



D'une PSSI d'unité de recherche à la PSSI d'établissement

Sylvie Vottier, RMSI, Université de Bourgogne
Alain TABARD, ICMUB – UMR CNRS 6302

SOMMAIRE

1. Éléments de contexte
2. Elaboration d'une PSSI d'unité de recherche
3. Vers la PSSI d'établissement
4. Organisation de la SSI à l'université de Bourgogne
5. Conclusion



Le Management de la Sécurité de l'Information aujourd'hui

- ❑ Cartographie des CSSI Chargés de Sécurité des Systèmes d'Information nommés
 - ❑ Charte d'usage des TIC
 - ❑ Gestion des incidents au coup par coup en s'appuyant sur le réseau des CSSI
 - ❑ Mise en place de mesures après incident
 - ❑ Au besoin, rédaction d'une note de service en réponse à l'incident
- ➔ Management de la Sécurité de l'Information de type « **POMPIER** »

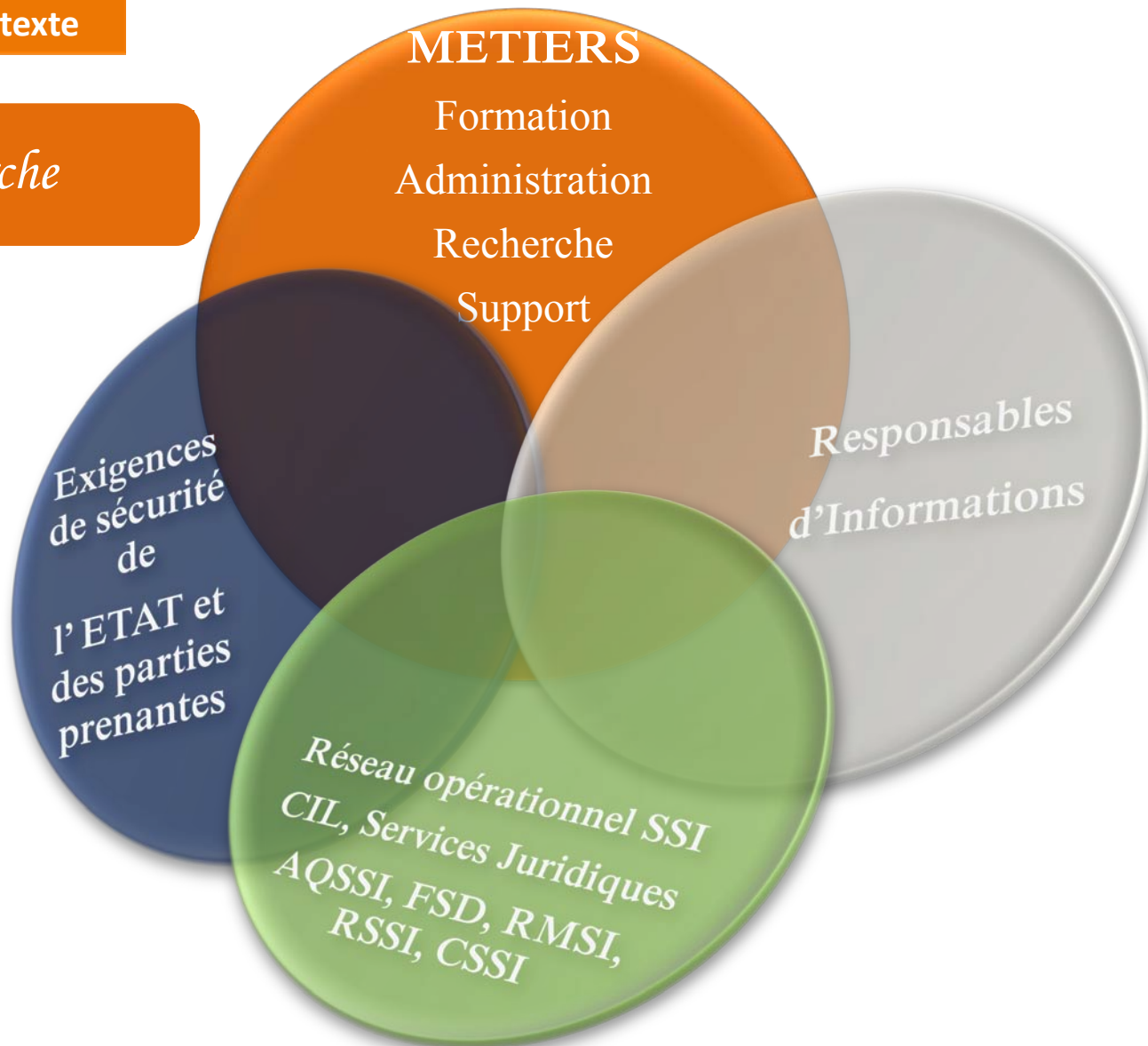


Le Management de la Sécurité de l'Information demain

- ❑ Etre **PROACTIF**
- ❑ Mettre en place un **Système de Management de la Sécurité de l'Information**
- ❑ **Analyser** les risques en amont – définir les menaces et les vulnérabilités du SI
- ❑ **Evaluer** les risques et définir les priorités
- ❑ Définir les mesures **techniques et/ou organisationnelles** pour minimiser les risques
- ❑ Mettre en place une **PSSI** d'établissement que chacun devra suivre
- ❑ **Sensibiliser** tous les acteurs afin que chacun devienne **acteur de la SSI**
- ❑ **Communiquer** sur les incidents
- ❑ Assurer une démarche **d'Amélioration Continue**



