Démarche de mise en œuvre et exemple d'une PSSI

EPSM Morbihan
Claude SALOMON
Chef du Centre Informatique – RSSI

Syndicat Interhospitalier de Bretagne – S.I.B
Yves NORMAND
Responsable de la Sécurité des Systèmes d'Information (RSSI)

Enjeux et objectifs d'une PSSI – Politique de Sécurité des Systèmes d'Information

« L'élaboration d'une PSSI doit reposer sur une démarche méthodologique. L'implication d'acteurs clés de l'établissement est nécessaire tant sur le plan de l'élaboration de la PSSI que celui de sa mise en œuvre.

A partir d'un sommaire type, les principaux chapitres d'une PSSI sont abordés avec des exemples.

La réussite d'une démarche globale de management de la sécurité de l'information repose, en partie, sur l'existence d'une PSSI, d'une organisation de la sécurité de l'information, et aussi de l'implication de l'établissement et des utilisateurs.

Des éléments de sensibilisation sont présentés, dans l'objectif de positionner la sécurité de l'information comme une valeur ajoutée contribuant aux missions de soins de l'établissement.

Le Responsable Informatique et RSSI de l'EPSM de St Avé (56) apportera son témoignage sur la mise en œuvre de sa PSSI.»

Agenda de l'Atelier

1. Contexte
2. Méthodologie(s) d'élaboration
3. Exemple d'une PSSI
4. Management de la sécurité de l'information
5. Conclusion / Valeur ajoutée de la SSI

1- Contexte

1 – Contexte
Le S.I.B.

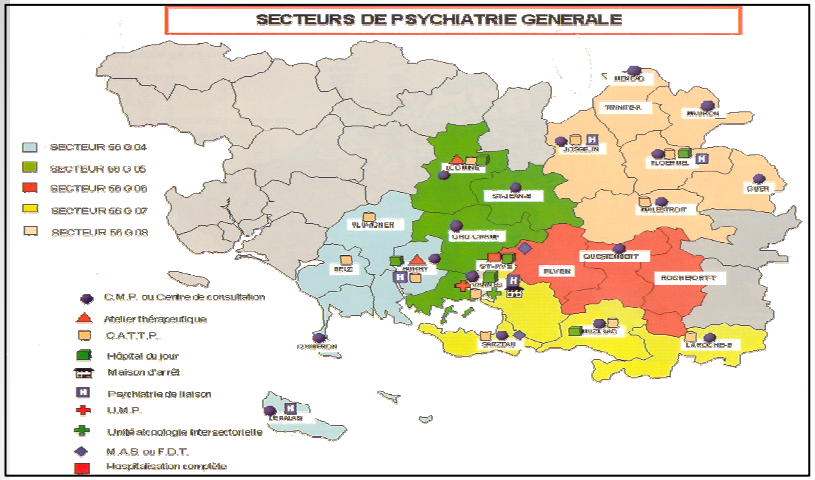
- Yves Normand
  - Responsable de la sécurité des systèmes d'information (RSSI)
  - Certifié « Lead Auditor ISO/IEC 27001:2005 »

- S.I.B : Établissement public spécialisé dans les prestations informatiques à destination des acteurs de la Santé Publique

- Domaines
  - Édition et diffusion de progiciels (30) pour la santé (médical, médico-technique, décisionnel):
    - Sillage, Génois, Sextant, Alfa Lima, …
  - Prestations d'intégration de solutions d'architectures techniques
    - Portail, annuaires, SSO, EAI,…
  - Hébergement et exploitation
    - Services relatifs à l'administratif – Paye, Factures, GRH.
    - Services relatifs aux données médicales - Offre Alfa Lima Télésanté.
  - Conseil et veille SIH, réseau et sécurités :
    - Schéma directeur, Audits, Politique sécurité, Charte des bons usages, PCA, Plan d'actions, …
    - Normalisation
    - Formation, Sensibilisation.

1 – Contexte
L'E.P.S.M Morbihan

L'EPSM - Morbihan est un établissement Public de Santé Mentale qui regroupe un ensemble de structures diversifiées de consultations, de soins et d'hébergement pour une population de 330 000 habitants (recensement de 1999).
Ces structures sont regroupées par pôles.

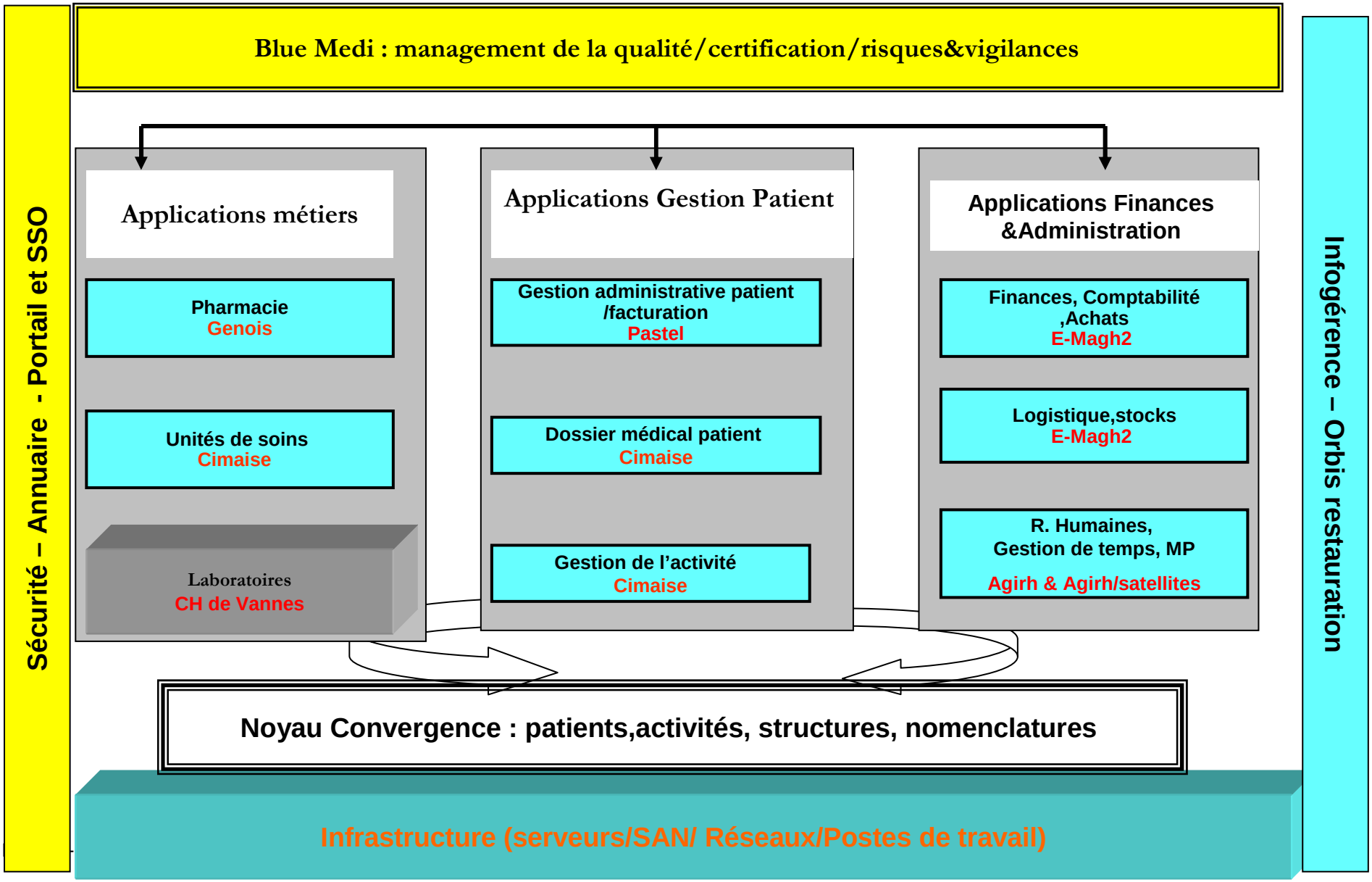


- **620** lits et places d'hospitalisation en Psychiatrie générale,
- **8 lits** & **95 places** d'hôpital de jour pour la Psychiatrie infantojuvénile
- **4 établissements** de type Médico social (MAS/FAM/EHPAD)

