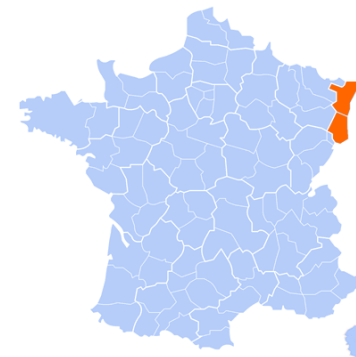




Mise en œuvre de la PSSI dans les unités

Site pilote
Délégation Régionale
ALSACE



05 avril 2007 : Lancement de la PSSI à la Délégation Alsace

Joseph ILLAND - Robert LONGEON
les membres de la CRSSI locale
le RSSI de l'Université (cotutelle)
5 directeurs d'unité

Quelques Réactions pendant la réunion

RSSI de l'Université:

« Votre projet est très séduisant, maintenant il reste à voir comment le mettre en œuvre et voir les effets produits concrètement sur le terrain »

Directeurs :

« Le labo vient d'acquérir un firewall récemment, nous sommes protégés »

« Je veux bien accepter une X-ième casquette mais dites-moi ce que je dois faire, comment je dois le faire et avec qui je dois le faire »

« C'est une charge supplémentaire, s'il faut le faire, on va le faire »

« Je crains que ce projet ne soit une boîte de Pandore. Priorité à mon travail scientifique »

« Je veux bien le faire mais je n'ai personne à mettre dessus et mon informaticien est déjà débordé »

« Il faut mutualiser tout ça. D'ailleurs le CRI s'en occupe déjà... »

18 juin 2007 : Demande de nomination CSSI aux directeurs

Envoi d'un courrier à tous les directeurs

En liaison avec les cotutelles : Accord dans le contrat quadriennal

Profil CSSI :

Pas forcément l'ASR (directeur adjoint, secrétaire général etc.) même si l'ASR fait forcément partie du processus.

Etat des nominations CSSI :

La moitié des laboratoires ont désigné un CSSI (sans relance) :

60 % de CSSI nommés dans les unités sensibles (ES, ES+, ERR)

39 % de CSSI nommés dans les unités non classées

Problèmes rencontrés :

Laboratoires regroupés : plusieurs SI pour une seule UMR

UMS : un seul SI pour plusieurs UMR (Misha)

Cotutelles IN2P3 : structure SSI interne à l'IN2P3

réflexion en cours : regroupement des fonctions CSSI & AE ?

Situation actuelle :

- Sensibilisation de la direction d'une grande unité (MISHA)
- Attente de la fin des constitution des dossiers de contractualisation (vague C)
- Mise à profit de ce temps d'attente pour former les ingénieurs soutiens et « peaufiner » la méthode de travail

Question :

Faire appel à un société spécialisée ⇔ Disposer d'un ingénieur « maison »?

METHODOLOGIE

pour la mise en place d'une PSSI opérationnelle dans les unités

Les documents et travaux de référence

« *Politique de Sécurité des Systèmes d'Information (PSSI)* », Joseph ILLAND

« *Charte pour l'usage de ressources informatiques et de services Internet* »,
Direction des affaires juridiques, publication Bulletin Officiel CNRS

« *La politique de Sécurité des SI dans les unités du CNRS* », Robert LONGEON

Méthodes d'audit EBIOS (DCSSI) & MEHARI (CLUSIF)

« *Guide pour l'élaboration d'une PSSI – section 2 Méthodologie* », DCSSI

Travaux du groupe CAPSEC

« *Liste de contrôle de sécurité des systèmes et des réseaux* », UREC

- Méthode simple
 - La sécurité, l'affaire de qui ?
 - Que faut-il protéger ? Dans quelles mesures ?
 - Quel est le niveau actuel de protection ?
 - Que faut-il corriger ? Et comment ?
 - Quelle conduite à tenir ?
- Diagnostic des services de sécurité à partir d'entretiens personnalisés avec les acteurs de la sécurité :

Direction – Responsables d'équipes de recherche – CSSI – ASR – ACMO ...

