présanse
PRÉVENTION ET SANTÉ AU TRAVAIL

Mise en œuvre de la Politique Générale de Sécurité des Systèmes d'Information en Santé en SPSTI

Webinaire – Mardi 8 octobre 2024 – 14h00-15h00

Mise en œuvre de la Politique Générale de Sécurité des Systèmes d'Information en Santé en SPSTI

Plan du webinaire

1. Introduction
2. Rappel sur la PGSSI-S
3. Présentation de l'outil « *Plan d'Actions PGSSI-S* »
4. Echanges avec les participants (Questions/Réponses)
5. Conclusion et projets

①

Introduction

Le réseau Présanse (1/2)

présanse
PRÉVENTION ET SANTÉ AU TRAVAIL

Prévention
Santé au travail
Services
Entreprises

Association à but non lucratif (loi 1901), Présanse est l'organisme représentatif des services interentreprises de Santé et de Prévention au Travail (SPSTI).

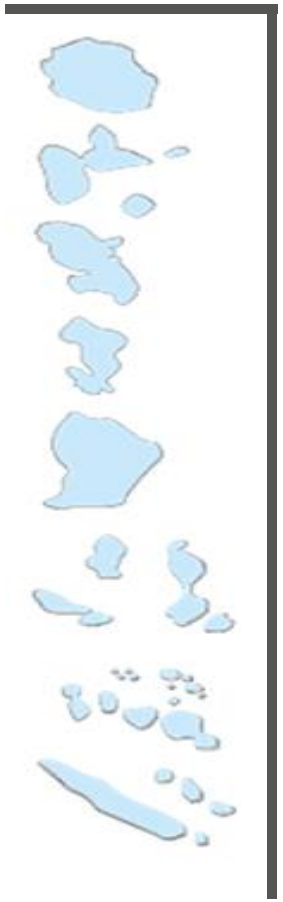
Présanse regroupe près de 160 SPSTI (hors SPSTI dédiés exclusivement au BTP) organisés sous la forme d'associations à but non lucratif et administrés par les bénéficiaires du système (employeurs et salariés). Ils couvrent l'ensemble du territoire national.

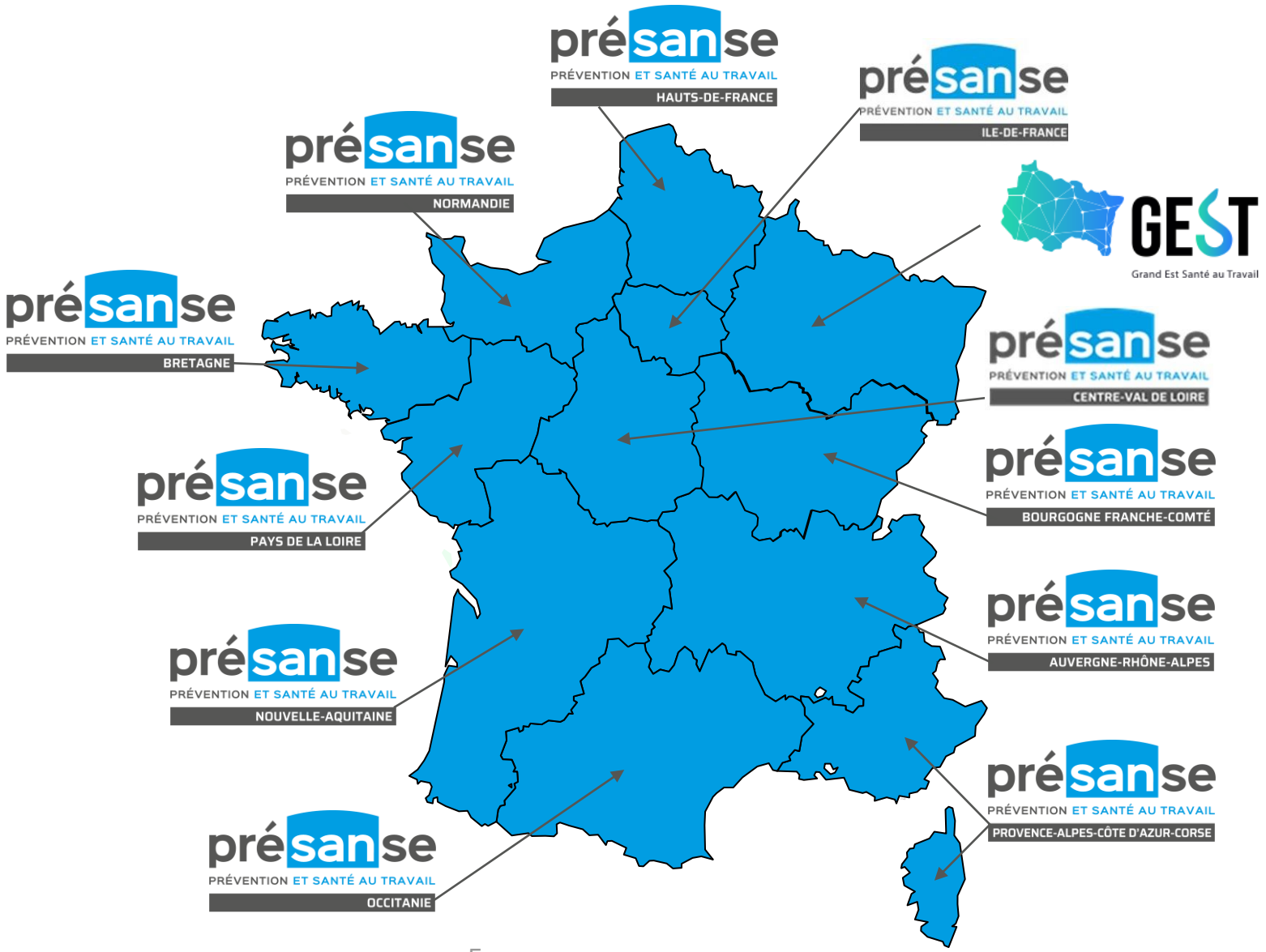
Ces Services emploient plus de 18 000 collaborateurs dont plus de 4 300 médecins du travail et 7 000 Intervenants en Santé au travail.

Présanse s'appuie sur des associations régionales de SPSTI.

