Tout savoir sur les Politiques de Sécurité des Systèmes d'Informations (ou presque)!

Séminaire SARI - 08 juin 2017

Marie David (CNRS/DR11)

Bernard Martinet (UGA)

Frédéric Sauveur (Grenoble-INP)

Ordre du jour

- Contexte et objectifs d'une démarche PSSI
- Panorama des PSSI institutionnelles : PSSI de l'Etat, PSSI du CNRS
- La PSSI des établissements universitaires de la COMUE UGA
- Le kit PSSI pour les UMR de la circonscription Alpes
- Questions / Réponses

Contexte : Compréhension des enjeux

De nombreuses **menaces** pèsent sur la production de la recherche

- Piratage/Vandalisme
- Intelligence économique
- Spam, phishing…
- Vol
- Négligence
- Etc…

Les unités de recherche sont soumises à des **exigences de sécurité**

- Réglementaires

  CNIL, droits d'auteur, obligation de moyen et de prudence, diffamation, etc.
- Tutélaires

  Protection du patrimoine scientifique, ZRR, etc…
- Contextuelles

  Vigipirate, …

Contexte : Compréhension des enjeux

De nombreuses **menaces** pèsent sur la production de la recherche

- Piratage/Vandalisme
- Intelligence économique
- Spam, phishing…
- Vol
- Négligence
- Etc…

Les unités de recherche sont soumises à des **exigences de sécurité**

- Réglementaires

  CNIL, dro
  de moye
  diffamati

  Règlement européen général sur la protection des données (RGPD)

- Tutélaires

  Protection du patrimoine scientifique, ZRR, etc…

- Contextuelles

  Vigipirate, …

Contexte : Difficultés dans la prise en compte de la sécurité de l'information

...Liées à un problème de formation/sensibilisation

- Membres de l'unité peu sensibilisés à la culture sécurité
- Mise en place de missions RSSI/CSSI sans formation complémentaire adéquate

…Liées à un problème de coûts

- Investissements en ressources matérielles
- Investissements en ressources humaines

…Entrainant de nombreux risques pour le laboratoire

- Pertes d'informations essentielles
- Divulgation d'informations sensibles
- Indisponibilité de services / arrêt de l'activité
- Problèmes juridiques/règlementaires
- Détérioration de l'image/perte de crédibilité
- Etc…

Contexte : Exemples d'incidents récents

- ✓ Ransomware sur le poste d'un chercheur avec le disque dur de « sauvegarde » connecté (perte totale des données)
- ✓ Défacement de plusieurs sites web institutionnels et d'unités (messages politiques, apologie du terrorisme, vente viagra…)
- ✓ Vol d'identifiant par phishing suivi d'émission de spam puis blocage du serveur de messagerie
- ✓ Vol du portable non protégé, non sauvegardé, d'un directeur d'unité occasionnant la perte de données importantes pour le laboratoire
- ✓ Plainte pour diffamation sur Facebook
- ✓ Panne de climatisation d'une salle serveur qui a entrainé l'arrêt des services pendant plusieurs heures
- ✓ Plainte d'un partenaire industriel suite à la diffusion et utilisation par la concurrence de productions de recherche dans le cadre d'un contrat

Contexte : équilibre à trouver entre productivité et sécurité

Equilibre à trouver entre ce qui est acceptable pour l'utilisateur et ce qui est nécessaire au bon fonctionnement de l'unité pour répondre à ses besoins de sécurité :

- Proposer des mesures en concertation et avec l'adhésion des utilisateurs autant que possible ;
- expliquer à quoi servent les procédures et leurs bienfondés pour l'organisation
- Éviter de multiplier les moyens de protection si ceux-ci ne sont pas respectés ;
- investir dans des procédures efficaces plutôt que dans des technologies sophistiquées
- Choisir les solutions les plus adaptées à sa propre structure, à son fonctionnement, au niveau de maturité de son unité

Contexte : équilibre à trouver entre productivité et sécurité

Equilibre à trouver entre l'évolution des technologies et des comportements et la mise en place de mesures qui constituent un frein à cette évolution :

- **Essor du cloud** : Qui fournit le service, a qui appartiennent légalement les données lorsqu'elles sont hébergées, comment les données sont-elles sauvegardées, que deviennent les données lorsque le service est arrêté ….?

- **Frontière entre vie professionnelle, vie publique et vie privée** :

  Utilisation pour le travail de « nouveaux » appareils personnels et faiblement sécurisés (BYOD)