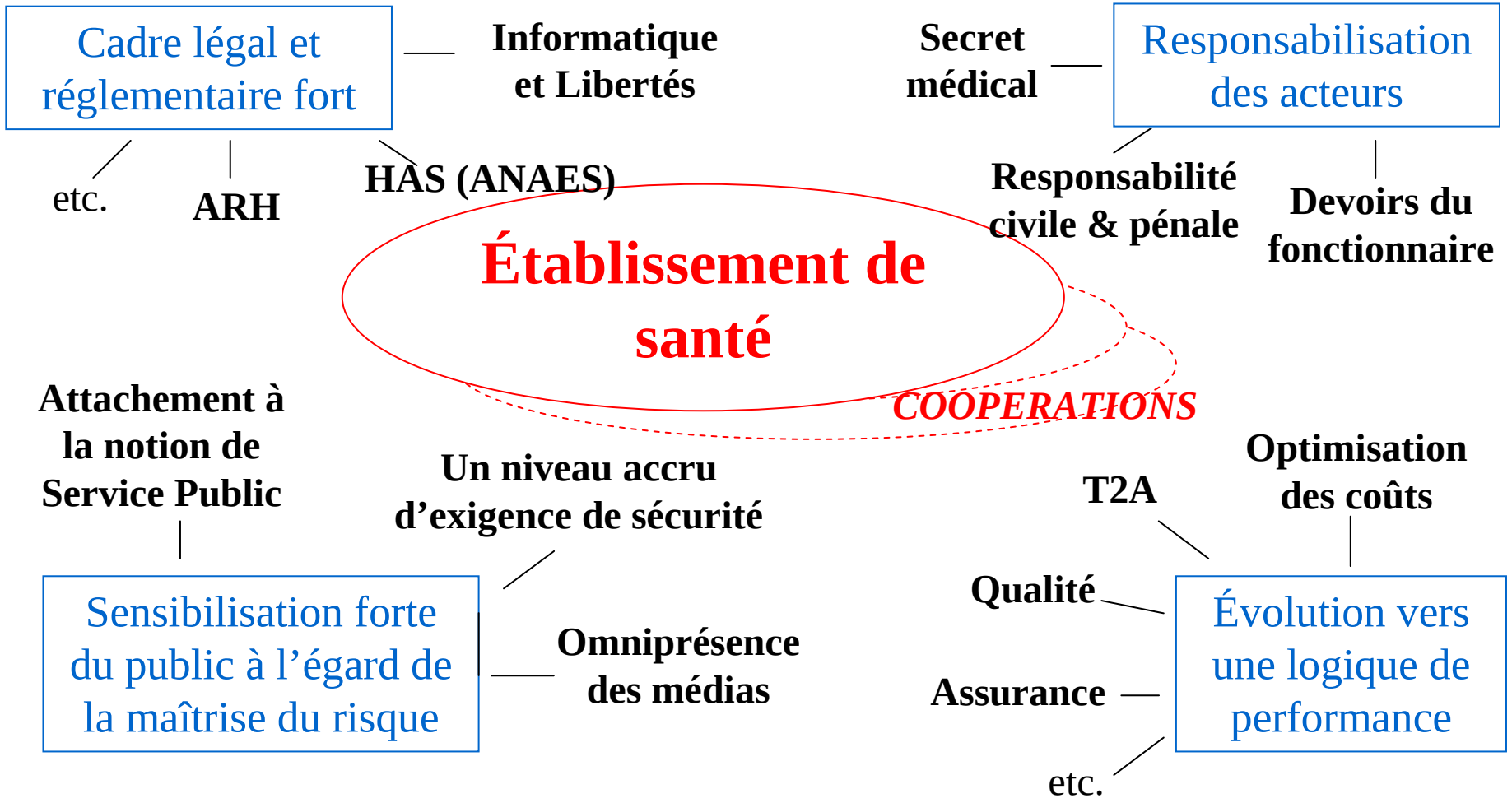
1 – Contexte
Le Système d'Information Hospitalier

- Le S.I. d'établissement – contexte
  - plus d'utilisateurs, d'applications, d'interface & technologies
- Relation au risque qui évolue
  - Acteurs
  - cadre législatif et réglementaire
  - Pression des médias et du public…..
- Des menaces en progression
  - Infection virale, pertes de services essentiels, pannes internes, erreur de conception & d'utilisation, évènements naturels, vols, fraudes ,divulgations, sabotage, intrusions…
- Contraintes

1 – Contexte
Le SIH – Ouverture et coopération



1 – Contexte
Un environnement complexe (source GMSIH)



2- Méthodologie(s) d’élaboration

2 – Méthodologie(s) d'élaboration

- Des Enjeux
  - Protéger les données de santé à caractère personnel
  - Favoriser le développement de la coopération entre professionnels de santé en instaurant un climat de confiance.
  - Contribuer à la stratégie et à l'image de marque de l'établissement
  - Être en conformité avec la réglementation et l'état de l'art
  - Protéger le patrimoine de l'établissement
  - Lutter contre les malveillances informatiques
  - Maîtriser les risques, et être complémentaire aux démarches de qualité et de gestion des risques.

2 – Méthodologie(s) d'élaboration

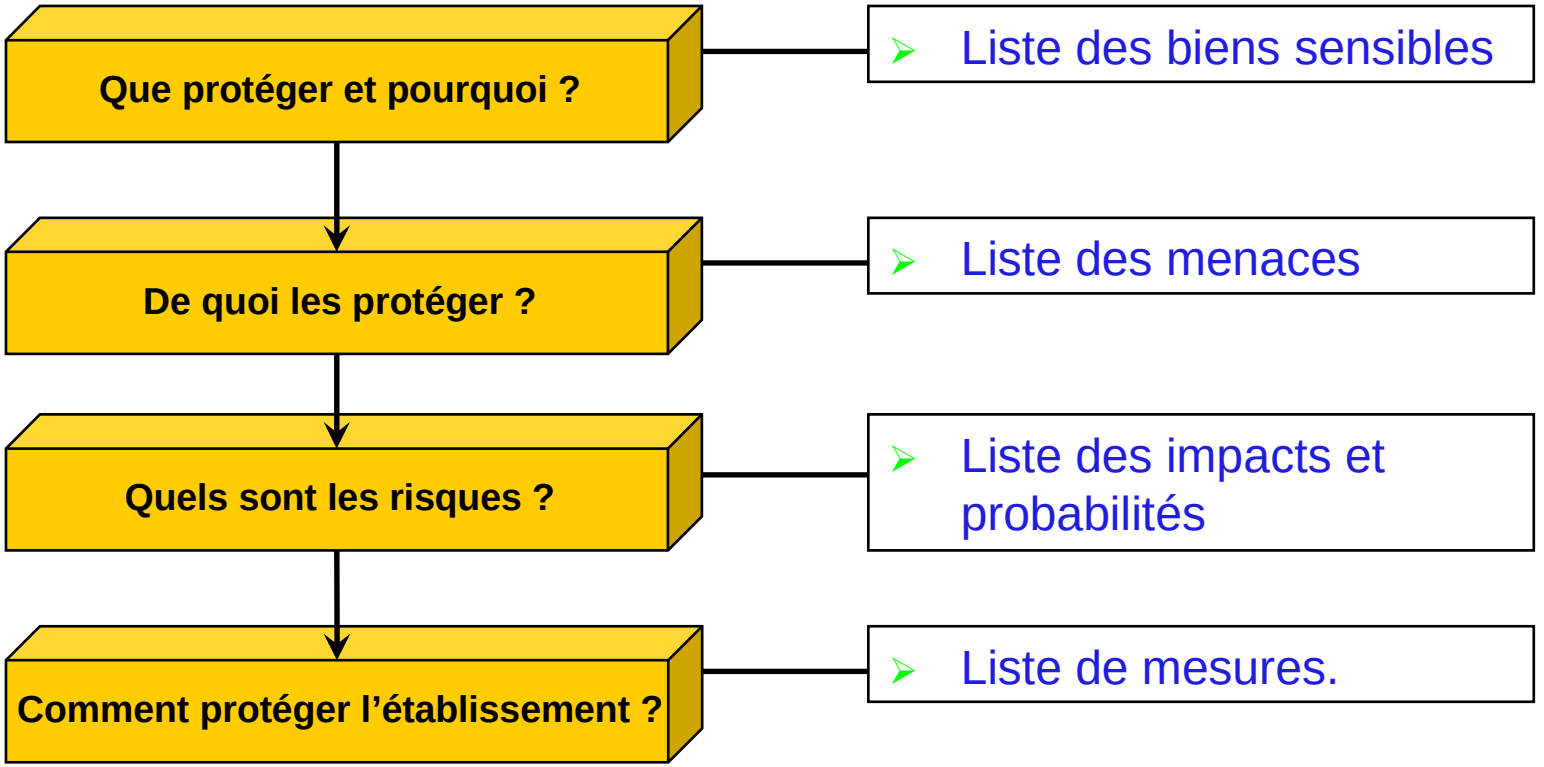
- Approche globale du système d'information

