les bénéfices pour les soignants : accès sécurisé, simplification des outils.

• Former les équipes IT et métiers.

Astuce : sensibiliser avec des cas concrets d'incidents dans d'autres hôpitaux a souvent plus d'impact que de longs discours.

Mesurer, ajuster, étendre

Le déploiement d'un CASB est un projet itératif :

• Suivez les KPIs : taux d'usages conformes, incidents évités, alertes DLP.

• Ajustez les politiques selon les retours terrain.

• Étendez progressivement à d'autres périmètres (filiales, groupements hospitaliers…).

Point de vigilance : prévoyez une gouvernance adaptée, avec des revues régulières et une collaboration DSI / RSSI / métiers.

Conclusion : ne pas subir le chaos SaaS, mais en faire un accélérateur sécurisé de la transformation hospitalière et de conformité avec la norme ISO 27001

Les RSSI des hôpitaux n'ont plus le choix : il faut reprendre la main sur les usages SaaS, non pas pour bloquer l'innovation, mais pour garantir un cadre sécurisé, conforme et résilient.

Le CASB n'est pas une baguette magique, mais c'est un outil incontournable pour sécuriser les usages cloud dans les établissements de santé. En combinant visibilité, contrôle, conformité et pédagogie, il permet de protéger les données sensibles sans bloquer l'innovation ni la mobilité des soignants.

Le CASB intégré dans une architecture SSE/ SASE est aujourd'hui la voie pragmatique, rapide et mesurable pour y parvenir, en conjuguant sécurité, visibilité et fluidité des usages.

Olfeo

www.olfeo.com

12. LES PROBLÈMES CONNUS

Les chausse-trapes sont légion, mais il faut tout de même s'arrêter sur les principales.

12.1 Confusion entre production documentaire et mise en place d'un SMQ

C'est le grand classique des nouveaux venus : croire que la qualité de son SMSI est proportionnelle au volume documentaire produit. Tout le monde est passé par là, y compris votre serviteur.

Cette lubie est d'ailleurs alimentée par les cabinets de conseil (voir ci-dessous), mais rien n'est plus faux. Un SMSI (hors annexe A) se gère dans son intégralité avec très peu de documents : moins de 15 en tout. Certains sont assez faciles à produire (la Politique de Sécurité de l'Information), d'autres au contraire nécessitent un nombre considérable de révisions pour aboutir à une version « auditable sans paire de baffes » (par exemple le Manuel SMSI). L'appréciation des risques (sur laquelle tout le monde fantasme) peut tenir en 4 onglets d'un tableur, alors que d'autres documents (le plan de formation) sont de véritables nids à problèmes.

Petite liste à la Prévert

En gros, un SMSI exige :

- *une Politique du SI : 1 page max ; c'est la réponse au 5.2 de la norme, à ne pas confondre avec la PSSI qui est la réponse au 5.1 de l'annexe A;*
- *un manuel SMSI ; attention ce document peut être très conséquent, plus que la PSSI d'ailleurs ; on peut mettre en annexe les fiches processus ;*
- *une politique de gestion documentaire (que certains annexent au Manuel SMSI) ;*
- *une appréciation des risques qui embarque la méthode retenue ; cela tient en un fichier tableur avec quelques onglets ; le plus important dans ce fichier, n'en déplaise, ce sont les échelles formalisées de probabilité et d'impact ;*
- *la DDA, bien entendu ;*
- *une PSSI, bien entendu ; il peut y avoir quelques annexes.*
- *les objectifs de sécurité, que certains annexent à l'appréciation des risques ;*
- *le plan de formation / sensibilisation ; peut aussi tenir sur un fichier tableur, attention il y a quelques onglets ;*
- *le dispositif de pilotage des processus ; c'est une nouveauté de la version 2022, certainement que le formalisme va se préciser ;*
- *le plan de contrôle général ;*
- *le plan de la revue de direction (document extrêmement important) ;*
- *le plan pluriannuel d'audit interne ;*
- *le dossier de suivi d'actions (ACT).*

Dès que vous dépassez 15 à 20 documents, posez-vous des questions !

12.2 Le pipeautage des ESN de conseil / accompagnement

Ils devraient être aidant, dans beaucoup (trop ?) de cas ils sont inutiles voire toxiques.

A titre personnel, j'ai rencontré des consultants qui ont tenté de me vendre 400 jours de prestations (vous avez bien lu : 400 jours) pour mettre en place un SMSI, alors que j'estime que 50 jours est le grand maximum, et encore sur un périmètre conséquent.

Cela vient notamment du fait que la plupart ont mis en place un SMSI initial (BUILD) mais n'ont jamais ou peu vu les cycles de renouvellement de certification suivants (RUN) : dit autrement, ces consultants ne savent pas ce qu'est une roue de Deming en mouvement.

12.3 Les auditeurs de certification

Ils ont tous leur marotte. Pour certains, c'est la gestion documentaire, pour d'autres l'analyse de la cause des anomalies, pour d'autres enfin l'audit interne. Dans des cas heureusement assez rares, on peut tomber sur des auditeurs qui surinterprètent la norme et collent des non-conformités majeures absolument non justifiées : le grand classique c'est une appréciation des risques faite sans recourir à la méthode EBIOS (la norme ne le demande pas et rien dans le chapitre 6 ne peut être interprété, de près ou de loin, en faveur d'une obligation d'EBIOS).

