REMERCIEMENTS

Nous souhaitons tout d'abord remercier M. Jean Pierre CALISTE notre tuteur et M. Gilbert FARGES pour leur aide, leurs encouragements et les précieux conseils qu'ils ont pu nous donner.

Nous pensons aussi à M. Stéphane PIERREFITTE, M. Gery MOLLET, M. Julien ROUSSELLE et Mme Agnès LIEDORP pour leurs réponses et les connaissances sur la sécurité des systèmes d'informations dans le milieu hospitalier qu'ils ont pu nous procurer. Votre aide nous a été d'une grande utilité.

Nous remercions aussi chaleureusement toute la promotion du Master Qualité pour avoir suivi notre projet pas à pas et nous avoir fait part de leurs remarques au cours des différents oraux.

SOMMAIRE

TABLE DES ILLUSTRATIONS

GLOSSAIRE

GMSIH : Groupement pour la Modernisation des Systèmes d'Information Hospitalier

HAS : Haute Autorité de Santé

ISO : International Standard Organisation (Organisation International de normalisation)

MQ : Management de la Qualité

OCDE : Organisation de Coopération de Développement Economique.

PDS : Planification Dynamique Stratégique

PHP : Hypertext Preprocessor

SMSI : Système de Management de la Sécurité d'Information

UTC : Université de Technologie de Compiègne

Introduction

Dans le cadre du projet d'intégration du M2 management de la qualité, nous avons choisi de porter notre attention sur la mise en place d'un outil d'autodiagnostic permettant d'évaluer le niveau de sécurité de l'information selon la norme ISO 27001 [24]. En effet, les systèmes d'informations ayant connu de nombreuses évolutions ces dernières années, il s'est avéré nécessaire d'assurer leur sécurité. Aujourd'hui, le nombre de certifications ISO/IEC 27001 dans le monde s'élève à 6826, tout secteurs confondus avec une forte disparité selon les pays comme nous pouvons le voir dans le document 1 suivant :

Japan	3632	Philippines	15	Macau	3
India	492	Pakistan	14	Portugal	3
China	483	Vietnam	14	Argentina	2
UK	453	Iceland	13	Belgium	2
Taiwan	371	Saudi Arabia	13	Bosnia Herzegovina	2
Germany	139	Netherlands	12	Cyprus	2
Korea	106	Singapore	12	Isle of Man	2
USA	96	Indonesia	11	Kazakhstan	2
Czech Republic	86	Bulgaria	10	Morocco	2
Hungary	71	Kuwait	10	Ukraine	2
Italy	60	Norway	10	Armenia	1
Poland	56	Russian Federation	10	Bangladesh	1
Spain	54	Sweden	9	Belarus	1
Malaysia	40	Colombia	8	Denmark	1
Ireland	37	Bahrain	7	Dominican Republic	1
Thailand	36	Iran	7	Jersey	1
Austria	35	Switzerland	7	Kyrgyzstan	1
Hong Kong	32	Canada	6	Lebanon	1
Greece	30	Croatia	6	Luxembourg	1
Romania	30	South Africa	5	Macedonia	1
Australia	29	Sri Lanka	5	Mauritius	1
Mexico	24	Lithuania	4	Moldova	1
Brazil	23	Oman	4	New Zealand	1
Slovakia	21	Peru	4	Sudan	1
Turkey	21	Qatar	4	Uruguay	1
UAE	20	Chile	3	Yemen	1
France	**19**	Egypt	3		
Slovenia	17	Gibraltar	3	**Total**	**6826**

Figure 2 : Nombres de certifications ISO/IEC 27001 délivrées par pays depuis l'édition de la norme (2005) disponible sur : http://www.iso27001certificates.com/

Parmi les 19 entreprises certifiées à ce jour en France, aucun hôpital n'est présent, la plupart des certifiés étant des sociétés d'infogérance. Le peu de certifications ISO 27001 recensées en France peut s'expliquer de plusieurs façons.

La première est la durée de la préparation à la certification qui dure en général pendant 1an, ce qui peut décourager les entreprises. De plus, il faudra fournir beaucoup d'efforts internes mais aussi obtenir une assistance externe. Notons aussi qu'il existe des normes, l'ISO 13335 et ISO 15408 qui sont des normes relatives aux technologies de l'information, techniques de sécurité et critères d'évaluation pour la sécurité, peut être ces normes sont-elles plus accessibles et plus faciles à mettre en place que l'ISO 27001.

Le secteur hospitalier est un lieu de transit important des informations, qu'elles soient sous format informatique ou papier. Ce domaine impose que les données circulantes soient disponibles, intègres et surtout qu'elles restent confidentielles.
Actuellement, une augmentation de l'utilisation de référentiel GMSIH (Groupement pour la Modernisation des Systèmes d'Information Hospitalier) de +14% a été constaté et un responsable sécurité est clairement identifié dans plus d'un tiers des hôpitaux. Par contre, seulement 7% des hôpitaux disposent d'un tableau de bord sécurité. De plus, d'après une enquête du CLUSIF [11] de juin 2010, 60% des hôpitaux ne font pas d'analyse de risque, 1/3 n'ont aucun contrôle des mots de passe et 31% n'ont pas connaissance que leur système de sécurité de l'information est soumis à une réglementation. En effet, la loi relative à la sécurité des systèmes d'informations [2] préconise le respect de la confidentialité, se traduisant par une charte de respect de la confidentialité, la loi Kouchner du 4 mars 2002 impose le secret professionnel avec une confidentialité des dossiers. Et enfin le référentiel de la Haute Autorité à la Santé [25], précise dans le chapitre 1, partie 2, référence 5 et critère E3 que « le dispositif de sécurité du système d'information est évalué et fait l'objet d'actions d'amélioration ». Le milieu hospitalier, bien que réalisant des efforts dans la gestion de la sécurité des informations, possède encore beaucoup de lacunes.

C'est pourquoi l'outil crée devra être adapté aux hôpitaux, pour qu'ils puissent gagner en efficience dans leur système de management de la sécurité des informations.

Afin de bien comprendre la situation, il est nécessaire de définir les termes suivants, dont la définition suit celle établie par la norme ISO 27001 [12]:

- Sécurité de l'information : protection de la confidentialité, de l'intégrité et de la disponibilité de l'information; en outre, d'autres propriétés, telles que l'authenticité, l'imputabilité, la non-répudiation et la fiabilité, peuvent également être concernées.
- Disponibilité : Propriété d'être accessible et utilisable à la demande par une entité autorisée.
- Confidentialité : Propriété selon laquelle l'information n'est pas rendue accessible ou divulguée à des personnes, entités ou processus non autorisés.
- Intégrité : Propriété de protection de l'exactitude et de l'exhaustivité des actifs.

