PSSI générique et management de la sécurité

Dominique Launay
Pôle SSI RENATER

Séminaire AMUE
28 Novembre 2012, Paris

agenda

- introduction au projet PSSI générique
- introduction aux normes ISO 2700x
- la PSSI et les normes 2700x
- l'organisation de la SSI dans un monde idéal
- dans notre monde (un monde pas encore idéal)
- l'apport de RENATER

Le projet PSSI générique

- PSSI = Politique de Sécurité des Systèmes d'Informations
- exécuté en 2010
- un document :
  - stratégique
  - acceptable par un établissement d'enseignement supérieur
  - adaptable
- une méthode :
  - EBIOS (Évaluation des Besoins et Identification des Objectifs de Sécurité)

Le projet PSSI générique (2)

- compatibilité avec les normes :
  - évaluer les risques : identifier des mesures à prendre à partir des besoins de sécurité
  - se référer aux mesures existantes dans les normes 27000 en les déclinant en règles
  - gérer la sécurité de l'information comme un processus
- réaliste et exhaustif :
  - mener l'étude sur plusieurs établissements

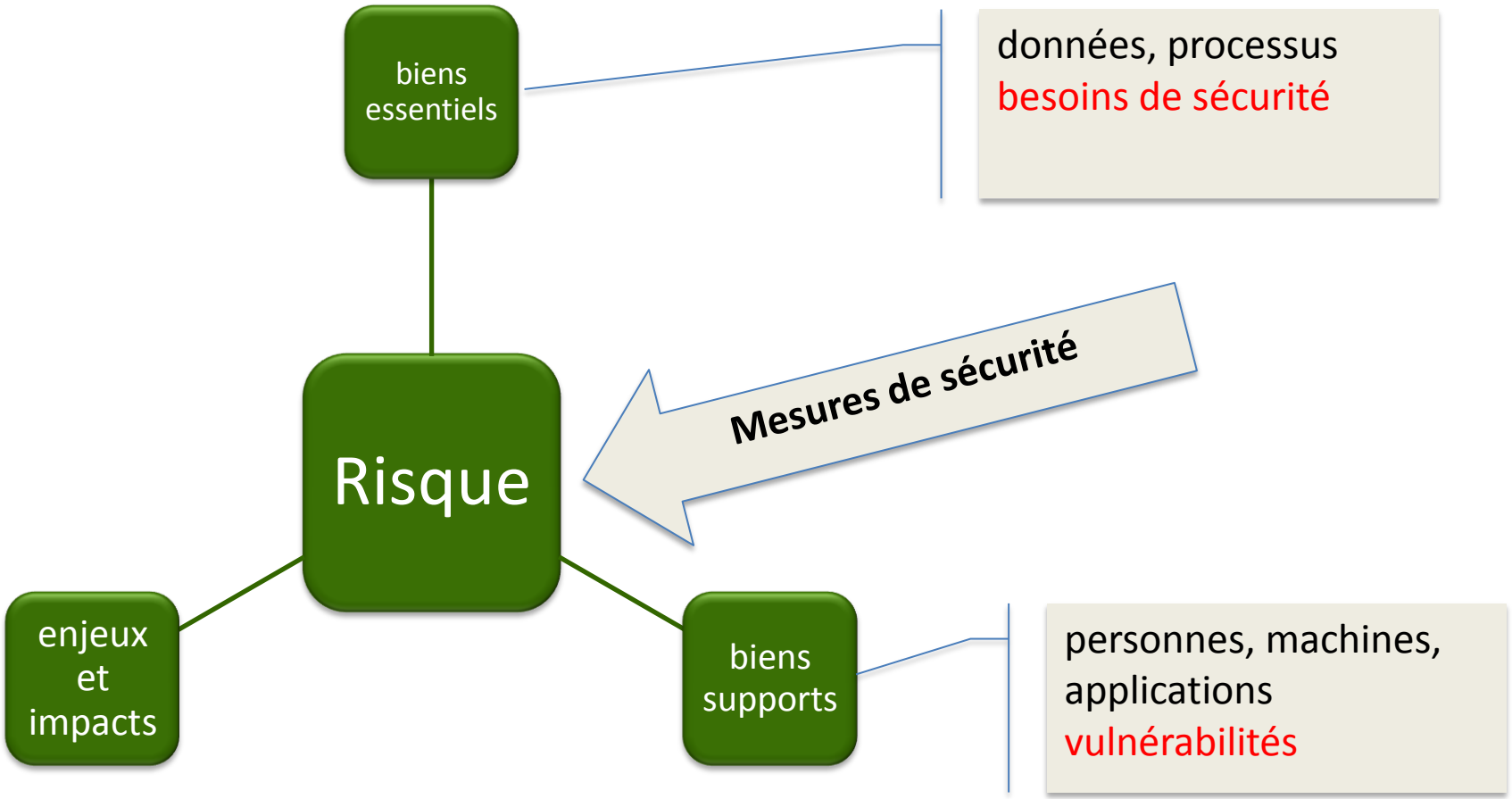
Appréciation des risques

- étude du contexte (enjeux stratégiques d'un établissement, ses biens, ses processus, ses biens supports)
- étude évènements redoutés :
  - quels sont les besoins en disponibilité, confidentialité, intégrité et preuve des données et processus
- étude des scénarios de menaces :
  - quel est la vraisemblance des menaces qui pèsent sur les biens supports ?

Appréciation des risques (2)

- objectifs de sécurité :
  - évaluation des risques et détermination de la stratégie de traitement du risque (hiérarchiser les priorités)
- étude des mesures :
  - quelles mesures prendre en fonction de cette stratégie ?

Appréciation des risques (3)



Bénéfice attendu

- l'analyse en parallèle de sept établissements sur un même référentiel pour :
  - valider l'expression d'axes stratégiques communs
  - valider l'expression de besoins de sécurité communs
  - valider la méthodologie
- répondre à la question « par où commencer ? »

les établissements pilotes

- Les établissements concernés:
  - Université Rennes 1
  - UNR-RUNN
  - Université de Limoges
  - Université de la Méditerranée
  - Grenoble Université
  - Université Nancy
  - Université de Bordeaux 1

Les documents génériques

- rédigés par le prestataire Fidens et remis en forme par le GT-PSSI
- documents quasiment utilisables tels quels
- certains chapitres sont à adapter à votre établissement :
  - nom de l'établissement
  - enjeux et missions
  - certaines dénominations
  - …
- ils doivent être approuvés par la gouvernance (par exemple le CA)