Quand vous tombez sur un désaccord entre l'auditeur et vous, il n'y a qu'une seule façon de le résoudre :

• soit « c'est écrit » dans la norme et sans aucune marge d'interprétation possible, dans ce cas l'auditeur a raison, point barre (et cela arrive souvent) ;

• soit il s'agit d'une divergence d'interprétation, celle de l'auditeur se valant autant que la vôtre, dans ce cas aucune non-conformité (même mineure) ne doit être mentionnée ; pas mal de points de la norme sont dans ce cas, en toute honnêteté ;

• soit enfin vous tombez sur un fou furieux qui veut imposer une interprétation de la norme sans aucun fondement, et dans ce cas il faut récuser l'auditeur, lui indiquer la porte, et prévenir l'organisme de certification que cette personne est non grata chez vous ; en général dites-vous que si vous avez des problèmes avec cet auditeur, vous n'êtes pas le seul et vous rendez service à tout le monde.

12.4 Points d'attention sur quelques parties de la norme

Certaines parties de la norme focalisent une énergie selon nous disproportionnée par rapport à l'enjeu réel : c'est le cas de l'appréciation des risques et de la PSSI, incroyable le nombre d'heures qui auront été passées là-dessus !

Par contre, curieusement, le manuel du SMSI (que certains appellent la politique du SMSI, à ne pas confondre avec la PSSI ni avec la PSI) est très compliqué à rédiger, nécessite un nombre élevé de revues, corrections, relectures. C'est par exemple dans ce document que j'écris en toutes lettres l'interprétation que je fais de certaines parties de la norme justement sujettes à interprétation - au moins cela annonce la couleur.

Autre piège : les risques et opportunités du SMSI lui-même. On est dans le grand classique d'un SMQ qui oblige à se regarder régulièrement son propre nombril, et souvent les SMSI sont plus que légers sur le sujet - sans parler de la revue de cette partie, qui est souvent absente. Un point d'ailleurs à ne pas oublier dans le manuel du SMSI ni dans le plan de la revue de direction.

La politique de gestion documentaire est en général bien adressée (non il n'est pas obligatoire de mettre ses documents dans une GED !), en revanche côté plan de formation avec évaluation des besoins et analyse de l'efficacité des formations, c'est souvent assez léger.

Piège suivant : le contrôle des processus (§ 8.1) et la surveillance des processus (§ 9.1), pour lequel pas mal d'interprétations diverses sont rencontrées. Mon conseil : préciser l'interprétation dans le Manuel du SMSI, et s'y tenir avec des méthodes simples tel le relevé trimestriel d'indicateurs de performance.

Pour la revue de direction, mon conseil : rédiger le plan le plus détaillé possible, déroulez ce plan en revue de direction, et mettez à jour le plan pour les prochaines revues en fonction des anomalies rencontrées et remontées par les audits.

Enfin pour ce qui concerne l'amélioration continue (§ 10), ne surtout pas oublier de renseigner une analyse de la cause pour chaque anomalie listée.

13. L'AVENIR

13.1 Une obligation pour toutes les DSI

La certification va dans le sens de l'Histoire, tout métier confondu. On parle de DORA, de Certification des comptes, de NIS, mais au final on retrouve toujours le même raisonnement : se conformer à des bonnes pratiques éprouvées, se faire auditer par un tiers, améliorer constamment le dispositif.

Les DSI ne peuvent plus être à la fois une fonction support critique dans un établissement de santé, et échapper à toute forme de certification. Ce qui est étonnant avec NIS 1 et NIS 2, c'est surtout que cela ne soit pas arrivé plus tôt.

En ce sens, la 27001 permet de factoriser pas mal de points techniques (l'annexe A) ou processus (le SMSI) et ne faire le boulot qu'une seule fois. Se faire certifier, c'est juste ne pas se faire « rattraper par la patrouille ».

13.2 Les autres normes ou bonnes pratiques en lien avec la 27001

Pour « vendre » la certification à une Direction Générale, on peut utiliser l'argument - réel - de la « factorisation » des démarches, au sens où ce qui est fait pour la 27001 sert pour d'autres normes ou obligations réglementaires.

13.2.1 Les autres obligations normatives dans un établissements de santé

On parle de l'ISO 15189 pour les laboratoires, et des équivalents pour l'oncologie et d'autres secteurs : la 27001 permet de régler toutes les questions informatiques de ces normes en une seule fois.

13.2.2 La certification des comptes

La partie concernant la gestion et le cycle de vie des identités, le PCA-PRA, la gestion des comptes à pouvoir (comptes admin techniques ou fonctionnels) est incluse dans la 27001.

13.2.3 NIS 1, NIS 2

Les 23 mesures de NIS 1 sont totalement calquées sur la 27001, avec certes une numérotation différente. Idem pour NIS 2.

13.2.4 Les assurances cyber

Les questionnaires des assureurs cyber se calquent de plus en plus sur la 27001, pour une raison simple : cela leur évite de réinventer un référentiel, ce qui est coûteux à maintenir.

13.2.5 Le RGPD

La certification correspondant au RGPD (27701) est une surcouche de la 27001 : il faut être 27001 d'abord pour être 27701.