Dans ce premier chapitre sera présenté le contexte auquel doivent faire face les hôpitaux concernant la sécurité de l'information. Puis, s'en suivra l'explication des enjeux que le projet représente pour le groupe d'une part et pour les centres hospitaliers d'autre part. Enfin en dernière partie de ce chapitre, la problématique du sujet à l'aide d'un diagramme d'Ishikawa. Le deuxième chapitre présentera la méthodologie adoptée pour la réalisation de l'outil et un troisième chapitre avec la réalisation.

1. Contexte

1.1. Situation

Aujourd'hui, les postes informatiques sont de plus en plus nombreux dans les hôpitaux, et ils débordent d'informations confidentielles telles que les dossiers médicaux des patients. La confidentialité des informations que les ordinateurs des hôpitaux contiennent est donc devenue un enjeu stratégique. Cependant, la sécurité de ces données n'est pas encore complètement assurée puisque, d'après l'article de Marie-Françoise DE PANGE, publié le 13 novembre 2009 dans Le Quotidien du Médecin (http://siteinfosecusante.free.fr/spip.php?article34) [7], un virus nommé Conficker a paralysé plusieurs hôpitaux entre janvier et juillet 2009. De plus, ce sont des mauvais choix qui entravent la sécurité des informations puisque, toujours selon cette même source, le service de néphrologie d'un hôpital aurait pris comme identifiant et mot de passe le couple « dialyse-dialyse » afin que le personnel puisse s'en souvenir, mais qui facilitait également l'accès aux hackers.

Le référentiel de la Haute Autorité à la Santé [22], précise dans le chapitre 1, partie 2, référence 5 que « le dispositif de sécurité du système d'information est évalué et fait l'objet d'actions d'amélioration ». La loi relative à la sécurité des systèmes d'informations [23], préconise le respect de la confidentialité, se traduisant par une charte de respect de la confidentialité, et la loi Kouchner du 4 mars 2002 impose le secret professionnel avec une confidentialité des dossiers.

Enfin le plan hôpital 2012, qui a pour but de fournir une aide allant de 5 millions d'Euros à 76,3 millions d'Euros à des centres hospitaliers afin de les moderniser, et notamment en matériel informatique, pourra être l'occasion d'investir du temps de formation dans l'outil d'auto diagnostic que nous allons créer.

Dans ce tableau est présenté les exigences du référentiel de la Haute Autorité à la santé [22] relatives aux systèmes d'informations par rapport aux exigences de la norme ISO 27 799 [17].

Exigences du référentiel de la HAS	Exigences de la norme ISO 27 799
Critère 5.a : Système d'information	Chapitre 5 : Sécurité de l'information
Critère 5.b : Sécurité du système d'information	Chapitre 5.5 Les menaces et les vulnérabilités relatives à la sécurité des informations de santé
Critère 5.c : Gestion documentaire	Chapitre 6.4.8 Jeu de documents du Système de gestion de la sécurité de l'information

Figure 2 : Parallèles des exigences du référentiel de la HAS et de la norme ISO 27 799

1.2. Enjeux

1.2.1. Les enjeux pour le groupe

Concernant le groupe projet, les enjeux sont au nombre de deux. En effet, l'enjeu majeur sera d'être capables de créer un outil d'autodiagnostic simple et efficace à destination des hôpitaux, tout en prenant connaissance du référentiel ISO 27799 [17]. Le second sera de rendre les livrables au bout du temps imparti, c'est-à-dire non seulement l'outil d'autodiagnostic, mais aussi le rapport écrit, et les synthèses lors des jalons.

Afin de clarifier la situation initiale, un QQOQCP a été réalisé dans un premier temps, puis une planification dynamique stratégique, présentés ci-dessous :

Donnée d'entrée : Évaluation de la sécurité de l'information au sein des hôpitaux	
QUI ?	Directs : Hôpitaux Indirects : Groupe projet, M.CALISTE
QUOI ?	Des données importantes et confidentielles peuvent être égarées, ne sont pas protégées ou sont accessibles à tous (dossiers médicaux, …)
OU ?	Dans les hôpitaux
QUAND ?	Chaque fois qu'un dossier confidentiel est créé, consulté, modifié ou stocké dans la base de données de l'hôpital
COMMENT ?	Avec un outil d'auto diagnostic (évolution avant/après)
POURQUOI ?	Pour fiabiliser la confidentialité des documents Pour sécuriser les données Pour assurer la disponibilité des documents
Donnée de sortie : Comment amener les hôpitaux à gagner en efficience dans le management de la sécurité de leur information ?	