« La sécurité, plus une affaire d'organisation que de technique. »

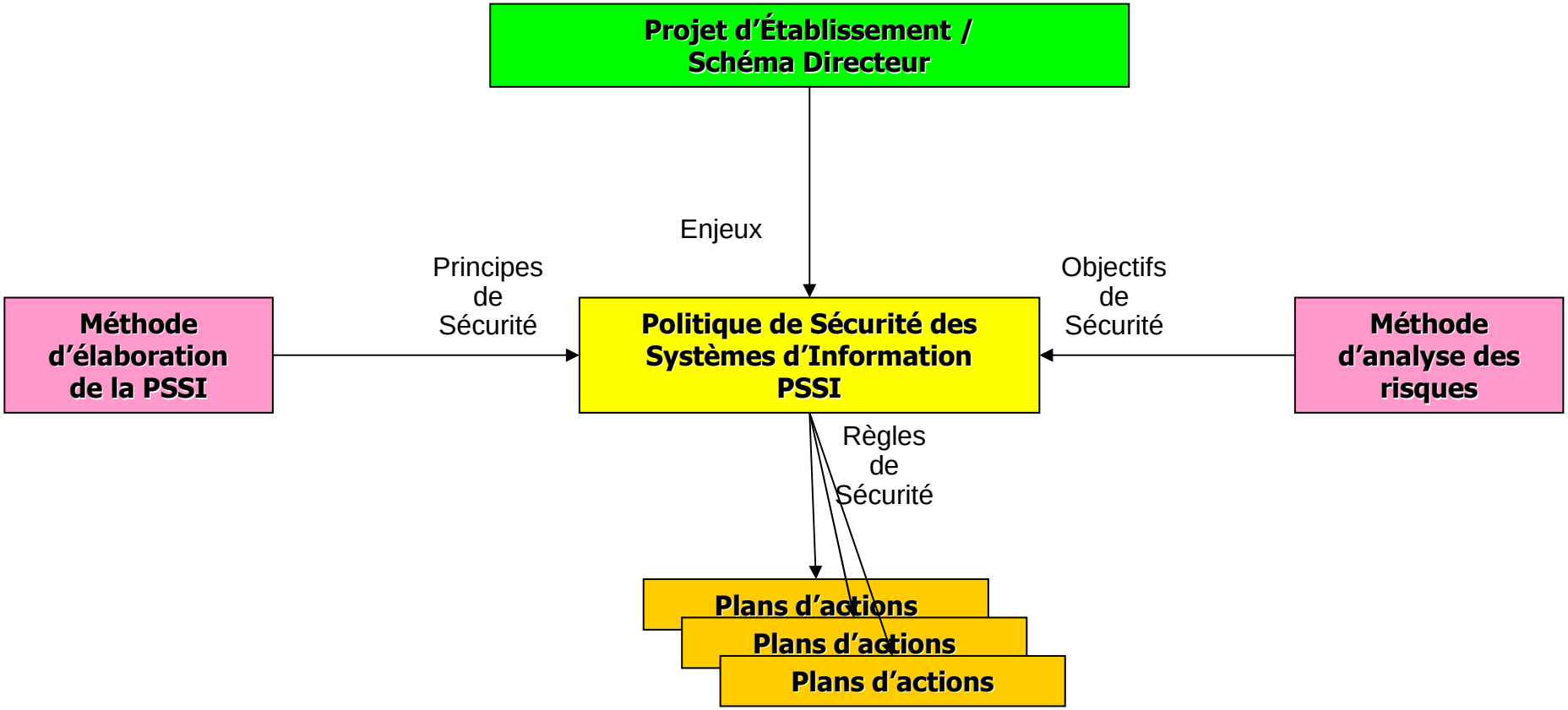
  - Domaines techniques
    - Sécurité de l'infrastructure informatique et des télécommunications
  - Domaines non techniques
    - Sécurité organisationnelle
    - Sécurité liée aux aspects humains
    - Sécurité liée à l'environnement
    - Sécurité liée aux aspects juridiques et assurantiels

