

La gestion du risque



## La PSSI d'unité

# Comment piloter la SSI ?



- Par les failles de sécurité ?
- Par le mimétisme et la pression commerciale ?
- Par les besoins de sécurité ?

Une PSSI qui permet le pilotage de la sécurité par les besoins



# La SSI est la gestion du risque sur les SI

Description du contexte de l'organisme : le système d'information, les éléments essentiels à protéger (informations, fonctions...), les entités sur lesquelles ils reposent, les enjeux liés au SI, les contraintes à prendre en compte...

Boucle d'affinage de l'appréciation et du traitement du risque

L'appréciation des risques SSI est l'ensemble du processus d'analyse et d'évaluation du risque.

Estimation de leur importance

Mise en évidence des composantes

Sélection des objectifs et exigences de sécurité pour réduire le risque (Refus, transfert ou conservation du risque)

Approbation par la direction des choix effectués lors du traitement du risque

Etude du contexte

APPRÉCIATION DU RISQUE (risk assessment)

Analyse du risque (risk Analysis)

Identification du risque

Estimation du risque

Hierarchisation du risque

Traitement du risque

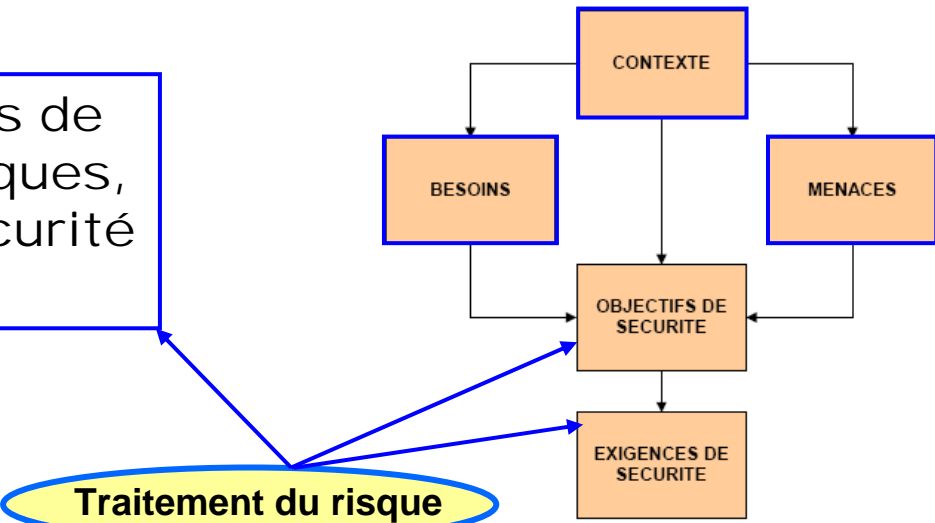
Consultations et communication

Suivi et contrôle des risques

# L'appréciation des risques

1. **Les besoins de sécurité** des éléments essentiels doivent être exprimés en termes de disponibilité, d'intégrité et de confidentialité.
2. **Les menaces** pesant sur le SI doivent être identifiées et caractérisées en terme d'opportunité (représentant l'incertitude de ces menaces).
3. Les risques doivent enfin être déterminés en confrontant les menaces aux besoins de sécurité.
4. **Identifier les objectifs de sécurité** en déterminant le mode de traitement (refus, optimisation, transfert ou prise de risque) et en tenant compte des éléments du contexte. Ces objectifs expriment la volonté de traiter les risques et ne préjugent pas des solutions à mettre en oeuvre.
5. Le traitement des risques se poursuit par **la détermination d'exigences de sécurité**, techniques ou non, satisfaisant les objectifs de sécurité identifiés et décrivant la manière de traiter les risques (dissuasion, protection, détection, récupération, restauration, compensation...).

La PSSI est l'ensemble des mesures de sécurité, techniques ou non techniques, spécifiées par les exigences de sécurité qui doivent être mises en oeuvre.