Figure 3 : Tableau récapitulatif du QQOQCP

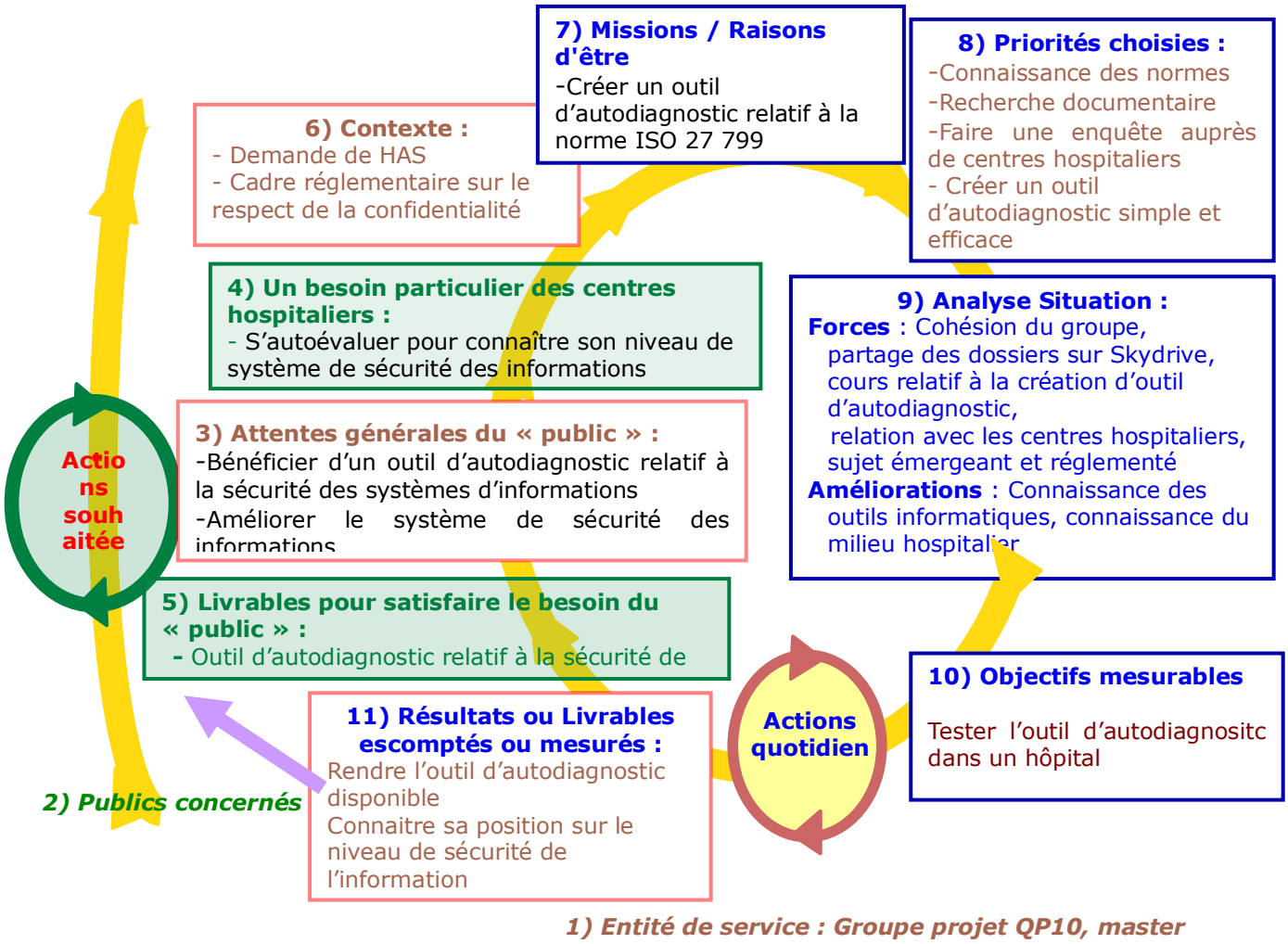


Figure 4 : Planification Dynamique Stratégique

Durant la durée du projet, différentes difficultés pourront apparaître. Des alternatives à ces risques ont été définies à l'aide du diagramme en arbre suivant (au préalable, un brainstorming et un vote pondéré ont été effectués pour identifier et sélectionner les risques et alternatives majeures).

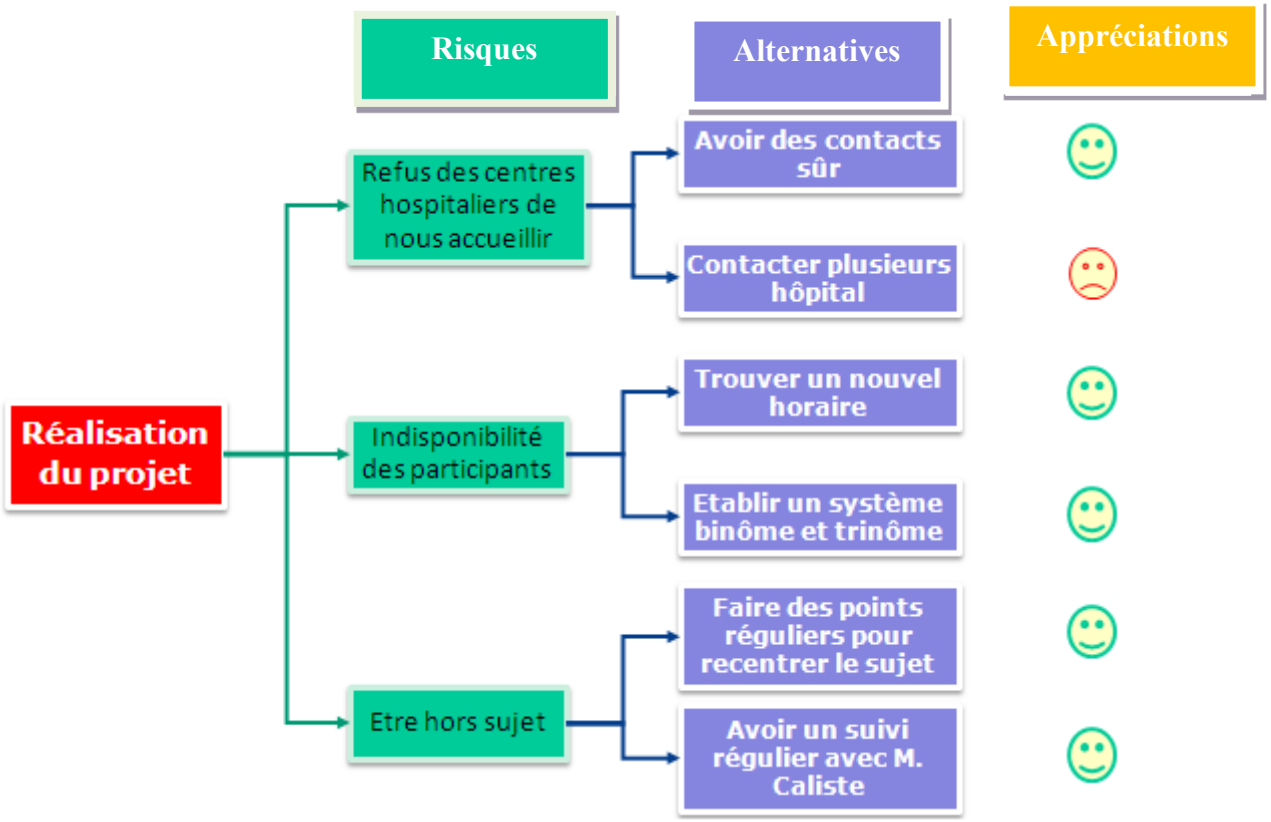


Figure 5 : Diagramme en arbre

1.2.2. Les enjeux pour les centres hospitaliers

Les centres hospitaliers sont confrontés à une demande accrue de consultation de l'information, pourtant, celles-ci ne doivent pas altérer la sécurité des renseignements.

L'enjeu premier de l'outil d'autodiagnostic crée sera de permettre aux hôpitaux d'évaluer facilement et rapidement leur niveau de sécurité de l'information. Une fois ce niveau défini, il leur permettra d'envisager des solutions d'amélioration adaptées et de mesurer leur efficacité en réutilisant cet outil quelques temps après.

Le second enjeu, et non pas le moindre, serait d'aboutir à une certification ISO 27799 , qui permettrait aux centres hospitaliers de devenir une référence en terme de système de gestion de l'information et ainsi améliorer leur image et leur compétitivité.

Finalement, le fait que les informations soient sécurisées, c'est-à-dire disponibles, intègres et confidentielles à 100% ne ferait que renforcer la confiance du patient en l'hôpital.