Le réseau Présanse (2/2)

En cours de structuration



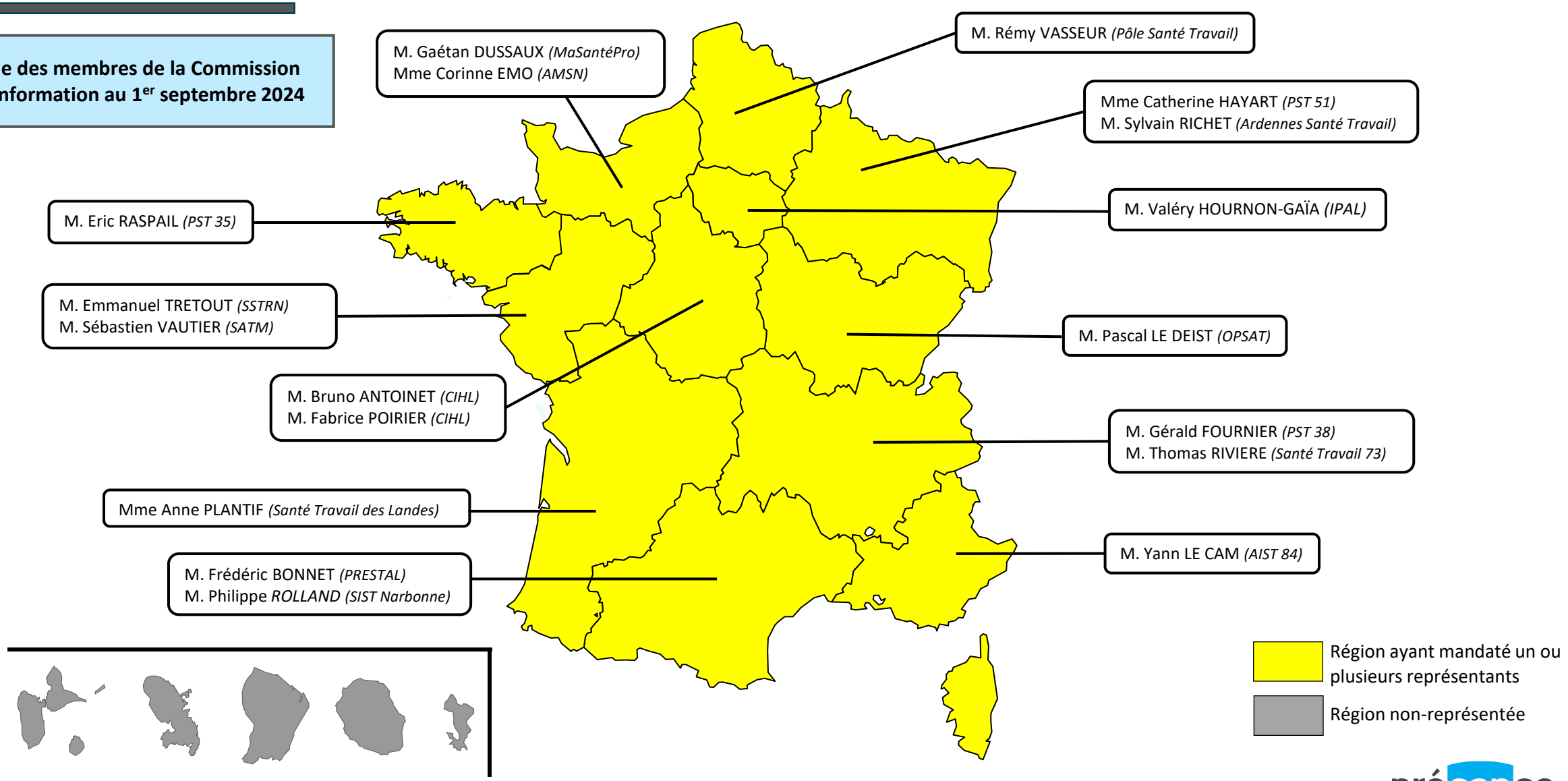


Les groupes de travail du Pôle Médico-Technique de Présanse

- Groupe Référents Thésaurus
- Groupe Médecins Relais
- Commission Système d'Information
- Groupes de travail Thésaurus
- Groupe de travail Fiches Médico-Professionnelles
- Groupe de travail Toxicologie
- Groupes de travail usage de la donnée et éthique
- Groupe de travail prévention des conduites addictives
- Groupe de travail pratiques infirmiers

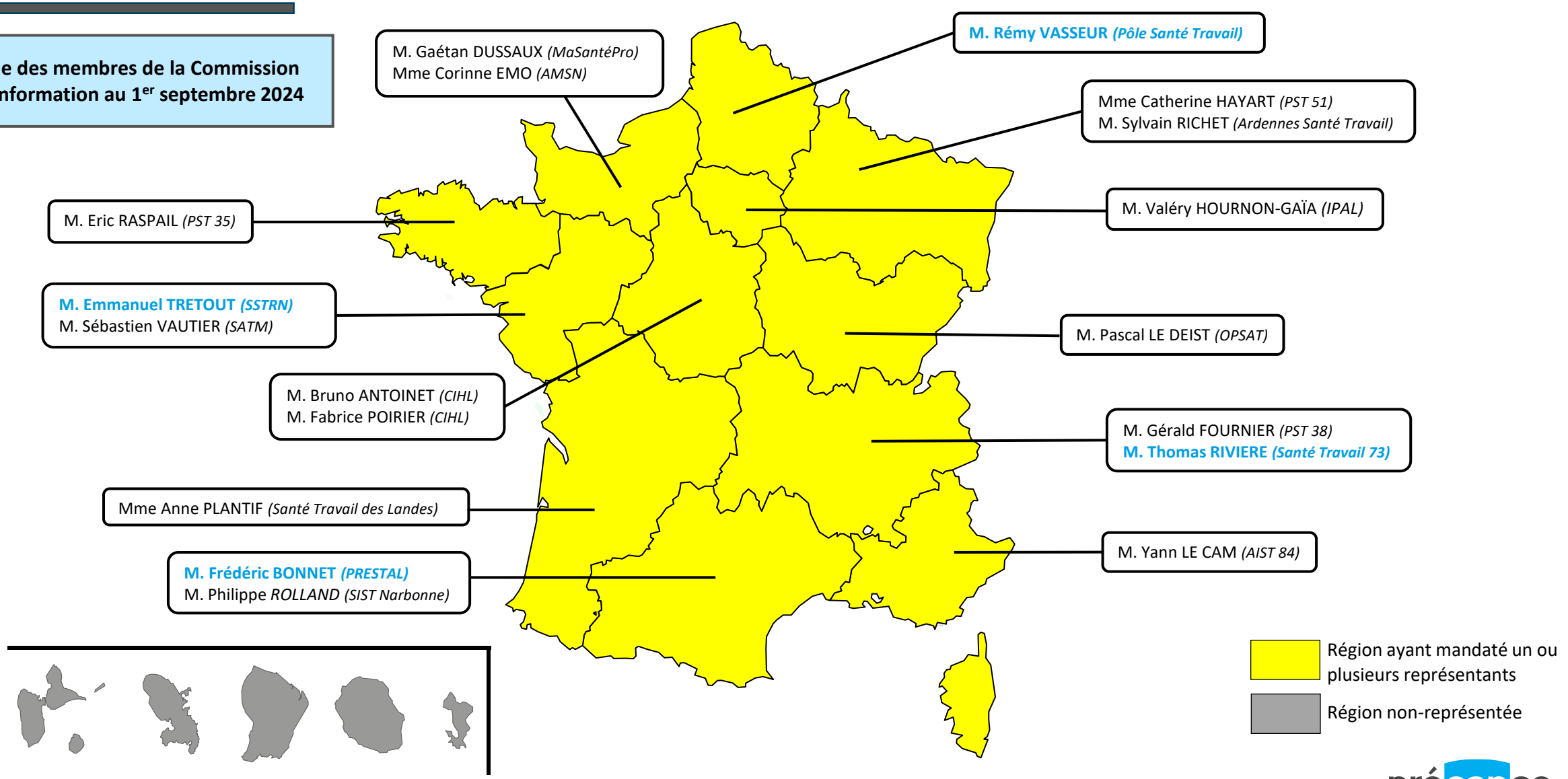
La Commission Système d'Information de Présanse

