RENCONTRES INTERNATIONALES
RENCONTRES INTERNATIONALES
de la Gouvernance des Risques en Santé

Exigences de sécurité des Systèmes d'Information pour les équipements biomédicaux des établissements de santé

Présentation du travail issu du groupe de travail RSSI/Ingénieurs biomédicaux/HFSSI

Guillaume Deraedt - RSSI CHRU de Lille – Animateur du Groupe de Travail
François Faure – IBMH CHU d'Angers – Représentant l'AFIB

Toulouse, 7 et 8 juin 2010

2 RENCONTRES INTERNATIONALES
RENCONTRES INTERNATIONALES

Sécuriser les dispositifs biomédicaux, pourquoi ?

- Des équipements biomédicaux de plus en plus informatique
(logiciel = Dispositif Médical)

- Des équipements biomédicaux de plus en plus vulnérable

CONFICKER 2009 - Apprendre du retour d'expérience

⇛ **Mission confiée par la FHF au travers du CNSI au RSSI du CHU de Lille de coordonner un groupe de travail sur ce thème en lien avec l'AFIB**

Participants au groupe de travail

Participants, corédacteurs, et relecteurs

AFIB	François Faure (CHU d'Angers) - Représentant de l'Association Française des Ingénieurs Biomédicaux
ANAP	Dominique Lepere, Directeur de projet
	Pierre Duclos, Directeur de projet
AP HM	Julien Martinez, RSSI
AP HP	Astrid.Lang, RSSI
	Marc Degrain, Ingénieur biomédical
	Jean-Eric Lefevre, Ingénieur biomédical
CHU d'Amiens	Julien Rousselle, RSSI
CHU de Bordeaux	Alex Franco, RSSI
CHU de Clermont-Ferrand	Joël Langlois, RSSI
CHRU de Lille	Guillaume Deraedt, RSSI et CIL
CHU de Limoges	Claude Delhaye, chargé de mission – RSSI
CHU de Montpellier	Christian Capelle, Ingénieur informatique, Cellule Sécurité du SIH
	Marc Fantoni, Ingénieur biomédical,
	Thierry Thibout, Ingénieur biomédical,
CHU de Nancy	Jean-Stanislas Tyzo, RSSI
CHU de Nantes	Cedric Cartau, RSSI
CHU de Rennes	Paul LeMagoarou, RSSI
CHU de Toulouse	Yan Morvezen, RSSI
Hôpitaux Universitaires de Strasbourg	
	Jean-Pierre LAURENT, ingénieur biomédical
	Fabrice Stalter, RSSI;
Institut Curie	Mylène Jarossay, DSI adjoint - RSSI
Ministère de la Santé	Eric Grospeiller, Fonctionnaire de SSI des ministères chargés des affaires sociales
	Philippe Loudenot, fonctionnaire de SSI des ministères chargés des affaires sociales
	Laurent Treluyer (MISS)
	Hiep Vu Thanh, Chargé de mission à la DHOS
Service de Santé des Armée	Michel Dubois, Capitaine, Officier de Sécurité des Systèmes d'Information

Participants au groupe de travail

Comité de validation

AFIB	François FAURE (CHU d'Angers)	- Représentant de l'AFIB
ANAP	Pierre Duclos, Directeur de projet	
CHU d'Amiens	Julien Roussel, RSSI	
CHU de Nancy	Jean-Stanislas Tyzo, RSSI	
CHU de Montpellier	Christian Capelle, Ingénieur informatique, Cellule Sécurité du SIH	
CHRU de Lille	Guillaume Deraedt, RSSI et CIL	
Hospices Civils de Strasbourg	Fabrice Stalter, RSSI;	
Institut Curie	Mylène Jarossay, DSIO adjoint - RSSI	
Ministère de la Santé	Eric Grospeiller, Fonctionnaire de SSI des ministères chargés des affaires sociales	
	Philippe Loudenot, fonctionnaire de SSI des ministères chargés des affaires sociales	
	Laurent Treluyer, MISS	
Service de Santé des Armée	Michel Dubois, Capitaine, Officier de Sécurité des Systèmes d'Information	

Logistique et compte-rendu de réunion

AFIB	François FAURE (CHU d'Angers)	- Représentant de l'AFIB
ANAP	Pierre Duclos, Directeur de projet	
Hospices Civils de Strasbourg	STALTER Fabrice, RSSI;	
CHRU de Lille	Guillaume Deraedt, RSSI et CIL	

Direction de projet et animation

CHRU de Lille	Guillaume Deraedt, RSSI et CIL

Agissant sous mandat de la Commission Nationale des Systèmes D'Information pour la FHF.