LA RÉSILIENCE ET LA CYBER

Par Yves Normand, Consultant, Formateur et auditeur en sécurité de l'information ; Auditeur de certification ISO27001, ISO27701 et HDS pour l'AFNOR

Approche métier : Point de vue d'Yves Normand

Que signifie le terme de résilience, selon le contexte ? La résilience est la capacité d'un écosystème à se rétablir après une perturbation extérieure, comme un incendie ou une tempête, par exemples, et avec des conséquences immédiates et importantes sur l'équilibre existant. Les êtres humains ont, aussi, une capacité à surmonter un évènement important et à vivre de manière satisfaisante en dépit de circonstances traumatiques ; mais des conséquences risquent de subsister.

La résilience pour une organisation publique ou privée, une entreprise, est sa capacité à maintenir ses activités essentielles en cas d'incident et à continuer à fonctionner dans un état acceptable.

La résilience pour un système d'information, qui est au service d'activités d'une organisation, est sa capacité à continuer à fonctionner en cas d'incident (ex. sinistre physique, cyberattaque,…) et sa capacité à revenir dans un état normal, dit normal, ou acceptable par l'organisme.

La compréhension de la résilience dans son organisation est essentielle, afin de mettre en œuvre des mesures, adpatées, qui vont permettre de maintenir et de remettre en fonctionnement des activités, à la suite d'un incident ayant des conséquences importantes.

Pour cela, nous pouvons débattre sur la définition des plans (PCA, PRA, PCI, PCO,…) à mettre en œuvre. Chaque expert, comme souvent, détient la vérité.

L'important est sans doute de comprendre d'abord ce qui est essentiel pour une organisation. Dit autrement : c'est quoi le minimum vitale pour que mon organisation puisse continuer à exister, et à rendre des services de base, en lien avec sa raison d'être. Les normes, les guides, les recommandations en la matière sont là pour apporter une aide méthodologique et aider à déterminer ce qui est essentiel à maintenir.

Réaliser des exercices de cybercrise, sans comprendre quoi en tirer pour améliorer ses pratiques en interne, et juste cocher la bonne case pour toucher de l'argent, et avoir l'indicateur de certification au vert : Et bien, cela ne fait pas beaucoup avancer le niveau de maturité en maîtrise de l'information de son organisation.

Dans le cadre d'un système d'information en santé, un objectif (simple à exprimer) est d'accéder, rapidement, aux informations médicales d'un patient pour sa prise en charge. En termes de critères de sécurité, l'accessibilité se traduit par l'intégrité et la disponibilité de l'information. Dit autrement, il s'agit de fournir la bonne information et au bon moment. Le respect de la confidentialité est un autre sujet : fournir l'information à la bonne personne.

La maîtrise de l'information, portée par le système d'information, est possible par

une démarche permanente d'amélioration continue et de management des risques. Des fondamentaux sont à considérer, dont une très bonne connaissance :

• Des processus métiers et des activités, dites essentielles, de l'organisation,

• Du patrimoine informationnel

• De l'efficacité des mesures actuelles (managérialles, organisationnelles et techniques)

• De l'interaction de l'environnement interne avec les environnements externes

• Des évènements, avec des origines internes ou externes à l'organisation, qui pourraient pertuber l'équilibre de fonctionnement des activités métiers

• Des capacités en interne pour renforcer la maturité en matière de résilience, et de réaction face à un incident.

La décision de mettre en place des plans particuliers (PCA, PRA, PCO, procédures dégradées,…) doit être la conséquence d'une statégie de l'organisation pour maintenir des activités, considérées comme essentielles. Et cette stratégie pourrait affirmer que certaines activités ferment, temporairement, en cas d'incident ayant des impacts importants, car l'activité n'est pas essentielle ou bien, parce que l'organisation n'a pas de solutions pour maintenir cette activité.

La formalisation de la stratégie est essentielle pour comprendre ce qui doit être réalisé. Cela permet de donner du sens aux décisions, et donc aux mesures mises en place.

Faire de la sensibilisation, par exemple, s'il n'y a pas de lien avec un objectif de sécurité, aligné avec la stratégie de l'organisation : Cela ne sert pas à grand-chose. Bon, en fait, cela sert toujours, mais l'efficacité de la mesure de sensibilisation restera limitée, par rapport aux moyens dépensés.

De la sérennité, du bon sens et l'intérêt général de l'organisation sont des critères de base, du quotidien, afin de répondre aux missions essentielles de prise en charge des patients.

Alors maintenant, si on parle un peu de méthode.

L'idée est de mettre en œuvre un système qui gère la résilience du système d'information. C'est le but d'un système de management de la continuité d'activité (SMCA). Les objectifs d'un SMCA sont de :

• Maintenir les activités essentielles de l'organisation à la suite d'un incident perturbant gravement le fonctionnement normal.

• Et améliorer les mesures de sécurité pour :

    • Renforcer l'efficacité actuelles des mesures,

    • Détecter au plutôt un incident,

    • Réagir rapidement et limiter les conséquences négatives

    • Et donc :

        • Se protéger contre les perturbations,

        • Réduire la vraisemblance de leur survenance,

        • Se préparer et répondre en cas de survenance de perturbations

        • Renforcer les pratiques et les mesures actuelles pour éviter

des incidents, et être préparés pour gérer la survenue d'un incident.

