PLAN de la présentation

- **Données administratives**
- **Fichiers génériques**
- **Conclusions**

Données administratives

- **Caractéristiques de ces données :**
  - **Restreintes, faciles à identifier(!), manipulées par un petit groupe de personnes**
- **Comment faire ?**
  - **Liste des données → long → données standards**
  - **Menaces / vulnérabilités → nécessité d'une liste**
  - **Listes Ebios → nécessité de « traduire » pour avoir des scénarios concrets**
- **Confidentialité : le seul critère**

Fichiers génériques

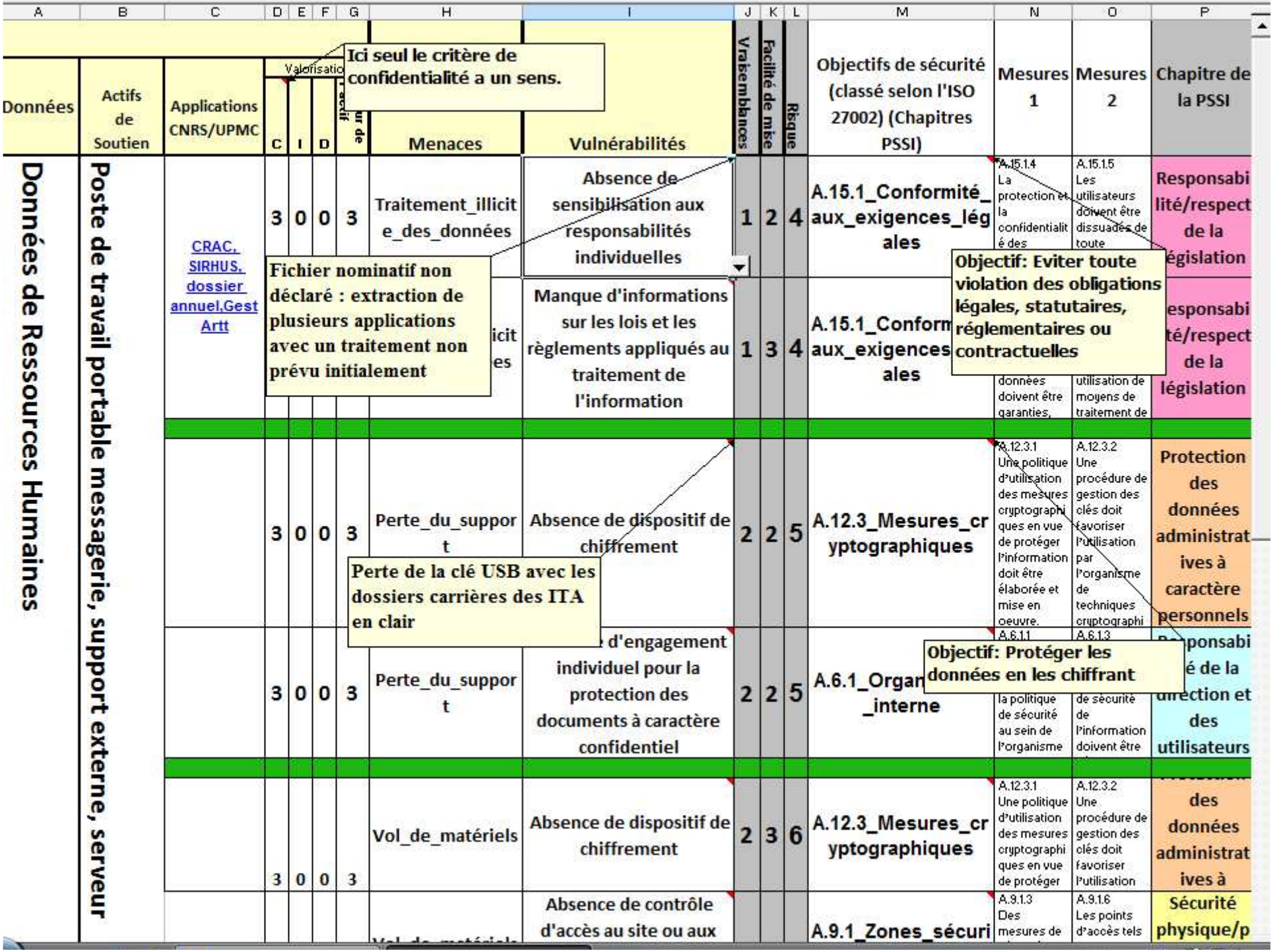
- **Domaine administratif: Liste « exhaustive » des applications des S.I CNRS et UPMC → classement par thème des données**
- **Un thème = un onglet → enjeu du labo**
- **Menus déroulants des menaces + vulnérabilités :**
  - **« plausibles » pour un labo**
  - **Possibilité de rajout et de suppression**