Cartographie des membres de la Commission Système d'Information au 1er septembre 2024



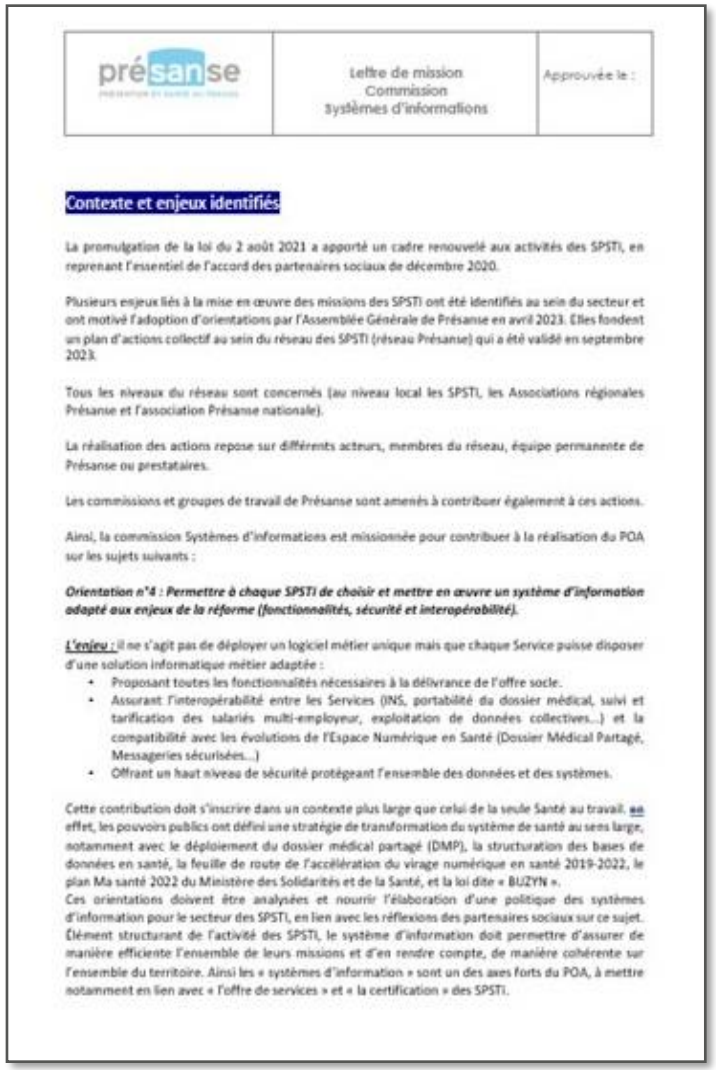
La Commission Système d'Information de Présanse

Cartographie des membres de la Commission Système d'Information au 1er septembre 2024



Les missions de la Commission Système d'Information (1/2)

Lettre de mission à la CSI articulée avec l'orientation n°4 du POA de Présanse : « ***Permettre à chaque SPSTI de choisir et mettre en œuvre un système d'information adapté aux enjeux de la réforme (fonctionnalités, sécurité et interopérabilité)*** »



présanse | Lettre de mission Commission Systèmes d'informations | Approuvée le :

Contexte et enjeux identifiés

La promulgation de la loi du 2 août 2021 a apporté un cadre renouvelé aux activités des SPSTI, en reprenant l'essentiel de l'accord des partenaires sociaux de décembre 2020.

Plusieurs enjeux liés à la mise en œuvre des missions des SPSTI ont été identifiés au sein du secteur et ont motivé l'adoption d'orientations par l'Assemblée Générale de Présanse en avril 2023. Elles fondent un plan d'actions collectif au sein du réseau des SPSTI (réseau Présanse) qui a été validé en septembre 2023.

Tous les niveaux du réseau sont concernés (au niveau local les SPSTI, les Associations régionales Présanse et l'association Présanse nationale).

La réalisation des actions repose sur différents acteurs, membres du réseau, équipe permanente de Présanse ou prestataires.

Les commissions et groupes de travail de Présanse sont amenés à contribuer également à ces actions.

Ainsi, la commission Systèmes d'informations est missionnée pour contribuer à la réalisation du POA sur les sujets suivants :

Orientation n°4 : Permettre à chaque SPSTI de choisir et mettre en œuvre un système d'information adapté aux enjeux de la réforme (fonctionnalités, sécurité et interopérabilité).

L'enjeu : Il ne s'agit pas de déployer un logiciel métier unique mais que chaque Service puisse disposer d'une solution informatique métier adaptée :

- Proposant toutes les fonctionnalités nécessaires à la délivrance de l'offre socle.
- Assurant l'interopérabilité entre les Services (INS, portabilité du dossier médical, suivi et tarification des salariés multi-employeur, exploitation de données collectives…) et la compatibilité avec les évolutions de l'Espace Numérique en Santé (Dossier Médical Partagé, Messageries sécurisées…)
- Offrant un haut niveau de sécurité protégeant l'ensemble des données et des systèmes.

Cette contribution doit s'inscrire dans un contexte plus large que celui de la seule Santé au travail. En effet, les pouvoirs publics ont défini une stratégie de transformation du système de santé au sens large, notamment avec le déploiement du dossier médical partagé (DMP), la structuration des bases de données en santé, la feuille de route de l'accélération du virage numérique en santé 2019-2022, le plan Ma santé 2022 du Ministère des Solidarités et de la Santé, et la loi dite « BUZYN ».
Ces orientations doivent être analysées et nourrir l'élaboration d'une politique des systèmes d'information pour le secteur des SPSTI, en lien avec les réflexions des partenaires sociaux sur ce sujet. Élément structurant de l'activité des SPSTI, le système d'information doit permettre d'assurer de manière efficiente l'ensemble de leurs missions et d'en rendre compte, de manière cohérente sur l'ensemble du territoire. Ainsi les « systèmes d'information » sont un des axes forts du POA, à mettre notamment en lien avec « l'offre de services » et « la certification » des SPSTI.

