PSSI générique et management de la sécurité

Dominique Launay
Pôle SSI RENATER

Séminaire des correspondants Sécurité
13 juin 2012, Strasbourg

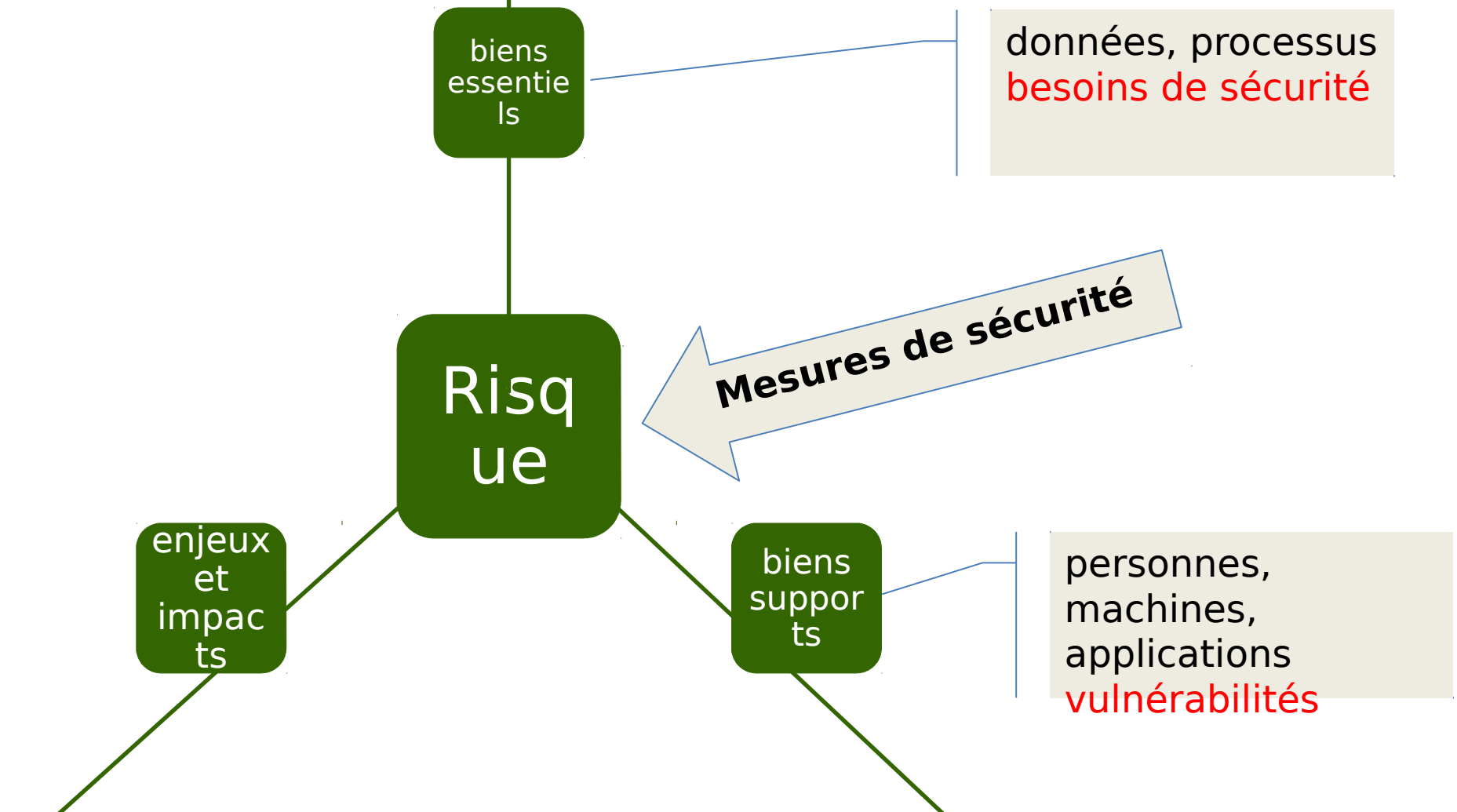
agenda

- 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

rappel du projet

- exécuté en 2010
- objectifs :
  - fournir une PSSI utilisable par les établissements d’enseignement supérieur
  - adaptable
  - basé sur les normes ISO2700x
- mode opératoire :
  - analyses de risques => identifier les mesures couvrant des risques réellement identifiés
  - sept établissements d’enseignement supérieur

appréciation des risques



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 :
  - méthode d’appréciation des risques

les normes ISO 27000 (suite)

- ISO 27003 :
  - implémentation d’un SMSI
- ISO 27004 :
  - indicateurs du SMSI

La PSSI et ces normes

- La PSSI générique implémente les mesures de la 27002 couvrant ou réduisant des risques identifiés
- nécessité de l’adéquation avec la 27001
- ¤¤ Politique de management de la sécurité

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…)
- si vous n’avez pas de PSSI, vous avez tout de même des mesures de sécurité à différents niveaux

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

Les comités

Comité de pilotage stratégique	• valide et gère la PSSI • 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 (tableaux de bord)
  - suivi des incidents de sécurité
  - prise en compte des évolutions et des nouveaux besoins
- 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
- votre hiérarchie ne se sent pas concernée/impliquée (barrez la mention inutile)

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

C’est déjà un embryon de SMSI !

comment le faire ?

- l’organisation **proposée** dans la PMSI concerne des rôles, pas des fonctions :
  - vous pouvez l’adapter à votre structure
- vous êtes correspondant SSI dans votre établissement
- vous avez des correspondants informatiques
- vous avez l’organisation du CERT OSIRIS :
  - mutualisation de l’expérience
  - acceptée par votre gouvernance
  - réactivité

ce qui est important

- la PSSI est un outil de communication et d'affirmation d'une politique, pas une finalité
- l'important est de gérer la sécurité, de l'améliorer et d'avoir la légitimité
- une bonne gestion étant bien documentée … la PSSI en découlera

Des établissements l'ont fait : pourquoi pas vous ?

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
  - attention : autorisation basée sur l'adresse email !
  - https://services.renater.fr/ssi/juridique/
- sécurité opérationnelle : CERT RENATER
  - https://services.renater.fr/ssi/cert/