2 RENCONTRES INTERNATIONALES
RENCONTRES INTERNATIONALES
de la Reconnaissance des Risques en Santé

Les objectifs fixés au Groupe de Travail :

1. **Rapprocher les IBMH et les RSSI**

   - renforcer la compréhension mutuelle des contraintes liées à leurs activités réciproques,

   - les former à un langage commun

2 RENCONTRES INTERNATIONALES
RENCONTRES INTERNATIONALES
de la Gouvernance des Risques en Santé

Les objectifs fixés au Groupe de Travail :

2. Leur apporter des outils adaptés et évolutifs

- pour sécuriser les dispositifs biomédicaux intégrant le SIH,

- pour définir ou intégrer les PCA et PRA

2 RENCONTRES INTERNATIONALES
RENCONTRES INTERNATIONALES
de la Reconnaissance des Risques en Santé

Les objectifs fixés au Groupe de Travail :

3. Rendre lisible et homogène les attentes des établissements de santé

- en proposant le même outils,
- outils adapté au niveau de maturité des organisations,

Les objectifs fixés au Groupe de Travail :

4. **Créer des documents qui pourraient servir de base à un futur cadre normatif ou réglementaire**

Le Cadre de référence :

- **La norme de sécurité ISO 27002**
- **Le Référentiel Général de Sécurité créé par l'article 9 de l'ordonnance n° 2005-1516 du 8 décembre 2005**
- **La Loi n° 78-17 du 6 janvier 1978 (CNIL)**
- **Les alertes issus du Centre d'Expertise Gouvernemental de Réponse et de Traitement des Attaques informatiques – CERTA**
- **Draft de la PGSSI (anc. Décret confidentialité)**

et pour les DM :

La Directive européenne 2007/47 sur les dispositifs médicaux (ordonnance de transposition du 12 mars 2010),

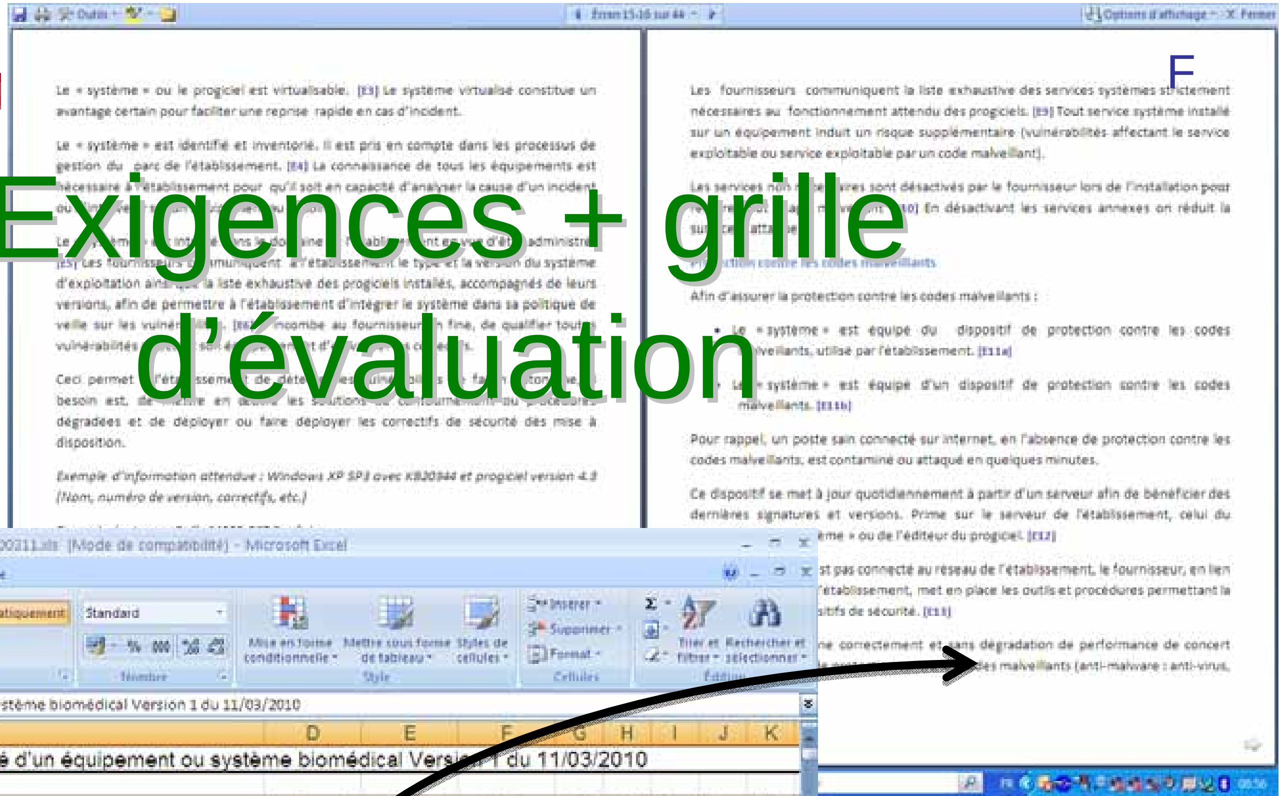
Le Décret n° 2001-1154 du 5 décembre 2001 relatif à l'obligation de maintenance