Les missions de la Commission Système d'Information (2/2)

Déclinaison de la lettre de mission en cinq actions :

- **Action 4.1.** : Actualiser le cahier des charges des fonctionnalités des SI attendues conformément au nouveau cadre législatif et réglementaire, et pour permettre l'interopérabilité, la portabilité des données et l'ouverture au numérique en santé

- **Action 4.2.** : Sur ces bases poursuivre le dialogue avec les éditeurs de logiciels pour qu'ils intègrent ces évolutions

- **Action 4.3.** : Produire des guides de mise en œuvre pour l'utilisation de l'INS, l'identitovigilance, les messageries sécurisées, l'accès aux Thésaurus.

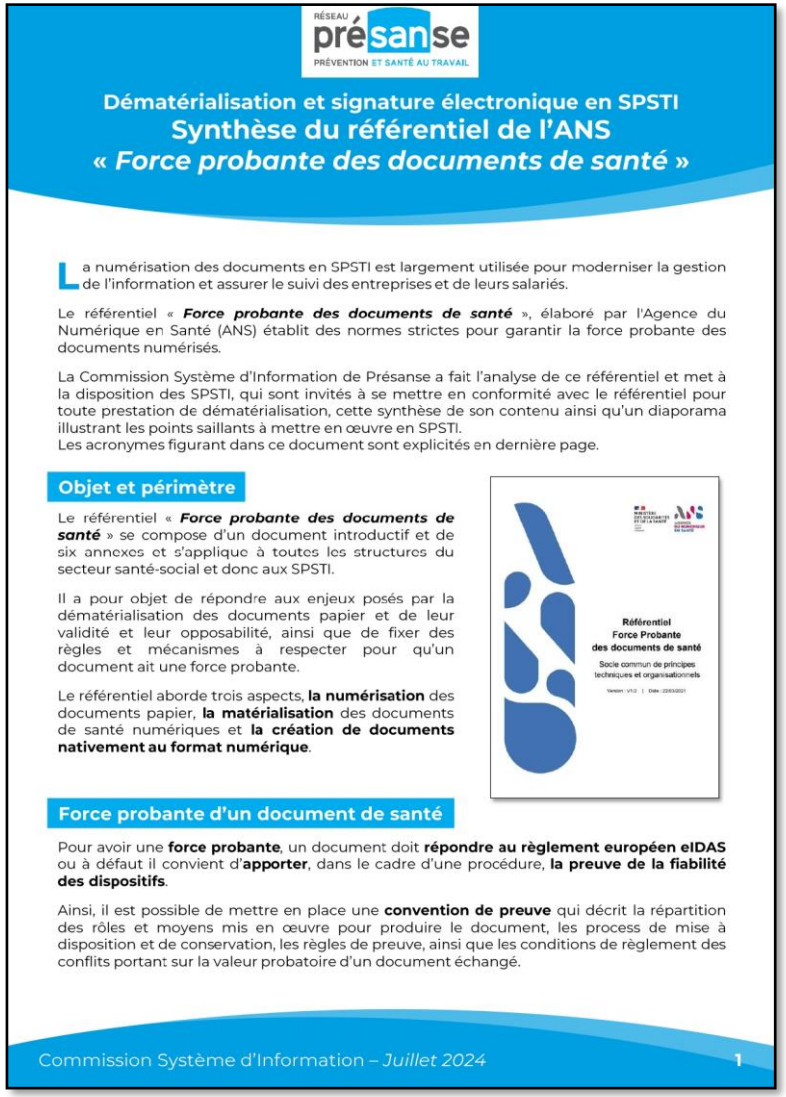
- **Action 4.4.** : Apporter un appui pour sécuriser les SI conformément aux normes en vigueur, notamment à partir du partage d'expériences, par exemple RGPD.

- **Action 4.5.** : Bâtir des scénarios d'exploitation des données de Santé au travail en lien avec les pilotes du système (Etat et partenaires sociaux) afin de valoriser l'action des SPSTI mais aussi d'agir sur l'efficience du SPSTI.

Les derniers livrables transmis au réseau (1/3)

- La Commission Système d'Information de Présanse a fait l'analyse du référentiel « ***Force probante des documents de santé*** » élaboré par l'Agence du Numérique en Santé (ANS) qui établit des normes strictes pour garantir la force probante des documents numérisés.

- Sont mis à disposition des Services une synthèse et un diaporama de présentation de ce référentiel relatif à la dématérialisation et à la signature des documents de santé (*juillet 2024*).



Les derniers livrables transmis au réseau (2/3)


RÉSEAU présanse
PRÉVENTION ET SANTÉ AU TRAVAIL

Identité Nationale de Santé et identitovigilance

GUIDE DE COMMANDE AUPRES DE L'ANS ET D'IMPLEMENTATION DES CERTIFICATS LOGICIELS

Les certificats logiciels permettent de **sécuriser l'identification électronique de personnes morales à des services numériques en santé** (DMP, INSi, etc.). L'Agence du numérique en santé (ANS) délivre **ces certificats, via son autorité de certification IGC-Santé, et vise à une simplification de leur obtention pour l'ensemble des acteurs.**

Les professionnels de santé peuvent accéder aux référentiels et services socles via leurs cartes CPS. Toutefois **les Services de prévention et de santé au travail interentreprises (SPSTI) peuvent utiliser un certificat** de la structure pour se connecter à ces services.

Le présent guide a été produit à partir du « ***Commande de certificats*** » mis à disposition par l'ANS en 2022. Il est spécifiquement dédié aux SPSTI dans les processus à mettre en œuvre.

Guide commande de certificats

SEGUR - Couloir médecine de ville

V0.4 - 12/12/2022

RÈGLES DE GESTION
DES MOYENS D'IDENTIFICATION ÉLECTRONIQUE

Les professionnels de santé des SPSTI utilisent la carte CPS pour accéder aux services et référentiels proposés. Pour les SPSTI, les certificats peuvent être commandés sous le **FINESS géographique de la structure**.

Règle de commande

Les SPSTI peuvent disposer d'un certificat pour l'alimentation du DMP et l'usage INSi. Le certificat doit être commandé sous le **FINESS géographique** du SPSTI. Par ailleurs, chaque professionnel de santé peut également utiliser sa carte CPS pour accéder aux DMP et à l'INSi.

Commission Système d'Information – *Juillet 2024* 1

- Dans le cadre de la mise en œuvre de l'INS et de l'identitovigilance dans les SPSTI, la Commission Système d'Information propose un « ***Guide de commande auprès de l'ANS et d'implémentation des certificats logiciels*** ».