La démarche



L'information matérielle

- Dossiers Contrats, Brevets, Valorisation, Projets ANR, ...
 - Dossiers RH, Gestion du Personnel
 - Dossiers Financiers, Justificatifs
 - Dossiers Stratégiques – Pilotage - Gouvernance
 - Dossiers expertises
-
- Courriers « papier » et colis
 - Carte Multi Services, Badges, clés, passes, transpondeurs
 - Cahier de laboratoire
 - Échantillons scientifiques

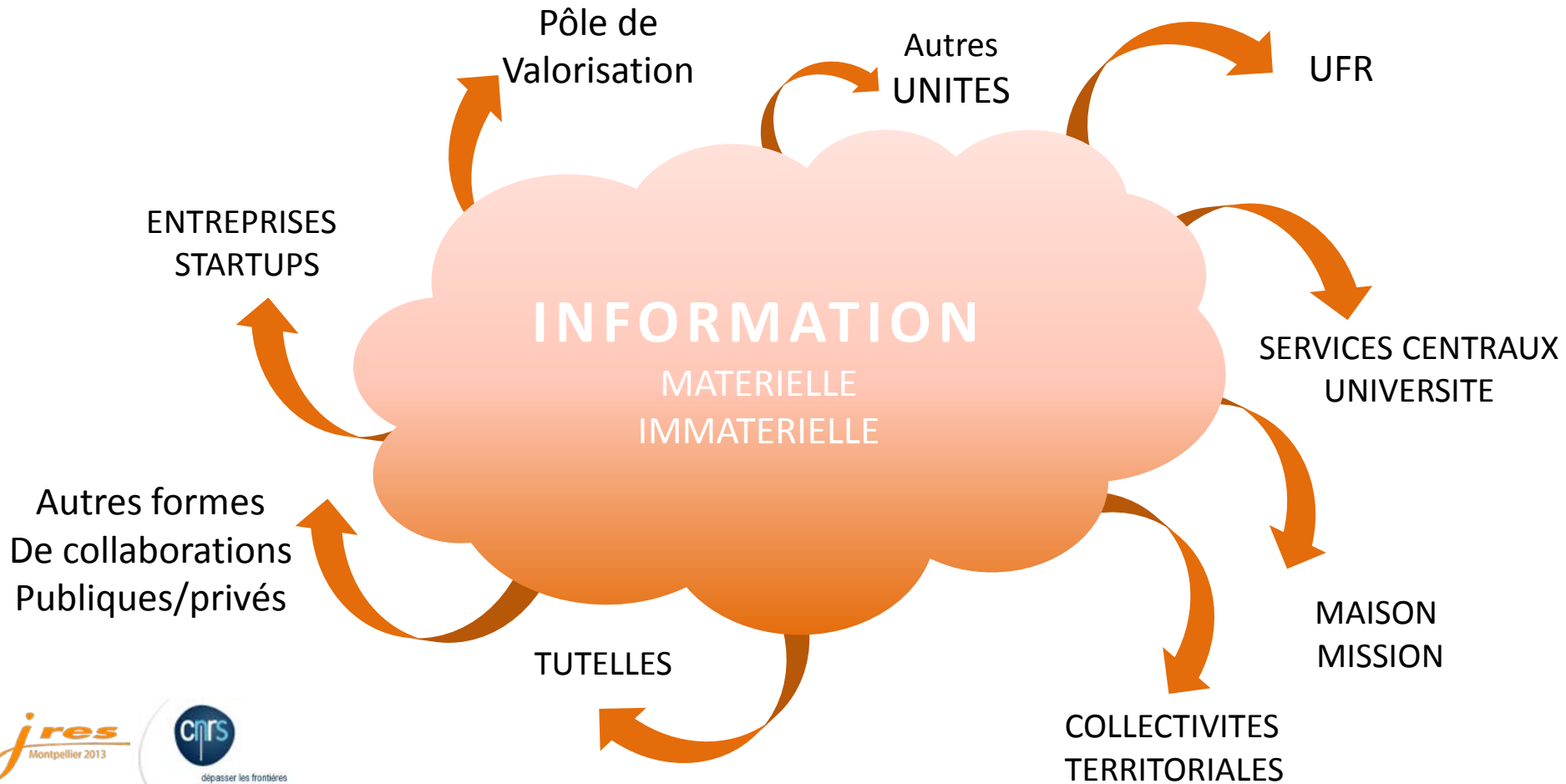


L'information immatérielle

- Equivalent électronique de l'information matérielle
 - Messagerie
 - Signature électronique d'un responsable
 - Résultats de recherche
 - Dossiers AERES, PRES,
- La personne elle-même



