# PSSI des unités : outils et méthode

UPMC SORBONNE UNIVERSITÉS

cnrs dépasser les frontières

# Politique de Sécurité du Système d'Information (PSSI) : protection de l'activité scientifique

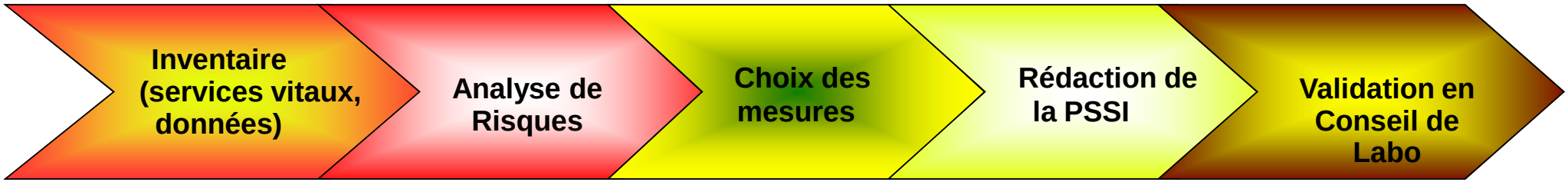
## Pourquoi un projet de PSSI d'unité :

- Protéger le patrimoine scientifique, disposer de ressources numériques fiables
- faire connaître à tous le contexte réglementaire et légal
- comprendre les menaces, la facilité d'exploitation des vulnérabilités, les impacts possibles
- savoir réagir en cas d'incident de sécurité pour minimiser les impacts
- pouvoir s'engager auprès de partenaires scientifiques ou industriels

## Conditions de réussite d'un projet de PSSI d'unité :

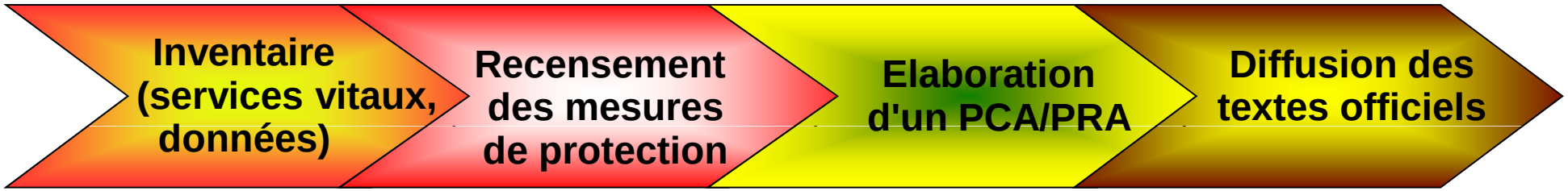
- Cerner les enjeux vitaux pour l'unité afin de décider des mesures de protection nécessaires
- Implication de tous : directeur d'unité, chercheurs porteurs des projets scientifiques de l'unité, personnel administratif et technique

# Etapes d'un Projet de PSSI d'unité




1. Nomination du CSSI par le directeur et constitution du groupe projet pour réalisation de l'inventaire des services vitaux, bases de données, fichiers nominatifs, etc.
2. Analyse de risques : formation des CSSI aux méthodes et outils de la PSSI proposée par le CNRS et l'UPMC
3. Appréciation des risques : résultats de l'analyse présentée au directeur par le CSSI et choix de mesures (ISO 27002) pour sécuriser le système d'information
4. Rédaction de la PSSI incluant les mesures choisies et détaillant en annexe les mesures techniques de protection et les procédures mises en place
5. Validation de la PSSI en conseil de laboratoire pour diffusion à l'ensemble des personnels

# Protection du système d'information d'une unité (version simplifiée)




1. **Nomination du CSSI (ou correspondant) par le directeur pour réalisation de l'inventaire des services vitaux, bases de données, fichiers nominatifs, etc.**

2. **Recensement par le CSSI des mesures de sécurisation déjà en place dans l'unité et vérification de l'existence des mesures de protection essentielles issues des PSSI des établissements de tutelle ==> choix de nouvelles mesures si nécessaire, validées par le directeur**

3. **Rédaction d'un PCA/PRA pour les services vitaux (soutien UPMC/CNRS possible)**

4. **Diffusion à l'ensemble des personnels des nouvelles mesures de protection issues des PSSI des tutelles, diffusion et affichage des chartes des tutelles**

# Analyse de risques : méthode

## Se poser les bonnes questions :

- Quels sont les enjeux du laboratoire ?
- Quelles menaces peuvent avoir un impact sur ces enjeux ?
- Quelles vulnérabilités peuvent être exploitées par une menace ?
- Quels objectifs de sécurité veut-on/peut-on mettre en place ?
- Quelles mesures de sécurité pour réduire le risque ?

## Sélectionner les enjeux :

- Données essentielles et leur typologie : administratives, contrats, projets,…
- Services vitaux : messagerie, base de données, serveur de fichiers,…
- Fixer le périmètre de la PSSI : commencer restreint pour élargir si nécessaire

## Etudier menaces et vulnérabilités en fonction des enjeux :

Retenir les menaces vraisemblables pour lesquelles aucune mesure n'est en place
Etablir des priorités entre les différents risques à couvrir en fonction des impacts

## Choisir les objectifs et les mesures de sécurité (ISO 27002)

Utiliser l'outil d'analyse de risques et s'inspirer des PSSI des tutelles pour établir des mesures de protection appropriées à l'unité

# En pratique : distinguer actifs primordiaux et actifs de soutien

## Actifs primordiaux :

**Ce sont les données essentielles du laboratoire, celles dont la perte (vol ou destruction) aurait un impact direct pour le laboratoire (pertes financières, image de marque,conséquences juridiques …)**

**→ Les chercheurs et le directeur d'unité ont connaissance de ces données, leur rôle est d'en informer le CSSI**

## Actifs de soutien :

**Ce sont les ressources informatiques hébergeant les services et les données de l'unité**

**→ les administrateurs de ces ressources doivent connaître les contraintes de disponibilité des services et les enjeux de confidentialité des données pour l'unité**

**→ le rôle de la direction est de valider ces contraintes et ces enjeux en y affectant les moyens nécessaires le cas échéant**

# Objectifs de sécurité vs mesures existantes : Commencer avec les systèmes vitaux administrés par le CSSI

**Disponibilité ?** **Existence d'un PRA ou d'une procédure de restauration validée ? Contrat de maintenance ?**

**Confidentialité des données ?** **authentification et autorisation, chiffrement des échanges serveur/client, chiffrement des données, déclarations CNIL ? RGS ?**

**Intégrité ?** **Existence d'un mécanisme permettant de vérifier l'intégrité des données ?**

**Journalisation ?** **journalisation des accès au service conforme aux politiques de gestion de journaux informatiques des tutelles ?**

# Elaboration de la PSSI de l'unité

## Appréciation des risques :

- Présenter une synthèse de l'analyse de risques au directeur d'unité
- Faire valider les mesures préconisées

## Calendrier de mise en oeuvre :

Lister l'ensemble des documents techniques à rédiger pour la mise en oeuvre des mesures

## Elaborer le document de PSSI pour présentation au conseil de labo :

utiliser le plan type de PSSI d'unité