- Ce guide a été produit à partir du document cadre de l'Agence du Numérique en Santé (ANS) « *Commande de certificats* » mis à disposition en 2022. Ce document a été entièrement revu et complété afin d'être spécifiquement dédié aux SPSTI dans les processus à mettre en œuvre (*juillet 2024*).

Les derniers livrables transmis au réseau (3/3)

- Les messageries sécurisées de santé, comme MSSanté, jouent un rôle essentiel pour garantir la confidentialité des échanges entre les professionnels de santé.

- La Commission Système d'Information a constitué, à partir d'un document de l'Agence du Numérique en Santé (ANS), un diaporama de ***présentation et d'utilisation des messageries sécurisées de santé à destination des personnels de la Santé au Travail*** (*septembre 2024*).

②

Rappels sur la PGSSI-S

Qu’est-ce qu’une donnée de santé ?

Définition issue du Règlement européen sur la protection des données personnelles (RGPD)

Les **données à caractère personnel concernant la santé sont les données relatives à la santé physique ou mentale, passée, présente ou future, d’une personne physique** (y compris la prestation de services de soins de santé) qui révèlent des informations sur l’état de santé de cette personne. Cette définition comprend donc par exemple :

- les **informations relatives à une personne physique** collectées lors de son inscription en vue de bénéficier de services de soins de santé ou lors de la prestation de ces services : un numéro, un symbole ou un élément spécifique attribué à une personne physique pour l’identifier de manière unique à des fins de santé ;
- les **informations obtenues lors du test ou de l’examen d’une partie du corps ou d’une substance corporelle**, y compris à partir des données génétiques et d’échantillons biologiques ;
- les **informations concernant une maladie, un handicap, un risque de maladie, les antécédents médicaux, un traitement clinique ou l’état physiologique ou biomédical** de la personne concernée (indépendamment de sa source, qu’elle provienne par exemple d’un médecin ou d’un autre professionnel de santé, d’un hôpital, d’un dispositif médical ou d’un test de diagnostic in vitro).

Cette définition permet d’englober certaines données de mesure à partir desquelles il est possible de déduire une information sur l’état de santé de la personne.

Qu’est-ce qu’un Système d’Information de Santé (SI-S) ?

Définition

- Un Système d'Information de Santé (SI-S) englobe l'ensemble des ressources matérielles, logicielles et humaines utilisées pour gérer les informations de santé, nécessitant une protection renforcée en raison de leur sensibilité.

Sensibilité

- Les données de santé sont hautement confidentielles et requièrent une protection renforcée en raison de leur nature privée et de leur utilisation critique dans le domaine de la santé.

Exemples

- Elle inclut les dossiers médicaux électroniques, les systèmes d’information et de gestion des salariés et les systèmes de télémédecine, tous contenant des données hautement confidentielles qui doivent être sécurisées.

PGSSI-S : Politique Générale de Sécurité des Systèmes d’Information en Santé

La PGSSI-S, c’est quoi ?

La PGSSI-S rassemble :

- Des référentiels et des documents opposables fixant les exigences relatives aux différents aspects de la sécurité des systèmes d’information en santé ;
- Des guides et des supports pratiques ou organisationnels incluant les recommandations en matière de sûreté des données.

Mieux comprendre la PGSSI-S

Pourquoi une PGSSI-S est essentielle ? (1/3)

Sécurité des données de santé - CONFIDENTIALITÉ

- La PGSSI-S est vitale pour protéger les informations sensibles et personnelles relatives à la santé des individus, garantissant ainsi la confidentialité et l'intégrité des données.

Confiance et fiabilité - INTÉGRITÉ

- La PGSSI-S renforce la confiance des patients et des partenaires en garantissant une gestion sécurisée des données de santé, ce qui est essentiel pour l'image et la réputation du SPSTI.

Continuité des activités - DISPONIBILITÉ

- La PGSSI-S permet de mettre en œuvre la continuité de l'activité et ainsi d'assurer le fonctionnement sans interruption du SPSTI.

Conformité légale

- Elle permet de respecter les obligations réglementaires telles que le RGPD, évitant ainsi des sanctions et des litiges juridiques liés à la protection des données de santé.

Pourquoi une PGSSI-S est essentielle ? (2/3)

ÉTAT DES LIEUX

+13%

de cyberattaques en entreprises en 2021[1]

730

incidents déclarés en 2021 par l'Agence du numérique en Santé (ANS)[2]

500 000

personnes ont été concernées par la fuite de données de santé en 2021[2]

34

incidents ont mis en danger la vie de patients en 2020[2]

x2

dans les établissements de santé[2]

27

attaques majeures sur des hôpitaux en 2020 et une par semaine en 2021[2]

70%

des professionnels de santé interrogés se disent également concernés par les questions de cybersécurité[2]

54 milliards d'€

investis en cybersécurité entre 2017 et 2021[1]

(1) Orange Cyberdefense Security Report
(2) Agence du numérique en santé
(3) Rapport Verizon 2022

5 TYPES DE CYBERATTAQUES

Écoute
Espionnage via les microphones pour collecter des informations sensibles

Attaque par déni de service
Saturation d'un réseau afin de la rendre indisponible

Logiciel malveillant ou malware
Programme développé dans le but de nuire à un système informatique, sans le consentement de l'utilisateur dont l'ordinateur est infecté

Hameçonnage ou Phishing
Technique frauduleuse destinée à leurrer l'internaute pour l'inciter à communiquer des données personnelles et/ou bancaires en se faisant passer pour un tiers de confiance

Rançongiciel ou Ramsomware
Logiciel malveillant qui prend en otage des données de différentes natures (personnelles, professionnelles...)

LE SAVIEZ-VOUS ?