  Des données personnelles de plus en plus présentes sur le réseau de l'unité

  Diffusion d'informations sur les réseaux sociaux

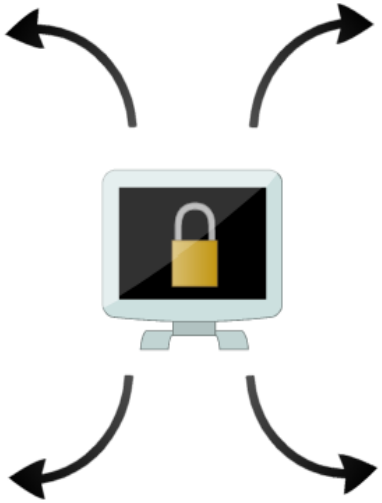
- ……

Objectifs

Améliorer la sécurité du système d'information de l'entité

Protéger le patrimoine scientifique du laboratoire

Répondre aux différentes exigences de sécurité



Renforcer l'image de marque du laboratoire et la confiance des partenaires

Améliorer l'efficience du système d'information, réduire les coûts

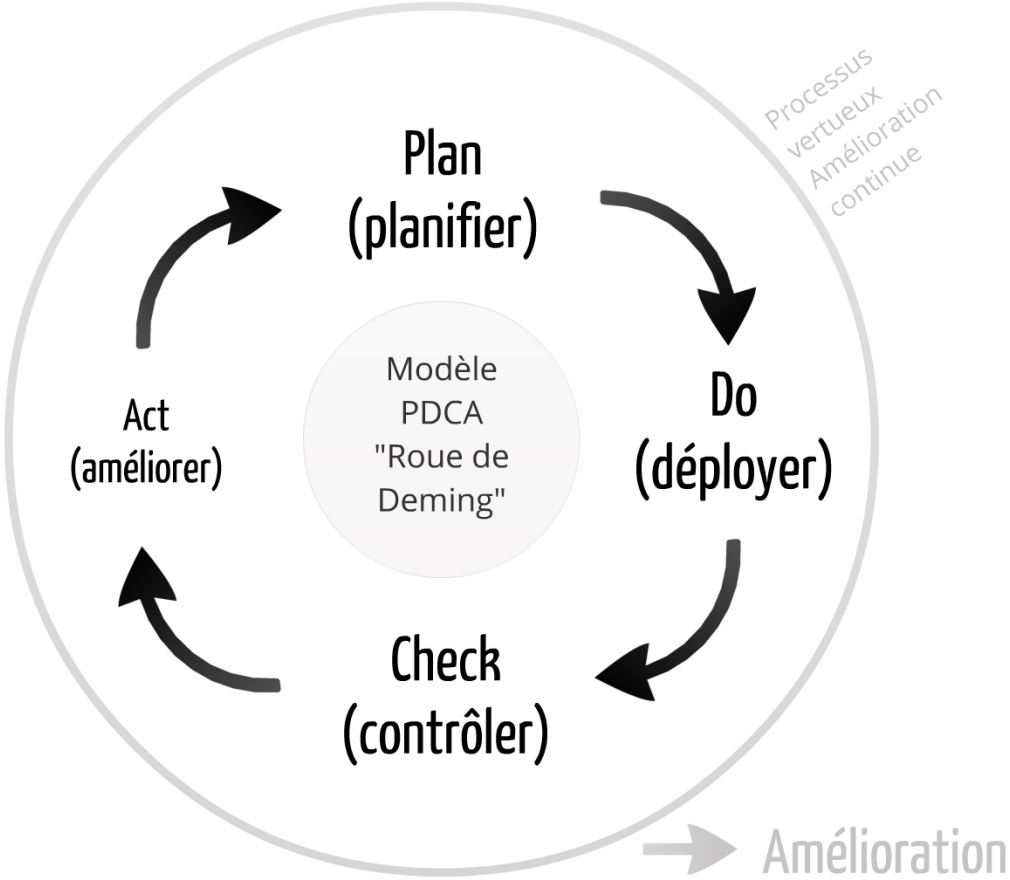
Stratégie

Comment améliorer la sécurité du système d'information de l'entité ?

- Engagement
  - Engagement de la direction
  - Implication des utilisateurs
- Moyens
  - Matériels
  - Humains
- Organisation
  - Rôles
  - Responsabilités

Méthode

- Mise en place d'un Système de management de la Sécurité de l'Information (SMSI) en suivant ISO 2700x

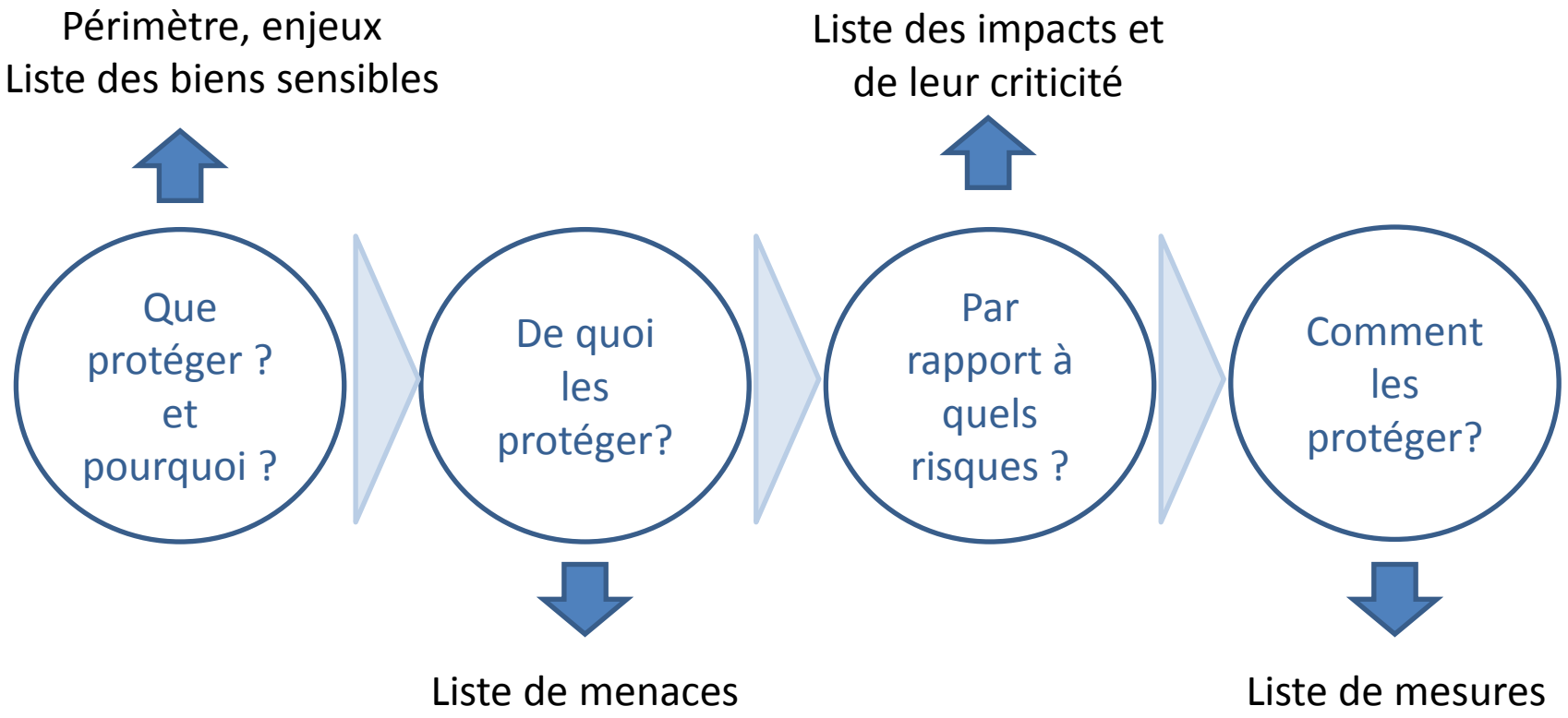


La PSSI

Au sein de ce processus, la **Politique de Sécurité du Système d'Information** (PSSI) tient une place essentielle.