Les documents génériques (2)

- PMSI : politique de management de la sécurité de l'information (ou politique de gouvernance de la sécurité de l'information) :
  - document décrivant l'organisation de la SSI dans votre établissement (instances de révision, veille, etc.)
  - document d'une vingtaine de pages
- PSSI : politique de sécurité du système d'information :
  - document recensant l'ensemble des règles de sécurité à mettre en œuvre et validées par le chef d'établissement
  - document d'une soixantaine de pages

les normes ISO 27000

- ISO 27001 :
  - définition d'un SMSI (système de management de la sécurité de l'information)
- ISO 27002 :
  - guide des bonnes pratiques de SSI
  - 133 mesures à adapter à votre environnement
- ISO 27005 :
  - normalisation du cadre de l'appréciation des risques

La PSSI et ces normes

- La PSSI générique implémente les mesures de la 27002 couvrant ou réduisant des risques identifiés
  - risques identifiés par une analyse de risques
- nécessité de l'adéquation avec la 27001
  - acquisition d'une culture de la gestion du risque
- ➔Politique de management de la sécurité

Exemples

Classification des biens

[ISO 27001 - A 7.2.1] Lignes directrices pour la classification

[GDB_01] Plan de classification

- Un plan de classification est défini au niveau de l'établissement pour hiérarchiser les niveaux de protection et gérer les biens conformément aux besoins de sécurité identifiés.
- Ce plan de classification définit les échelles de sensibilité à partir des critères confidentialité, intégrité, et disponibilité.

Exemples (2)

Inventaire des biens

[ISO 27001 - A 7.1.1] Inventaire des biens

[GDB_02] Identification et inventaire des biens sensibles

- On qualifie de « bien sensible » toute composante qui traite d'information ou de fonction de niveau 2 selon le plan de classification. On appelle « critique » un bien supérieur au niveau 3 selon le plan de classification.
- Les biens sensibles participant au fonctionnement du système d'information (informations, biens logiciels, biens physiques, services, etc.) sont inventoriés par domaine. Chaque bien recensé fait l'objet d'une identification renseignant le niveau de classification (établi sur la base du plan mentionné ci-dessus), son détenteur ou responsable, et les personnes qui y ont accès (pour les données).
- Un extrait de l'inventaire est réalisé afin d'identifier les biens « critiques » parmi l'ensemble des biens constituant le système d'information de manière à pouvoir protéger les éléments vitaux de l'organisme identifiés en cas de sinistre majeur.