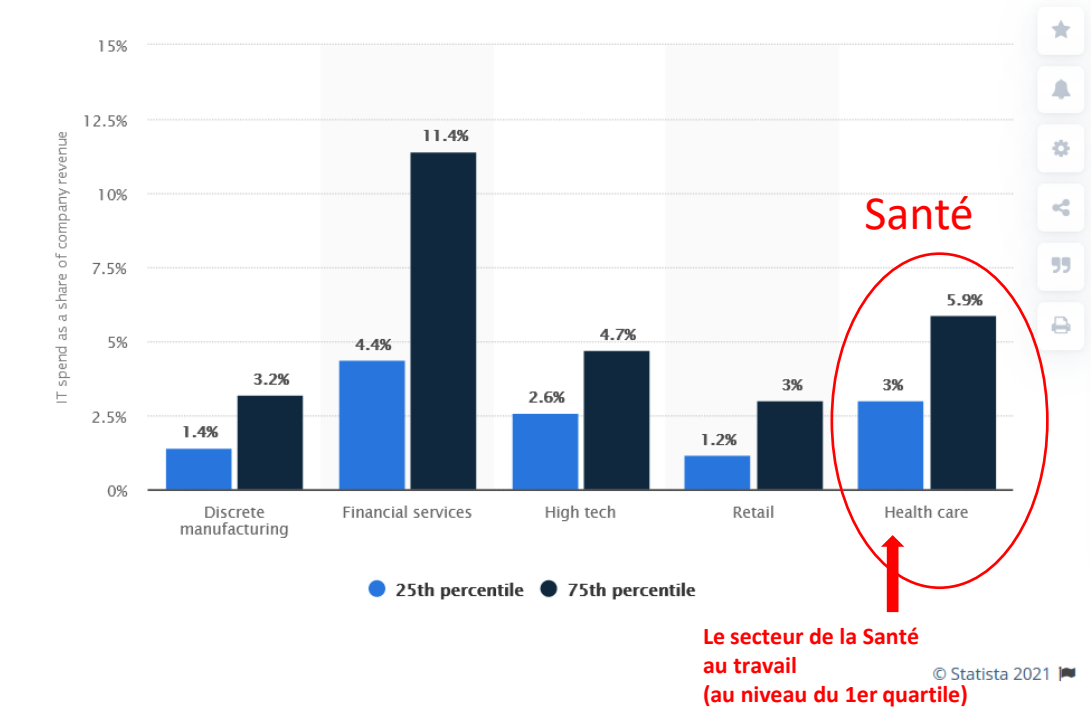
Si une mauvaise sécurité des systèmes d'information et des logiciels obsolètes sont souvent tenus pour responsables des violations de données...

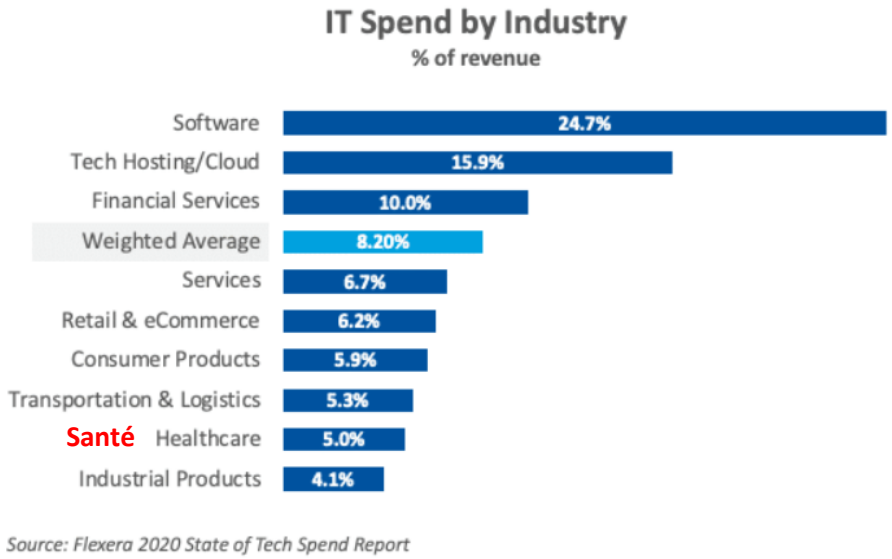
...la vérité est que l'erreur humaine est responsable de 80%[3] des cas de cyberattaques.

Autrement dit, une personne sur huit qui reçoit un mail de phishing clique sur le lien malveillant qu'il contient !

Pourquoi une PGSSI-S est essentielle ? (3/3)

Dépenses informatiques en part du chiffre d'affaires de l'entreprise en 2020, par secteur économique (OCDE)





- **Coûts Informatiques** : Les dépenses informatiques du secteur de la santé, bien qu'importantes, ne sont pas aussi élevées que celles d'autres secteurs, en investissant, tous coûts confondus entre 3% et 5,9% de son chiffre d'affaires.

- **Investissement en Sécurité des Systèmes d'Information** : Cette part du chiffre d'affaires inclut les investissements en sécurité des systèmes d'information. Cette proportion montre une attention notable mais pourrait bénéficier d'une augmentation pour atteindre les standards des secteurs plus avancés technologiquement.

Les enjeux : mieux vaut prévenir que guérir !

Coût de réparation

- Les coûts de restauration à la suite d'un incident de sécurité (restauration des données, réparations, perte de productivité) sont très souvent supérieurs à ceux de la prévention, nécessitant des ressources financières considérables.

Exemple : Coût de la cyberattaque de l'Hôpital de Dax en 2021 : 2,3 millions d'€

Perte d'exploitation

- Les cyberattaques peuvent interrompre les activités, entraînant des pertes financières et opérationnelles considérables pour l'association.

Perte d'image et de confiance

- Un incident de sécurité peut gravement nuire à la réputation de l'association, impactant sa crédibilité et sa relation avec les différentes parties prenantes.

Le cadre légal et de certification

RGPD

Depuis le 25 mai 2018, le SPSTI a l'obligation de protéger les données personnelles, sous peine de lourdes sanctions en cas de non-conformité

LOI INFO. & LIBERTE

Il est crucial de respecter les autres cadres légaux pertinents pour éviter des litiges juridiques et assurer la conformité aux exigences de sécurité des systèmes d'information en santé

SPEC 2217

Etablie des exigences spécifiques pour la protection, la conservation et la transmission des données de santé, imposant un cadre et des contraintes spécifiques aux SPSTI.

Gestion des risques

Identification des risques

- Il est essentiel d'identifier les menaces potentielles telles que les cyberattaques, les pannes techniques et les erreurs humaines, pour mieux les prévenir et les contrer efficacement, le cas échéant.

Nécessité de définir d'un plan d'actions

Stratégies de prévention

- L'implémentation de mesures préventives telles que les pares-feux, les antivirus et les politiques de sécurité permet de réduire les risques et de renforcer la résilience des systèmes d'information de santé.

Impact d'une perte d'exploitation

- Il est crucial de démontrer les conséquences négatives (financières, réputationnelles, opérationnelles) d'une gestion inadéquate des risques pour sensibiliser sur l'importance de leur gestion proactive.

4 axes stratégiques pour une PGSSI-S efficace

01 Processus

- La mise en place de procédures claires pour la gestion des incidents et des accès contribue à une meilleure réactivité face aux incidents de sécurité et à une gestion efficace des accès aux données de santé.

02 Formation

- La formation continue du personnel sur les bonnes pratiques de sécurité est primordiale pour renforcer la résilience face aux menaces et maintenir un niveau élevé de sécurité informatique.