La norme ISO 22301 précise comment mettre en œuvre un SMCA. Ici, nous ne cherchons pas l'obtention d'une certification, mais de considérer une méthodologie reconnue.

La démarche vise aussi à considérer les bénéfices du SMCA selon différents points de vue : activités métiers, finances, parties intéressées, processus internes,… C'est clairement un principe fondamental d'une démarche d'un système de management, à savoir : c'est quoi les bénéfices pour notre organisation ? Dit autrement, en quoi un système de management peut-il aider le fonctionnement de mon organisation.

Un conseil à retenir est d'être sur une démarche de type Système de management, ici un SMCA, dans la lignée d'un système de management de la sécurité de l'information (SMSI, selon la norme ISO 27001). C'est beaucoup de bon sens. Associé à ce principe fondamental, il sera nécessaire de considérer également des guides, des bonnes pratiques, développés pour le système d'information en santé, dont les éléments proposés par l'ANS. Le guide de la Continuité d'activité du SGDSN est également un excellent guide ; ou celui de l'AFNOR. D'autres guides sont édités aussi par des associations, et des concepts pour renforcer les architectures d'infrastructure sont bien entendus à prendre en compte. Une confiance dans le socle technique est nécessaire.

Ces éléments constituent une boîte à outils. A chacun de prendre décision, en toute conscience, de ce qui lui convient, en tenant compte des métiers d'une DSI et des attentes des métiers de l'organisation. Nous retrouvons bien entendu les thématiques habituelles en sécurité de l'information. Les termes de cybersécurité ou de cyberésilience n'ont rien apporté de novateur, sauf pour le marketing.

Objectivement, la mise en place d'un système de management (SMCA, SMSI) est totalement possible pour une organisation en santé. C'est une démarche vertueuse d'amélioration continue de la sécurité de l'information, en s'intégrant avec les processus métier de l'établissement. Cela permet de répondre aussi à des exigences réglementaires (HAS, Certification des Comptes, CaRE, NIS2,…).

Cela peut nécessiter une phase importante de changements, tant aux niveaux organisationnels, des pratiques ou techniques, avec peut-être des remises en cause de pratiques dans la DSI ou des Services métiers.

L'entraînement face à des crises, ou des incidents avec des conséquences graves, est nécessaire. C'est une certitude. Et à condition, d'avoir un système solide et qui soit perpétuellement en évolution, afin d'élever le niveau de maturité en sécurité de l'information.

La conduite du changement est à considérer nécessairement. L'humain est, et doit être un maillon fort, avec une cohésion forte des équipes. Gardez à l'esprit ce qui est essentiel dans cette activité de cyber-résilience. Chacun pourra méditer sur ce point !

14. QUELQUES CONSEILS PLUTÔT UTILES

Conseil 1 : Une certification ISO n'a pas pour objectif d'obtenir un bout de papier, mais de faire progresser la maturité de l'organisation. La faire réaliser en majorité par des consultants externes est un non-sens absolu.



Conseil 2 : Le meilleur service que pourra vous rendre le consultant qui ne vous alerte pas sur le conseil 1 est de prendre la porte.

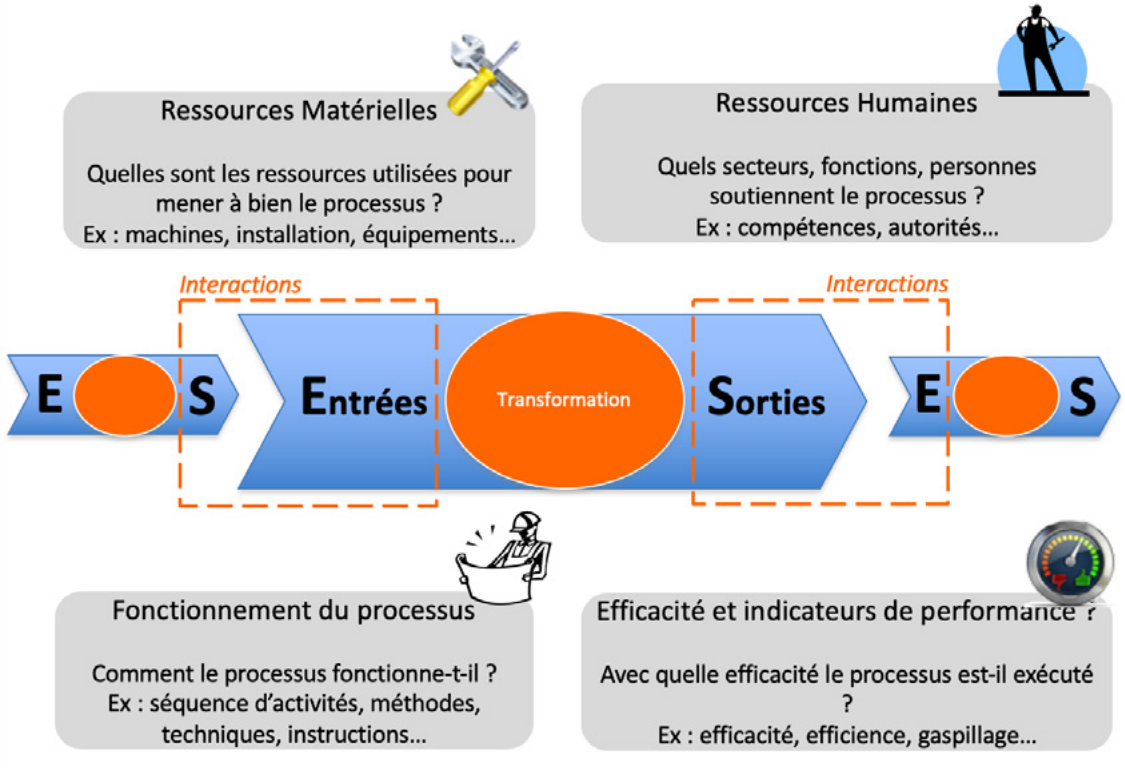
Conseil 3 : La mesure de la maturité organisationnelle est souvent inversement proportionnelle à la quantité de documentation pondue.