- Gros effort de sensibilisation à tous les niveaux

Sensibilisation de ... la Direction

Pourquoi faut-il se protéger

La PSSI est LA réponse à vos obligations légales et juridiques

La PSSI, c'est beaucoup d'organisation et un peu de technique

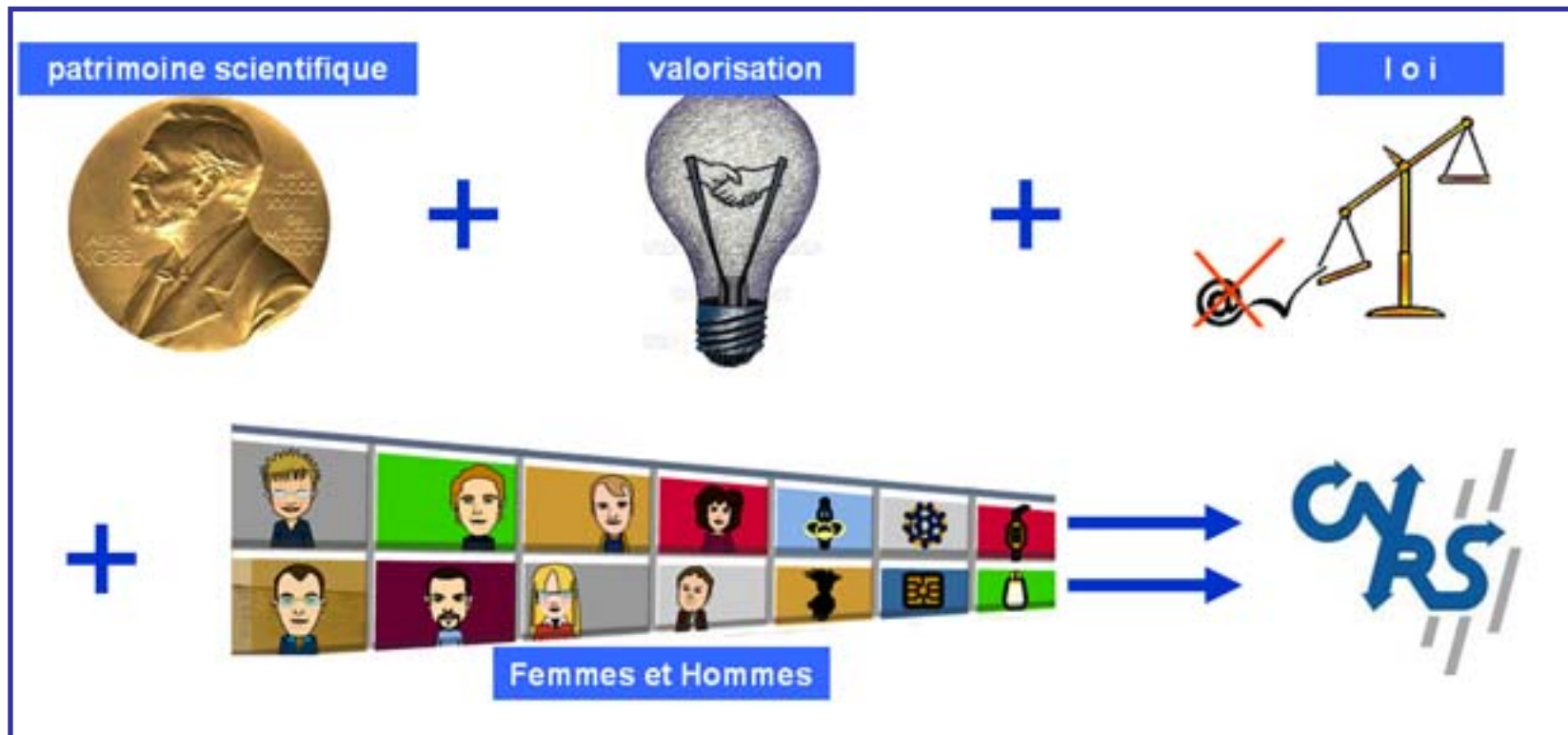
La PSSI est un outil pour piloter et maîtriser la sécurité de son SI