Contexte collaboratif



Profil des unités de recherche

- ❑ Unité 1 – environ 300 personnes
 - ❑ *Unité répartie sur 3 sites territoriaux*
 - ❑ *À Dijon, 3 ailes d'un même bâtiment sur 5 étages*
 - ❑ Collaboration avec la **filiale de valorisation de la recherche** de l'uB
 - ❑ Collaboration avec des **pôles de compétitivités**
 - ❑ Présence de **Startup (s)** et de plusieurs **projets en incubation**

- ❑ Unité 2 – environ 150 personnes
 - ❑ *Unité répartie sur une aile de bâtiment – 5 étages*
 - ❑ Un **Plateforme technologique d'analyse**
 - ❑ Collaboration la filiale de valorisation de la recherche de l'uB
 - ❑ Collaboration avec des pôles de compétitivités
 - ❑ Présence de startup(s) et de plusieurs projets en incubation

➔ Niveau de Maturité SSI différent



Présentation de la démarche

- ❑ **Participative**
 - ❑ *Tous les personnels sont concernés*
 - ❑ *La Direction porte la démarche et **Valide** à toutes les étapes*
 - ❑ *L'ensemble des personnes interviewées se sent **acteur de la démarche***
 - ❑ *Comité SSI*

- ❑ **Orientée Processus METIERS**
 - ❑ *Recherche/Enseignement*
 - ❑ *Gestion / Finance / Administration*
 - ❑ *Informatique*

- ❑ **Pilotage de la Sécurité par le Management des Risques**

- ❑ **Audit organisationnel**



Déroulement de la démarche

- ❑ **Identifier les informations sensibles et leurs flux**
 - ❑ Visite des unités de recherche
 - ❑ Entretiens réalisés auprès des personnes détenant des informations
- ❑ **Evaluation des risques**
 - ❑ Elaboration du Tableau d'appréciation des risques → informations (menaces/vulnérabilités)
 - ❑ Réunions de travail avec le Comité SSI
 - ❑ Réunions de travail avec les personnes interviewés – Réunion « METIER »
 - ❑ Evaluation des risques **par les personnes interviewées** (impact CID, ...)
- ❑ **Mise en place d'un Plan de Traitement des Risques : FEUILLE de ROUTE**
- ❑ **Elaboration de la PSSI d' Unité**
- ❑ **Appropriation de la démarche** par les acteurs et le comité SSI
→ **Amélioration Continue**



Mise en place d'une démarche ISO2700x

LANCEMENT de la DEMARCHE

Engagement
Confidentialité

Présentation Mission

Visite de laboratoire

Création Comité SSI



COMITÉ Sécurité des Systèmes d'Information

- Directeur d'unité de recherche
- Chargé (s) de Sécurité des Systèmes d'Information
- RA et Gestionnaire(s) (Administration contrats – brevets, accès, demande HFDS ...)
- Responsable(s) ou représentant(s) d'équipe (Gestion de contrats – brevets)
- Responsable(s) ou représentant(s) de plateformes techniques (ISO 9001)
- Représentant(s) Hygiène et Sécurité
- Représentant(s) du service informatique
- Chercheurs en simulation numérique ou expérimentateurs
- Représentant de la gestion du patrimoine (bâtiment – Accès)
- Correspondant Informatique et Liberté



Analyse De l'Activité dans une unité de recherche - Méthodologie ADAC

LANCEMENT de la DEMARCHE

Engagement
Confidentialité

Présentation Mission

Visite de laboratoire

Création Comité SSI

CONDUITE d'ENTRETIENS « METIER »

Administratif (4 unité1, 7 Unité2)

Rech/Ens (10 unité1, 17 unité2)

Informatique (3 unité1, 1 unité2)

Processus RECHERCHE

Sous processus/Activités

Gestion des Contrats; brevets
 Gestion des Echantillons
 Gestion des Résultats de recherche
 Expérimentations
 Protocole de mesures
 Gestion des Dossiers expertises
 Gestion des Dossiers RH
 Recherche par Simulation numérique
 Gestion des Rapports d'activités équipe
 Enseignement

Processus ADMINISTRATION

Sous processus/Activités

Gestion des Contrats; brevets
 Dossiers Administratifs
 Gestion du personnel
 Gestion des missions
 Gestion du courrier
 Gestion des accès
 Comptabilité
 Demande HFDS
 Rapports d'activités labo
 Dossiers d'expertise



Analyse De l'Activité dans une unité de recherche - Méthodologie ADAC

LANCEMENT de la DEMARCHE

Engagement
Confidentialité

Présentation Mission

Visite de laboratoire

Création Comité SSI



CONDUITE d'ENTRETIENS « METIER »

Administratif (4 unité1, 7 Unité2)

Rech/Ens (10 unité1, 17 unité2)

Informatique (3 unité1, 1 unité2)



IDENTIFICATION DES INFORMATIONS SENSIBLES

MATERIELLES

IMMATERIELLES



APPRECIATION DES RISQUES

Menaces

Vulnérabilités

Valorisation impacts
(CID)Vraisemblance de la
menaceFacilités d'exploitation
des vulnérabilités

TRAITEMENT du RISQUE

Acceptation

Réduction

Externalisation

Refus (risque trop élevé)



Mise en place d'une démarche ISO2700x

TRAITEMENT du RISQUE

Acceptation du risque

Réduction du risque

Externalisation

Refus (risque trop élevé)

La Direction prend le risque et assume cette responsabilité

Le niveau de risque n'est pas acceptable.
La Direction décide de mettre des mesures techniques/organisationnelles en place pour minimiser le risque et le rendre acceptable.