1.3. Problématique

Dans le but de recenser les problèmes liés à la sécurité de l'information, une enquête dans les établissements de santé a été réalisé. Les résultats sont recensés dans le diagramme Ishikawa ci-dessous :

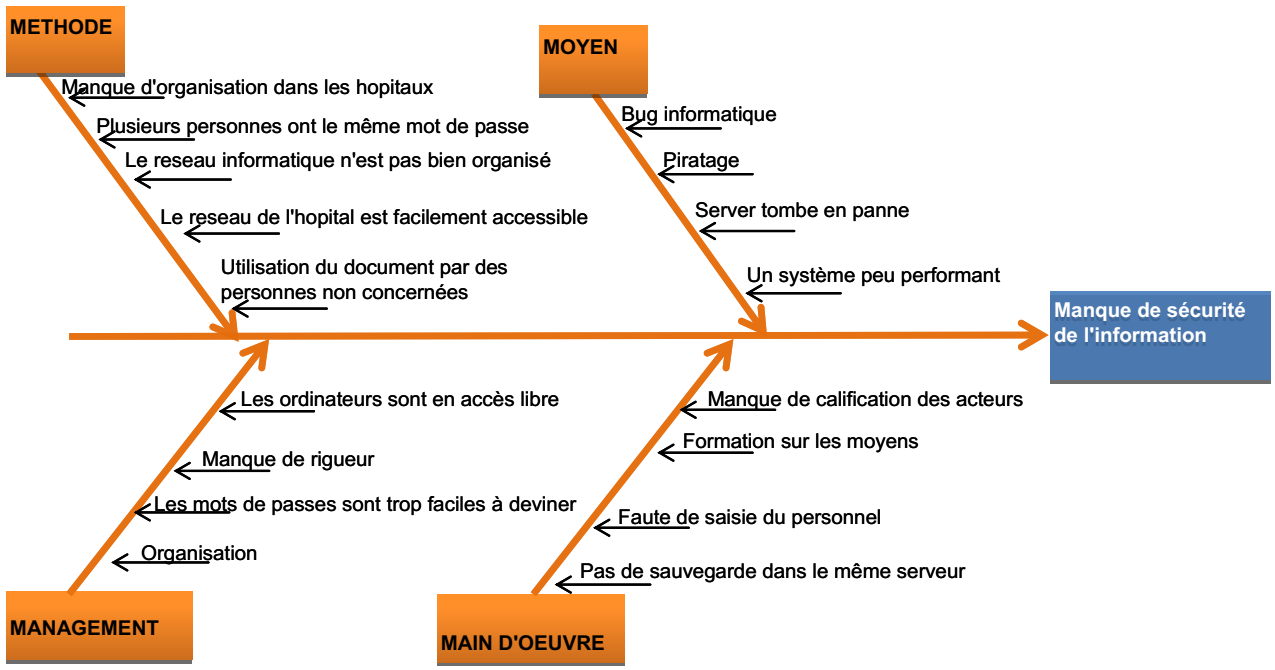


Figure 6 : Diagramme de cause-effet ou diagramme d'Ishikawa

2. Méthodologie

2.1. Communication

2.1.1. Réseau Skydrive

La réalisation de l'outil s'est faite à l'aide d'une plateforme de stockage de documents appelée Skydrive. Celui-ci permet à tous les membres du groupe de créer, de consulter et de modifier tous les documents relatifs aux projets.

2.1.2. Prise de contact

Dans le but d'obtenir des coordonnées de contacts éventuellement intéressés par le projet, une description du projet a été réalisé et envoyée par mail aux différents contacts de M.Farges. Cela nous a permis d'être en contact direct avec des personnes intéressées. De plus, un responsable communication au sein du groupe a été nommé afin de faciliter les échanges externes, et un tableau regroupant les coordonnées de tous les contacts a été établie.

2.1.3. Création d'une grille d'entretien

Ensuite, pour préparer les échanges avec les différents hôpitaux, une grille d'entretien a été construite. (annexe 2). Elle est décomposée en 4 grandes parties :

- Identité de la personne questionnée
- Système de gestion des informations
- Utilisation des informations
- Retour d'expérience

L'objectif est de réalise un état de l'art relatif à la sécurité des systèmes d'informations dans les hôpitaux.

2.2. Mise en œuvre

Après dépouillement des grilles, les informations ont permis d'identifier quelles étaient les causes racines des problèmes de sécurité de l'information (cf. Figure 5). Afin de résoudre les problèmes, plusieurs solutions ont été pensées :

- Créer un outil d'autodiagnostic
- Concevoir un logiciel de surveillance
- Développer des procédures
- Réaliser un audit

Dans le but de déterminer quelle solution sera la plus adaptée, ci dessous est répertorié les avantages et inconvénients de chacun suivant :

Solutions	Avantages	Inconvénients
Création d'un outil d'autodiagnostic	• Simple d'utilisation • Prend en compte toutes les facettes du problème • Peut être créé en version papier et version informatisée	• Prise de temps
Création d'un logiciel de surveillance	• Permet d'éviter le piratage du système informatique	• Connaissances en informatique requises • Ne concerne que les problèmes de type informatique
Développement de procédures	• Peu coûteux	• Non respect par certaines personnes
Réalisation d'un audit	• Création d'un plan d'action	• Prise de temps • Mal perçue dans les établissements

Figure 7 : Tableau comparatif des solutions et inconvénients des solutions proposées

La solution de créer un outil d'autodiagnostic a été retenue.

3. Réalisation

L'outil d'autodiagnostic doit permettre aux hôpitaux d'évaluer leur système de sécurité des informations afin de les amener à gagner en efficience. Le diagramme de décision ci-après a permis de choisir le format de l'outil.