2 – Méthodologie(s) d'élaboration

- Des questions essentielles



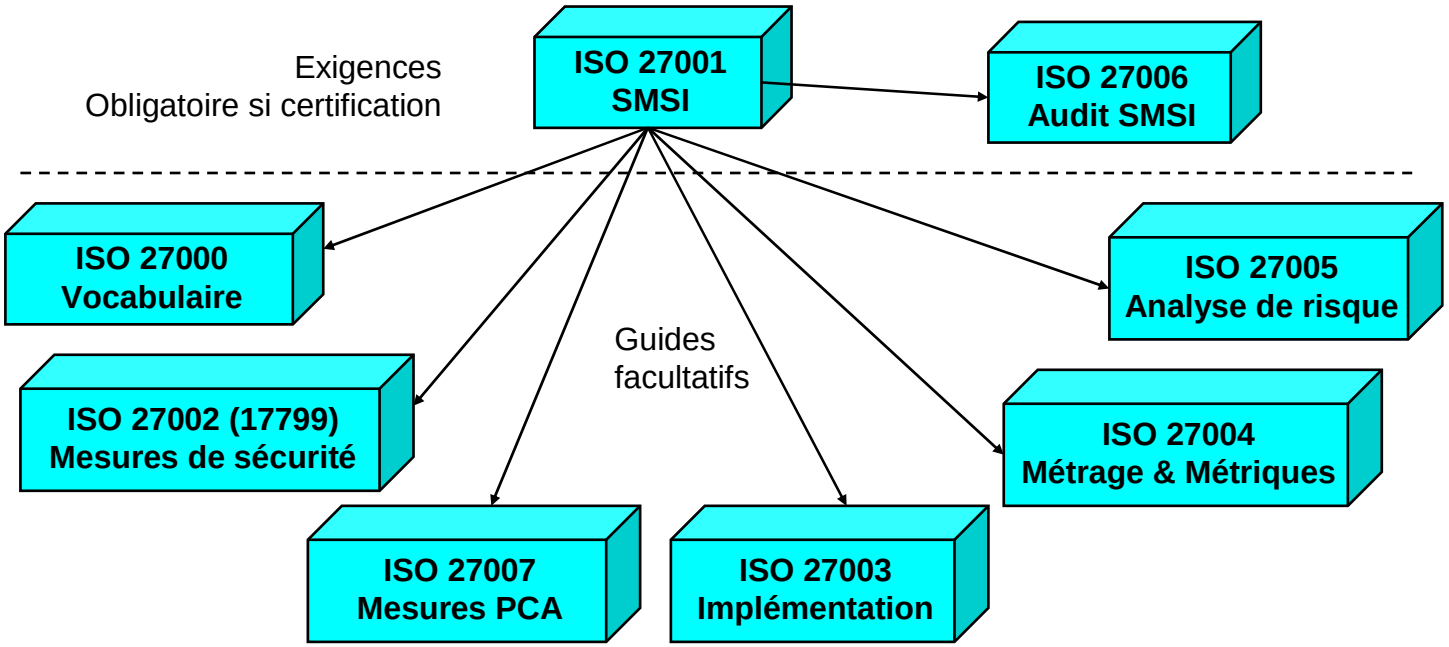
2 – Méthodologie(s) d'élaboration



2 – Méthodologie(s) d'élaboration

Référentiels

- Normes ISO 2700x



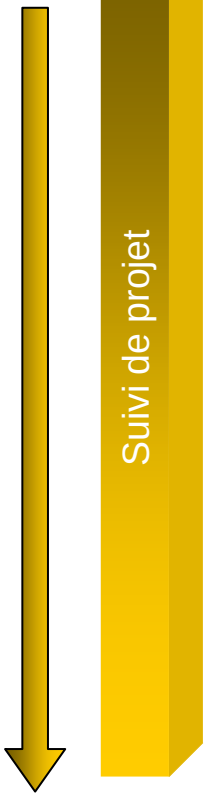
- Guide PSSI
  - DCSSI (Direction Centrale de la Sécurité des Systèmes d'Information – Service du 1er Ministre)
- EBIOS (DCSSI)
  - Expression des Besoins et Identification des Objectifs de Sécurité
- Guide d'élaboration d'une Politique sécurité
  - GMSIH (Groupement pour la Modernisation du Système d'Information Hospitalier)
- Référentiel Général Sécurité (RGS) – Déclinaison Santé

2 – Méthodologie(s) d'élaboration
Démarche projet

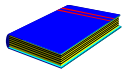
Ce qu'il faudrait faire ….

Comité de pilotage

- Direction,
- Représentants du corps médical,
- RSSI,
- …

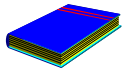


Phase 1
Engagement de la démarche



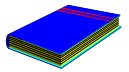
Note de stratégie et de cadrage

Phase 2
Identification
des éléments stratégiques



Éléments stratégiques

Phase 3
Sélection des principes et
rédaction des règles de sécurité



Principes et règles de sécurité

Phase 4
Finalisation de la PSSI

PSSI

Déclinaison opérationnelle des règles de sécurité de la PSSI
Comité Sécurité : suivi de la PSSI et de pilotage des actions
Audit de la PSSI

2 – Méthodologie(s) d'élaboration

PSSI : vers une généralisation

- **Sous l'évolution des contraintes**
  - Postes de travail partagés entre plusieurs professionnels avec de courtes sessions de travail
  - Mobilité du personnel soignant
  - Ressources informatiques limitées
  - Exacerbation du besoin de communiquer
  - Associations technologiques (TOIP)
  - Certification HAS
- **La perception de l'indisponibilité a changée**
  - **Tolérance de panne Jour → heure → minute**
  - Fenêtre de maintenance réduite
- **Besoins spécifiques : confidentialité et traçabilité**

2 – Méthodologie(s) d'élaboration

Principes de base pour la Sécurité du Système d'Information

- La définition et la gestion d'une politique de sécurité conduit nécessairement
  - à une approche globale pour obtenir une sécurisation cohérente et homogène en maîtrisant les coûts par rapport aux enjeux
  - à la définition d'une organisation interne, de méthodes, d'outils pour l'élaboration et le suivi de l'application de la politique de sécurité

- A la rédaction d'une politique de sécurité
- A une validation par direction de l'établissement
- Peut servir de base à l'élaboration d'un volet SSI du Schéma Directeur du Système d'Information

2 – Méthodologie(s) d'élaboration

Nécessité d'un accompagnement

- Accompagnement du GMSIH dans la définition et la mise en place d'une politique de sécurité des systèmes d'information (40 sites expérimentateurs)
  - sensibiliser et apporter une aide aux établissements de santé participants,
  - tester et valider les outils et méthodes proposés par le GMSIH
  - Opération débute en octobre 2005 pour se terminer en juin 2006
- Livrables - guide PSC-SI
  - Norme de référence ISO/IEC 17799
  - Outil d'auto-évaluation
- Courant 2008 : site pilote dans le cadre du programme d'accompagnement à la mise en œuvre du projet confidentialité

2 – Méthodologie(s) d'élaboration

Démarche méthodologique

- **Phase 0 :** Initialisation
- **Phase 1 :** Autoévaluation
  - Analyser la qualité de la sécurité (niveau de maturité)
  - Analyser les risques (niveau d'exposition de l'établissement aux risques liés au SIH)
- **Phase 1 :** Sélection à partir de l'autoévaluation des principes de sécurité autour desquels seront construits les projets prioritaires susceptibles:
  - De corriger les faiblesses révélées par l'autoévaluation
  - De réduire les risques majeurs pesant sur le système d'information de l'établissement
- **Phase 3 :** Rédaction des règles de sécurité permettant de valider les principes
- **Phase 4 :** Validation et diffusion de la politique de sécurité – Elaborer un plan d'actions

2 – Méthodologie(s) d'élaboration

Organisation en projet PSSI

- Créer une structure dédiée à la gestion de la sécurité des SI, même sans ressource permanente : le comité sécurité
  - Chef de projet désigné
  - Un groupe de travail pluridisciplinaire
- Disposer d'un accompagnement méthodologique : consultant sécurité
- Des outils doivent aider à la définition de la politique de sécurité
- Un calendrier conçu en fonction des étapes de la méthode
- Des livrables identifiés (note de cadrage, synthèse de l'autoévaluation, PSSI, plan d'action)

3- Exemple d’une PSSI

3 – Exemple d'une PSSI

- Exemple de sommaire
  - Partie 1 – Fondements et Éléments stratégiques.
    - Chapitre 1 – Champ d'application de la PSSI.
    - Chapitre 2 – Enjeux et orientations stratégiques.
    - Chapitre 3 – Cadre réglementaire.
    - Chapitre 4 – Échelle des besoins.
    - Chapitre 5 – Expression des besoins de sécurité.
    - Chapitre 6 – Objectifs de sécurité.
  - Partie 2 – Organisation et règles de sécurité
    - Chapitre 7 – Organisation de la sécurité.
    - Chapitre 8 – Règles de sécurité.

3 – Exemple d'une PSSI
Partie 1 : Fondements & éléments stratégiques

- Décrire les domaines d'activités à couvrir.
- Inclure la Note Stratégique de la Direction

« […] La continuité et la qualité des missions de soins, le bon fonctionnement permanent des applications informatiques métiers et de l'infrastructure technique nécessitent une sécurisation croissante de l'information et du système d'information hospitalier (SIH). L'établissement doit assurer :
- la disponibilité constante de son outil informatique dont il est de plus en plus dépendant.
- l'intégrité de l'information stockée et transmise.
- la confidentialité de cette information.

L'établissement se doit également d'assurer l'ouverture et l'interopérabilité de son système d'information en vue des coopérations, des réseaux, de plate-forme(s) de santé et du Dossier Médical Personnel (DMP), ainsi que jusqu'au patient lui-même.