03 Technologie

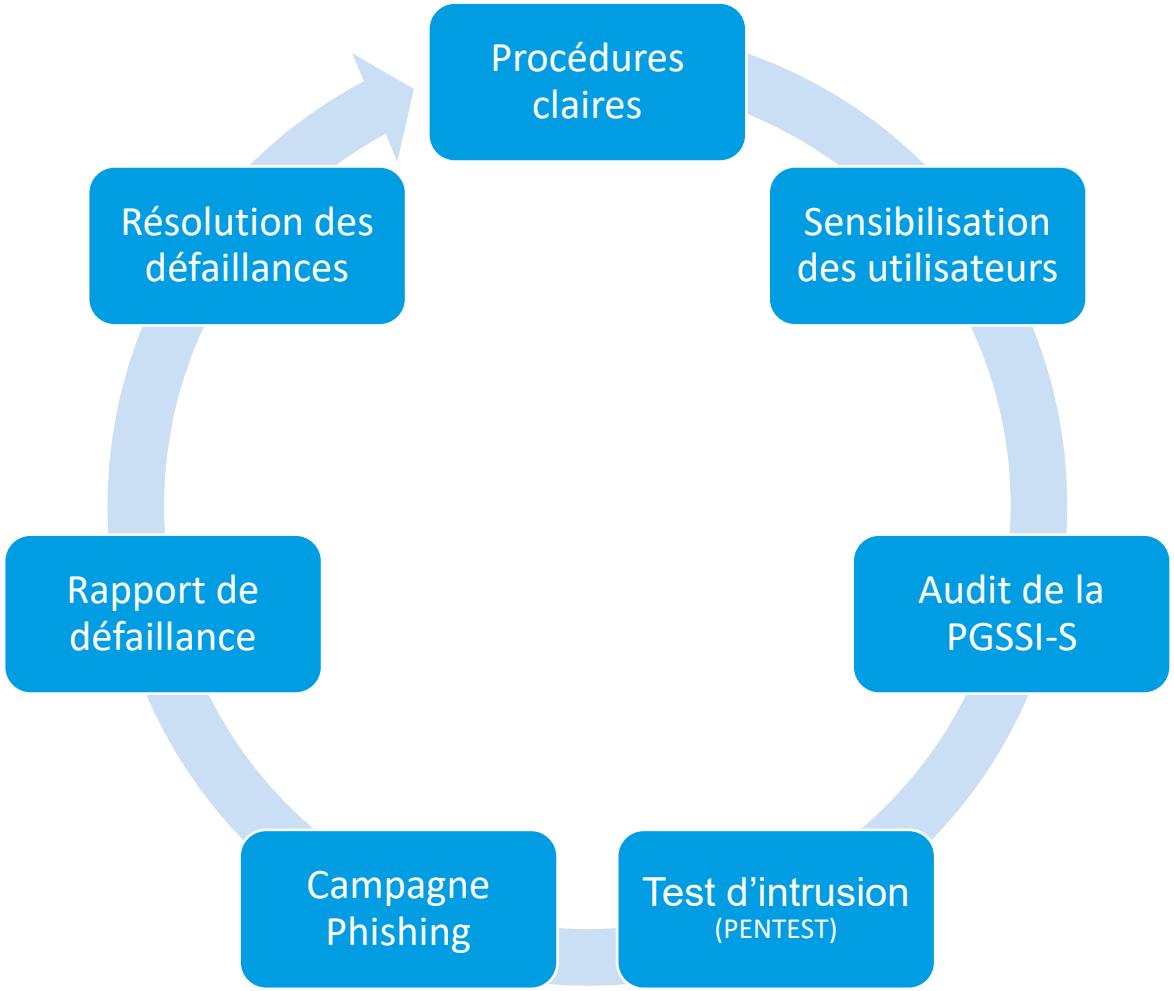
- L'utilisation de solutions techniques telles que le chiffrement, les pares-feux et les systèmes de détection d'intrusion joue un rôle crucial dans la protection des données de santé contre les cybermenaces.

04 Relation fournisseurs

- La maitrise et le contrôle des process de son prestataire est un enjeu majeur dans la prévention des risques autour des systèmes d'information.

Démarche d'amélioration continue

- La mise en place d'une PGSSI-S est **cruciale pour préserver la confidentialité des données de santé**, respecter les obligations légales et renforcer la confiance des parties prenantes.
- Il est essentiel de **prioriser la mise en place d'une PGSSI-S** pour assurer la sécurité et l'intégrité des informations de santé au sein de votre SPSTI.
- Déploiement sous une forme de **démarche d'amélioration continue** pour être dans une vraie démarche de progrès



③

Présentation de l’outil « *Plan d’Actions PGSSI-S* »

Un outil Excel pour mettre en œuvre la PGSSI-S dans les Services (1/2)

- L'outil "*Plan d'actions SI sur la PGSSI-S*"* présente une **série de points clés à questionner** pour guider le SPSTI dans la mise en place et la gestion de sa PGSSI-S

- Cet outil vise à **renforcer la sécurité des systèmes d'information au sein du SPSTI**, tout en garantissant la protection des données sensibles.

- Il constitue une **feuille de route progressive**, pour une gestion proactive et efficace de la sécurité des systèmes d'information.

*Outil proposé dont l'utilisation est laissée libre à chaque SPSTI

Un outil Excel pour mettre en œuvre la PGSSI-S dans les Services (2/2)