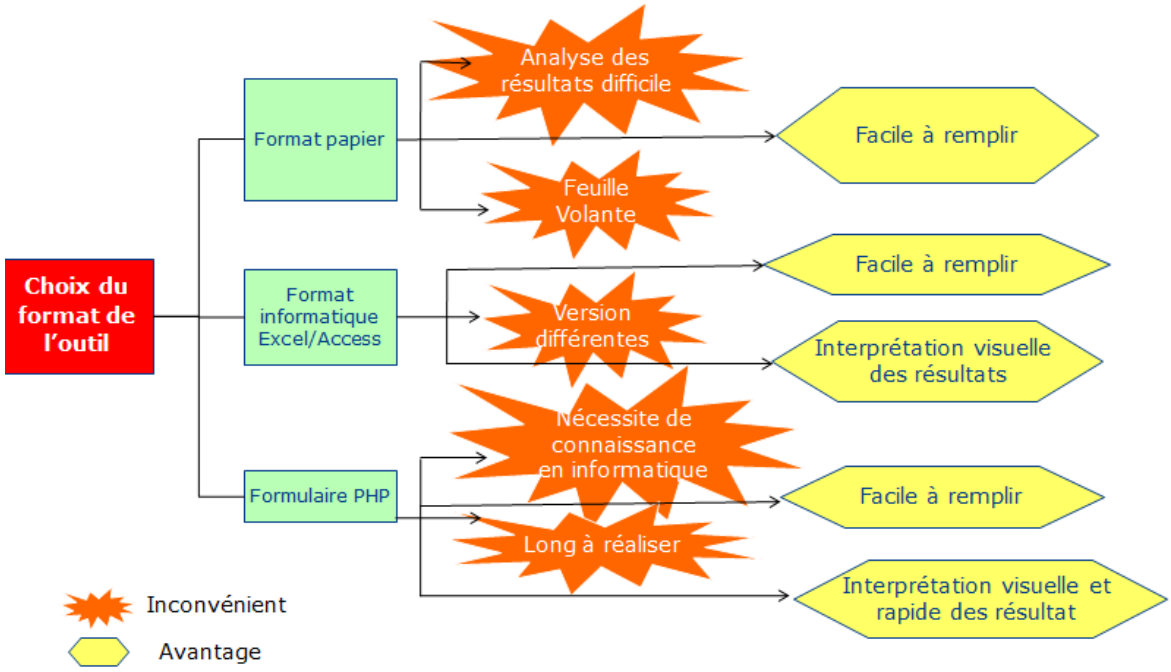


Figure 8 : Choix du format de l'outil

Le format informatique Excel/Access a donc été choisi. La réalisation de l'outil sous forme de formulaire PHP nécessite plus de temps en réalisation donc ce support ne sera pas sélectionné.

3.1. Création de l'outil

Après analyse de la norme ISO 27 799, trois grands thèmes ont été identifiés :

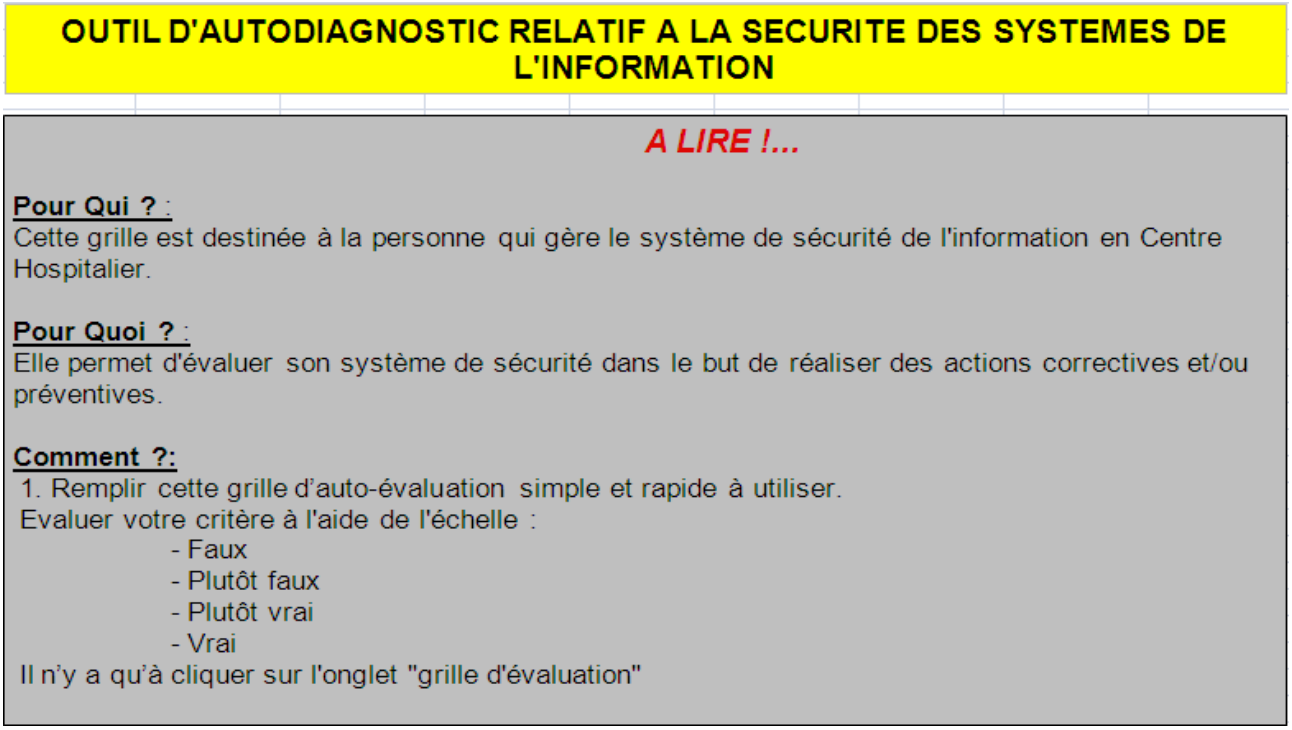
- Amélioration continue,
- Gestion de la documentation,
- Gestion des risques.

L'ensemble de ces thèmes comprend 55 exigences, convenances comprises. L'échelle de véracité suivante a été choisie :

- Faux : L'action n'est jamais réalisée
- Plutôt faux : L'action est peu souvent réalisée
- Plutôt vrai : L'action est aléatoirement réalisée
- Vrai : L'action est réalisée, des documents le prouvent.

Le choix d'utiliser cette échelle s'explique du fait que l'outil peut être destiné à des non-initiés n'ayant pas toujours de culture qualité. En effet, une échelle à 6 cotations nécessiterait d'utiliser du

vocabulaire plus spécifique à la qualité. Enfin, l'échelle ayant une médiane n'a pas été sélectionnée car l'utilisateur de la grille pourrait être influencé par le milieu. De plus, un système de protection des cellules a été mis en place afin de ne pas modifier malencontreusement les formules. Ci-dessous, le modèle de grille élaboré.



OUTIL D'AUTODIAGNOSTIC RELATIF A LA SECURITE DES SYSTEMES DE L'INFORMATION

A LIRE !...

Pour Qui ? :
Cette grille est destinée à la personne qui gère le système de sécurité de l'information en Centre Hospitalier.

Pour Quoi ? :
Elle permet d'évaluer son système de sécurité dans le but de réaliser des actions correctives et/ou préventives.

Comment ?:
1. Remplir cette grille d'auto-évaluation simple et rapide à utiliser.
Evaluer votre critère à l'aide de l'échelle :
- Faux
- Plutôt faux
- Plutôt vrai
- Vrai

Il n'y a qu'à cliquer sur l'onglet "grille d'évaluation"

Figure 9 : Grille d'autodiagnostic

3.2. Résultats obtenus

Une fois la grille d'autodiagnostic fonctionnelle, elle a été validée par notre tuteur M. Caliste. Une fois l'accord obtenu, le responsable communication du groupe a diffusé notre outil à la liste de contacts, afin de le faire tester et d'obtenir des retours en vue de l'améliorer. Cependant, à ce jour, aucun hôpital ne nous a répondu, peut être que cela a été dû aux périodes de vacances ou alors par faute de temps.