« La PSSI constitue la principale référence en matière de SSI au sein de l'organisme. Elle en est un élément fondateur définissant les objectifs à atteindre et les moyens accordés pour y parvenir. »

Les questions à se poser pour construire une PSSI



Ce que l'on doit y trouver

- Champ d'application
- **Enjeux** et orientations stratégiques
- Cadre réglementaire
- Expression des besoins de sécurité (biens, menaces, impacts)
- Définitions des objectifs de sécurité (engagement pour couvrir les risques)
- Description de l'organisation mise en place

Amélioration Continue

- On ne peut pas tout résoudre d'un coup
  - Arbitrage suivant
    - Niveau de risque
    - Impacts redoutés
    - Moyens financiers et humains
    - Etc.
- Évolution du contexte, de la technologie, de la maturité en sécurité…

Bénéfices attendus

- Amélioration de la sécurité
- Réduction des coûts
- Amélioration de l'image de marque
- Protection du patrimoine scientifique
- Réponse aux obligations de moyens

Historique des PSSI enseignement/recherche

- quelques PSSI d'unités avant 2006
- PSSI du CNRS, 2006
- PSSI générique des Etablissements d'Enseignement Supérieur (Renater et 7 établissements pilotes, dont Grenoble), 2011
- PSSI du CNRS, 2014
- PSSI de l'Etat, 2014
- Kit PSSI des laboratoires site Alpes, 2016

Ordre du jour

- Contexte et objectifs d'une démarche PSSI
- Panorama des PSSI institutionnelles : **PSSI de l'Etat**, PSSI du CNRS
- La PSSI des établissements universitaires de la COMUE UGA
- Le kit PSSI pour les UMR de la circonscription Alpes
- Questions / Réponses

PSSI de l'État

Après les révélations d'E. Snowden de l'espionnage généralisé, volonté des états de protéger leur système d'information régalien.

En France :

Consolidation du pilotage des SI de l' État ; renforcement de l'Agence Nationale de Sécurité des SI (nombre de personnels multiplié par 3)

PSSI de l’ État : principes

Lorsque la maîtrise de ses systèmes d'information l'exige, l'administration fait appel à des opérateurs et des prestataires de confiance.
Tout système d'information de l'État doit faire l'objet d'une analyse de risques permettant une prise en compte préventive de sa sécurité, adaptée aux enjeux du système considéré. Cette analyse s'inscrit dans une démarche d'amélioration continue de la sécurité du système, pendant toute sa durée de vie. Cette démarche doit également permettre de maintenir à jour une cartographie précise des systèmes d'information en service.
Les moyens humains et financiers consacrés à la sécurité des systèmes d'information de l'État doivent être planifiés, quantifiés et identifiés au sein des ressources globales des systèmes d'information.
Des moyens d'authentification forte des agents de l'État sur les systèmes d'information doivent être mis en place. L'usage d'une carte à puce doit être privilégié.
Les opérations de gestion et d'administration des systèmes d'information de l'État doivent être tracées et contrôlées.
La protection des systèmes d'information doit être assurée par l'application rigoureuse de règles précises. Ces règles font l'objet de la présente PSSIE.
Chaque agent de l'État, en tant qu'utilisateur d'un système d'information, doit être informé de ses droits et devoirs mais également formé et sensibilisé à la cybersécurité. Les mesures techniques mises en place par l'État dans ce domaine doivent être connues de tous.
Les administrateurs des systèmes d'information doivent appliquer, après formation, les règles élémentaires d'hygiène informatique.
Les produits et services acquis par les administrations et destinés à assurer la sécurité des systèmes d'information de l'État doivent faire l'objet d'une évaluation et d'une attestation préalable de leur niveau de sécurité, selon une procédure reconnue par l'ANSSI (« labellisation »).
Les informations de l'administration considérées comme sensibles, en raison de leurs besoins en confidentialité, intégrité ou disponibilité, sont hébergées sur le territoire national.

PSSI de l' État : principes

Lorsque la maîtrise des systèmes d'information l'exige, faire appel à des prestataires de confiance

sécurité, adaptée aux enjeux du système considéré. Cette analyse s'inscrit dans une démarche d'amélioration continue de la sécurité du système, pendant toute sa durée de vie. Cette démarche doit également permettre de maintenir à jour une cartographie précise des systèmes d'information en service.

Les moyens humains et financiers consacrés à la sécurité des systèmes d'informations doivent être planifiés, quantifiés et identifiés

d'une carte à puce doit être privilégié.

Les opérations de gestion et d'administration des systèmes d'information de l'État doivent être tracées et contrôlées.

La protection des systèmes d'information doit être assurée par l'application rigoureuse de règles précises. Ces règles font l'objet de la présente PSSIE.

Chaque agent de l'État, en tant qu'utilisateur d'un système d'information, doit être informé de ses droits et devoirs mais également formé et sensibilisé à la cybersécurité. Les mesures techniques mises en place par l'État dans ce domaine doivent être connues de tous.

Les administrateurs des systèmes d'information doivent appliquer, après formation, les règles élémentaires d'hygiène informatique.

Les produits et services acquis par les administrations et destinés à assurer la sécurité des systèmes d'information de l'État doivent faire l'objet d'une évaluation et d'une attestation préalable de leur niveau de sécurité, selon une procédure reconnue

Les informations considérées comme sensibles, en raison de leurs besoins en confidentialité, intégrité ou disponibilité, sont hébergées sur le territoire national

PSSI de l’ État : contenu

- 182 mesures réparties en 13 sections (et 34 objectifs de sécurité)

– Politique, organisation, gouvernance	7
– Ressources humaines	6
– Gestion des biens	4
– Intégration de la SSI dans le cycle de vie des SI	10
– Sécurité physique	16
– Sécurité des réseaux	16
– Architecture des SI	3
– Exploitation des SI	71
– Sécurité du poste de travail	26
– Sécurité du développement des systèmes	9
– Traitement des incidents	4
– Continuité d'activité	8
– Conformité, audit, inspection, contrôle	2
Total	182

PSSI de l'État : mise en œuvre ?

- Quelques mesures très éloignées des pratiques
  - L'hébergement des données sensibles de l'administration sur le territoire national est obligatoire, sauf accord du HFDS, et dérogation dûment motivée et précisée dans la décision d'homologation.
  - Les postes de travail (ordiphones, équipements informatiques nomades et fixes ou de supports de stockage amovibles) utilisés dans le cadre professionnel sont fournis et gérés par l'équipe locale chargée des SI.

Ordre du jour

- Contexte et objectifs d'une démarche PSSI
- Panorama des PSSI institutionnelles : PSSI de l'Etat, **PSSI du CNRS**
- La PSSI des établissements universitaires de la COMUE UGA
- Le kit PSSI pour les UMR de la circonscription Alpes
- Questions / Réponses

PSSI du CNRS

On parle plutôt en termes de **PGSI** et **PSSIO**

- Les grands principes de la Politique Générale (PGSI) sont les suivants :
  - L'ensemble du périmètre placé sous la responsabilité du CNRS doit être couvert ;
  - Toutes les exigences légales et réglementaires doivent être prises en compte ;
  - La gestion des risques doit être réalisée de façon systématique suivant la règlementation Française et les normes internationales en vigueur ;
  - L'organisation qui est mise en place pour piloter et mettre en œuvre cette politique doit disposer des moyens humains compétents en nombre suffisant ;
  - Les mesures de protection devront être complétées par des mesures de défense active efficaces ;
  - L'application de cette politique est contrôlée