# Le risque en SSI

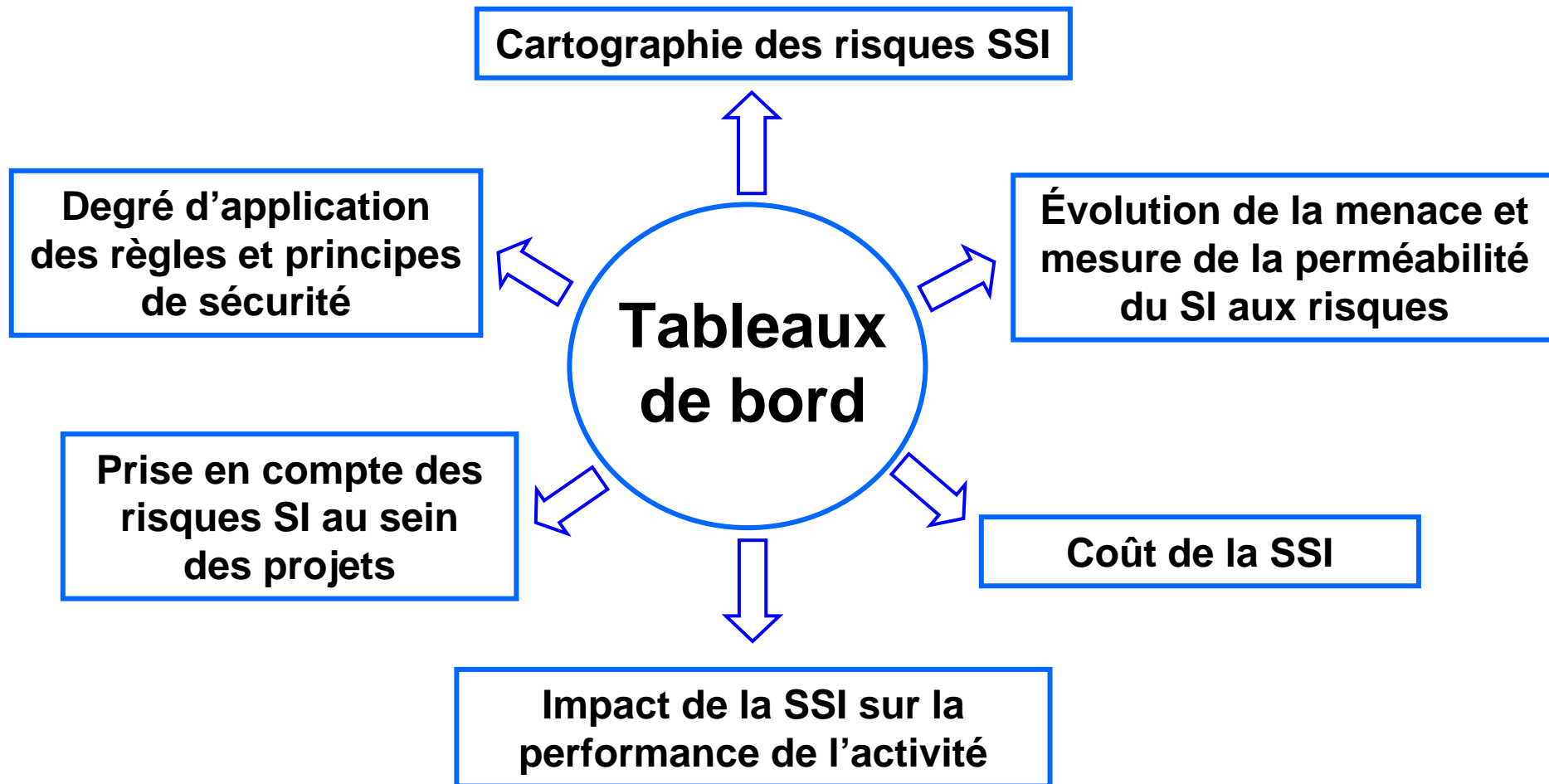
**Le risque<sup>[1]</sup> en SSI est une combinaison d'une menace et des pertes qu'elle peut engendrer**

Composantes d'un risque : exemple

<b>Méthode d'attaque</b>	piégeage du logiciel (introduction d'un ver)
<b>Élément menaçant</b>	un pirate expérimenté engagé par un concurrent
<b>Entité</b>	réseau WiFi
<b>Vulnérabilité</b>	possibilité d'administrer le réseau à distance
<b>Opportunité</b>	jugée moyenne
<b>Atteinte des éléments essentiels</b>	atteinte à la confidentialité (vol d'informations)
<b>Impact sur l'organisme</b>	perte d'avantages concurrentiels