Le risque est élevé. La Direction pense que ce n'est pas le cœur de métier du laboratoire ou que l'unité n'a pas les compétences ni les ressources nécessaires et externalise le processus.

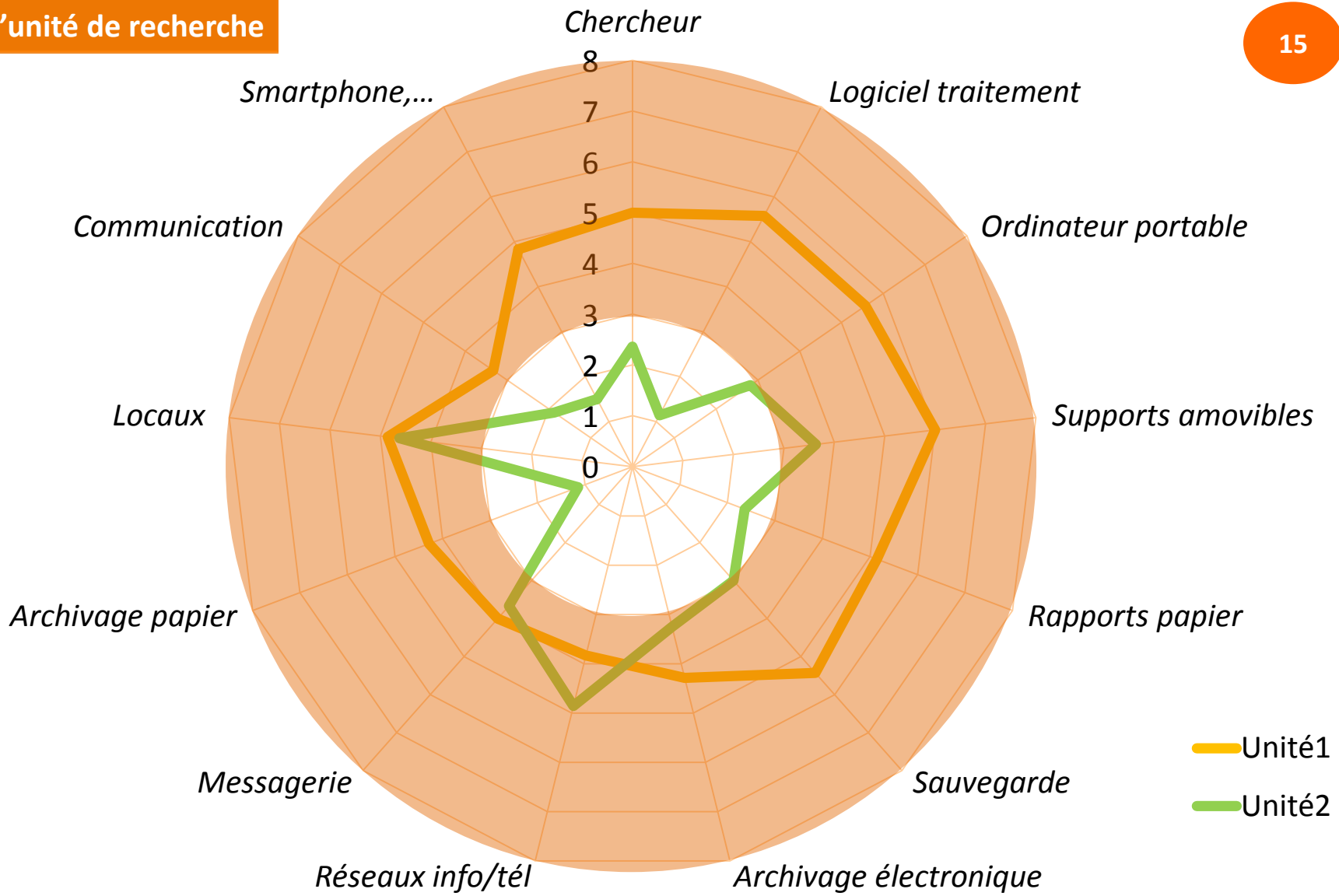
Le risque est beaucoup trop élevé. La Direction pense que l'activité doit être arrêtée.