La réalisation de la PSSI est un acte de direction

Nous vous proposons un mode opératoire et un accompagnement

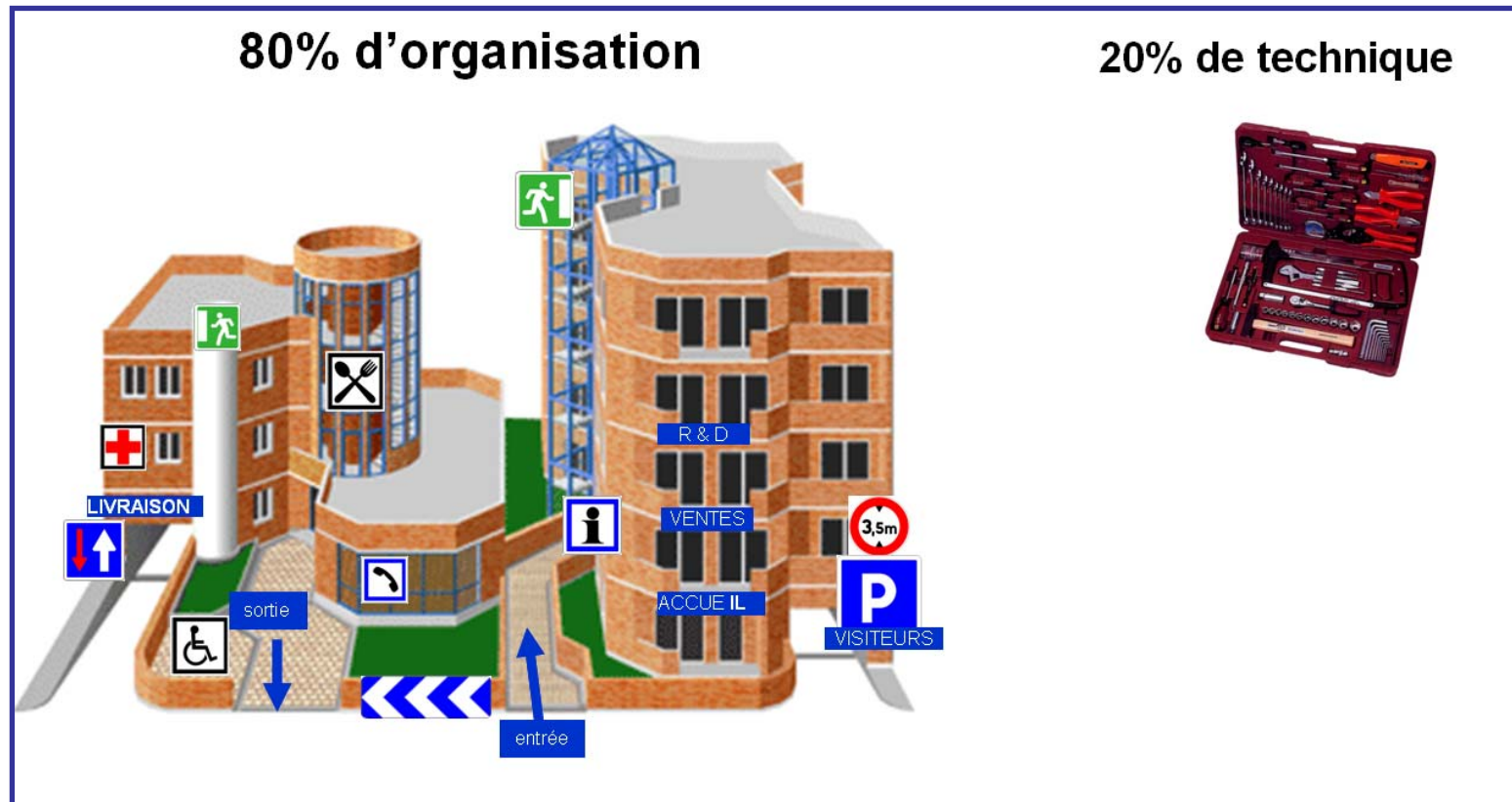
Sensibilisation de ... la Direction

Pourquoi faut-il se protéger



Sensibilisation de ... la Direction

La PSSI, c'est
beaucoup d'organisation et
un peu de technique



Sensibilisation de ... tous les utilisateurs du SI

aborder la SSI par des choses que l'utilisateur connaît et pratique tous les jours (messagerie, messagerie instantanée, clé usb, firewall, antivirus,...)

exemples
réels et concrets

faire prendre conscience qu'il est un maillon essentiel de la chaîne sécurité

la sécurité, c'est compliqué...