Face à ces défis, la Politique de Sécurité du Système d'Information (PSSI) doit être perçue comme un référentiel de l'établissement, comme une réglementation particulière, dont l'objectif est de décrire clairement la façon de gérer, de protéger, d'accéder et de diffuser les informations et autres ressources sensibles. […] »

3 – Exemple d'une PSSI

Partie 1 : Fondements & éléments stratégiques

➢ Présenter le référentiel légal, réglementaire et contractuel

« […]

•La loi informatique et libertés (CNIL) - Loi 78-17 du 6 janvier 1978 modifiée par la loi n°2006-64 du 23 janvier 2006.

• Les textes relatifs à la cryptologie et à la signature électronique.
  - Les dispositions relatives à la cryptologie,
  - Les dispositions relatives à la signature électronique (Décret n°2001-272 du 30 mars 2001, …)

• Loi du 4 mars 2002 (« Kouchner ») sur les droits des malades a consacré l'obligation d'information des professionnels de santé: «Toute personne a le droit d'être informé sur son état de santé».

• Décret n°2007-960 du 15 mai 2007 relatif à la confi dentialité des informations médicales conservées sur support informatique ou transmises par voie électronique.
  - Sécurisation physique des matériels et locaux et les sauvegardes.
  - Modalités d'accès aux traitements, dont identification et authentification.
  - Contrôle des identifications et des habilitations, avec les traçabilités
  - Garantie de la confidentialité des informations médicales à caractère personnel
  - Obligation d'utiliser la carte CPS pour tout accès aux données de santé à caractère personnel

• « Le fait d'obtenir ou de tenter d'obtenir ces informations [à caractère secret] […] est puni d'1 an d'emprisonnement et de 15.000 Euros d'amende. » Article L.1110-4 du CSP.

3 – Exemple d'une PSSI

Partie 1 : Fondements & éléments stratégiques

- Définir une échelle de mesure permettant une expression objective des besoins de sécurité

Une échelle de mesure est définie permettant l'expression objective des besoins de sécurité. Elle se caractérise par le vecteur sécurité DICP dont les critères de sécurité sont :

- **D**isponibilité :
  Propriété d'un élément essentiel d'être accessible au moment voulu par les utilisateurs autorisés.
- **C**onfidentialité :
  Propriété d'un élément essentiel de n'être accessible qu'aux utilisateurs autorisés.
- **I**ntégrité :
  Propriété d'exactitude et de complétude d'un élément essentiel.
- **P**reuve, Auditabilité, Traçabilité :
  Attribution de la responsabilité d'une action à un utilisateur ou à un système de telle sorte qu'elle ne puisse pas être désavouée par la suite.

Un élément essentiel est une fonction ou une information du système ayant au moins un besoin de sécurité non nul.

3 – Exemple d'une PSSI

Partie 1 : Fondements & éléments stratégiques

- Identifier les besoins de sécurité associés à chaque domaine d'activités.
- Identifier les impacts sur l'établissement

Impacts retenus :
- Atteinte à la qualité des soins.
- Atteinte à la protection de l'information.
- Engagement de la responsabilité.
- Atteinte à l'image de marque.
- Pertes financières.
- ….

Éléments essentiels, stratégiques, à protéger :
- Informations :
  - Données nominatives du personnel (I.RH)
  - Données médicales des patients (I.Medical)
  - Données de gestion financières et comptables (I.Finan)
  - Données de configuration (I.ConfSI)
  - …
- Fonctions :
  - Gestion administrative des agents (F.GRH)
  - Gestion du dossier patient informatisé (F.DPI)
  - Infrastructure de communication et messagerie (F.Communication)
  - Gestion des identifiants (F.Annuaire)
  - …

Informations / Besoins	Disponibilité	Intégrité	Confidentialit	Preuve
I.RH	1	3	3	3
I.Medical	4	4	4	4
I.Finan	1	3	4	3
I.ConfSI	4	3	3	2

3 – Exemple d'une PSSI

Partie 1 : Fondements & éléments stratégiques

- Identifier et caractériser les menaces
  - Liste générique Ebios
- Formaliser les risques et le niveau de criticité

- Définir les objectifs sécurité de l'établissement
  - Reflètent l'engagement de l'établissement pour couvrir les risques.

3 – Exemple d'une PSSI

Partie 1 : Fondements & éléments stratégiques

- Un système d'information gère des Biens. Un Bien est une ressource qui a de la valeur pour l'établissement et qui est nécessaire à la réalisation de ses objectifs.
  - personnels, bâtiments, équipements, informations, …
- Mais les Biens sont sensibles à des Menaces.
  - accidents, erreurs, malveillances, …
- Les Menaces sont liées à des Vulnérabilités du SI.
  - vulnérabilités intrinsèques, bugs, chevaux de Troie, …
- Les Vulnérabilités sont exploitées par des Attaques.
  - internes ou externes
- Des Attaques peuvent provoquer des Dysfonctionnements.
  - déni de service, divulgation d'information, atteinte à l'image, …
- L'estimation du Risque permet d'évaluer la probabilité d'occurrence d'une attaque et l'impact du dysfonctionnement.
  - R = P x I
- L'analyse de risque permet de choisir, de justifier, les Mesures adaptées.
  - Techniques, organisationnelles, assurantielles, juridiques,…

3 – Exemple d'une PSSI

Partie 1 : Fondements & éléments stratégiques

- Exemples de menaces
  - Incendie,
  - Dégâts des eaux,
  - Défaillance de la climatisation,
  - Vol de supports ou de documents,
  - Vol de matériels,
  - Divulgation interne ou externe,
  - Informations sans garantie de l'origine,
  - Piégeage du logiciel,
  - Usurpation de droits,
  - Fraude,
  - Panne matérielle,
  - Saturation du matériel
  - Dysfonctionnement logiciel,
  - Erreur d'utilisation , …

- Exemples de vulnérabilités
  - Absence de matériels de remplacement
  - Matériel disposant d'interface de communication écoutable
  - Utilisation de mots de passe simples
  - Possibilité d'ajout d'un logiciel d'écoute de type cheval de Troie
  - Absence de conservation des traces des traitements
  - Possibilité d'administrer le système à distance
  - Absence de dispositif de chiffrement des communications
  - Absence de politique de sauvegarde
  - Absence de plan de secours
  - Absence de politique de sécurité, …

- Exemples technique d'attaques
  - Interception de signaux
  - Cheval de Troie
  - Virus
  - Usurpation d'identité, de droits
  - Cryptanalyse,…

3 – Exemple d'une PSSI

Partie 1 : Fondements & éléments stratégiques

- Formaliser les risques et le niveau de criticité

Famille de risques	Risque (Menace)	Probabilité				Impact				Criticité			
		1	2	3	4	1	2	3	4	1	2	3	4
Atteinte à l'intégrité physique des composants du système	R.Incendie (01)	X							X				**X**
	….												
Perturbation du fonctionnement des composants du système	R.Clim (11)		X					X				**X**	
	R.SaturSI (30)		X				X				**X**		
	….												
Utilisation malveillante du système	R.UsurpDroits (40)			X				X				**X**	
	R.RenieActions (41)	X						X			**X**		
	….												
Compromission des fonctions et des informations relatives à des données privées ou médicales	R.Ecoute (19)	X					X				**X**		
	R.DysfLog (31)		X				X				**X**		
	….												

3 – Exemple d'une PSSI

Partie 1 : Fondements & éléments stratégiques

- Définir les objectifs sécurité de l'établissement

O.ConfDonnees	**La confidentialité des données médicales à caractère personnel et des données privées des agents doit être absolument garantie.**
Cet objectif porte sur le respect de la confidentialité des données d'ordre privé ainsi que les données médicales. L'établissement doit absolument garantir la confidentialité et l'intégrité de ces données qui ne lui appartiennent pas.	

O.PhySI	**L'accès aux salles informatiques et aux locaux techniques doit être protégé contre toute malveillance.**
Cet objectif porte sur l'intégrité physique des salles informatiques et des locaux techniques associés. L'accès à certaines zones ne peut s'effectuer que sur un contrôle renforcé. Ces accès sont réservés aux personnes habilitées.	