➔ **Contrat de service (interne/externe)**
Contrat d'externalisation

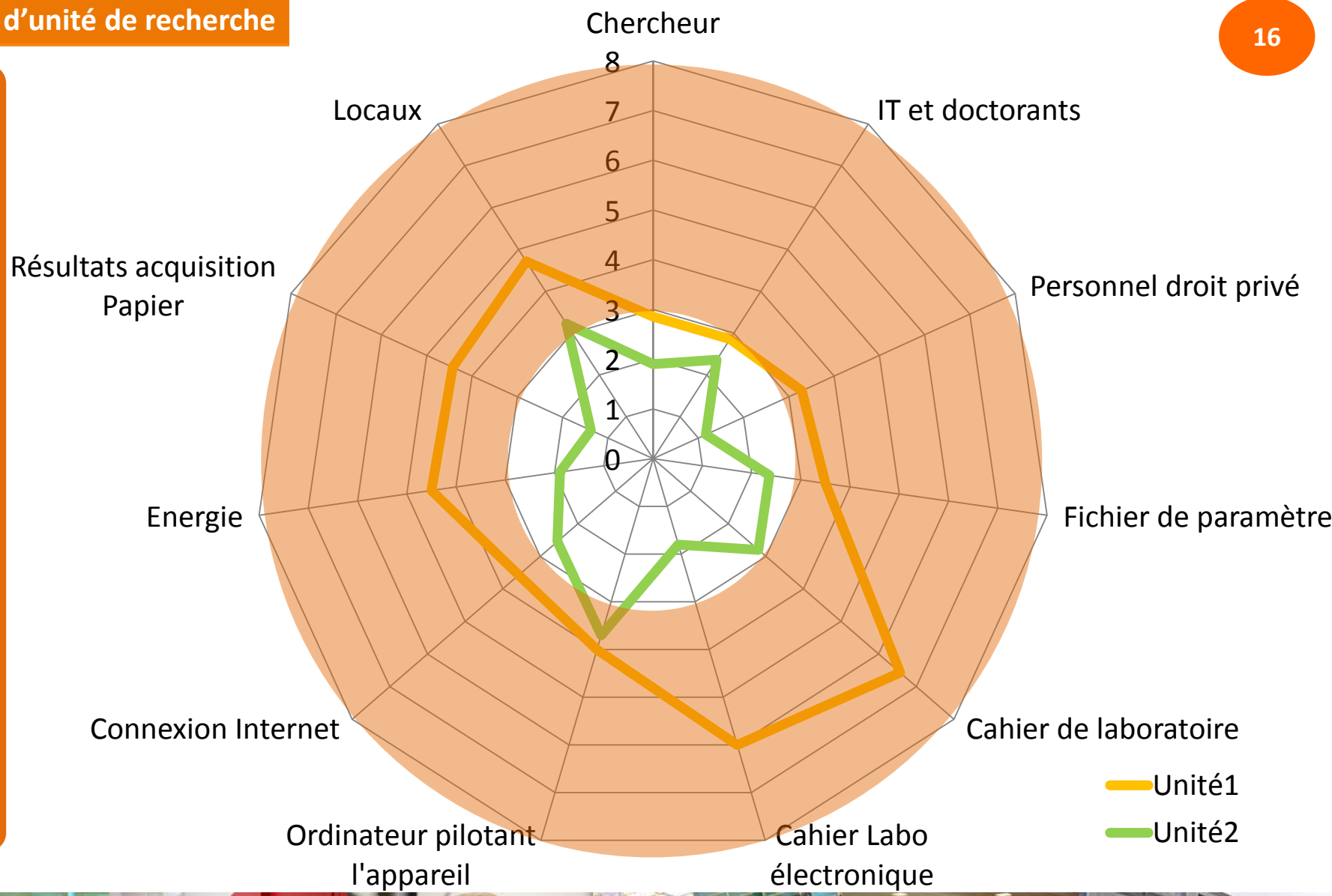
Évaluation des risques de 0 à 8 ➔



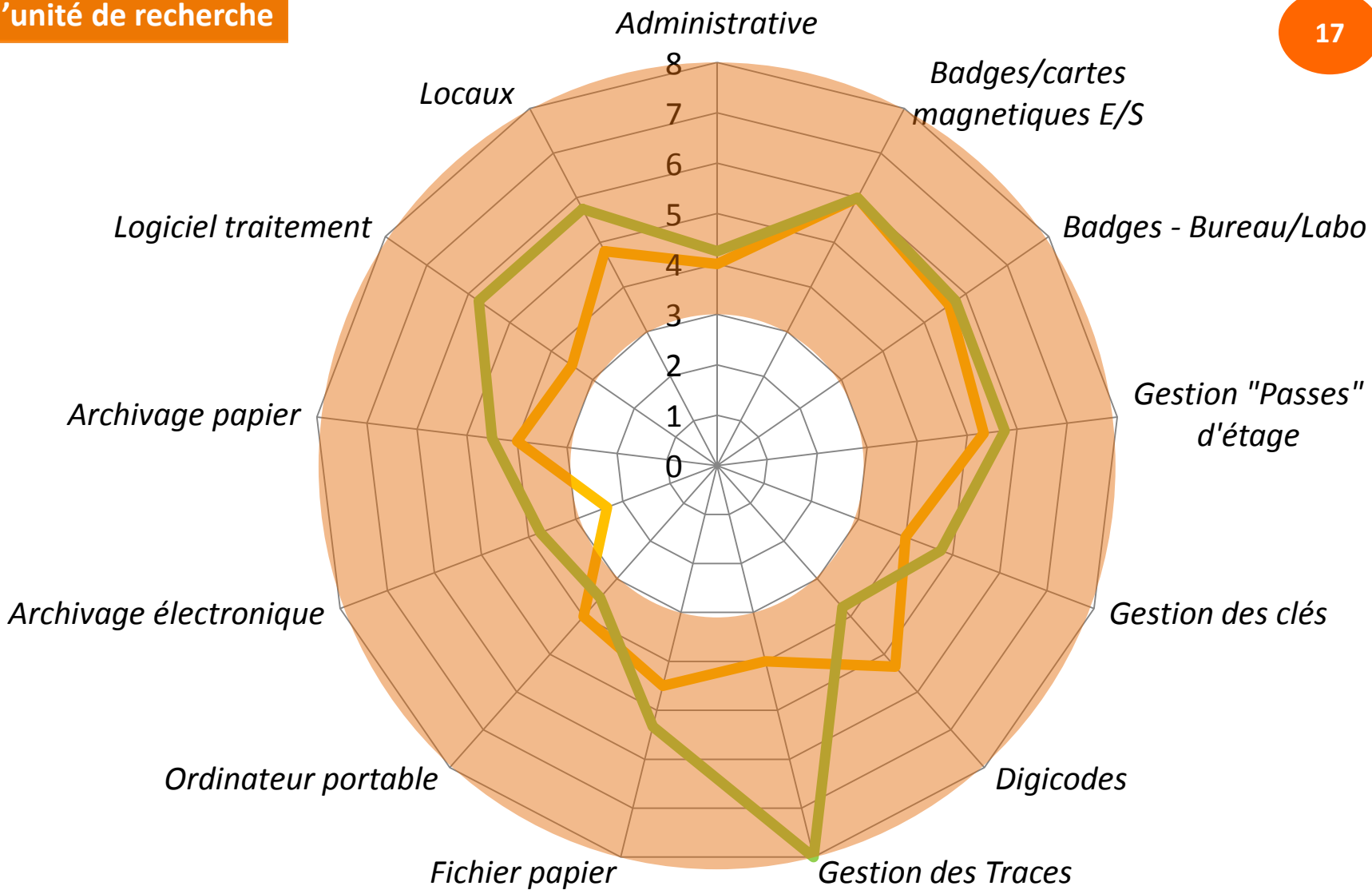
Processus Recherche
Sous processus Gestion des résultats de recherche