Exemples (3)

Utilisation de matériel hors des locaux

[ISO 27001 - A 9.2.5] Sécurité du matériel hors des locaux

[NOMAD_05] Dispositifs de sécurité installés sur les nomades

- Tout poste nomade comprend par défaut :
  - Un antivirus / anti-spam.
  - Un logiciel de chiffrement de disque et/ou des fichiers.
- Selon les besoins identifiés et les informations traitées, des configurations durcies peuvent être mises à disposition des usagers : authentification forte pour la connexion au poste, outil de sécurisation de la connexion VPN, outil de chiffrement des disques durs, support amovible sécurisé, outil de contrôle de double connexion.

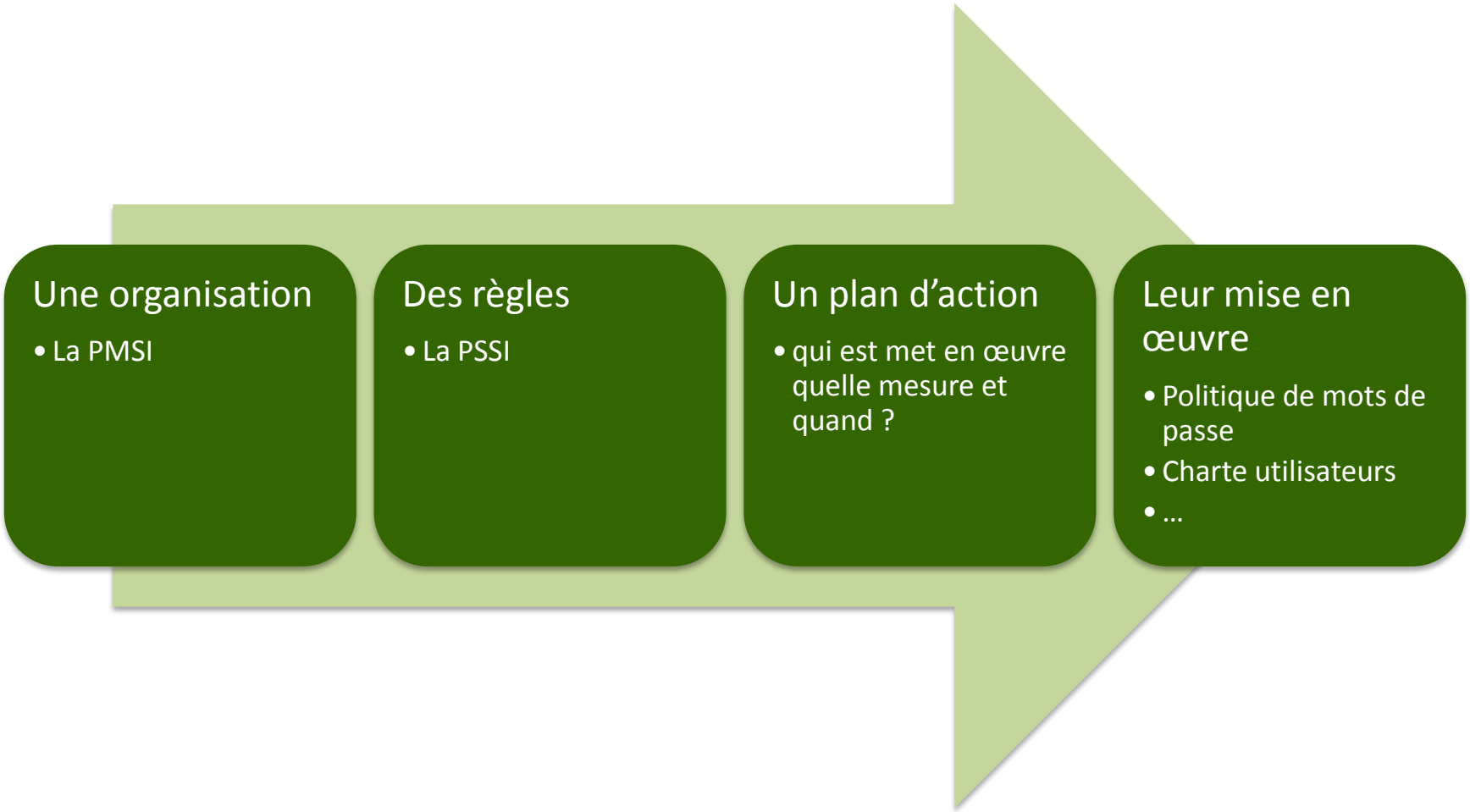
pourquoi une PMSI ?