3 – Exemple d'une PSSI

Partie 2 : Organisation et règles de sécurité

- Définir l'organisation en charge de la sécurité de l'information, et le rôle de chacun des acteurs.

L'organisation propre à la sécurité de l'information de l'établissement se compose des fonctions suivantes :
- Le Responsable de la sécurité de l'information (RSSI),
- Le Comité de Sécurité,
- Les Responsables opérationnels,
- Les Référents utilisateurs,
- L'expertise externe,
- L'Audit,
- …

Le RSSI a pour rôle :
- Définition et contrôle de l'application de la PSSI,
- Définition et mise en œuvre du PCA,
- Définition du plan sécurité pluriannuel,
- Sensibilisation et promotion de la sécurité de l'information auprès des utilisateurs et des responsables métiers.
- Relation avec la Direction et les responsables métiers (tableaux de bord, niveau de sécurité,…)
- Veille, dont CERT/A, […]

Le Comité Sécurité a pour rôle de :
- valider et approuver la PSSI,
- établir et évaluer le plan d'actions pluriannuel,
- s'assurer de la mise en application des règles de la PSSI,
- organiser la réaction nécessaire en cas d'incidents de sécurité afin de garantir la disponibilité du système d'information, […]

3 – Exemple d'une PSSI

Partie 2 : Organisation et règles de sécurité

Utilisateurs

Comité sécurité

Plan
Identification des objectifs

Act
Amélioration des pratiques

Management de la sécurité de l'information

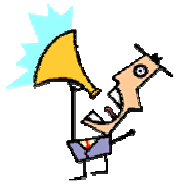
Do
Définition et mise en oeuvre

Check
Supervision et vérification

Audit externe

RSSI

Correspondants sécurité



Contrôle interne

Responsables opérationnels

3 – Exemple d'une PSSI

Partie 2 : Organisation et règles de sécurité

- Instancier les principes de sécurité en règles de sécurité propres au contexte et à l'analyse du système

Les principes et règles de sécurité sont issus de la norme ISO27002 :

1. Politique de sécurité
2. Management de la sécurité
3. Inventaire et classification des biens
4. Sécurité et ressources humaines
5. Sécurité physique et environnementale
6. Exploitation informatique et gestion des réseaux
7. Contrôle d'accès logique
8. Intégration, développement et maintenance des applications et systèmes
9. Gestion des incidents liés à la sécurité de l'information
10. Gestion de la continuité des activités
11. Conformité

3 – Exemple d'une PSSI

Partie 2 : Organisation et règles de sécurité

4 – Sécurité et ressources humaines

→ *Sensibiliser, responsabiliser et impliquer les utilisateurs du SI à la sécurité de l'information*

5 – Sécurité physique et environnementale

→ *Empêcher tout accès physique non autorisé, tout dommage, vol ou intrusion.*

7 – Contrôle d'accès logique

→ *Maîtriser l'accès à l'information et les accès utilisateurs par le biais d'autorisations.*

9 – Gestion des incidents liés à la sécurité de l'information

→ *Garantir une gestion cohérente et efficace des incidents, et la mise en œuvre d'actions correctives*

10 – Gestion de la continuité des activités

→ *Protéger les processus métiers les plus sensibles contre toute interruption*

11 – Conformité

→ *Éviter toute violation des obligations (légales, réglementaires, contractuelles, …)*

3 – Exemple d'une PSSI

Partie 2 : Organisation et règles de sécurité

7 – Contrôle d'accès logique

7.1 Expression des exigences métiers de contrôle d'accès

7.2 Gestion des accès utilisateurs

7.3 Responsabilités des utilisateurs

7.4 Contrôle d'accès au SIH

7.5 Contrôle d'accès aux applications

7.6 Postes nomades et accès distants

3 – Exemple d'une PSSI

Partie 2 : Organisation et règles de sécurité

7 – Contrôle d'accès logique

Règle : xxx	**Identification et authentification des utilisateurs**

Tous les accès des utilisateurs au système d'information doivent être identifiés et authentifiés.
A minima, le procédé d'authentification repose sur l'usage d'un mot de passe statique.
L'accès à des informations sensibles ou confidentielles doit reposer sur un moyen d'authentification renforcé (certificat logiciel, carte matricielle, …) ou forte (carte à puce, clé USB, …).
Cependant, tout accès à des données de santé à caractère personnel doit être réalisé avec une Carte de Professionnel de Santé.
Les accès distants au SI doivent mettre en œuvre un procédé d'authentification renforcée ou d'authentification forte.
En cas d'échec de l'authentification, le système ne doit fournir aucune information explicite relatif à l'échec de l'utilisateur.

Règle : xxx	**Élaboration et gestion des mots de passe**

L'élaboration d'un mot de passe statique utilisateur doit répondre aux critères suivants :
1. La longueur minimale d'un mot de passe est de 8 caractères.
2. Le mot de passe contient des lettres minuscules, majuscules et des chiffres. Il peut également contenir des caractères spéciaux.
3. Le mot de passe ne doit pas être trivial (pas le nom de famille, pas le prénom de ses enfants, pas le numéro et le nom de sa rue, pas un mot du dictionnaire,…).
4. Il est conseillé, aux utilisateurs, d'élaborer un mot de passe facile à retenir par eux-mêmes (exemple par anagramme).
5. Un ancien mot de passe ne doit pas être réutilisé. Un historique gère les changements de mot de passe sur une périodicité de 5 changements.
6. La périodicité de changement d'un mot de passe est de 3 à 6 mois.
7. Les mots de passe relatifs aux activités professionnelles doivent être différents de ceux relatifs aux activités extraprofessionnelles.[…]

3 – Exemple d'une PSSI - EPSM Morbihan
Le Périmètre

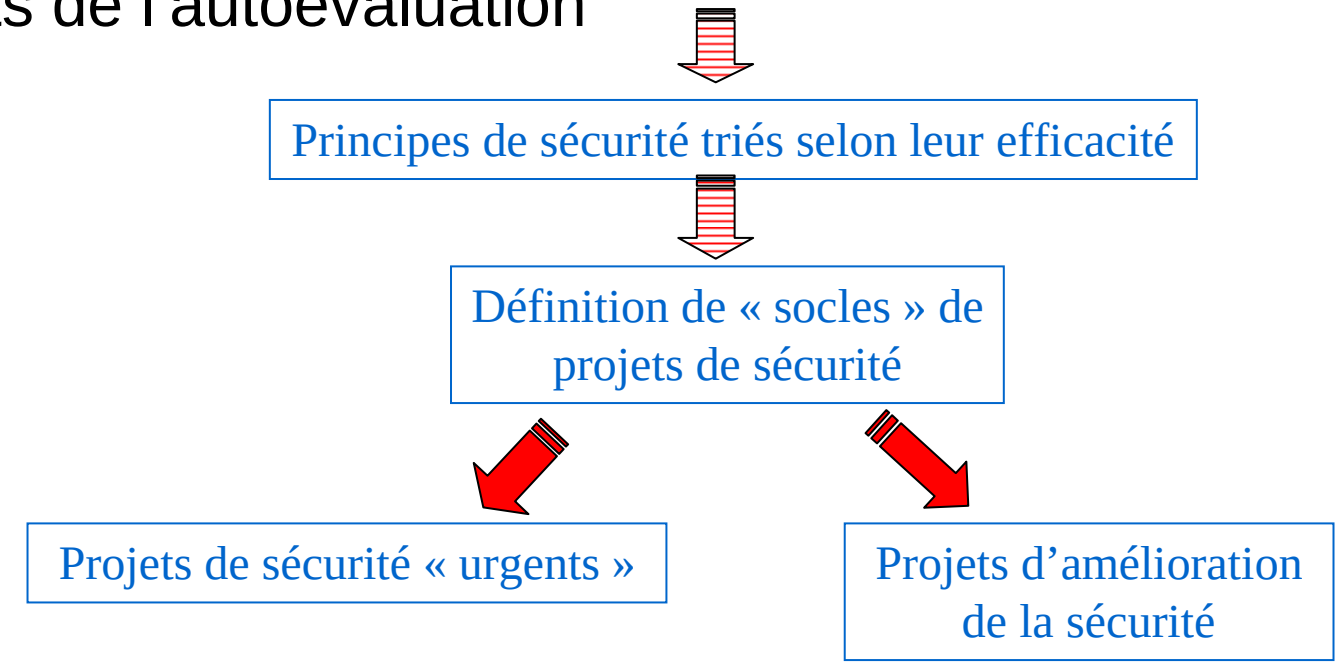
- Sécurité physique et environnementale
  - Sécurité incendie/dégâts des eaux …..
- Protection de l'infrastructure
  - Disponibilité
  - Accès au système d'information
- Continuité des activités
  - Anticiper les perturbations d'activité/situation d'urgence
  - Sauvegarde de recours
- Collaboration
  - Favoriser la communication des données
  - Conformité au cadre juridique avant des phases dématérialisation
- Vie privée
  - Traçabilité, imputabilité
- ……