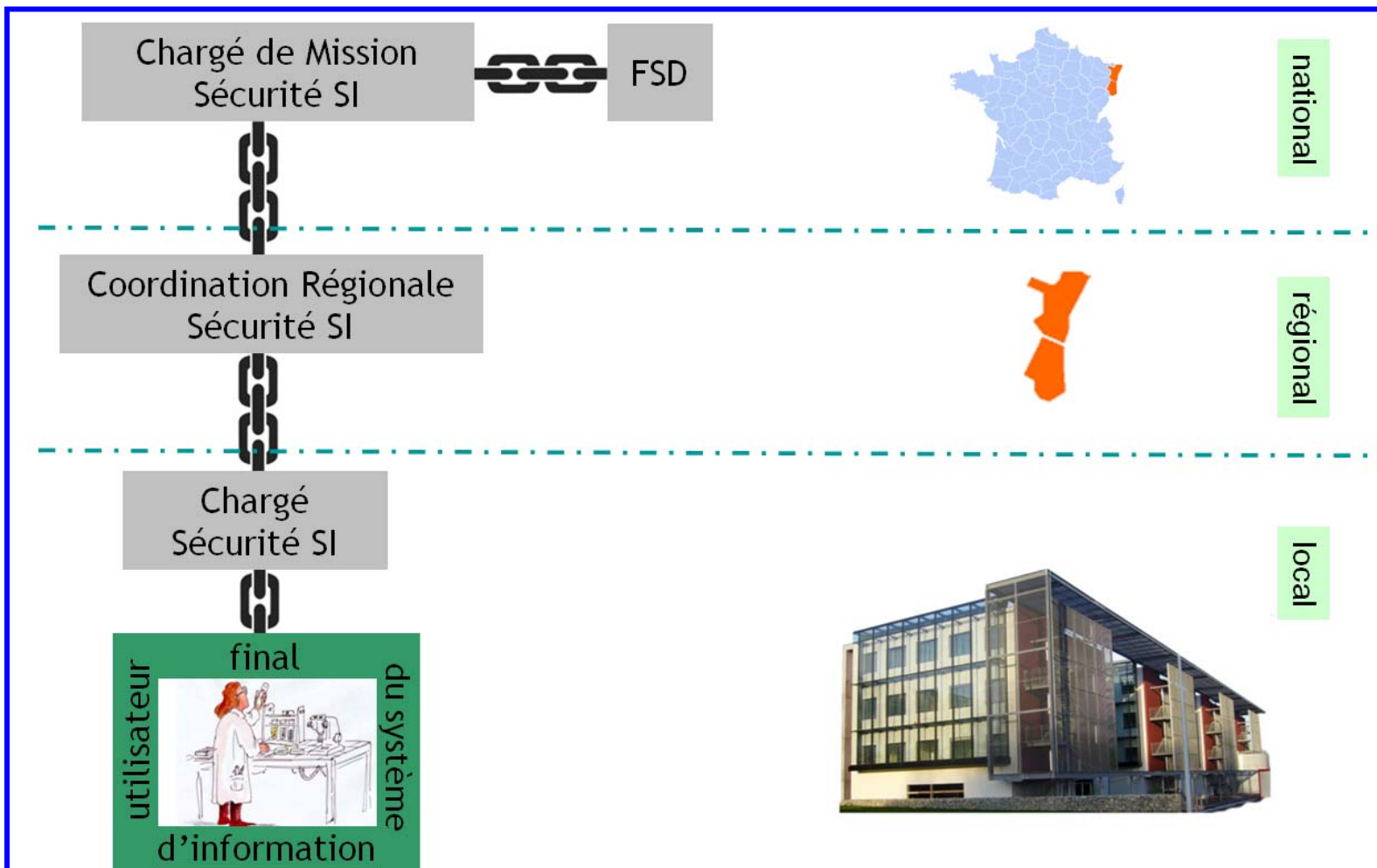
... mais on réduit considérablement les risques en appliquant TOUS des gestes simples et quotidiens

10 règles d'or de la sécurité de l'information

droits et devoirs

Sensibilisation de ...
tous les utilisateurs du SI

faire prendre conscience qu'il est un
maillon essentiel de la chaîne sécurité



Sensibilisation de ...
tous les utilisateurs du SI

10 règles d'or
de la sécurité
de l'information

10 Règles d'Or...

1- Respectez la législation et la charte de l'utilisateur du système d'information

2- Votre poste de travail doit comporter à minima: antivirus (à jour!), pare-feu et mises à jour logicielles

3- Dupliquez régulièrement vos données sur un espace protégé du Labo

4- Classifiez vos informations et protégez les en conséquence

5- Choisissez des mots de passe forts, gardez-les secrets

6- Soyez prudent lorsque vous recevez du courrier électronique

7- Ne manipulez pas des données sensibles dans des lieux publics

8- Soyez vigilant lors de vos téléchargements

9- Signalez sans délai tout évènement suspect

10- Votre CSSI et votre Administrateur du SI sont vos interlocuteurs privilégiés en matière de sécurité du SI, consultez-les.