- la sécurité est un processus avec tous ses attributs :
  - cahier des charges
  - validation hiérarchique
  - vérification de conformité
  - amélioration
- il doit s'insérer dans l'organisation des métiers de l'établissement
- sa gestion doit être formalisée et avalisée par la gouvernance

pourquoi une PMSI ?

- la PMSI définit l'organisation qui encadre l'évolution et la mise en œuvre des mesures définies dans la PSSI
- cette organisation permet d'évaluer la pertinence des mesures (efficacité, applicabilité, impacts organisationnels ou financiers…)
  - organisation pérenne, pas un projet
- si vous n'avez pas de PSSI, vous avez tout de même des mesures de sécurité à différents niveaux

organisation générale



Plan de la PMSI

- 1. Introduction
- 2. Contexte
- 3. Grands principes
  - 3.1. Principes de gouvernance
  - 3.2. Principes de sécurité
- 4. Gestion des risques
  - 4.1. Stratégie
  - 4.2. Critères
  - 4.3. Audit et contrôle

Plan de la PMSI (2)

- 5. Organisation de la sécurité
  - 5.1. Le Comité de Pilotage Stratégique
  - 5.2. Le Comité de Sécurité Opérationnelle
  - 5.3. Les comités de liaison
  - 5.4. Fonctions présentes aux comités
  - 5.5. Rôles et responsabilités
- 6. Mesure et amélioration de la sécurité
  - 6.1. Amélioration du niveau de sécurité
  - 6.2. Amélioration du processus SMSI
  - 6.3. Gestion du document de politique SMSI

gérer la sécurité

- connaître son périmètre ;
- connaître les enjeux de son établissement ;
- connaître les mesures mises en œuvre ;
- formaliser toutes les procédures (PRA, politique de mots de passes, inventaires,…) ;

gérer la sécurité

- connaître les responsabilités :
  - qui est responsable de la mise en œuvre d'une mesure donnée ?
  - qui prévenir en cas de difficulté de mise en œuvre d'une mesure ? (pertinence, contraintes trop grandes pour les utilisateurs,…)
  - qui décide de l'évolution d'une mesure ?
- connaître le contexte légal et réglementaire

organisation introduite par la PMSI générique

- définition des comités
- définition des fonctions présentes dans ces comités
- définition des rôles et responsabilités

dans un monde idéal

- appui de votre hiérarchie
- une PSSI approuvée par votre chef d'établissement
- une gestion de la sécurité en amélioration continue : mise en œuvre de la PMSI

un projet approuvé et compris par tous

Les comités

Comité de pilotage stratégique	• valide et gère la SSI (PSSI, documents d'application) • 1 réunion par an
Comité de sécurité opérationnel	• évolution de la PSSI, analyse et traitement des risques • processus de suivi • 3 à 4 réunions par ans
Comité de liaison	• relais des décisions de sécurité vers les composantes • gestion des incidents • réunions régulières

le comité de pilotage stratégique

- gère la mise en œuvre de la SSI dans l'établissement :
  - conçoit et promeut la PSSI
  - approuve le plan de traitement des risques
  - valide les actions de sensibilisation
- orientation claire et soutien de la direction
- constitution (rôles) :
  - chef d'établissement
  - DSI
  - RMSI (responsable management de la SSI)=> peut être le RSSI
  - RSSI
  - DRH
  - FSD
  - CIL et service juridique
  - Ingénieur Hygiène et sécurité
- se réunit au minimum une fois par an

comité de sécurité opérationnelle

- coordonne les activités quotidiennes liées à la sécurité :
  - appréciation du risque
  - pilotage et suivi les plans d'action (ex: tableaux de bord)
  - suivi des incidents de sécurité
  - prise en compte des évolutions et des nouveaux besoins
    - anticipation
- relai des décisions du comité de pilotage stratégique
- constitution :
  - RSSI
  - DSI
  - correspondants sécurité métier
  - un représentant RH
  - représentant service juridique
- se réunit au minimum 3 fois par an

comités de liaison

- organisés par le RSSI au sein de chaque composante
- pilotent les projets de sécurité
- recueillent les problématiques d'implémentation, les incidents et informations d'état de la sécurité
- remontent au niveau du comité de sécurité opérationnel les besoins de sécurité des composantes

dans un monde pas encore idéal

- votre établissement n'a pas encore de PSSI
- votre structure est petite et il est difficile :
  - de mobiliser l'énergie nécessaire à la gestion d'un tel projet
  - de formaliser une telle organisation
- vous ou votre direction pensez que la SSI est une affaire de technicien

(barrez les mentions inutiles)

ce que vous pouvez faire

- une PSSI peut se construire pas à pas
  - des mesures de sécurité existent et se retrouvent dans la charte
  - ces mesures peuvent être améliorées
  - vous pouvez adopter de nouvelles mesures
  - les UMR ont elles aussi des mesures héritées de leurs différents organismes de tutelle

C’est déjà un embryon de SMSI !

comment le faire ?