<sup>[1]</sup> Le vocabulaire lié au risque et à la gestion des risques SSI est décliné du Guide ISO73 – *Management du risque – Vocabulaire – Principes directeurs*

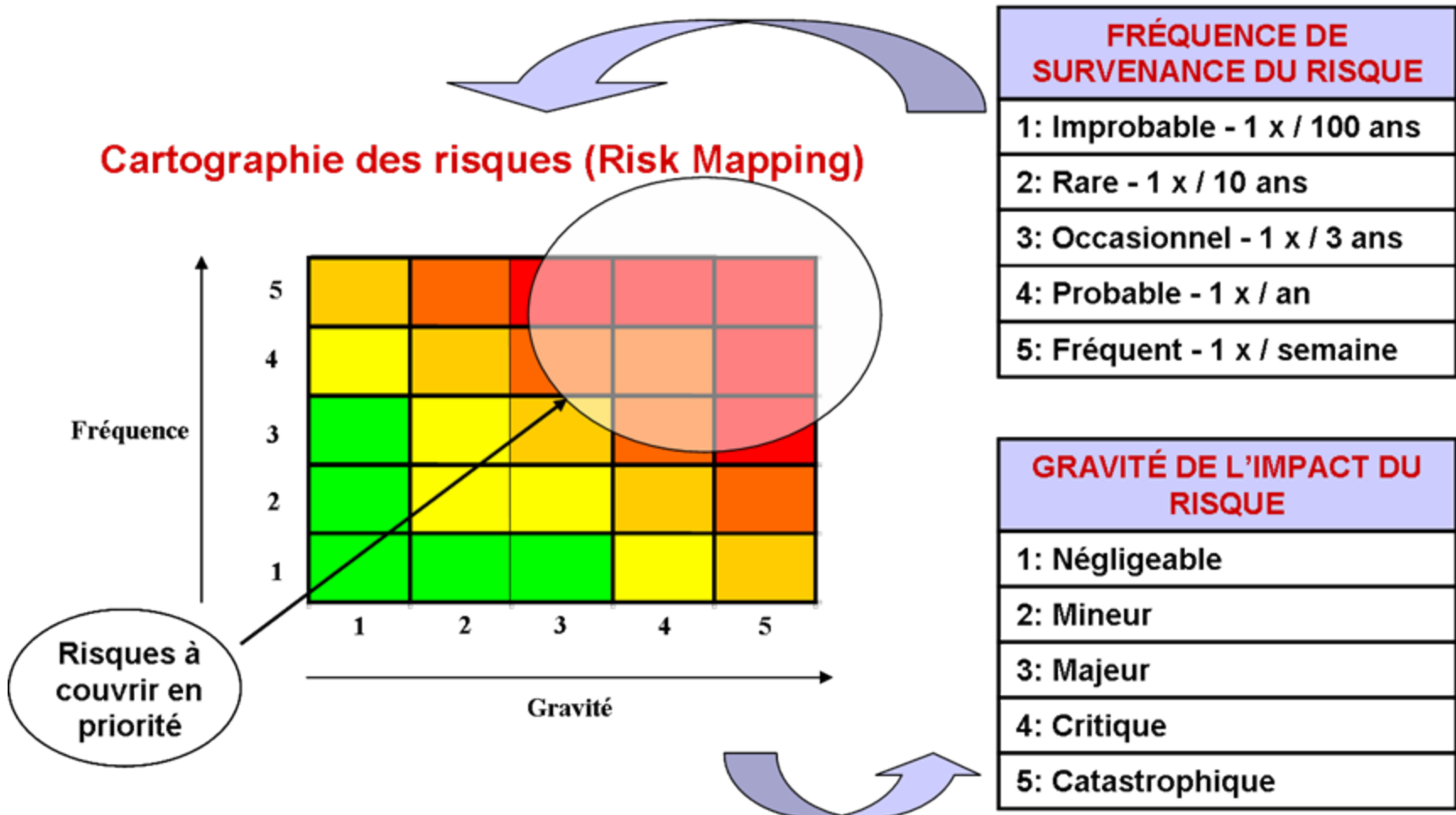
# Tableaux de bord SSI

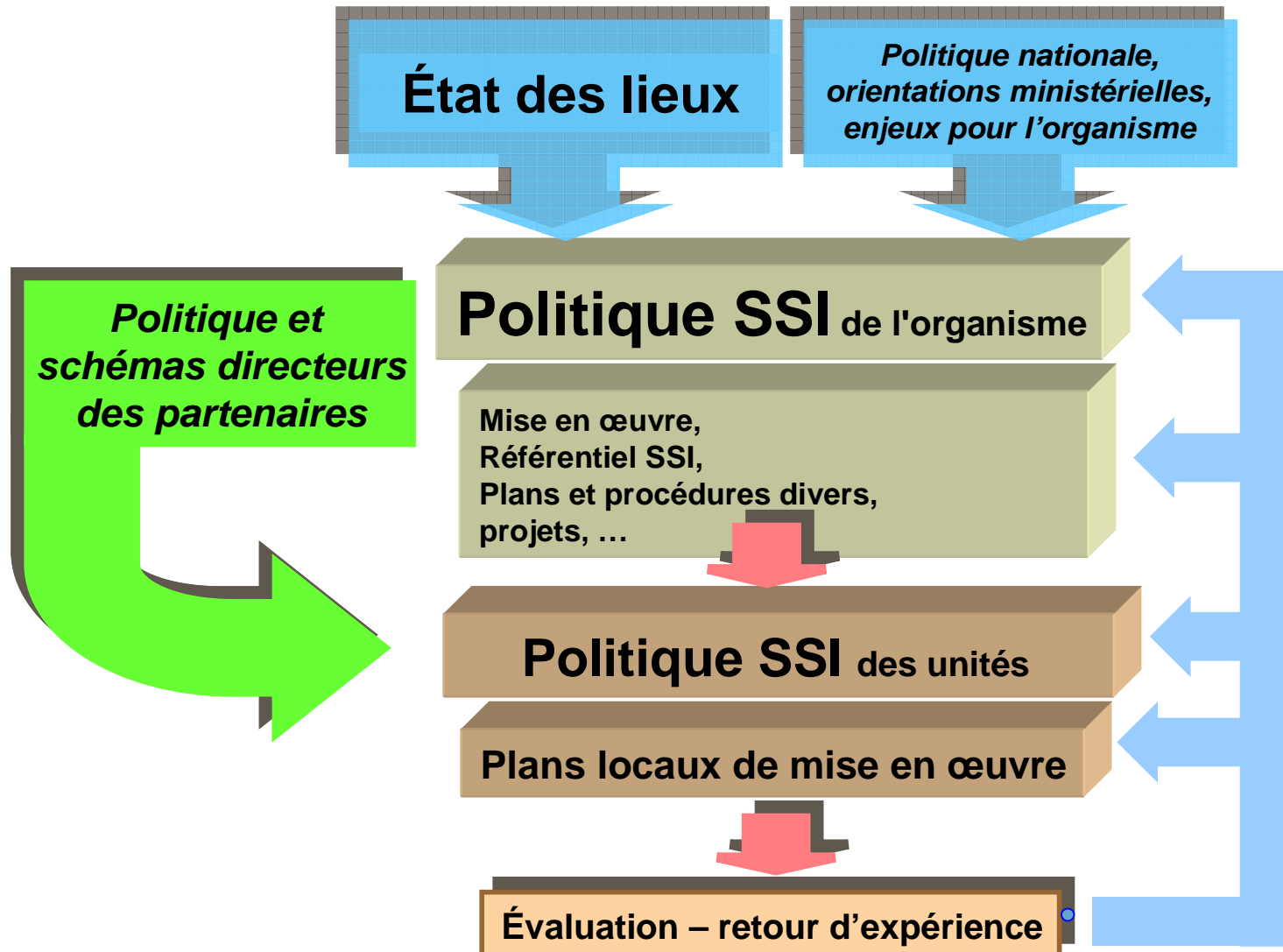


# La cartographie du risque

Elle fait partie des outils de management du risque, mais ne traite que du risque statistique, non de l'incertain

## Cartographie des risques (Risk Mapping)





# Origine d'un incident

## 1. Naturelles

- Pannes, bogues logiciel, événements inattendus
- Sinistres
- Accidents

## 2. Environnementales

- Catastrophe
- Inondation
- Tempête

## 3. Humaines

### → Involontaires

- Étourderies, inattention, indolence, Négligences, laisser-aller, passivité, Irréflexion, Imprévoyance, irresponsabilité
- Manque de moyens
- incompétence.