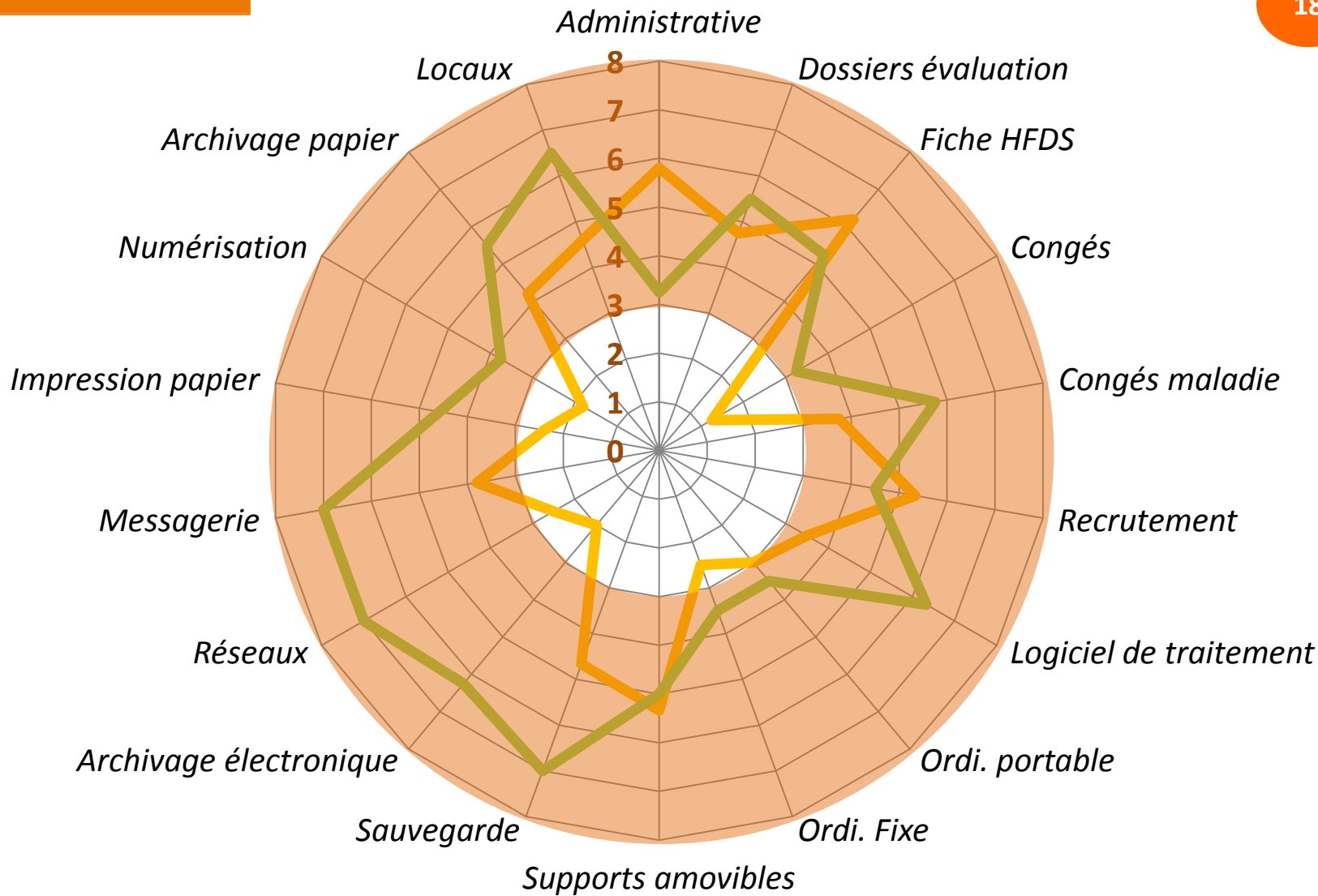
Processus Recherche
Sous processus Gestion du Protocole de mesures