Conseil 4 : Quand on est certifié, on a du mal à comprendre comment on faisait pour travailler avant sans le cadre formel et protecteur de la norme.

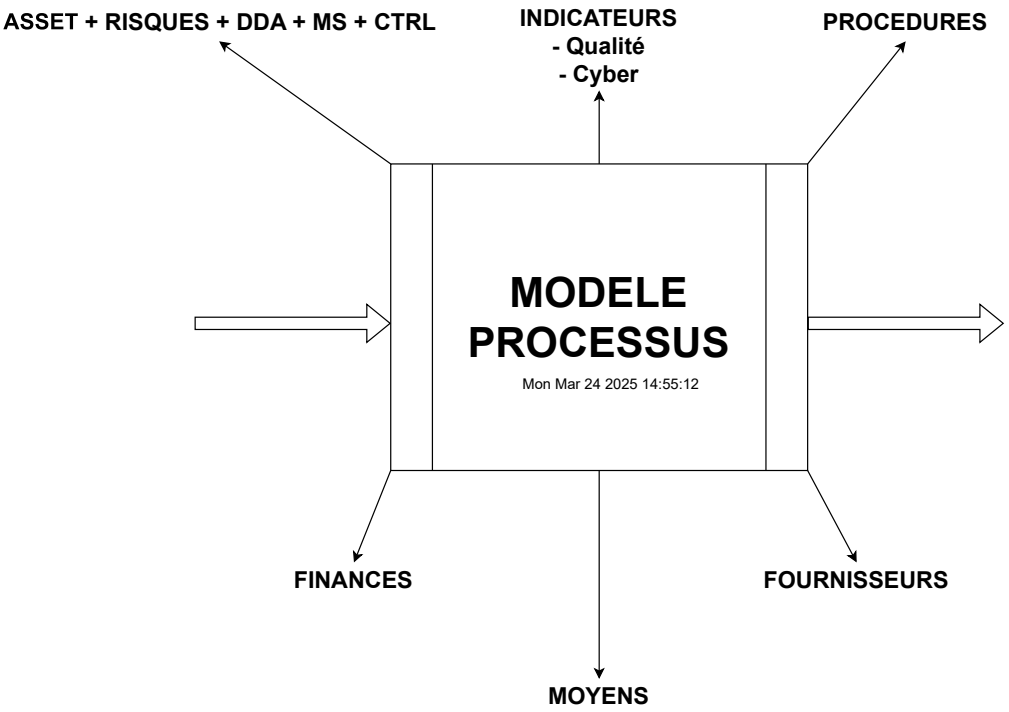
Conseil 5 : Si vous constatez une inflation non maîtrisée du volume documentaire produit, cela doit vous alerter car un SMSI ne réclame justement que peu de documents, comme évoqué à plusieurs reprises.

15. ANNEXES

Le modèle de la Tortue de Crosby



Un dérivé du modèle de Crosby



16. RESSOURCES

16.1 Bibliographie

« La sécurité du système d'information des établissements de santé »

Cédric CARTAU, Presses de l'EHESP, 2ème édition

« Management de la sécurité de l'information »

Alexandre FERNANDEZ-TORO, Eyrolles

Cet ouvrage est longtemps resté LA référence sur le sujet. Il a un peu vieilli car il adresse la version 2013 de la norme, mais pas mal de ses chapitres restent totalement d'actualité.

Les Guides de cyber résiliences publiés à l'APSSIS

https://apssis.com/nos-actions/publications

16.2 Sites Web

www.dsih.fr

La référence des revues sectorielles dédiée aux SI en santé

https://www.club-27001.fr : le site du Club 27001 français.

Il existe des clubs régionaux affiliés au club national.

17. ARTICLES

17.1 Article DSIH, février 2025 : Pourquoi 27001 et NIS ne disparaîtront jamais

Dans les dîners en villes (enfin, ceux des RSSI), le sujet hype c'est NIS 2.

Y être ou ne pas y être, combien ça va coûter, ceux (les boites) qui vont être concernés, ce (le périmètre) que cela va concerner, le temps laissé à tout ce beau monde pour se mettre d'équerre (des années), etc.

Etonnamment, on n'a pas (trop) entendu la rengaine habituelle de la multiplication des normes et des obligations réglementaires, on n'a pas (encore) entendu les chouineurs de services qui pestent contre l'inflation normative, preuve s'il en est que nous n'en sommes qu'au début de l'avant-premier round.