PSSI du CNRS

- Deux Politiques des SI (PSSI) opérationnelles (Services, Laboratoires) précisent l'organisation.
- Des règles pragmatiques, applicables, classées en 3 catégories *,**,*** sur l'ensemble des domaines IS:
  - **Niveau ***: niveau fort *(unité incluant des SI ou manipulant des informations dont le niveau de sensibilité est «critique», unité déclarée protégée au titre de la PPST et incluant une ZRR)*
  - **Niveau **:** niveau standard *(unité incluant des SI ou manipulant des informations dont le niveau de sensibilité est «très sensible», unité de type administratif (DR, unité du Siège, etc.)*
  - **Niveau ***: niveau élémentaire (*unité dans tous les autres cas)*
- Des fiches détaillées pour chacune des règles

PSSI du CNRS

- Ces PSSI opérationnelles définissent les mesures et procédures applicables sur l'ensemble des domaines suivants :
  - **1. Politique de sécurité** (identification des règles et modalités d'application en fonction du niveau sécurité cible)
  - **2. Organisation** (définition détaillée des rôles et responsabilités en SSI)
  - **3. Gestion des actifs** (niveaux de classification des informations et des biens en fonction de leur sensibilité et mesures de protection applicables)
  - **4. Ressources humaines** (mesures de protection des informations liées à la gestion des ressources humaines)
  - **5. Sécurité physique** (mesures SSI liées à la gestion des sites et locaux abritant l'information)
  - **6. Exploitation** (mesures SSI concernant l'acquisition, la configuration, l'attribution et l'exploitation des matériels qui traitent les informations : réseaux, serveurs, postes de travail fixes et mobiles, etc.)
  - **7. Contrôle d'accès** (mesures SSI concernant la gestion des droits d'accès aux systèmes d'information et aux moyens d'authentification des utilisateurs)
  - **8. Intégration de la sécurité dans les projets** (mesures SSI liées à l'acquisition, la conception, le développement et la maintenance des SI de gestion et scientifiques)
  - **9. Gestion des incidents** (mesures concernant la gestion des incidents de sécurité liés aux SI)
  - **10. Continuité d'activité** (mesures liées à la prise en compte des besoins de continuité d'activité des SI)
  - **11. Conformité** (mesures concernant la prise en compte du référentiel législatif et réglementaire, l'homologation SSI et mesures concernant les audits de l'application de la PSSI

En résumé

Plusieurs catalogues de mesures de sécurité :

- longs,
- cohérents mais différents,
- mesures plus ou moins pertinentes, plus ou moins bien rédigées,
- à choisir après une analyse de risques, à adapter au contexte

mais ces PSSI sont à appliquer obligatoirement !

Ordre du jour

- Contexte et objectifs d'une démarche PSSI
- Panorama des PSSI institutionnelles : PSSI de l'Etat, PSSI du CNRS
- La PSSI des établissements universitaires de la COMUE UGA
- Le kit PSSI pour les UMR de la circonscription Alpes
- Questions / Réponses

Un projet inter-universitaire pilote national

- Objectifs
  - Produire une politique de sécurité pour l'« Université de Grenoble »
  - Fournir des éléments génériques, « boite à outils » nationale

- Périmètres fonctionnels
  - **Gestion**
  - **Formation**
  - **Recherche**

- Périmètre établissements universitaires du PRES
  - Examen détaillé des services mutualisés (SIMSU)
  - Examen des domaines fonctionnels par échantillonnage parmi les établissements
  - Examen succinct de laboratoires : projet PSSI d'UMR, commun avec le CNRS

- Pilotage
  - comité de pilotage interuniversitaire des systèmes d'informations (CPISI)
  - correspondant informatique et libertés
  - chefs de projet

Quelques risques identifiés

ALIM_ENERGIE.1: Une défaillance de la tête d'alimentation entraîne une coupure d'alimentation sur le site.

DIVULGATION 3 : Un membre d'un centre de recherche répond à des sollicitations sans vérification de l'origine de la demande, et divulgue ainsi de l'information sensible

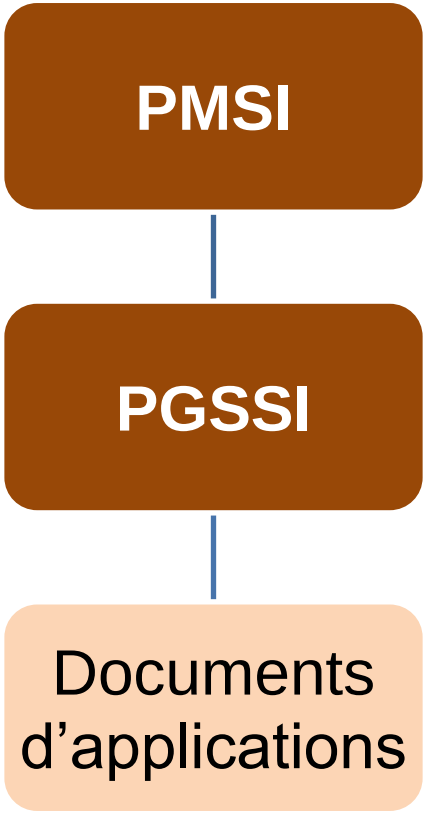
UTILISATION_ILLICITE.4: Un poste nomade dévolu à la gestion est utilisé à des fins familiales, prêté à des tiers, … Le poste est infecté par un malware, ou des données sensibles sont récupérées par des tiers.

VOL_SUPPORT.3 : Un personnel emporte avec lui des documents ou supports sensibles, qu'il souhaite étudier lors d'une conférence, à son domicile, … Ces documents ou supports lui sont dérobés lors de ses déplacements, à l'hôtel ou à son domicile.

MAINTIEN_SI.1 : La complexité du système d'information le rend difficile à maîtriser, se répercutant sur la maintenabilité des équipements.

ERREUR_UTILISATION.1 : Un utilisateur envoie par erreur un mail contenant des informations confidentielles au mauvais destinataire, provoquant la divulgation de ces informations.