Une comparaison entre les résultats obtenus et les objectifs fixés au début du projet est nécessaire. Pour cela, les exigences définies dans la PDS (cf. figure 3) ont été comparées avec nos résultats :

Etapes PDS	Exigences PDS	Résultats obtenus	Etat des objectifs
Attentes générales	Bénéficier d'un outil d'autodiagnostic Améliorer le système	Outil crée L'autoévaluation permet d'identifier les faiblesses du système et donc de l'améliorer	Atteint
Besoin particulier	S'auto-évaluer	Outil simple d'utilisation avec une note d'explication avant utilisation	Atteint
Livrable	Outil d'autodiagnostic	Outil crée	Atteint
Contexte	HAS et cadre réglementaire sur la confidentialité	Prise en compte de la demande de l'HAS et du cadre sur la confidentialité	Atteint
Mission	Créer l'outil	Outil créé	Atteint
Objectif mesurable	Test de l'outil	Outil diffusé aux contacts mais aucune réponse reçue	Non atteint

Figure 10 : Tableau récapitulatif des résultats obtenus

Au vu du tableau précédent, une amélioration peut être proposée: diffuser plus largement l'outil d'autodiagnostic afin d'obtenir des retours en vue d'améliorer l'outil. De plus, il aurait été intéressant de créer cet outil sous format PHP afin de proposer à nos contacts un outil plus agréable et plus interactif à utiliser.

4. Perspectives d'avenir et enseignements tirés

L'enseignement QP10 nous a beaucoup appris.

Tout d'abord, sur le plan humain, grâce à un travail de groupe efficace alors que chacun des membres du groupe venait d'horizons différents. Cela nous a beaucoup enrichi puisque d'un pays à un autre, d'une culture à une autre, nous avions des regards distincts sur le projet.

Nous avons aussi pu développer notre esprit d'organisation, possédant des contraintes de temps et de disponibilité, nous n'avons eu d'autre choix que de travailler main dans la main afin de mener à bien ce projet. La programmation de réunions régulières et la répartition du travail ont sans doute été les clefs de notre réussite.

De plus, notre projet a porté sur un domaine bien précis qu'est le secteur hospitalier.

Aucun d'entre nous n'avait eu l'occasion auparavant d'aborder ce milieu. Ce fût donc une totale

découverte et nous pouvons à présent comprendre comment fonctionnent les systèmes d'informations dans les hôpitaux et notamment comment ils sont sécurisés.
La création de l'outil d'autodiagnostic nous a aussi permis d'étudier en profondeur la norme ISO 27799 et de comprendre quels en sont les enjeux. Nous avons ainsi pu nous apercevoir qu'elle comporte certaines nuances (par exemple la différence entre une exigence et une convenance), cela pourra nous servir pour l'étude d'autres normes.
La création de l'outil a aussi été très instructive, certains d'entre nous n'en avaient jamais créé, nous sommes maintenant capables d'en concevoir un via Excel et de l'adapter aux besoins.

Sur un plan un peu plus propre au groupe, le module QP10 nous a permis, grâce aux différents jalons d'apprendre à mener efficacement des recherches et de partager nos informations. Les différents passages de jalon nous ont aussi permis de nous exprimer en publique, exercice parfois peu facile, et de discuter de notre travail et de nos avancées.

Conclusion du projet

Lors de ce projet d'intégration, notre mission était de trouver une solution afin que les hôpitaux puissent évaluer leur niveau de sécurité des systèmes d'informations. Ayant au préalable identifier et étudier les différentes sources de problèmes et menaces grâce à un questionnaire envoyé à nos contacts en milieu hospitalier, nous avons cherché un moyen adapté pour leur permettre de s'auto-évaluer. La création d'un outil d'autodiagnostic nous a semblé être le choix le plus judicieux de par les avantages qu'il présentait.

Afin de créer cet outil et de répondre aux exigences de la norme ISO 27799 relative à la sécurité des systèmes d'information en milieu hospitalier, nous avons étudié la norme en profondeur et déterminé quelles étaient les exigences et convenances à satisfaire.

Une fois ce travail effectué, nous avons diffusé notre outil aux hôpitaux en vue de le faire tester. L'hôpital d'Amiens ayant répondu à notre appel, et ayant testé notre outil, nous avons pu y apporter les améliorations nécessaires.

Nous pouvons donc dire que notre objectif a été atteint puisque le but de ce projet était de permettre aux hôpitaux de s'évaluer, ce qui est chose faite. Notre équipe est donc très satisfaite de la réalisation de la mission, et nous aurons eu la satisfaction d'avoir eu de mise en situation de l'outil. Aussi, rien ne nous empêche par la suite de proposer à d'autres hôpitaux de le tester.

Cet outil maintenant créé, il serait intéressant de l'utiliser pour évaluer les différents services de l'hôpital, certaines variations pourraient peut-être enregistrées d'un service à l'autre.

Bibliographie

Colloques :

1/ OCDE(2002), Lignes directrices de l'OCDE régissant la sécurité des systèmes et réseaux d'information : vers une culture de la sécurité, Edition : OCDE, 30p.

2/ HAS (9 février 2010), La contribution des systèmes d'information à la performance des établissements de santé : Edition HAS, 9p

Thèses :

3/ TOGOLA Tidiani(2010), Etude de l'implémentation d'un système de management de la qualité centré sur la sécurité de l'information à l'agence nationale de télésanté et d'information médicale, Thèse professionnelle : NQCE à l'Université technologique de Compiègne, 36p.

Ressources Internet :

4/ le 30/09/10 Site internet : www.techniques-ingenieur.fr

Sujet : Comment évaluer l'efficacité des mesures de sécurité d'un SMSI ?
Lien : http://www.techniques-ingenieur.fr/actualite/informatique-electronique-telecoms-thematique_193/comment-evaluer-l-efficacite-des-mesures-de-securite-d-un-smsi-article_4662/

5/ le 30/09/10 Site internet : www.techniques-ingenieur.fr

Sujet : Quel script pour un bon audit de systèmes d'informations
Lien : http://www.techniques-ingenieur.fr/actualite/informatique-electronique-telecoms-thematique_193/quel-script-pour-un-bon-audit-de-systemes-d-informations-article_5320/

6/ le 6/10/10 Site internet : http://www.orange-business.com/fr/entreprise/

Sujet : le centre hospitalier Henri Laborit soigne la sécurité de ses données
Lien : http://www.orange-business.com/fr/entreprise/contenus/temoignages-clients/consulting/

7/ le 6/10/10 Site internet : http://siteinfosecusante.free.fr/

Sujet : informatique hospitalière, sécurité et confidentialité
Lien : http://siteinfosecusante.free.fr/spip.php?article34

8/ Le 6/10/10 Site internet : http://www.decret-confidentialite.org

Sujet : Quand l'hôpital prend soin des données de ses malades
Lien : http://www.decret-confidentialite.org/invitation.html