Alors j'anticipe : va-t-on - enfin - assister à une simplification normative dans la cyber ? Par période ou vague on assiste en effet à des poussées de fièvre, la dernière dans le secteur date d'il y a environ 5 années (en tout cas dans la santé) quand on a vu arriver en peu de temps l'instruction 309, la certification HDS (anciennement agrément), les obligations de déclaration des incidents, etc. Là en peu de temps on se prend quand même dans la figure HDS v2, NIS 2, ISO 27001 version 2022, un début d'alignement du RGPD sur les normes ISO, et j'en oublie certainement. Dans le grand public quand on évoque le thème de la simplification, on pense surtout à l'uniformisation des taux de TVA, des boulons de calibre 12 et des 2893 règles permettant de calculer son impôt après les 154 cas d'exonération et les 18 formulaires CERFA, mais jamais de la cyber.

Alors, cela va-t-il un jour se simplifier ?

Allez je vous spoile : la réponse est non. Plus précisément, la réponse est : « non, et même certainement jamais ». Et ceci pour trois raisons, une endogène et deux exogènes.

La première raison c'est que la complexité de la cyber n'est pas intrinsèque ni une cause, elle est le reflet ou la conséquence de la complexité de l'IT en général, des SI en particulier et encore plus de la complexité des SI de santé. Juste pour rire deux minutes, lors du prochain pince-fesses à petits fours, quand vous causez avec un DSI d'un autre secteur (banque, agroalimentaire, telco, etc.), faites-lui remarquer que lui connaît ses clients en face-à-face. Alors que dans la santé, le client (patient), dès fois il arrive sur ses deux jambes et peut dire qui il est, dès fois non (coma), dès fois il ne le pourra plus (il est mort), des fois on a même du mal à savoir quelle tête il avait avant de mourir (corps repêché dans le fleuve 3 semaines après), dès fois on a qu'on bout du client (organe). Va te faire de l'identito-vigilance avec ça mon petit père ! (d'expérience après le coup du repêché dans le fleuve votre interlocuteur y va mollo sur les petits fours).

La deuxième raison, c'est que le schéma est toujours le même : un secteur commence à faire face à des soucis de nature diverses, qui deviennent des bonnes pratiques documentées, puis des normes, puis une loi et son chapelet de décrets (d'aucun prédisent d'ailleurs la fin de 27001 avec l'arrivée de NIS 2 même si je n'y crois pas trop). Or, dès que

l'on franchit le stade de la norme, ne pas la respecter fait courir des risques juridiques non nuls : on voit cela dans le domaine de l'environnement, le premier DSI hospitalier qui se retrouvera devant un juge à la suite de la mort d'un patient consécutif à une panne informatique aura intérêt à bien être certifié 27001.

La troisième raison est plus terre à terre : c'est que les normes, cela fait vivre un paquet de gens. Ceux qui les écrivent, ceux qui forment les auditeurs et les auditeurs des auditeurs, les auditeurs eux-mêmes, les consultants qui vous expliquent comment les appliquer, les consultants vous permettant de valider le conseil des consultants, etc. YYuval Noah Harari explique, dans son dernier ouvrage « Nexus », que si le corpus documentaire de la religion juive est aussi fourni, c'est parce que la Torah a été interprétée par des « sages » qui ont couché par écrit leurs interprétations (la Mishna), mais qu'ensuite il a fallu interpréter ces interprétations (le Talmud), et ainsi de suite[3]. Quelquefois dans l'écosystème du conseil en IT j'ai un peu cette même impression : des textes, des gens pour vous aider à les comprendre, d'autres pour vous aider à les appliquer, d'autres pour contrôler, et c'est sans fin - d'ailleurs j'en fais partie.

A ce stade votre meilleur pote c'est un bon logiciel de Mind Mapping et un tableur (il en existe d'excellents en version gratuite) : je vais encore me faire des potos, mais quand on voit l'inflation et les évolutions normatives, y'a intérêt à utiliser des outils simples pour cartographier les idées et les concepts, car tout schéma mental devient vite obsolète.

De rien.

17.2 Article DSIH, février 2025 : Match 27001 versus RSSI : 1 à 0

L'autre jour je tombe sur un problème de fond, le genre métaphysico-sinusoïdal de classe alpha plus[4] avec lequel j'adore me triturer les neurones : le mécanisme d'alerte du RSSI auprès de la Direction sur les dysfonctionnements structurels graves dans le SMSI. Bon pas de panique je vais traduire.

J'appelle un ami - un confrère - et lui pose la question suivante : « Brad, dis-moi un truc, comment fait-on quand on pilote un SMSI pour dire à l'Organisation que, en gros, ils travaillent comme des goré-gougnafiers et qu'en gros ils vont se vautrer grave à la prochaine visite de certification et que ce sera bien fait pour leur grouin ? ».

Là, Brad me rétorque qu'il ne faut pas parler comme ça et qu'il faut être un minimum diplomate dans ce genre de situation. Bon je reformule : comment dire à l'Organisation qu'il y a de graves dysfonctionnements dans leurs processus de travail, qui mettent potentiellement en jeu le fonctionnement même du SMSI et que la perte de la certification les guette. Et que ce sera bien fait pour leur grouin.