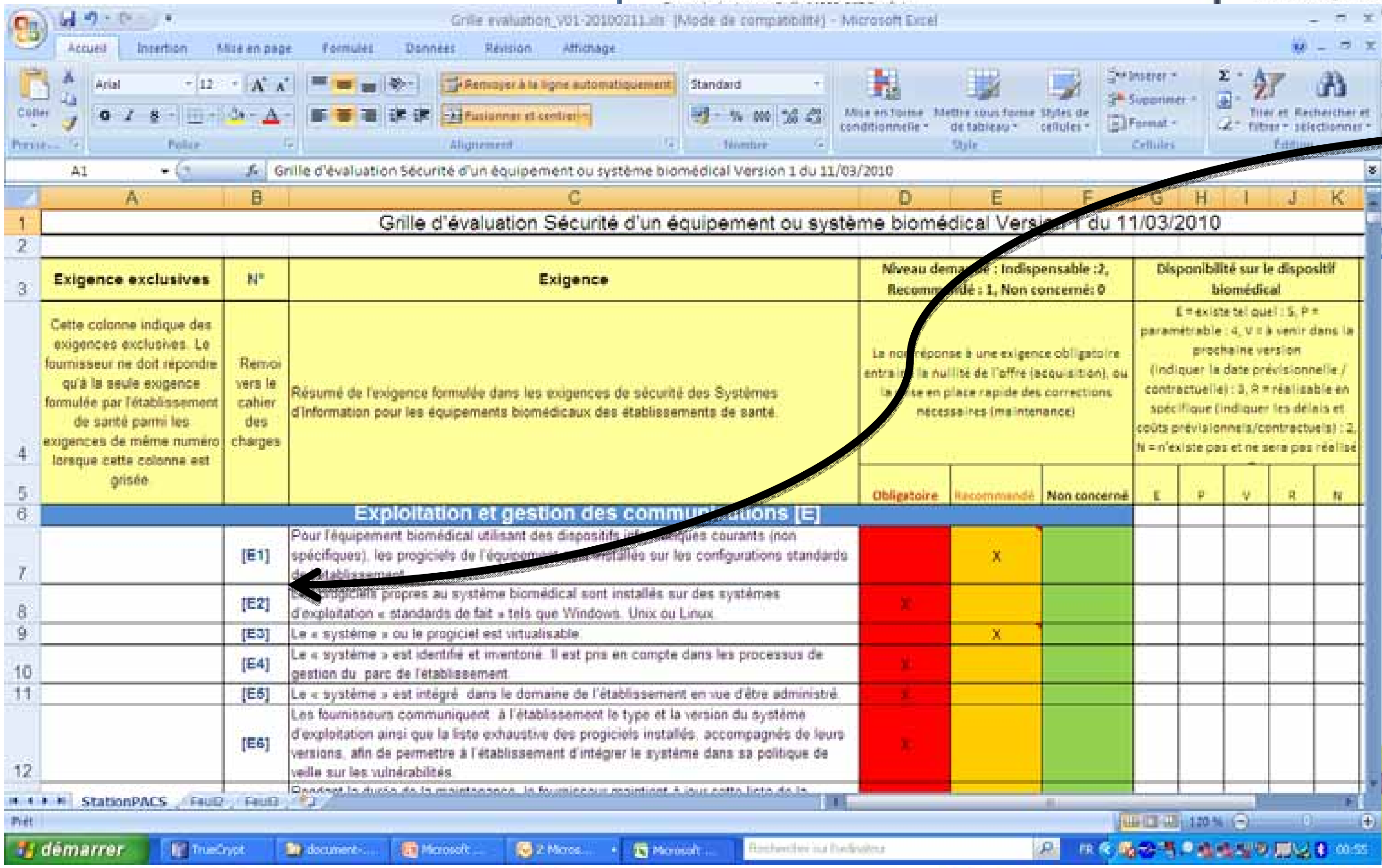
Le travail réalisé :