Documents constitutifs de la PSSI



- 3 documents d'analyse de risques (Gestion, Pédagogie, Recherche)

- Politique de Management de la Sécurité de l'Information
  - Description de l'organisation, énoncé des principes généraux
- Politique Générale de Sécurité du Système d'Information
  - Document décrivant le principe de management de la sécurité et les exigences de sécurité conformément à la norme ISO 27002
- Documents d'applications / Plan d'action de traitement des risques
  - Documents basés sur l'analyse de risques, décrivant les actions correctives et préventives décidées et leur plan de déploiement.
  - Documents annexes (Chartes, Politique de traces…)

Politique de management de la SSI

Les niveaux	Le niveau **Stratégique** « la politique »	Le niveau **Opérationnel** « le terrain »
Le niveau **Établissement**	**Le Comité de Pilotage Stratégique** ■ composition : comité de pilotage du système d'information de l'établissement ■ 1 réunion par an dédiée à la SSI	Le **RSSI** et sa **chaîne fonctionnelle SSI**
Le niveau **Inter-U**	**Le Comité de Sécurité Opérationnel** ■ compositi… DGS, … RSSI ■ 3 … ar an minimum Recomposition en cours à l'échelle de la COMUE	**Le Comité de Liaison** ■ composition : les RSSI + personnes concernées ■ 1 réunion par semaine

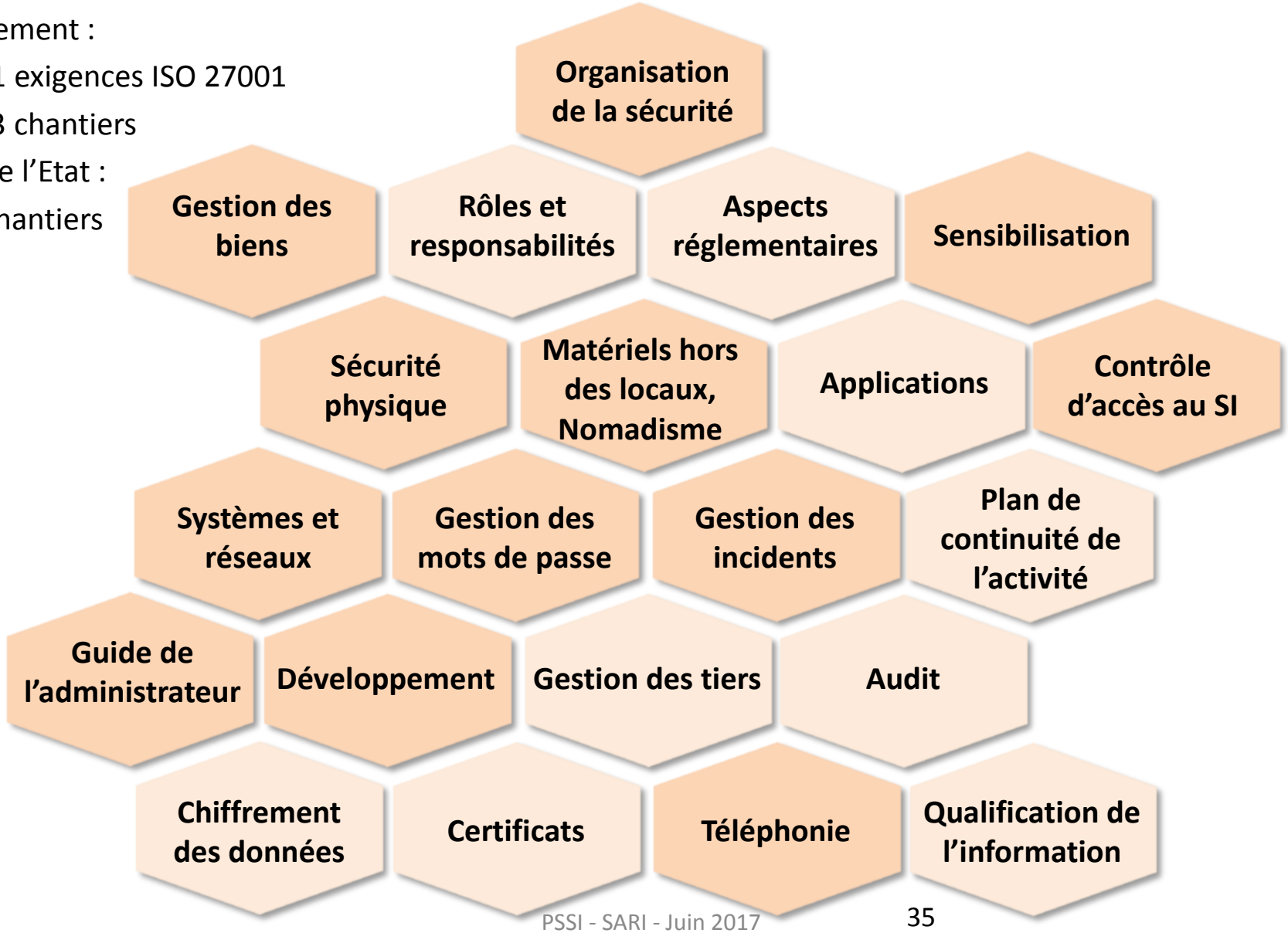
Mesures de sécurité / chantiers

Initialement :