...de la Sécurité de l'Information

Mise en œuvre de la PSSI dans les unités : *Mode opératoire*

Le mode opératoire se compose en 7 phases :

- 0 - Préalables
- 1 - Organisation du projet
- 2 - Périmètre et expression des besoins
- 3 - Etude et analyse des risques
- 4 - Traitement des risques
- 5 - Finalisation
- 6 - Mise en œuvre

pour chaque phase sont définis :

- une liste d'acteurs identifiés
- Une liste de tâches
- Un ou des livrables
- Des validateurs

Phase 0 – Préalables

Tâche(s)

Information des tutelles et partenaires

Nomination du CSSI

Acteurs :

FSD
Délégué Régional
Directeur Unité

Livrable(s)

- Lettre de désignation des CSSI
- Support de présentation de la PSSI

Phase 1 – Organisation du projet

Tâche(s)

Présentation du projet PSSI à la Direction de l'unité

Constitution d'une équipe projet (3 ou 4 personnes)

Planification du projet

Acteurs :

Délégué Régional
Directeur Unité
CRSSI
CSSI

Livrable(s)

- Note de cadrage

Phase 2 – Périmètre et expression des besoins

Tâche(s)

Définition du périmètre d'application de la PSSI

Définition des « éléments essentiels »

Expression des besoins de sécurité par élément essentiel

Acteurs :

Equipe Projet

Livrable(s)

- Périmètre d'application et exigences de sécurité

Phase 3 – Etude et analyse des risques

Tâche(s)

Identification des entités (composant des éléments essentiels)

Evaluation du niveau des services de sécurité

Détermination des écarts (niveau souhaité et niveau constaté)

Identification des vulnérabilités

Recommandations organisationnelles et techniques

Acteurs :

Equipe Projet

ASR

Utilisateurs

Livrable(s)

- Evaluation du niveau des services de sécurité (DCI)
- Ensemble de recommandations

Phase 4 – Traitement des risques

Tâche(s)

Elimination, réduction ou acceptation de chaque risque
Planification des opérations de réduction des risques

Acteurs :

Directeur Unité
Equipe Projet

Livrable(s)

- Document synthétique de gestion des risques

Phase 5 – Finalisation

Tâche(s)

Rédaction de la PSSI d'unité

Détermination des indicateurs de contrôle

Acteurs :

Equipe Projet

Livrable(s)

- **PSSI d'unité**
- Liste des indicateurs de contrôle

Phase 6 – Mise en œuvre

Tâche(s)

Présentation de la PSSI d'unité aux personnels

Mise en œuvre des opérations de réduction des risques (do)

Suivi de l'avancement du plan d'action (check)

Prise en compte de modification du périmètre (act)

Acteurs :

CSSI

ASR

Livrable(s)

- Support de présentation de la PSSI d'unité à l'usage de tous les utilisateurs du SI

0- Préalables	FSD Délégué Régional Directeur Unité	Lettre de désignation des CSSI Support de présentation de la PSSI
1- Organisation du projet	Délégué Régional Directeur Unité CRSSI CSSI	Note de cadrage
2- Périmètre et expression des besoins	Equipe Projet	Périmètre d'application et exigences de sécurité
3- Etude et analyse des risques	Equipe Projet ASR Utilisateurs concernés	- Evaluation du niveau des services de sécurité - Ensemble de recommandations
4- Traitement des risques	Directeur Unité Equipe Projet	Document synthétique de gestion des risques
5- Finalisation	Equipe Projet	PSSI d'unité Liste des indicateurs de contrôle
6- Mise en œuvre	CSSI ASR	Support de présentation de la PSSI d'unité à l'usage de tous les utilisateurs du SI

0- Préalables	<ol style="list-style-type: none"> 1. Information des tutelles et partenaires 2. Nomination du CSSI
1- Organisation du projet	<ol style="list-style-type: none"> 1. Présentation du projet PSSI à la Direction de l'unité 2. Constitution d'une équipe projet (3 ou 4 personnes) 3. Planification du projet
2- Périmètre et expression des besoins	<ol style="list-style-type: none"> 1. Définition du périmètre d'application de la PSSI 2. Définition des « éléments essentiels » 3. Expression des besoins de sécurité par élément essentiel
3- Etude et analyse des risques	<ol style="list-style-type: none"> 1. Identification des entités (composant des éléments essentiels) 2. Evaluation du niveau des services de sécurité 3. Détermination des écarts (niveau souhaité et niveau constaté) 4. Identification des vulnérabilités 5. Recommandations organisationnelles et techniques
4- Traitement des risques	<ol style="list-style-type: none"> 1. Décision d'élimination, réduction ou acceptation de chaque risque 2. Planification des opérations de réduction des risques
5- Finalisation	<ol style="list-style-type: none"> 1. Rédaction de la PSSI d'unité 2. Détermination des indicateurs de contrôle
6- Mise en œuvre	<ol style="list-style-type: none"> 1. Présentation de la PSSI d'unité aux personnels 2. Mise en œuvre des opérations de réduction des risques (do) 3. Suivi de l'avancement du plan d'action (check) 4. Prise en compte de modification du périmètre (act)