Fichiers génériques

- **Parti pris de certains critères**
- **Ex: administratif (confidentialité):**
  - **Très souvent des copies de données extraites du SI → Rarement dans le périmètre direct**
- **1 menace/vulnérabilité = mini scénario plus concret**
- **Liste des Objectifs et mesures (27002)**

Fichiers génériques

- **Le labo doit choisir les scénarios plausibles**
  - **Assez facile**
  - **En fonction des mesures déjà en place**
- **Puis valoriser le risque (vraisemblance, facilité de mise en œuvre)**
- **Présentation des risques à la direction**
- **Pas de notion de risque « résiduel ». Faire « simple » !!!**
- **Présentation des mesures à mettre en place**


Ici seul le critère de confidentialité a un sens.
Fichier nominatif non déclaré : extraction de plusieurs applications avec un traitement non prévu initialement
Perte de la clé USB avec les dossiers carrières des ITA en clair
Objectif: Eviter toute violation des obligations légales, statutaires, réglementaires ou contractuelles
Objectif: Protéger les données en les chiffrant
Données
Actifs de Soutien
Applications CNRS/UPMC
Valorisation actif
C
I
D
Menaces
Vulnérabilités
Vraisemblance
Facilité de mise
Risque
Objectifs de sécurité (classé selon l'ISO 27002) (Chapitres PSSI)
Mesures 1
Mesures 2
Chapitre de la PSSI
Données de Ressources Humaines
Poste de travail portable messagerie, support externe, serveur
CRAC, SIRHUS, dossier annuel,Gest Artt
3 0 0 3
Traitement_illicite_des_données
Absence de sensibilisation aux responsabilités individuelles
1 2 4
A.15.1_Conformité_aux_exigences_légales
A.15.1.4 La protection et la confidentialité des
A.15.1.5 Les utilisateurs doivent être dissuadés de toute
Responsabilité/respect de la législation
Manque d'informations sur les lois et les règlements appliqués au traitement de l'information
1 3 4
A.15.1_Conform aux_exigences ales
données doivent être garanties,
utilisation de moyens de traitement de
esponsabilité/respect de la législation
3 0 0 3
Perte_du_support
Absence de dispositif de chiffrement
2 2 5
A.12.3_Mesures_cryptographiques
A.12.3.1 Une politique d'utilisation des mesures cryptographiques en vue de protéger l'information doit être élaborée et mise en oeuvre.
A.12.3.2 Une procédure de gestion des clés doit favoriser l'utilisation par l'organisme de techniques cryptographi
Protection des données administratives à caractère personnels
3 0 0 3
Perte_du_support
d'engagement individuel pour la protection des documents à caractère confidentiel
2 2 5
A.6.1_Organ _interne
A.6.1.1 la politique de sécurité au sein de l'organisme
A.6.1.3 de sécurité de l'information doivent être
ponsabilité de la direction et des utilisateurs
3 0 0 3
Vol_de_matériels
Absence de dispositif de chiffrement
2 3 6
A.12.3_Mesures_cryptographiques
A.12.3.1 Une politique d'utilisation des mesures cryptographiques en vue de protéger
A.12.3.2 Une procédure de gestion des clés doit favoriser l'utilisation
des données administratives à
Absence de contrôle d'accès au site ou aux
A.9.1_Zones_sécuri
A.9.1.3 Des mesures de
A.9.1.6 Les points d'accès tels
Sécurité physique/p

Conclusions

- **Clarté des scénarios…**
- **Vouloir être exhaustif (listes)**
- **Ne pas sombrer dans la paranoïa (listes)**
- **En oublier la notion d'impact réel**
- **Valoriser les bonnes données :**
  - **Ex: données RH (→ impact!)**
  - **Données hors périmètre (celui de la DSI!)**
  - **Données de valorisation (brevet, contrats,..)**