Processus Administration
Sous processus Gestion des accès



Processus Administration
Sous processus Gestion RH



Feuille de route

Sensibilisation des personnels

Déploiement de la sauvegarde des postes

Chiffrement des portables et ordinateurs fixes

Messagerie
Externalisation vers DSI de l'université

Installation d'un équipement réseau de type NETASQ
Délégation d'administration

Stockage de données
externalisé à la DSI de l'université

- Politique d'achat

- Contrat de service : démarche ITIL
- Guide d'externalisation ANSSI

- Contrat de service : démarche ITIL
- Guide d'externalisation ANSSI

- Contrat de service : démarche ITIL
- Guide d'externalisation ANSSI



Feuille de route

Hébergement des startups/spin-off

- Convention d'hébergement avec Volet SSI - Guide d'externalisation ANSSI

Archives des cahiers de laboratoire

- lieux dédiés avec accès restreints

Archives contrats – missions - ...

- lieux dédiés avec accès restreints

Restructuration des locaux

- Audit sur l'usage des clés/passes/badges
- Partage des bureaux ou délocalisation de certains bureaux
- Sortie des salles d'enseignement du périmètre laboratoire

Cloisonnement du laboratoire

- gestion des accès - anti-intrusion



Elaboration de la PSSI

PSSI d'unités de recherche (Déclaration d'applicabilité)

Les mesures imposées par la norme 27001

Les mesures prévues dans la PSSI ou la charte du CNRS

Guide d'élaboration d'une PSSI opérationnelle d'unité de recherche du CNRS

Les mesures imposées par le contexte

Les mesures imposées par le référentiel SSI du CNRS

Les bonnes pratiques

Les mesures existantes

Les mesures choisies suite à l'appréciation des risques : feuille de route



Bilan de la démarche

❑ Orientée Processus METIERS

*Le propriétaire de processus est **acteur** de la SSI*

*Le propriétaire de processus se **responsabilise** face à la SSI*

*Le propriétaire de processus intègre la SSI dans ses **projets métiers***

❑ Participative

Forte sensibilisation à la SSI

Maturité SSI plus grande de l'organisation

❑ Analyse des RISQUES de l'Information

Les risques sont évalués, priorisés

La direction se responsabilise face à la SSI et fait ses choix de traitement

Les flux de l'information induisent une sensibilisation des partenaires/prestataires