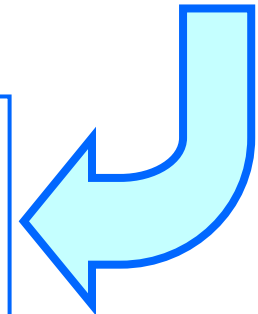
### → Volontaires

- Transgressions
- Malveillances

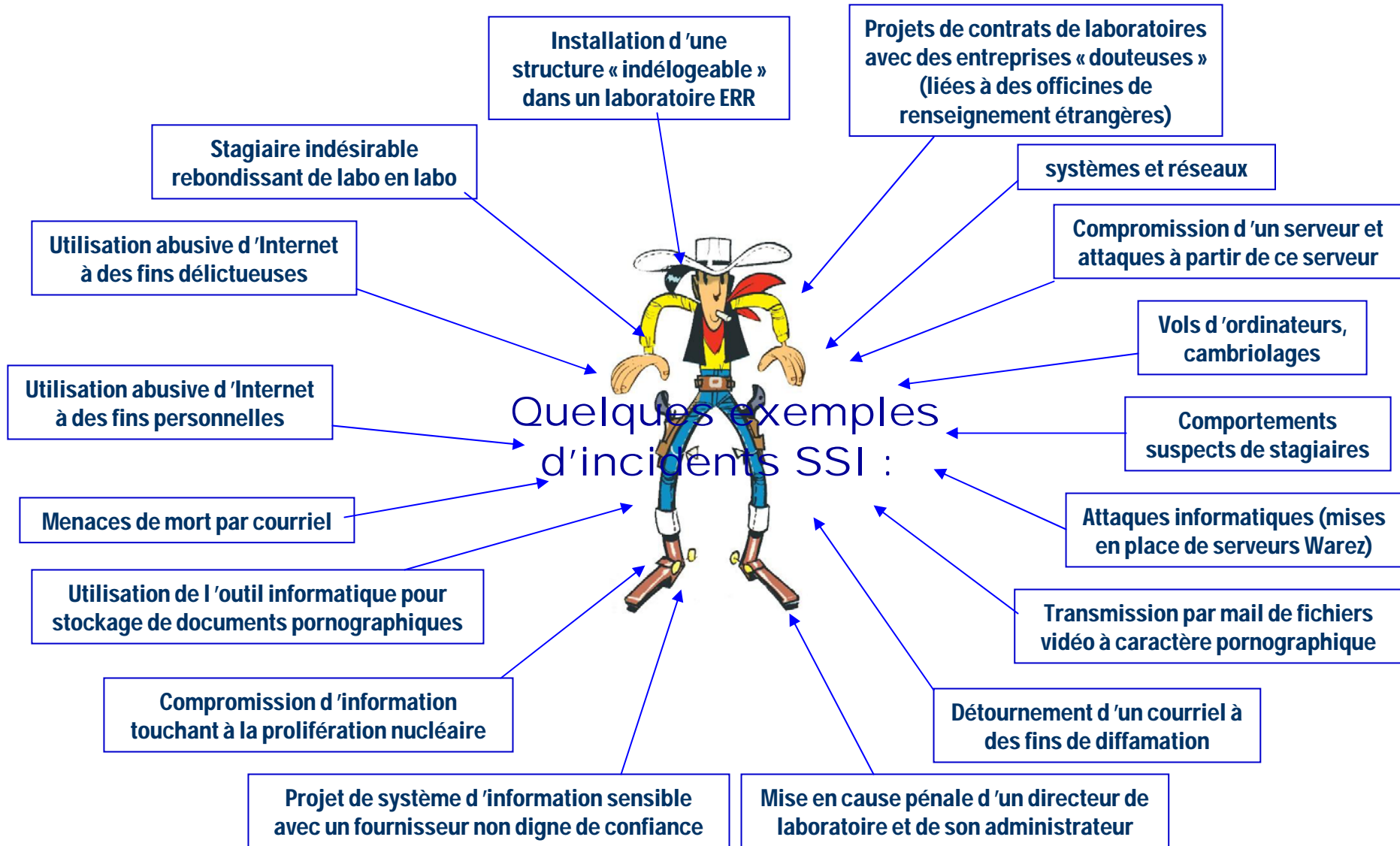
- Passives
- Actives (défig, CdT pirat, télé, pièges, etc.)