Si vous allez décortiquer le chapitre 9.3 de la norme sur la revue de direction (seul point de contact institutionnalisé entre le RSSI et l'Organisation), nulle mention de cette possibilité. Certes le 9.3.1 (Généralités)

3 Si j'ai bien compris

4 Oui je sais cela ne veut rien dire, c'est juste pour faire genre

est assez vague et on peut y coller pas mal d'items, mais dans le 9.3.2 nada, bernique et peau de balle. En plus d'appeler Brad j'ai aussi appelé George (qui m'a donné peu ou prou la même réponse), et la solution n'est pas si triviale. En fait il y a trois solutions, par ordre croissant de pertinence.

Solution 1 : le 9.3 décrit le minimum syndical de ce que doit comprendre une revue de direction, rien n'empêche de rajouter des éléments additionnels, tel que le point objet du présent filet. Mouais, ça marche mais je n'aime pas trop, intervenir sur le code source pour faire un fork j'ai donné dans ma précédente vie de développeur, on finit par se le prendre dans la face un jour ou l'autre.

Solution 2 : utiliser l'audit interne, et faire remonter ce point pour qu'il apparaisse dans le rapport d'audit interne, qui sera (comme c'est pratique) un entrant de la revue de direction. J'aime mieux, les points de passage obligés de l'audit interne peuvent faire rentrer cela sans difficulté (9.2.1 b et 9.2.2.a pour les intimes, je vous laisse vérifier).

Solution 3 (que je pensais inadéquate au départ, mais qui au final est la meilleure, et qui implique un léger changement de paradigme, vous allez voir) : la revue de direction impose d'examiner le retour des parties intéressées (PI). Or, ma remarque de départ (vous bossez comme des tanches) est celle d'un RSSI : il suffit donc de considérer le RSSI comme une PI. Conséquence directe : la séparation entre le RSSI (Responsable Sécurité Système d'Information) et le RSMSI (le responsable du fonctionnement du SMSI), et le fait que le RSMSI comptabilise le RSSI dans la liste des PI.

Alors je sais, je sais, vous allez me sortir les arguments habituels : on coupe les cheveux en quinze, on a déjà du mal à avoir un RSSI si en plus il faut un RSMSI, et en plus c'est souvent la même personne, et blablabla et blablabla. Mais là n'est pas le plus important. Le plus important, c'est que :

• les rôles RSSI / RSMSI sont bien distincts ; la 27001 le découvre juste, la 9001 le sait depuis des lustres ;

• un SMSI, ce n'est pas de la cyber : c'est un système de management, la distinction des deux rôles le démontre bien ;

• un argument de plus (s'il en fallait encore un) pour bien dire que le RSSI ne peut pas être dans la DSI (sinon il ne pourrait pas être une PI à lui tout seul).

Mais ce qui m'a le plus impressionné dans cette réflexion, c'est la souplesse et la solidité de la norme : incroyable qu'un document aussi court (11 pages hors annexes) puisse à la fois faire face aux situations les plus simples comme les plus complexes. Normal, il ne faut tout de même pas oublier qu'elle est le résultat de milliers d'heures de jus de cerveau, depuis plus de 20 ans, par des centaines de personnes. On ne va tout de même pas la prendre en défaut aussi facilement.

De rien.

18.1 Article InCyber : Les visions comparées de la 27001

https://incyber.org/article/visions-comparees-iso-27001/

Mickaël Ferton (Digitémis) et moi-même avons lancé une instance locale nantaise du club ISO 27001, et lors d'une des dernières réunions une table ronde s'est tenue sur un thème absolument passionnant : quelle vision de la 27001 par trois acteurs totalement différents, un auditeur très expérimenté, un RSSI dont l'organisation est certifiée depuis plus de 5 ans et un RSSI récemment certifié. Et les échanges avec la salle ont montré que ce n'était pas seulement trois versions de l'histoire que l'on pouvait raconter à une Direction Générale, mais plus.

La question peut sembler triviale mais ne l'est pas : comment expliqueriez-vous une démarche ISO 27001 à une Direction Générale qui, à priori n'y connaît rien et n'est pas experte en démarche qualité ? En effet, avant de convaincre une DG de signer un chèque substantiel (entre les coûts financiers direct et la charge RH on arrive vite à un devis à 6 chiffres), encore faut-il la convaincre de ce que cela apporte, de ce que cela implique et accessoirement du risque à ne pas faire. Allons directement à la conclusion : la vision de la 27001 reflète très exactement la maturité de votre interlocuteur - et la votre.

Quand on débute sur le sujet, la première vison que l'on en a est celle de la production documentaire : être certifié c'est maintenir une pile de procédures, de mode opératoires, de politiques. Vision par ailleurs alimentée par pas mal de discours de consultants dont certains ont pour objectif de forcer le devis - plus il faut produire, plus c'est long et plus il faut de monde.

Vient ensuite la vision réglementaire ou business. Être certifié c'est avoir un avantage concurrentiel dans les appels d'offre, sorte de sélection naturelle des prestataires qui auront réussi à obtenir le précieux certificat. Côté clients et grands comptes, c'est à l'avenant car il s'agit d'anticiper une obligation normative qui ne manquera pas d'arriver, voire de répondre plus facilement à des obligations normatives réelles. Par exemple être 27001 permet de cocher plus de 80 % des obligations de la directive NIS à périmètre constant.