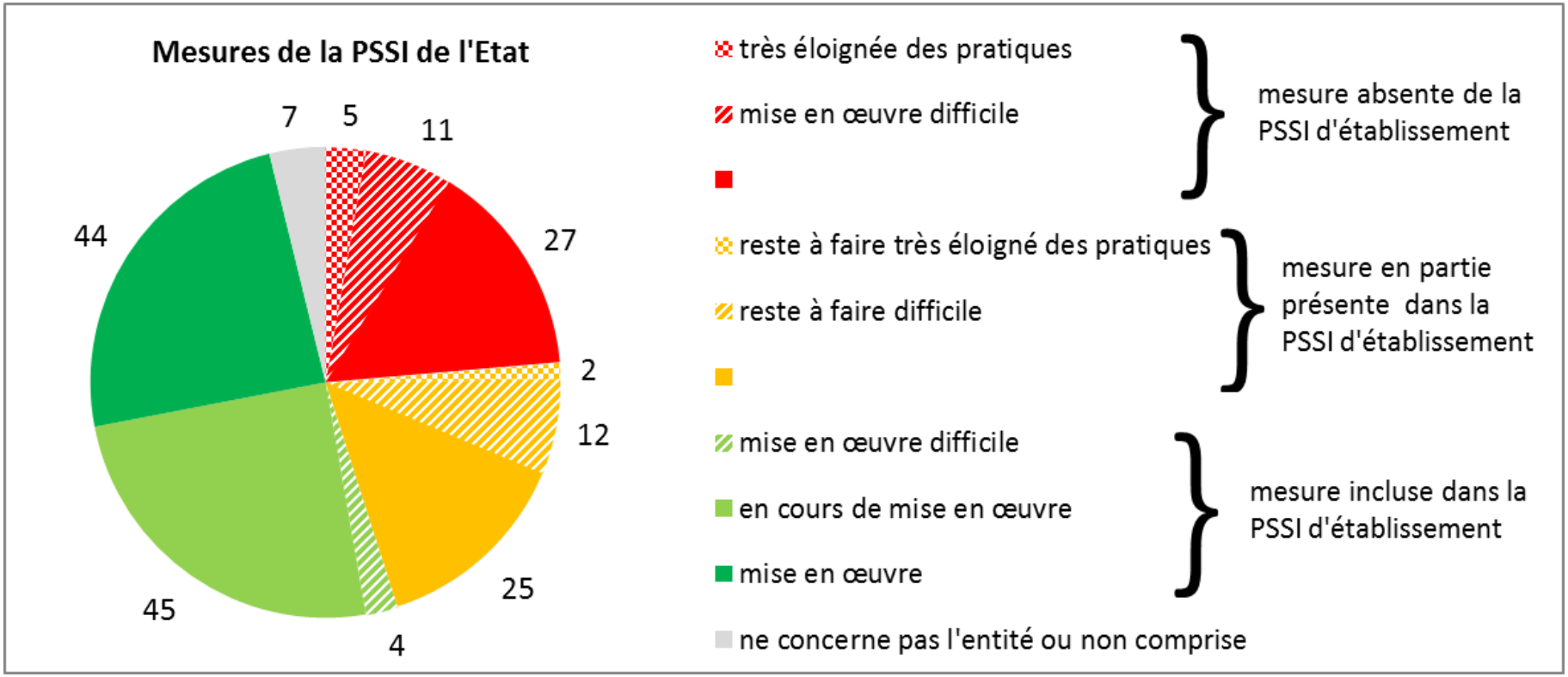
- 41 exigences ISO 27001
- 13 chantiers

PSSI de l'Etat :

+ 8 chantiers



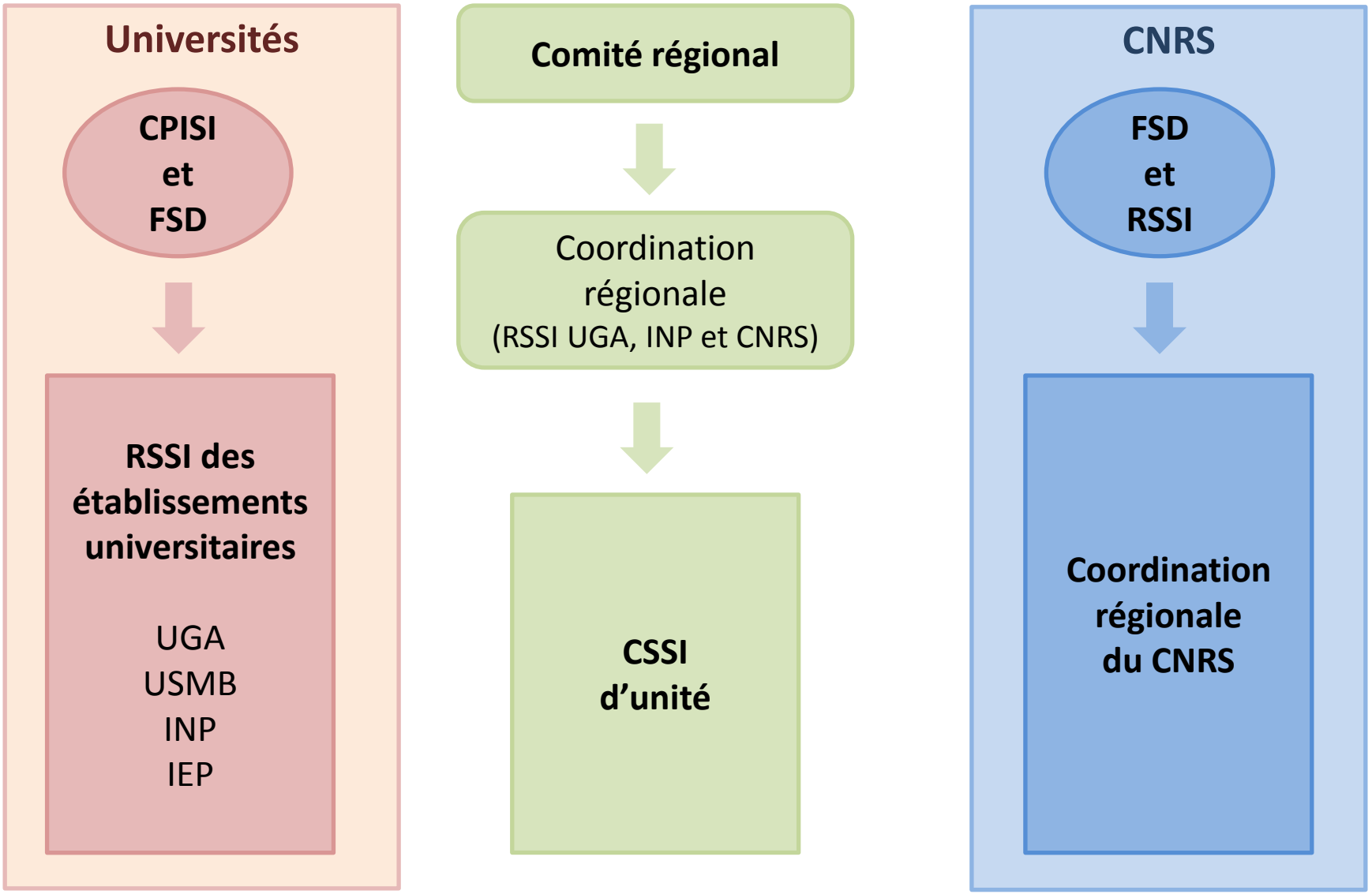
Etat des lieux PSSI UdG vs PSSI Etat (fin 2014)



Ordre du jour

- Contexte et objectifs d'une démarche PSSI
- Panorama des PSSI institutionnelles : PSSI de l'Etat, PSSI du CNRS
- La PSSI des établissements universitaires de la COMUE UGA
- Le kit PSSI pour les UMR de la circonscription Alpes
- Questions / Réponses

Management de la SSI sur le site Alpes



Organisation institutionnelle sur la circonscription Alpes : le comité d'orientation et de cadrage de la SSI des UMR