9/ Le 6/10/10 : Site internet : http://www.lexpress.fr/
Sujet : Hôpital 2012, la carte des rénovations d'hôpitaux
Lien : http://www.lexpress.fr/actualite/sciences/sante/hopital-2012-la-carte-des-renovations-d-hopitaux_590893.html

10/ Le 9/12/10 Site internet : http://www.iso27001certificates.com/
Registre international des certifications ISMS

11/ Le 10/12/10 Site Internet : http://www.clusif.asso.fr/fr/production/ouvrages/pdf/CLUSIF-MIPS2010-Hopitaux.pdf Menaces informatiques et pratiques de sécurité en France publié par le CLUSIF

12/ Le 9/12/10 Site internet : http://www.fhv.ch/ Site de la Fédération des hôpitaux vaudois

25/ Le 12/12/10 Site internet : http://www.has-sante.fr/portail/jcms/j_5/accuei Site de la Haute Autorité de la Santé

Lois et Règlements:

23/ Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés : article 29, disponible sur http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=LEGITEXT000006068624&dateTexte=20101009 (consulté le 9/10/10)

Normes :

24/ AFNOR(2007), ISO 27001: Techniques de sécurité-Système de gestion de la sécurité de l'information, Edition: AFNOR, 44p

13/ AFNOR(2005), ISO 27002: Technologies de l'information-Techniques de sécurité-Code de bonne pratique pour la gestion de la sécurité de l'information, Edition : AFNOR, 136p.

14/ AFNOR (2010), ISO 27003 : Technologies de l'information- Techniques de sécurité- Lignes directrices pour la mise en œuvre du système de management de la sécurité de l'information, Edition : AFNOR, 78p.

15/ AFNOR(2009), ISO 27004 : Technologies de l'information-Techniques de sécurité-Management de la sécurité de l'information-Mesurage, Edition : AFNOR, 66p.
16/ AFNOR(2008), ISO 27005, 71p.

17/ AFNOR(2008), ISO27799 : Gestion de la sécurité de l'information relative à la santé en utilisant l'ISO/CEI27002, Edition : AFNOR, 77p.

22/ HAS (Juin 2009) : Manuel de certification des établissements de santé V2010 ; Direction de l'Amélioration de la Qualité et de la Sécurité des Soins, 99p

Autres :

18/ Secrétariat général de la défense nationale et la Direction centrale de la sécurité des systèmes d'information (2003), Le Guide PSSI

19/ Secrétariat général de la défense nationale et la Direction centrale de la sécurité des systèmes d'information(2005), Elaboration de tableaux de bords SSI : TDBSSI, Edition : Bureau conseil de la DCSSI, 58p.

20/ Secrétariat général de la défense et la Direction centrale de la sécurité des systèmes d'information (2007), Maturité SSI : approche méthodologique, Edition : Bureau conseil de la DCSSI, 24p.

21/ Secrétariat général de la défense nationale et la Direction centrale de la sécurité des systèmes d'information (2004), Guide pour l'élaboration d'une politique de sécurité de système d'information, Edition : Bureau conseil de la DCSSI, 29p.

Annexes

Annexe 1 : Note de clarification

Dates	Version	Auteur
27/09/10	1	Léa
30/09/10	2	Groupe projet
08/11/10	3	Anisseh

1. Contexte

Les centres hospitaliers traitent et gèrent 2 grands types d'informations : informations administratives et financières du Ministère de la Santé et les dossiers patients. Cependant, les réseaux étant de plus en plus utilisés, les organisations doivent accroitre leur sécurité face aux menaces éventuelles. Selon la norme ISO27001 :2005, la sécurité de l'information est la protection de la confidentialité, de l'intégrité et de la disponibilité de l'information ; en outre, d'autres propriétés telles que l'authenticité, l'imputabilité, la non-répudiation et la fiabilité peuvent également être concernées.

2. Données d'entrée :

Normes ISO 27000, études, contacts, thèse NQCE…

3. Définition du projet :

3.1. Problématique

Comment un centre hospitalier peut il évaluer son niveau de sécurité de l'information ?

3.2. Objectif

Créer ou développer un outil d'autodiagnostic relatif à la SI dans le secteur hospitalier

3.3. Critères de réussite

- ✓ Respect des délais et de l'organisation
- ✓ Répartition des tâches
- ✓ Mise à jour de notre réseau Skydrive
- ✓ Motivation de chacun

3.4. Dates du projet

Date de début : 27/09/10
Date de fin : 27/01/11

4. Produit du projet

- ✓ Outil d'autodiagnostic simple d'utilisation
- ✓ Questions précises et claires
- ✓ Nombre de questions ?

5. Acteurs du projet et attentes

Types	Acteurs	Attentes
Directs	Maître d'œuvre : le groupe projet	Connaissance des normes SI Savoir créer un outil d'autodiagnostic Développer l'esprit d'équipe Manager un projet Mettre en pratique les outils qualité
	Maître d'ouvrage : M.Caliste	Obtenir un outil d'autodiagnostic
Indirects	Les centres hospitaliers	Pouvoir réaliser un autodiagnostic

Animateur : Zarji Anisseh

6. Risques liés à la réalisation du projet et alternatives

Afin d'anticiper les éventuelles risques pendant la réalisation de notre projet, nous avons listé l'ensemble des risques du projet QP10. Nous nous sommes réunis afin de réaliser un brainstorming et ainsi définir nos alternatives. Ces dernières ont été classées par la réalisation d'un vote pondéré.