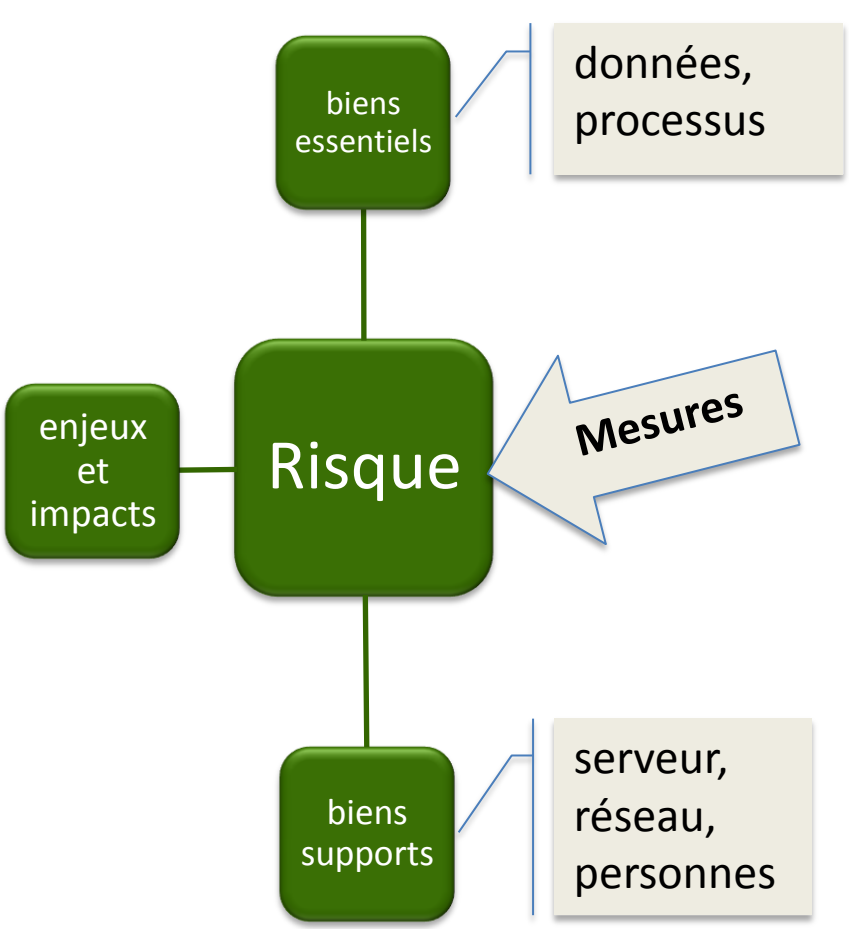
- l'organisation **proposée** dans la PMSI concerne des rôles, pas des fonctions :
  - elle peut être adaptée à votre structure
  - mais certains rôles et fonctions peuvent être incompatibles
- il y a probablement des correspondants informatiques dans les différentes composantes
- les composantes de votre établissement sont parfois des UMR : une organisation existe probablement dans leur organisme de tutelle, n'hésitez pas à l'intégrer à la vôtre

ce qui est important

- la PSSI est un outil de communication et d'affirmation d'une politique, pas une finalité
- ne jamais oublier ce qu'il faut protéger et pourquoi
- l'important est de gérer la sécurité, de l'améliorer et d'avoir la **légitimité**
- une bonne gestion étant bien documentée (mais pas trop) … la PSSI en découlera naturellement

Des établissements l'ont fait : pourquoi pas vous ?

les deux diapositives à retenir



nos services et votre organisation

- organisation SSI :
  - intranet des RSSI et espace PSSI
  - accessible aux RSSI
  - https://services.renater.fr/ssi/rssi/
- information juridique liée à la SSI :
  - intranet SSI juridique
  - accessible à tous les correspondants sécurité (parrainage par le RSSI) : abonnement à la liste ecorses@groupes.renater.fr
  - https://services.renater.fr/ssi/juridique/
- sécurité opérationnelle : CERT RENATER
  - https://services.renater.fr/ssi/cert/