La construction d'un outils constitué d'une liste d'exigences et d'une grille de pondération et d'évaluation répondant aux objectifs fixés.

- Le 1er document liste les exigences de sécurité applicables aux équipements biomédicaux dés qu'ils traitent ou échangent des informations de santé.
- Cette liste et la grille d'évaluation associée forment un tout cohérent et doivent être considérés dans leur ensemble.
- Ce document et la grille d'évaluation associée peuvent servir de base aux services biomédicaux et aux RSSI ou chargés de la sécurité du Système d'Information, pour **définir la politique de sécurité à appliquer aux équipements biomédicaux sur leur Établissement puis à faire évoluer cette politique dans le temps**.
- Ils peuvent également servir dans le cadre de consultation pour l'acquisition de nouveaux équipements biomédicaux à préciser les attentes de l'établissement en termes de sécurité de l'information.

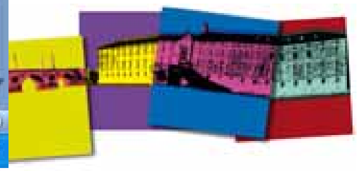
Exigences + grille d'évaluation





Grille d'évaluation Sécurité d'un équipement ou système biomédical Version 1 du 11/03/2010

Exigence exclusives	N°	Exigence	Niveau demandé : Indispensable :2, Recommandé : 1, Non concerné: 0			Disponibilité sur le dispositif biomédical				
Cette colonne indique des exigences exclusives. Le fournisseur ne doit répondre qu'à la seule exigence formulée par l'établissement de santé parmi les exigences de même numéro lorsque cette colonne est grisée	Renvoi vers le cahier des charges	Résumé de l'exigence formulée dans les exigences de sécurité des Systèmes d'Information pour les équipements biomédicaux des établissements de santé.	La non réponse à une exigence obligatoire entraine la nullité de l'offre (acquisition), ou la mise en place rapide des corrections nécessaires (maintenance)			E = existe tel quel : 5, P = paramétrable : 4, V = à venir dans la prochaine version (indiquer la date prévisionnelle / contractuelle) : 3, R = réalisable en spécifique (indiquer les délais et coûts prévisionnels/contractuels) : 2, N = n'existe pas et ne sera pas réalisé				
			Obligatoire	Recommandé	Non concerné	E	P	V	R	N
		Exploitation et gestion des communications [E]								
	[E1]	Pour l'équipement biomédical utilisant des dispositifs informatiques courants (non spécifiques), les progiciels de l'équipement sont installés sur les configurations standards de l'établissement		X						
	[E2]	Les progiciels propres au système biomédical sont installés sur des systèmes d'exploitation « standards de fait » tels que Windows, Unix ou Linux	X							
	[E3]	Le « système » ou le progiciel est virtualisable		X						
	[E4]	Le « système » est identifié et inventorié. Il est pris en compte dans les processus de gestion du parc de l'établissement.	X							
	[E5]	Le « système » est intégré dans le domaine de l'établissement en vue d'être administré.	X							
	[E6]	Les fournisseurs communiquent à l'établissement le type et la version du système d'exploitation ainsi que la liste exhaustive des progiciels installés, accompagnés de leurs versions, afin de permettre à l'établissement d'intégrer le système dans sa politique de veille sur les vulnérabilités.	X							



Utilisation de la grille de pondération et d'évaluation :

La grille de pondération et d'évaluation va permettre :

- D'adapter chaque critère à son propre environnement,
- De définir ses exigences vis-à-vis d'un fournisseur,
- De définir ainsi sa politique de sécurité

Les exigences sont pondérées selon 3 niveaux **conformes au Référentiel Général d'Interopérabilité (RGI) et à la RFC 2119**.