Les Informations sensibles sont connues, ... donc maîtrisables

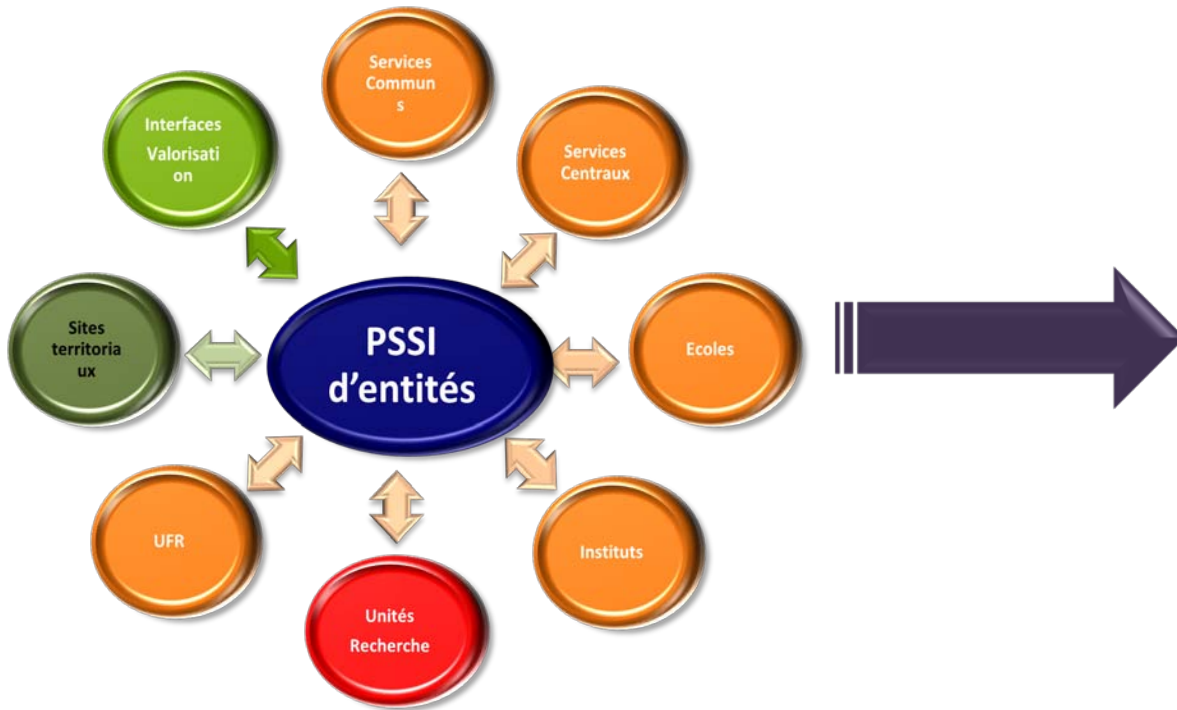
❑ Amélioration continue

Le Comité SSI prend le relais en interne et assure une amélioration continue

*Le Comité SSI est garant du caractère **participatif** de la démarche*



D'une PSSI d'unités de recherche à la PSSI d'établissement



Projets d'établissement

Points de progrès	Réponse établissement
Sensibilisation	Travail de terrain + formation + colloque
Sauvegarde des données automatiques	Projet de Datacenter
Dématérialisation	Entrepôt de données
Chiffrement des ordinateurs	Politique de chiffrement établissement
Gestion de l'archivage papier	Recrutement d'une archiviste Formation à l'archivage
Gestion des cahiers de laboratoires	Politique d'archivage – lieux dédiés
Attribution des locaux	Restructuration – réaffectation des locaux
Gestion des accès - Traces Eviter les multiplications badges/clés/passes	Carte multi-services Technologie sans contact Etude sur la cohérence des annuaires de tutelles
Sécurisation réseau	Politique d'uniformisation des équipements réseaux Délégation d'administration
Gestion du courrier papier	Etude du flux du courrier / colis
Serveurs collaboratifs	Contrat d'externalisation avec les partenaires
Dans tous les projets	Mettre un volet SSI



Missions du Responsable du Management de la Sécurité de l'Information

Création du Poste de RMSI

- Mener à bien ces projets d'établissement
- L'université a mesuré les enjeux de la sécurité de l'Information
- Les rôles et missions du RMSI – Présentation ANSSI 2012
- Positionnement du RMSI – MOA
- Positionnement du RMSI dans la chaîne fonctionnelle SSI



Missions du Responsable du Management de la Sécurité de l'Information

La mission principale consiste à développer une **culture** de la Sécurité de l'Information à l'uB.

Il s'agit d'une mission **transversale**

Le rôle principal est d'assurer la **cohérence et le management** de la **Sécurité de l'Information** de l'établissement

MISSIONS

- Mettre l'établissement en conformité avec le **RGS**
- Protéger le Potentiel Scientifique et Technique (**PPST**)
- Sensibiliser TOUS** les acteurs de l'établissement
- Avoir un rôle de **conseil, d'expertise** dans tous les projets
- Mettre en place une **démarche QUALITE ISO27001** de la Sécurité de l'Information



Organisationnel Stratégique



AQSSI

FSD

RMSI

Comité de Pilotage Stratégique
Valide et gère la PSSI,
Fait les choix concernant les **risques majeurs.**

RSSI

Comité Sécurité Opérationnel
Pilote de manière **opérationnelle** la SSI
Coordonne les **activités quotidiennes** liées à la SSI

CSSI

Comités SSI
Relai des décisions de sécurité
→ Pôles et 52 composantes
Gestion des incidents sur le terrain remontée TBDSSI

Opérationnel



CONCLUSION



- Chaîne fonctionnelle SSI
- Vice Président Numérique
- Service juridique
- CIL
- Responsables d'Informations
- Comités SSI

ACTEURS

EXTERNES

- FSSI - MESR
- Bureau HFDS MESR
- DRRI - DCRI
- ANSSI/CERTA
- RENATER / CERT

TUTELLES partenaires

- Chaînes fonctionnelles
- Services Juridiques

PARTENAIRES

ORGANISATIONNELS

- Entités Administratives
- Entités Recherche
- Entités Formation
- Pôles

TECHNIQUES

- Services
- Pôles
- Composantes

AUDIT ISO27006

SENSIBILISATION

- Formations/Séminaires
- Communications

MANAGEMENT RISQUES

- Mise en œuvre **PPST**
- Analyse risques **ISO27005**
- Gestion des Incidents
- Alertes de Sécurité
- Tableau de Bord, Veille

PILOTAGE SI

DOCUMENTS

- Lettre de Mission
- Déontologie métiers
- Bonnes pratiques
- Articles, Notes, Fiches SSI
- Liens ANSSI, CNIL
- Site Web Sécu. Information

PSSI ETABLISSEMENT

- PSSI entités
- Schéma Directeur SI → SDN

REFERENTIELS

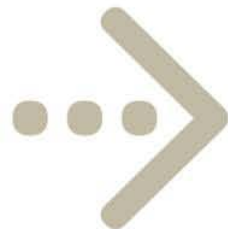
RÔLES

- Sensibilisation, Conseil
- Management Risques
- Contrôle de Conformité entre PSSI et CNIL

PROJETS

Volet Sécurité de l'Information

PROJETS METIERS



Merci de votre attention