Le cadre de référence de la PSC propose 39 principes directeurs déclinés en 168 règles générales et regroupés en 10 chapitres,

- 2 pour le volet organisationnel
- 8 pour le volet maîtrise des risques

3 – Exemple d'une PSSI - EPSM Morbihan
Principes opérationnels

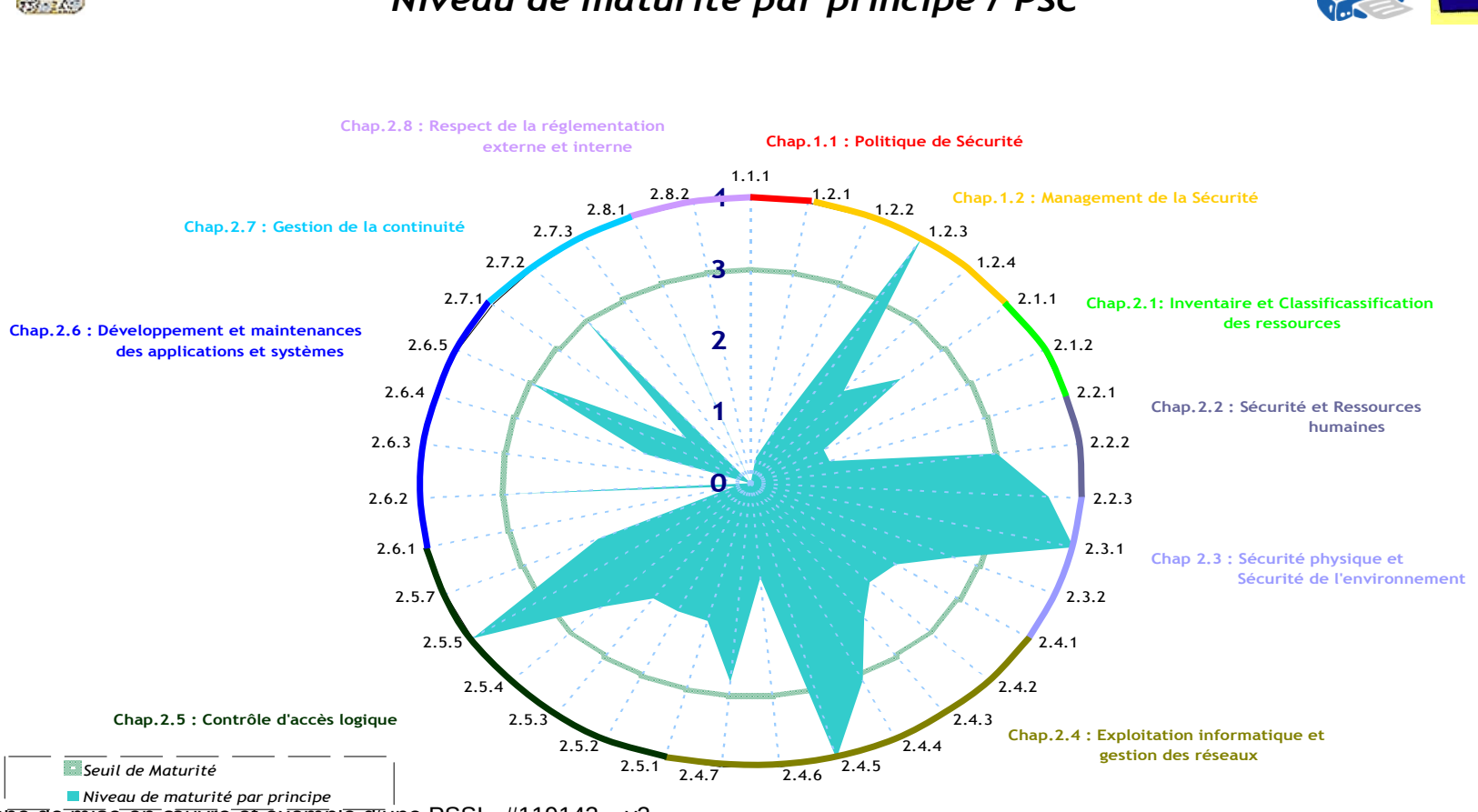
- Revue de l'organisation sécurité de l'établissement sur le plan stratégique, organisationnel et technique
  - 100 questions soumis au groupe de travail
- Résultats de l'autoévaluation



❑ Orienter l'établissement dans la construction de son plan d'actions prioritaires permettant de réduire les risques mis en évidence

3 – Exemple d'une PSSI - EPSM Morbihan
Principes opérationnels : Autoévaluation

- Résultats chiffrés (de 0 à 4) de l'état des lieux représentant la maturité des principes de l'établissement



3 – Exemple d'une PSSI - EPSM Morbihan
Exemple : règles de sécurité issues de la PSSI

- Principes : Contrôle d'accès logique 2.5
  - Principe 2.5.2 gestion des accès des utilisateurs
    - L'accès au SIH ne peut être réalisé que par des utilisateurs habilités.
  - Principe 2.5.3 : responsabilité des utilisateurs
    - L'établissement prend les mesures de sécurité nécessaires au contrôle de l'accès aux informations…

- Règles 2.5.1.X : registre des utilisateurs
  - L'établissement définit et diffuse une procédure formalisée pour l'enregistrement initial des utilisateurs ainsi que pour la révocation de leurs droits.
    - Utilisation d'identifiants uniques et non redondants, propres à chaque utilisateurs
    - Vérification des habilitations
    - Remise d'une charte de l'information…..

3 – Exemple d'une PSSI - EPSM Morbihan
Exemple : actions sécurité issues de la PSSI

Les enjeux majeurs

❑ Mise en oeuvre d'une architecture de sécurité pour l'accès au SIH dans le cadre du décret confidentialité

Les axes de travail

- Mise en œuvre d'un média d'authentification
- Mise en œuvre d'un référentiel d'identité basé sur un annuaire d'établissement (AES) centralisant les données liées aux personnes et aux structures - Alimentation /synchronisation RPPS
- Déployer une solution à valeur ajoutée comme l'authentification unique (Single Sign-On) couplée avec un annuaire d'établissement
- Mise en œuvre d'une stratégie de sécurisation - plan de continuité d'activité : PCA