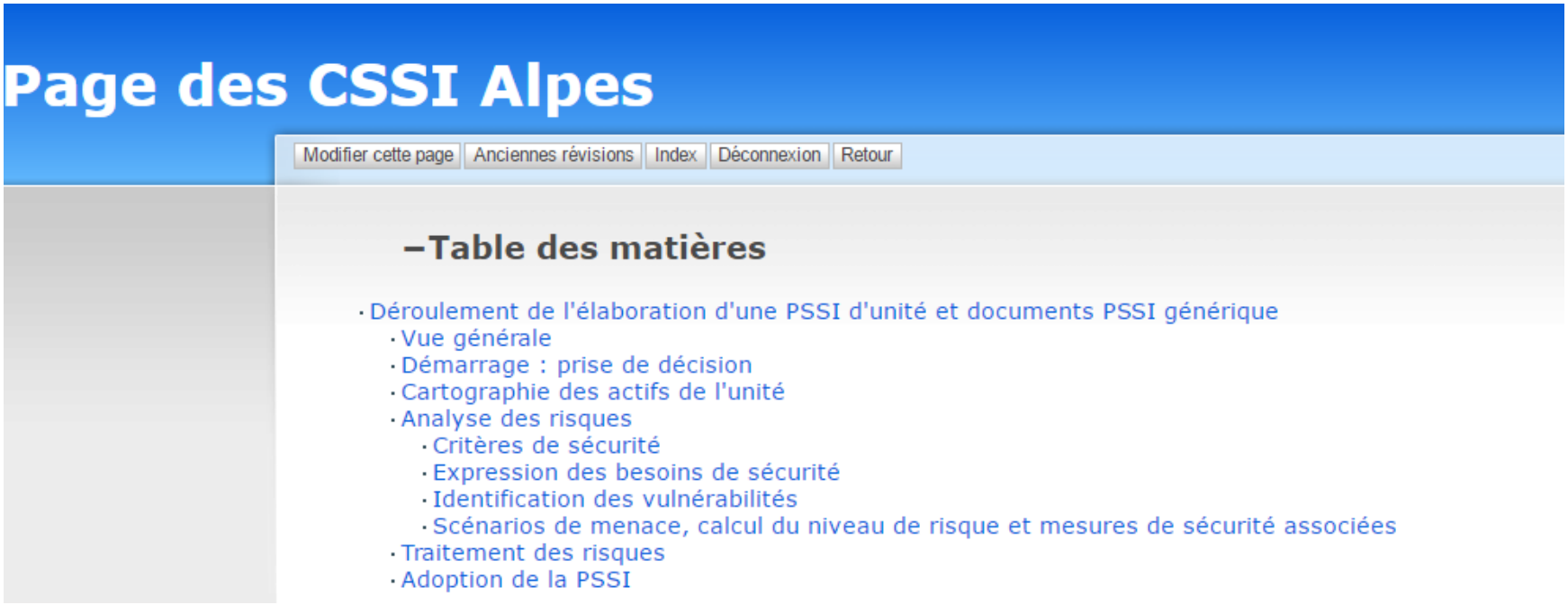
- Composition
  - Le délégué régional du CNRS
  - Un représentant du CPISI
  - Les représentants désignés par les universités et le CNRS (VP Recherche, FSD, RSSI)
  - La coordination régionale

- Rôle
  - Pilotage collégial de la SSI des Unités de Recherche
  - Cadrage de la SSI des UMR : cohérence avec la SSI des tutelles
  - Animation du réseau des CSSI : délégation aux coordinateurs
  - Mise en place des principes de partage et de responsabilité