**Les malveillances  
sont à caractère**

- |                |                |
|----------------|----------------|
| 1. stratégique | 4. idéologique |
| 2. terroriste  | 5. ludique     |
| 3. cupide      | 6. vindicatif  |



# Impacts des menaces



# Mise en œuvre de la SSI

## dans les unités

### En déclinaison des objectifs de SSI définis nationalement :

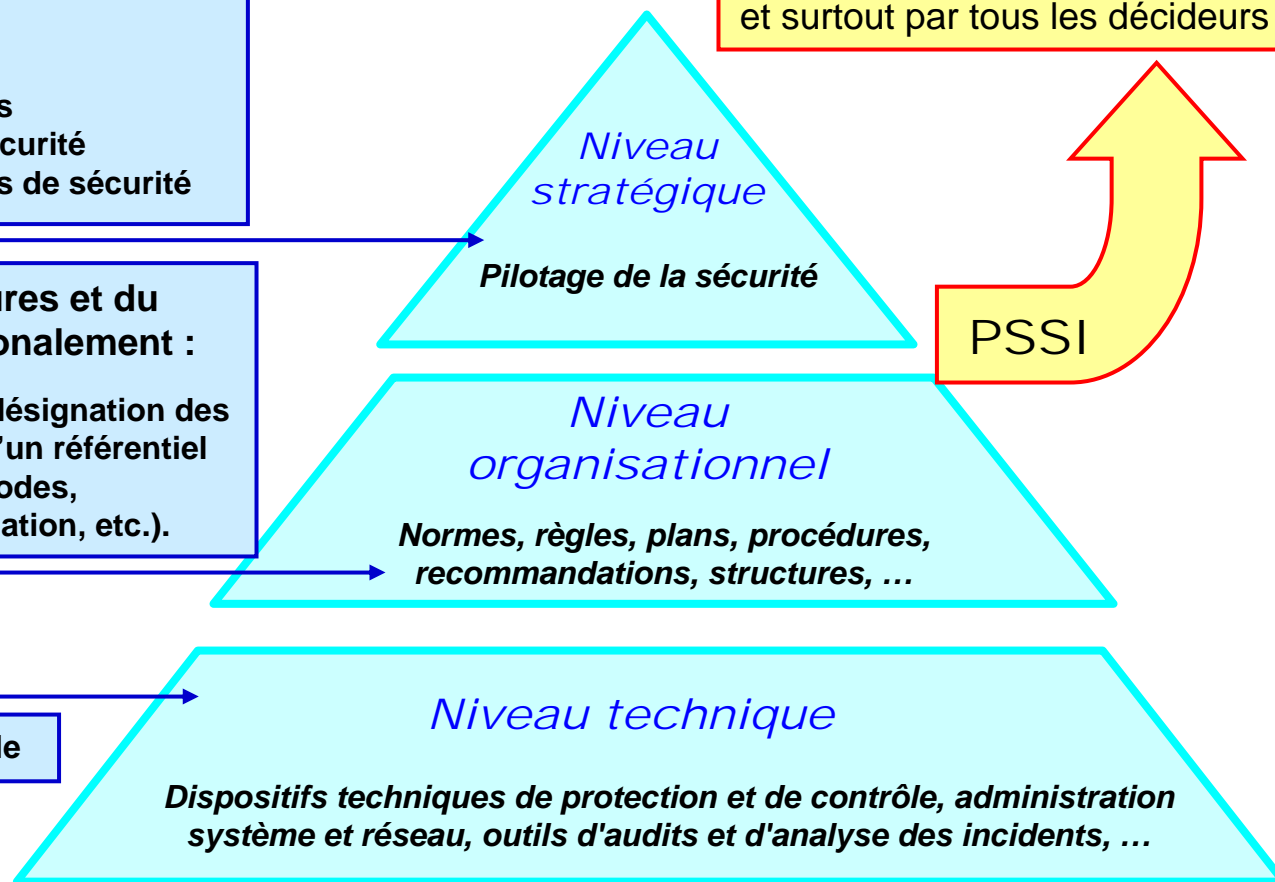
- Identification des enjeux
- Délimitation des périmètres
- Analyse des besoins de sécurité
- Détermination des objectifs de sécurité

### En déclinaison des structures et du référentiel SSI définis nationalement :

Mise en place de la structure, désignation des responsables, établissement d'un référentiel d'unité (applicatif, outils, méthodes, instructions, dispositif de formation, etc.).