3 – Exemple d'une PSSI - EPSM Morbihan
Éléments de réflexion

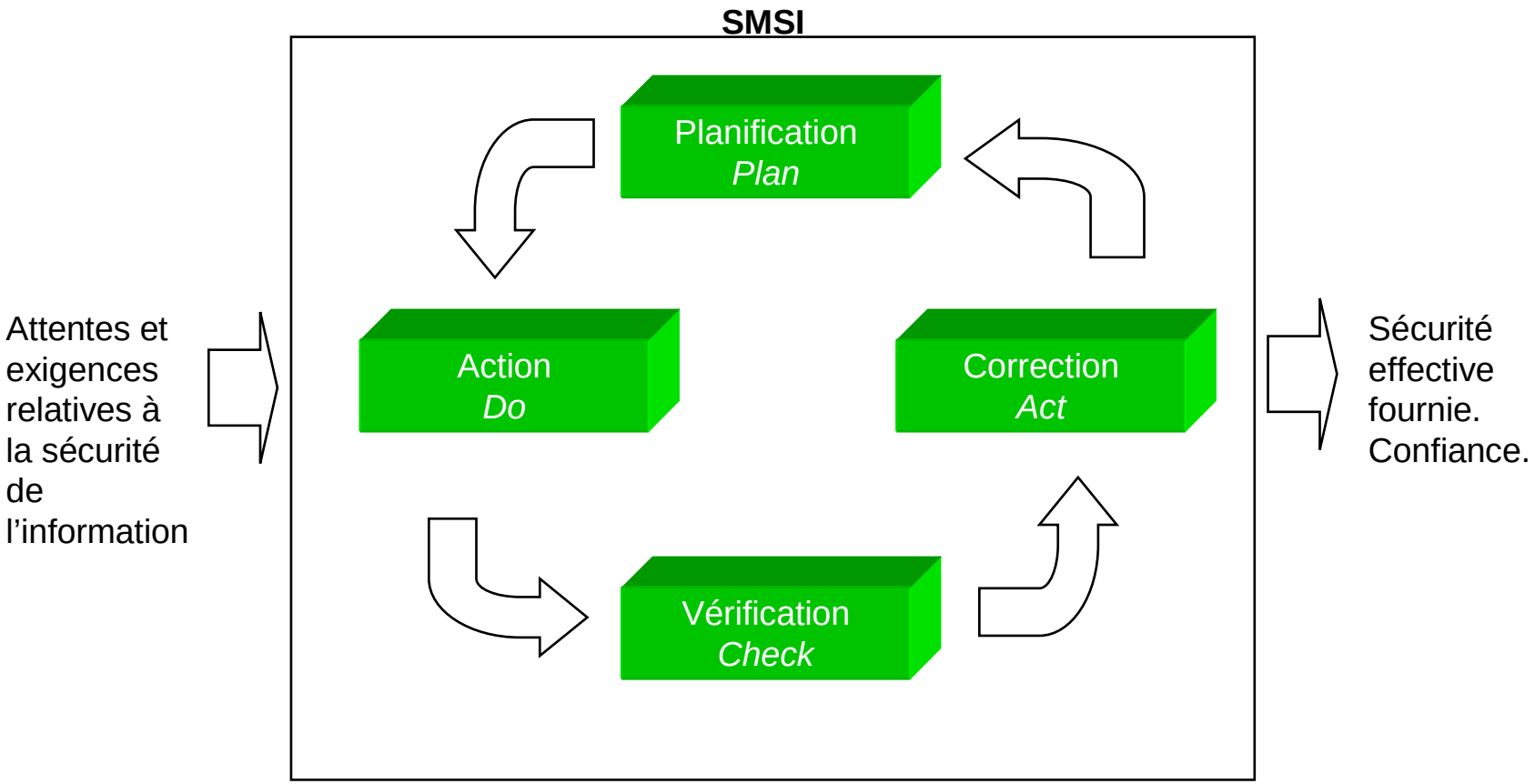
- Points faibles :
  - Motivation des participants
  - Ressources informatiques limitées
- Préalable au plan d'action : nommer un RSSI pour de s'assurer de la continuité/cohérence de la vision « sécurité » sur l'ensemble des activités/projets
- Commencer par la rédaction d'une politique de sécurité, qui va permettre de décrire les grands principes guidant la sécurisation du SI (et en particulier son cadre réglementaire et juridique), ainsi que son organisation.
- Réalisation préalable d'une analyse des risques SSI facilite l'élaboration d'une PSSI (méthode EBIOS)

4- Management de la sécurité

4 – Management de la sécurité

- Système de management de la sécurité de l'information – ISO27001
  - Spécifier les exigences pour la mise en place de mesures de sécurité
    - Adaptées aux besoins de l'organisation
    - Adéquates et proportionnées.
  - Afin de
    - Fournir une protection des biens et du patrimoine de l'établissement.
    - Apporter la confiance aux parties prenantes
  - Principe de facteurs d'amélioration : PDCA (Plan, Do, Check, Act)
  - Ensemble Bonnes pratiques
    - Mesures de sécurité : ISO27002 (ex ISO17799)
  - En outre, le RGS (Référentiel Général de Sécurité) fera référence à l'ISO27001

4 – Management de la sécurité



4 – Management de la sécurité

- Sensibilisation des acteurs
  - « L'efficacité des mesures de sécurité reste dépendante des individus. »

  - Formation et communication
    - A la sécurité, par rapport au contexte métier de chacun.
    - Aux outils et aux fonctions offertes
      - Message électronique sécurisée : signature électronique, chiffrement des messages
      - Carte CPS
      - …

    - Charte des bons usages
      - Règles de bonne utilisation des ressources du SI
      - Relève du bon sens
      - Assurer le bon fonctionnement du SI pour chacun dans le respect de l'éthique et de la loi
      - Droits et devoirs de la direction, des administrateurs et des utilisateurs
      - Information claire sur les sanctions

    - Sensibilisation lors de la Journée des nouveaux arrivants

5 – Conclusion / Valeur ajoutée de la SSI

5 – Conclusion / Valeur ajoutée de la SSI

- PSSI – Politique de Sécurité des Systèmes d'Information

  → Document fondateur d'une démarche de SSI.

  - Disposer d'un cadre de référence et de cohérence pour l'ensemble des activités et des acteurs de l'organisme.
    - Mettre en évidence des objectifs de sécurité, des obligations, les biens sensibles et des engagements de l'établissement.
    - Exprimer les responsabilités, les principes et règles de sécurité à respecter.
    - Informer et sensibiliser les acteurs concernés.
  - Élaborer un Espace de confiance
    - Confiance dans l'identité des personnes.
      - Savoir qui est qui.
    - Confiance dans la qualification des personnes.
      - Reconnaître les rôles et les habilitations de chacun.
    - Confiance dans l'information, en terme d'intégrité et de qualité.
      - Avoir confiance dans l'échange et la finalité du traitement.
    - Confiance par rapport aux agressions externes, inviolabilité de l'espace.
      - Se protéger des agressions externes.

5 – Conclusion / Valeur ajoutée de la SSI

- Considérer la sécurité de l'information comme une valeur ajoutée dans la réalisation des processus métiers.

  - Avoir une démarche méthodique (justifiable), mais rester pragmatique.
    - Permettre une structuration des actions sur la durée
    - Être dans une démarche de conformité d'une norme ou d'un référentiel.
    - Établir des mesures de sécurité en fonction de besoins identifiés.
  - Impliquer les acteurs clés de l'établissement.
    - Projet d'établissement
  - Établir un projet sécurité de l'établissement
    - Les normes et référentiels ne donnent pas la solution
  - Être dans une démarche de management de la sécurité
  - Être conscient des obligations, des responsabilités et de l'intérêt du patient.
  - Sensibiliser le personnel sur la valeur de l'information manipulée, et de l'engagement de l'établissement et personnel sur les opérations effectuées.
  - Considérer que le projet de sécurité de l'information est une valeur ajoutée du système d'information.

5 – Conclusion / Valeur ajoutée de la SSI

- Projet très vaste , couvrant de nombreux domaines
- Sujet nouveau
- Compte tenu de la diversité des risques et des environnements informatiques,il n'y a pas de solution toute faite
- Culture sécurité à développer
- Évolution budgétaire modérée
- Opportunités plan hôpital 2012

Merci de votre attention …