- **0** : **Non concerné, aucune exigence n'est demandée**.
- **1** : **Recommandé, bien qu'il ne s'agisse pas d'une exigence, l'établissement estime ce critère sécurité comme important.**
- **2** : **Obligatoire. La non-conformité au critère sécurité correspondant entraîne des mesures correctives immédiates, ou dans le cadre d'une opération d'achat, la nullité de l'offre.**

Utilisation de la grille de pondération et d'évaluation :

La **politique de sécurité à appliquer aux équipements biomédicaux** peut être décrite à l'aide de plusieurs grilles :

- une première grille décrivant les exigences minimales applicables à la majorité des équipements biomédicaux
- des grilles complémentaires spécifiques à certaines catégories d'équipement.

Les Exigences :
1- Intégrer les équipements dans le parc informatique de l'établissement

- Exploitation et gestion des communications, Interconnexions réseau
  - Maîtrise des flux réseaux et les attaques extérieures (Sécurité périmètrique)
- Configuration de base
  - Inventorier, « Maintenabilité », gestion des évolutions d'OS (Connaître pour protéger)
- Protection contre les codes malveillants
  - (Défense en profondeur): Protéger le dispositif dans un environnement corrompu

Les Exigences :
2- Assurer confidentialité et traçabilité

- **Contrôle d'accès**
  - **CNIL / PGSSI – anc. Décret confidentialité -**
- **Authentification**
  - **Carte d'établissement / Carte CPS / authentification**
- **Habilitations**
  - **Gestion des métiers/affectations et rôles applicatifs**
  - **Matrice des droits / AES**
- **Traçabilité**
  - **RGS / PGSSI / CNIL**

2 RENCONTRES INTERNATIONALES
RENCONTRES INTERNATIONALES

Les Exigences :
3- Garantir la confidentialité des échanges inter applicatif, l'intégrité et la pérennité de leur conservation

- **Export, extraction et échange de données**
  - Garantir l'anonymat des patients et réduire les fuites de données
- **Interfaces**
  - S'assurer de la présence d'I/O normalisées et maintenues pour communiquer avec d'autres applicatifs
- **Identito-vigilance**
  - S'assurer de l'inter connexion avec l'identité patient véhiculée par le SIH
- **Stockage / Sauvegarde / Destruction**
  - Pour les données le nécessitant

Les Exigences :
4- Gérer les correctifs, la maintenance à distance et les liens avec l'OS

- Acquisition, développement et maintenance des systèmes d'information
  - Maîtriser les évolutions technologiques et la reprise d'information en cas de défaillance de l'éditeur ou d'évolution forcée du Système d'Exploitation
  - Imposer le support des correctifs critiques (alertes du CERTA)
- Maintenance
  - Doit être compatible avec la **politique de maintenance biomédicale**
  - Accès VPN uniquement
  - Se prémunir des fuites de données

Les Exigences :
5- Intégrer les équipements biomédicaux dans les PCA et les PRA des processus auquel ils participent

- Gestion de la continuité d'activité
  - S'assurer pour les équipements critiques de la redondance des fonctions assurées par l'équipement biomédical
  - Prévoir en accord avec le fournisseur de l'équipement des modes de fonctionnement dégradé en cas de panne
    - Y compris avec des établissements partenaires

L'ETAPE SUIVANTE

F

Assurer une dynamique au-delà de la conception des outils proposés

- Le club RSSI, qui regroupe trimestriellement les RSSI et FF de RSSI, va proposer en lien avec l'AFIB:
  - Un kit pédagogique à destination des ingénieurs biomédicaux
  - Un partage des déclinaisons des critères de SSI exigés par catégorie de dispositif
- L'AFIB se fait le relais auprès de la communauté biomédicale et participe à la création et diffusion des outils complémentaires dont des actions de formation à destination de ses membres.

G

_ Le FSSI, assure le relais sur le plan extrahospitalier:

Documents transmis au Syndicat des éditeurs biomédicaux (SNITEM)

Documents réutilisés par l'ANSSI sur le plan européen (anc. DGSSI)

Volonté politique de sécurisé les dispositifs biomédicaux depuis Conficker

Vocation à faire évoluer le marquage CE

2 RENCONTRES INTERNATIONALES
RENCONTRES INTERNATIONALES
de la Renaissance des Risques en Santé

Merci de votre attention