Mise en œuvre opérationnelle

C'est un document de pilotage et de communication. Il doit donc être simple et concis pour pouvoir être lu par tous les utilisateurs du SI ... et surtout par tous les décideurs !



**Responsabilité du directeur de l'unité qui nomme un « Chargé de la Sécurité des Systèmes d'Information » (CSSI) pour lui déléguer le pilotage de la SSI :**

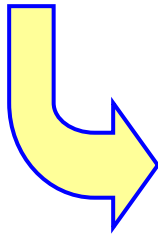
- **Le CSSI appartient à l'unité ou à une autre unité dans le cas d'une mutualisation de la SSI (par exemple de petites unités)**
- **Dans le cas des UMR : principe de l'unicité du CSSI et de la PSSI vis-à-vis de toutes les tutelles**
- **Conséquence : définition d'une tutelle de référence SSI ou du « *qui fait quoi* »**



# Missions principales

du CSSI en unité

Mission : piloter la SSI de l'unité !



# La PSSI opérationnelle d'unité

## Principes génériques d'une PSSI d'unité



Spam en Océanie



# Ce qu'implique la PSSI

pour les utilisateurs

La définition des procédures de sauvegardes

La nécessaire identification de « leurs » données sensibles

La nécessaire administration par les responsables informatiques des postes individuels

Les précautions à prendre à l'extérieur), en particulier en missions dans les pays « à risques » (postes nomades, wifi, messagerie ...)

- Connaissance de leurs de la chaîne fonctionnelle SSI
- Identification de leur « CSSI » d'unité

Une meilleure sensibilisation à la SSI

Le devoir de protection :

- sécurisation du poste de travail,
- sécurisation des outils nomades,
- sécurisation des échanges
- sécurisation de leurs applications informatiques

La connaissance du dispositif de gestion des traces arrêté au niveau de l'unité

Connaissance de leurs

- responsabilités (accès au réseau, obligations de recouvrement, etc.),
- droits et devoirs : en particulier se référer à la charte utilisateur.



# Conclusion

La PSSI que vient de promulguer le Directeur du CNRS nous permet de dépasser le stade purement technique de la SSI.

**Elle doit se décliner dans chaque unité par une PSSI opérationnelle.**

Qui est un outil :

- De pilotage
- De sensibilisation des utilisateurs
- De discussion avec nos partenaires
- De maîtrise de la SSI



# Vos contacts FSD

<b>Protection du patrimoine scientifique</b>	<b>Jean-Luc Toffart</b> Courriel : <a href="mailto:jean-luc.toffart@cnrs-dir.fr">jean-luc.toffart@cnrs-dir.fr</a> tél : 01 44 96 41 5
<b>Sécurité des systèmes d'information</b>	<b>Robert Longeon</b> Courriel : <a href="mailto:robert.longeon@cnrs-dir.fr">robert.longeon@cnrs-dir.fr</a> tél : 01 44 96 48 76  + <i>François MORRIS</i> Courriel : <a href="mailto:francois.morris@impmc.jussieu.fr">francois.morris@impmc.jussieu.fr</a> tél : 01 44 27 37 85
<b>Missions à l'étranger – Formations - Habilitations</b>	<b>Josiane Pauchont</b> Courriel : <a href="mailto:josiane.pauchont@cnrs-dir.fr">josiane.pauchont@cnrs-dir.fr</a> tél : 01 44 96 41 84
<b>Secrétariat technique</b>	<b>Christine Pierre</b> Courriel : <a href="mailto:christine.pierre@cnrs-dir.fr">christine.pierre@cnrs-dir.fr</a> tél : 01 44 96 41 85
<b>Le Fonctionnaire de Sécurité de Défense</b>	<b>Joseph Illand</b> Courriel : <a href="mailto:joseph.illand@cnrs-dir.fr">joseph.illand@cnrs-dir.fr</a> tél : 01 44 96 41 88



**Site Web :** <http://www.sg.cnrs.fr/FSD/default.htm>

**Courriel :** [Fonc-Def-Sec@cnrs-dir.fr](mailto:Fonc-Def-Sec@cnrs-dir.fr)