Le Kit PSSI

https://cssi.grenoble.cnrs.fr/dokuwiki/

Déroulé de l'élaboration d'une PSSI

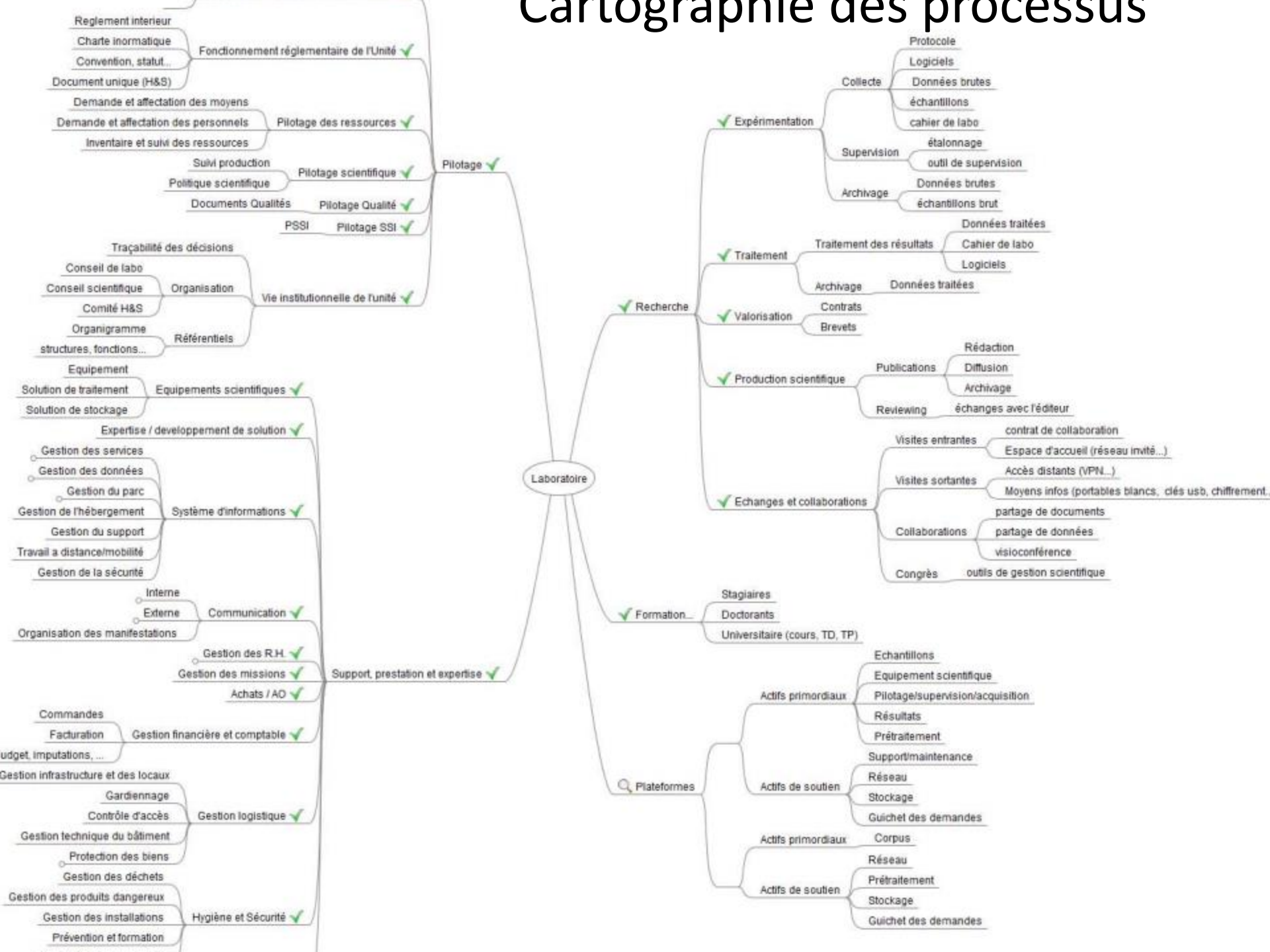


Organisation type

Préconisation d'organisation de la PSSI dans l'unité

Niveau	Niveau **Stratégique** « la politique »	Niveau **Pilotage** « La mise en œuvre »	Niveau **Opérationnel** « le terrain »
Responsabilités	Le directeur d'unité et le conseil de laboratoire 1 fois par an mis à l'ordre du jour du CL	**Le Comité de Sécurité de l'information** ▪ composition : - 1à N représentant de la direction, - 1 à N représentants des équipes de recherche, - 1 à N représentant administratif, - le CSSI de l'unité ▪ 1 réunion par trimestre	**Le CSSI et sa chaîne fonctionnelle SSI**
Rôle	▪ Responsabilité de la SSI ▪ Cadrage stratégique ▪ Déclinaison des moyens ▪ Validation des objectifs annuels	▪ Lancement et communication sur la PSSI ▪ Mise en Œuvre et suivi de la PSSI ▪ Revue annuelle de la PSSI et fixation des objectifs d'amélioration continue	▪ Garant de la mise en œuvre des mesures de sécurité ▪ Accompagnement des métiers, formations et sensibilisations ▪ Alerte sur incident et accompagnement ▪ Participation à la chaine fonctionnelle SSI régionale

Cartographie des processus



Expression des besoins de sécurité

Laboratoires témoins

périmètre Support

Regroupement	processus	Description (actifs primordiaux)	Applications utilisées	D	I	C	P	Commentaires / impacts
Gestion des Ressources Humaines	Carrières	dossier d'évaluation, primes	- CNRS : Sirhus, papier - INP et UJF : Safia - CNRS : crac (primes) - Application locale	0	1	3	2	D: I : C: P: 0 à 2 selon les laboratoires
	Fonctions et compétences	Fiches de postes, entretiens d'activités	Sirhus, Safia, papier	0	1	3	1	D: I : C: P: 0 à 2 selon les laboratoires
	Recrutement et accueil	noemi, candidatures, contrats de travail, dossiers visiteurs, doctorants, post-docs, stagiaires	Mail, application locale, papier	1	1	3	2	D: I : C: P: 0 à 2 selon les laboratoires
	Congés, absences Agendas	congés, CET, justifications d'absences, agendas	application locale, papier	0	1	2	2	D: I : C: P:
	Formation du personnel	PFU, DIF, PIF		0	1	2	2	D: I : C: 0 à 2 selon les laboratoires et les processus P: 0 à 2 selon les laboratoires et les processus
Gestion financière et comptable	Dépenses	commandes, factures, dépenses de personnel	Applications des tutelles ou financeurs (Geslab, Sifac) ; bureautique	1	3	3	2	D: I : C: P:
	Recettes	colloques, recettes contrat et brevets, prestations	- Applications des tutelles ou financeurs (Sifac, Geslab) ; - Colloques : terminal carte paiement, papier	1	3	2	2	D: 0 à 3 selon les laboratoires, les processus, le calendrier I : C: P: 1 à 3 selon les laboratoires, les processus
	Budget, Imputations	demandes moyens, tableaux financiers, budget prévisionnel	Applications des tutelles ou financeurs (Geslab, Sifac) ; bureautique	1	3	2	2	D: I : C: P:
Gestion des missions	Missions	demandes, ordres, justificatifs, documents mission étranger	Applications des tutelles ou financeurs (Geslab, Sifac, Simbad) ; bureautique	2	2	1	2	D: I : C: 1 sauf pour les missions à l'étranger. P:

Homogène (identique ou très proche si un labo a donné plusieurs valeurs, distantes de 1 au max)
Proches (max-min=1)
Données d'un seul laboratoire
Hétérogène (max - min = 2 ou 3)

Déclaration d'applicabilité et tableau de bord de mise en œuvre

Mesures ISO 27001:2005 Annexe A			Références et commentaires	Niveau de risque des 3 laboratoires pilotes				Laboratoire UMRXXXX				
				Niv. 4	Niv. 3	Niv. 2	Niv. 1	Niv. de la mesure (1 2 3 4)	Traitement des risques	Mesure	Mise en œuvre	Commentaires de mise en œuvre
Clause	Numér	Objectif / Mesure										
	11.5.1	Ouverture de sessions sécurisées										
	11.5.2	Identification et authentification de l'utilisateur	AUT-1			*	*		Accepter	Seuls les comptes individuels (non partagés) sont autorisés pour l'identification préalable à l'accès aux ressources informatiques	0%	
	11.5.3	Système de gestion des mots de passe				*	*		Accepter	Les mots de passe doivent être complexes, changés régulièrement, stockés de manière chiffrée. Les mots de passe sont personnels et incessibles.	0%	
	11.5.4	Emploi des utilitaires système										
	11.5.5	Déconnexion automatique des sessions inactives			2/3	*	*		Accepter	Les sessions applicatives doivent être déconnectées après une période d'inactivité définie au cas par cas.	0%	
	11.5.6	Limitation du temps de connexion										
	11.6	Contrôle d'accès aux applications et à l'information										
	11.6.1	Restriction d'accès à l'information										
	11.6.2	Isolement des systèmes sensibles										
	11.7	Informatique mobile et télétravail										
	11.7.1	Informatique et communications										
	11.7.2	Télétravail										
	12.1	Exigences de sécurité applicables aux systèmes d'information										
	12.1.1	Analyse et spécification des exigences de sécurité										
	12.2	Bon fonctionnement des applications										
	12.2.1	Validation des données en entrée			*	*	*		Accepter	Dans chaque application, un mécanisme de validation de la cohérence des données entrées doit être mis en place.	0%	
	12.2.2	Mesure relative au traitement interne										
	12.2.3	Intégrité des messages										
	12.2.4	Validation des données en sortie										
	12.3	Mesures cryptographiques										
	12.3.1	Politique d'utilisation des mesures cryptographiques	PDI-2		*	*	*		Accepter	Identifier les données sensibles. Chiffrer selon l'état de l'art les flux et supports matériels mobiles sur lesquels transitent ces données sensibles.	0%	
	12.3.2	Gestion des clés										
	12.4	Sécurité des fichiers système										
Acquisi										Seuls les logiciels, dont la provenance est connue et homologués, peuvent être installés sur les différents systèmes. Les		

Ordre du jour

- Contexte et objectifs d'une démarche PSSI
- Panorama des PSSI institutionnelles : PSSI de l'Etat, PSSI du CNRS
- La PSSI des établissements universitaires de la COMUE UGA
- Le kit PSSI pour les UMR de la circonscription Alpes
- Questions / Réponses