Puis c'est la vision conformité, dans le sens du respect des bonnes pratiques. Les mesures techniques à mettre en place préconisées par la 27002 constituent un guide, au même titre que les mesures d'hygiène de l'ANSSI, ou la bibliothèque ITIL, etc. Cette vision est utile vis-à-vis d'une DSI (ne pas réinventer la roue), moins avec une DG. Par contre elle confère un avantage certain au RSSI qui la met en place : une fois obtenue, la certification (que personne ne veut perdre) devient dans certains cas contraignante (dans le bon sens du terme) : il faut faire ceci (ou ne pas faire cela) car c'est une obligation de la norme.

Ensuite c'est la vision traçabilité, extension de celle des bonnes pratiques. Dans un système de management de la qualité (SMQ, dont la 27001 est une déclinaison), tout est tracé, imputable et surtout on peut facilement trouver l'action à l'origine d'une erreur, voire attribuer des taches de remédiation à chaque propriétaire d'actif et tracer ces remédiations. Dans les faits, la traçabilité doit être vue comme un bénéfice collatéral d'une certification 27001 plutôt que sa finalité, mais c'est par contre un très

bon axe d'explication après d'une DSI.

Inévitablement, au bout d'un certain temps on comprend que la 27001 est faite pour gérer des risques. Cela paraît une tautologie, mais ce n'est pas si trivial. En effet on ne traite pas seulement des risques opérationnels directement lié au SI, mais aussi des risques indirects de fonctionnement de l'ISO 27001 à proprement parler - sorte de méta risques.

Enfin c'est la vision système de management qui arrive à ce stade. Il faut un bon moment pour comprendre véritablement ce qu'est un SMQ - 3 ans au bas mot et je n'exagère pas - et surtout diffuser cette compréhension auprès de tous les acteurs du périmètre. Ma définition - et qui n'engage que moi - est : macro-processus fractal auto-apprenant et auto-nettoyant. Et il me faudrait un tableau blanc et un bon moment pour expliquer chaque terme et le sens général de la phrase. Bon en gros retenez la culture processus.

Le plus fascinant dans la 27001 - et dans tous les SMQ en général - est que la vision que l'on en a évolue constamment. Il est probable que si je réécris ce même article dans 5 ans, je pourrai proposer une vision de plus, ni tout à fait différente des précédentes ni tout à fait identique. Qu'un concept en apparence aussi simple (PDCA, 4 lettres en tout) et aussi concis (le manuel AFNOR tient en 11 pages hors annexes) suscite autant de débats, réactions, divergences d'interprétation, est absolument déroutant.

Dans l'Histoire des SI, c'est très certainement l'une des plus grosses ruptures de paradigme auquel une DSI ait à faire face.

18. ACRONYMES

AFNOR : Association Française de Normalisation

ANS : Agence du Numérique en Santé

ANSSI : Agence Nationale de la Sécurité des Systèmes d'Information

APSSIS : Association Pour la Sécurité des Systèmes d'Information de Santé

CaRE : Cyber Acceleration et Résilience des Etablissements de santé

CERT : Computer Emergency Response Team

CH : Centre Hospitalier

CHU : Centre Hospitalo-Universitaire

CVE : Common Vulnerabilities or Exposers

CPU : Central processing unit

DDA : Déclaration d'Applicabilité

DG : Direction Générale

DORA : Digital Operational Resilience Act

DSI : Direction des Syctèmes d'Information

BIOS : Expression des Besoins et Identification des Objectifs de Sécurité

ESN : Entreprise de Services du Numérique

ETP : Équivalent Temps Plein

GED : Gestion Electronique des Documents

HAS : Haute Autorité de Santé

ISO : Organisation Internationale de Normalisation

IT : Technologie de l'information

ITIL : Information Technology Infrastructure Library

MOA : Maîtrise d'Ouvrage

NIS / NIS2 : Network and Information System Security

OIV : Opérateur d'Importance Vitale

PCA-PRA : Plan de Continuité d'Activité - Plan de Reprise d'Activité

PCO : Plan de Continuité Opérationnelle

PDCA : planifier (Plan), développer ou réaliser (Do), contrôler (Check) et agir ou ajuster (Act).

PI : Parties Intéressées

PMSI : Programme de Médicalisation des Systèmes d'Information

PSSI : Politique de Sécurité des Systèmes d'Information

RGPD : Règlement Général de Protection des Données

RSMSI : Responsable du SMSI

RSSI : Responsable de la Sécurité des Systèmes d'Information

SGDSN : Secrétariat Général de la Défense et de la Sécurité Nationale

SI : Sécurité de l'Information ou Système d'Information

SMCA : Système de Management de la Continuité d'Activité

SMSI : Système de Management de la Sécurité de l'Information

SMQ : Système de Management de la Qualité



APSSIS

Association Pour la Sécurité des SI de Santé

84 rue du Luart
72160 Duneau

06 29 36 59 95

secretaire@apssis.com

www.apssis.com

Licence du document
Auteur : Cédric CARTAU

Ce document est sous licence Creative Commons BY-NC-ND-SA :
- BY : attribution de l'auteur initial
- NC : interdiction de tirer un profit commercial
- ND : impossible d'intégrer le document dans une œuvre composite
- SA : partage de l'œuvre, avec obligation de rediffuser selon la même licence ou une licence similaire (version ultérieure ou localisée)

Création graphique : Corvy-Graphisme