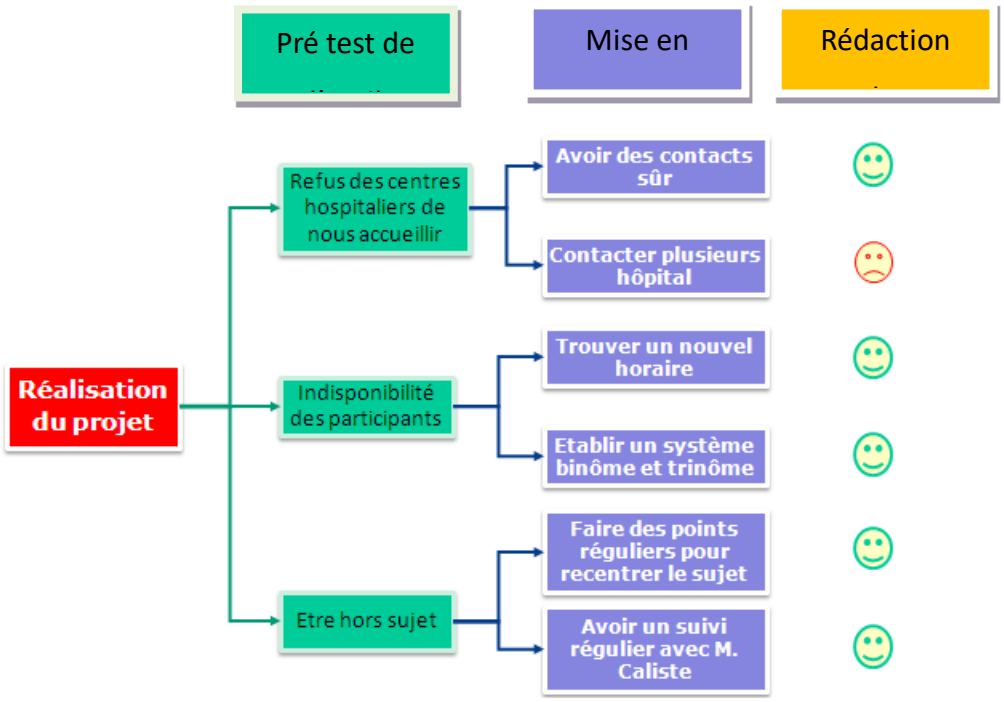


Figure : Diagramme des décisions

Annexe 2 : Grille d'entretien

	Grille d'entretien	Doc. Réalisé le 21/10/10 Groupe QP10 n°4
Interviewer :		Page 1/3
Personne questionnée :		

Question	Réponse
Identité de la personne questionnée et de l'établissement associé :	
Dans quel hôpital travaillez-vous ?	
Dans quel service exercez-vous ?	
Quelle est votre fonction ?	
Depuis combien de temps ?	
Votre établissement est-il certifié? Si oui, quelles sont ces certifications ?	
Système de gestion des informations	
Y a-t-il un responsable du système d'information ? Si oui, qui est-ce ?	
Etes-vous soumis à une réglementation particulière en matière de sécurité des informations ?	
Avez-vous une politique relative à votre système d'informations ?	
Y a-t-il des procédures relatives au système de sécurité de vos informations ?	
Avez-vous des sauvegardes de vos documents? Si oui, sous quel format ? (papier, informatique, …)	
Combien de temps sont archivées les informations ?	
Avez-vous un système Wifi? Si oui, le réseau est-il sécurisé ? Comment ?	

	Grille d'entretien	Doc. Réalisé le 21/10/10 Groupe QP10 n°4
Interviewer :		Page 2/3
Personne questionnée :		

Y a-t-il un moyen d'identification des risques provenant de tiers ? (sous-traitants, …)	
Utilisation des informations :	
Disponibilité (propriété d'être accessible et utilisable à la demande par une entité autorisée)	
Où sont situées les informations ? (dossier des patients, informations internes à l'hôpital, …)	
Vous est-il déjà arrivé de ne pas pouvoir obtenir des informations recherchées? Si oui, à quelle fréquence ?	
D'après vous, quelles en sont les raisons ?	
Tout le personnel a-t-il accès à toutes les informations ? Si non, comment l'accès est-il restreint ?	
Votre établissement est-il certifié? Si oui, quelles sont ses certifications ?	
Confidentialité (propriété selon laquelle l'information n'est pas rendue accessible ou divulguée à des personnes, entités ou processus non autorisés)	
L'accès aux différentes informations est-il protégé ? Si oui, de quelle façon ? (mots de passe, codes, …)	
Les informations sont-elles placées dans des lieux ouverts au public ?	

	Grille d'entretien	Doc. Réalisé le 21/10/10 Groupe QP10 n°4
Interviewer :		Page 3/3
Personne questionnée :		

Intégrité (propriété de protection de l'exactitude et de l'exhaustivité des actifs)	
Avez-vous déjà observé des erreurs lors de la consultation d'informations ? (informations concernant les patients)	
Votre administration vous a-t-elle déjà demandé plusieurs fois le même document ? (ex : RIB)	
Quelle est la marche à suivre en cas de panne réseau ?	
Retour d'expérience :	
Ressentez-vous des faiblesses à ce sujet dans votre établissement ?	
Avez-vous déjà réalisé des actions correctives en réponse à un problème rencontré ? Si oui, pouvez-vous nous présenter ce plan d'action ?	
Comment répondez-vous aux besoins du personnel et des patients en matière de système de sécurité ?	
Y a-t-il déjà eu des réclamations concernant la sécurité des informations par le personnel ? Et par les patients ?	

Annexe 3 : Coordonnées contacts

Personne	Service	Lieu
Gery MOLLERS	Responsable Sécurité du Système d'Informations	Cliniques Universitaires Saint-Luc, BRUXELLES, Belgique
Stéphane PIERREFITTE	Direction des Systèmes d'Information et des Plateaux Techniques	Centre Hospitalier Sainte Anne 1 rue Cabanis 75 674 PARIS
Agnès LIEDORP	Responsable Qualité	Centre Hospitalier de Laon 0200
Pierre LEGUYADER	Ingénieur biomédical	Institut de cardiologie Montréal

D'autres hôpitaux ont été contactés par nos soins, sans cependant posséder de contact direct :

- CHRU de Lille via un formulaire
- CH Arras : direction@ch-arras.fr
- CHU Amiens : chu@chu-amiens.fr
- Hôpital de Béthune : nchalmin@ch-béthune.fr
- CH Hénin-Beaumont : edouard-hardy@rubisoft.net

Résumé

Dans le but d'aider les hôpitaux à connaître leur niveau de sécurité de leur système d'informations, un outil d'autoévaluation au regard des exigences de l'ISO 27799 (Gestion de la sécurité de l'information relative à la santé en utilisant l'ISO/CEI 27002) a été créé. En effet, il leur est nécessaire de pouvoir maîtriser la disponibilité de leurs documents, leur intégrité et leur confidentialité. La maîtrise de ces trois éléments leur permet de gagner en efficience dans le management de la sécurité de leur information. Il permet aux hôpitaux de satisfaire les exigences relatives aux systèmes de sécurité de l'Information, du référentiel de la HAS.

Mots clés : ISO 27799, disponibilité, confidentialité, intégrité, sécurité, système d'information, HAS.

Summary

On purpose to help hospitals to learn the security level of their information system, an auto-evaluation tool has been created on base of ISO27799 (Information security management in health using ISO/IEC 27002). In fact, it's necessary for hospitals to be able to ensure availability, integrity and confidentiality of their documents and data. By well control of these three elements, hospitals could efficiently maintain the security of their information system, as well as satisfying the information security requirements of HAS (French National Authority for Health).

Key words : ISO27799, availability, integrity, confidentiality, security, information system, HAS.

概 要

为了帮助医院了解自身信息系统的安全性，特创建了一个基于 ISO27799（使用 ISO/IEC 27002 的医疗信息安全管理）的自我评估工具。事实上，医院必须确保其文件和信息的实用性、完整性和保密性。通过管理这三个要素，医院能够有效管理其信息系统的安全性，同时满足 HSA（法国国家健康总署）对信息安全的要求。

关键词 ：ISO27799，实用性，完整性，保密性，安全，信息系统, HAS.。