présanse
PRÉVENTION ET SANTÉ AU TRAVAIL

PGSSI-S
PLAN D'ACTION

Denière mise à jour : 30/09/24

		PLAN D'ACTION SECURITE				PLANIFICATION ET SUIVI											
						Situation initiale			Déploiement								
Règles de sécurité Réf.	Thématique	Prio	Mesures	Périmètre concerné / Moyens du SI	Resp. mise en œuvre	% déjà en œuvre	Reste à faire Charge (j.h)	Coût (k.Euros)	Date: % cible	% atteint	% att/ci	Date: % cible	Commentaires	Actions prioritaires (indispensable à déployer)	Niveau adéquat de conformité	Gestion avancée (Plus coûteux)	Exemples d'outils
	Assurer la sécurité physique des Equipements Informatique du SI		R&ay														
3.1	Maîtriser l'accès aux équipements du SI qui sont nécessaires à l'activité de la structure et assurer leur	1												Identifier et catégoriser les locaux à risque			
3.1.1	Assurer la protection physique des équipements informatiques d'infrastructure du SI, qui contiennent des données sensibles	1				3%								Sécuriser les salles Serveurs : gestion canforme de salle serveur: gestion elostrique (double alim, onduleur), gestion thermique (clim) gestion incendie detection avec extinction automatirée contrelor d'accès naminatifrb adapr Simplicité: confier la gestion à des spécialistes	Gestion en datacenter	Avoir les datacenter dans les centres gestion de PRA en réplication sécuriser les salle informatiques dans les centres	
3.1.2	Assurer la protection physique des postes de travail, qui contiennent des données sensibles	1				0%								chiffrement des disques des parter de travail Politique de gestion des locaux avec limitation de l'accès des outil infra au public		système automatique d'effacement à distance	
3.1.3	Assurer la protection physique des équipements amovibles qui contiennent des données sensibles (dont les données de santé à caractère personnel)	1				0%								Chiffrement des clé au des équipement amovible autorisés Scan automatique d'équipement amovible	autoriser certains matériels précis		
3.1.4	Assurer la destruction de données lors du transfert de matériels informatiques	1				0%								politique de transfert aux recyclage des matériel informatique (inclus dans la politique de gestion des actifs) qui prend en compte la formatage, la destruction des matériel en fonction du niveau de risque sur les données (certificat de destruction,)	politique de transfert aux recyclage incluant le formatage avant réattribution matériel et destruction définitive des disques sensibles		
	Protéger les infrastructure Informatiques du SI		Thomas														
4.1	Maîtriser le parc informatique	1				0%											
4.1.1	Identifier physiquement chaque équipement informatique ou dispositif médical connecté détenu par la structure					0%								inventorier le matériel dans un fichier : 1 Nom et description de l'équipement, 2 Numéro de série, 3 Localisation physique (bureau, DC, Salle Serveur, Baie Barrage, TAD) et Localisation, 5 Date d'acquisition, 6 Responsable ou propriétaire, 7 Config Materielle et logicielle, 8 Date de fin de vie prévue	**Classification des équipements** (Non Sensibles, sensibles, critiques, hautement critiques), **Gestion des accès physiques** (identification Zones, contrôle des accès physiques, suivi des accès, formation et sensibilisation, surveillance et alarme, réversion réquilibres) avec inventaire automatique	**Traçabilité et auditabilité** (journal des mouvements/accès aux zones restreintes, modif équipements, Audit périodique), **Mesures de protection physique** (contrôle d'accès physique, sas de sécurité, câblage sécurisé, aménagement physique, protection contre les dommages environnement, surveillance et détection d'intrusion, formation et sensibilisation), **Responsabilités et sensibilisation** (formation, manuel de sécurité, sensibilisation continue, mesures périodiques, schémas de formation) créés avec la gestion des interventions (ex GLPI),	GLPI(Opensource), PDQ Inventory, RMM

présanse
PRÉVENTION ET SANTÉ AU TRAVAIL

Décomposition de l'outil : 7 thématiques

1. Répondre aux obligations légales
2. Promouvoir et organiser la sécurité
3. Assurer la sécurité physique des Equipements Informatique du SI
4. Protéger les infrastructure Informatiques du SI
5. Maîtriser les accès aux informations
6. Acquérir des Equipements, Logiciels et services qui préservent la sécurité du SI
7. Limiter la survenue et les conséquences d'incidents de sécurité

Présentation de l'outil « *Plan d'Actions PGSSI-S* » (2/8)

❶ Répondre aux obligations légales

Objet de la thématique :

Les SPSTI doivent répondre à la règlementation de 2018 sur la RGPD tout en garantissant le respect du secret médical.

Actions à mettre en œuvre :

- Désignation d'un DPO et de la gouvernance relative à la protection des données personnelles.
- Rédaction d'une politique de protection des données des salariés et des adhérents.
- Rédaction des procédures permettant le respect du consentement, de l'accès aux données, de la durée de conservation des dossiers et de réponses aux demandes des modifications des données à caractère personnel.
- S'assurer du maintien en conformité réglementaire des procédures établies.

Outils / Documents clés

Registre de traitement

Politique de protection des données des salariés et des adhérents

Analyse d'impact

Revue des traitements

Présentation de l'outil « *Plan d'Actions PGSSI-S* » (3/8)

❷ Promouvoir et organiser la sécurité

Objet de la thématique :
Mise en place d'une organisation.

Outils / Documents clés

PSSI

Gouvernance Sécurité

Actions à mettre en œuvre :

- Identification de la gouvernance :
  - Définir les indicateurs de la sécurité.
  - Définir les instances (Comité sécurité).
  - Identification du rôle des acteurs (internes / externes).
  - Identification des moyens de communication.
- Définition d'une politique de sensibilisation :
  - Formations / Communication initiale et continue sur la sécurité informatique.
  - Action de phishing et audits sécurité.
- Charte informatique interne et prestataire.
- Définition et validation de la politique de sécurité du système d'information (PSSI) et suivi de sa mise en application.

Présentation de l'outil « *Plan d'Actions PGSSI-S* » (4/8)

❸ Assurer la sécurité physique des Equipements Informatiques du SI

Objet de la thématique :

Cette thématique traite de la sécurité des équipements, des locaux et de leur cycle de vie.

Présentation de l'outil « *Plan d'Actions PGSSI-S* » (5/8)

❹ Protéger les infrastructures informatiques du SI

Objet de la thématique :
Avoir une connaissance claire de la composition des infrastructures du SI et mettre en place des moyens adaptés pour les protéger.

Actions prioritaires

- Entretenir la connaissance sur le si : inventorier le matériel, lister les logiciels et leurs flux, les licences, les équipements réseaux, vérifier leur état de mises à jour
- Avoir une charte informatique incluant les mesures de sécurité personnelles
- Sécuriser le réseau périmétrique et endpoint (firewall, EDR, Chiffrement des postes)
- Gestion des habilitations et établissement d'un suivi des comptes notamment pour les comptes à privilèges

Niveau adéquat de conformité

- Gestion plus fine des cartographies incluant des évaluations de criticités, des dépendances
- Segmentation des réseaux, gestion de filtrage de contenu
- Actions de sensibilisation des utilisateurs, renforcement de la politique de mot de passe
- Mise en place de mécanismes d'automatisation des mises à jour (OS, Logiciels, firmwares réseau)

Gestion avancée

- Mise en place d'outil de collecte et d'analyse et d'alerte sur des évènements du réseau et des applications (SIEM)
- Gestion automatisée des identités
- Audit des respects de pratiques
- Mesure de protection physique des équipements

Outils / Documents clés

- Cartographie Applicative
- Cartographie Réseau
- Gestion de parc
- EDR, Firewall

Présentation de l'outil « *Plan d'Actions PGSSI-S* » (6/8)

❺ Maîtriser l'accès aux informations

Objet de la thématique :
S'assurer que les accès aux informations sont conformes et limiter les risques associés.

Actions prioritaires

- Formaliser et mettre en place une politique de gestion des accès :
- Listing des accès et habilitations
- Formalisation des règles de sécurités des comptes
- Bannir les protocoles d'échanges obsolètes

Niveau adéquat de conformité

- Gestion de sécurité de comptes (SSO, authentification multi facteur, badge pour impression)
- Revue des actions suspectes sur les comptes utilisateurs
- Utiliser des flux d'échanges sécurisés (impressions, chiffrement des échanges)

Gestion avancée

- Gestion automatisée des identités et l'attribution des droits associés
- Mise en place d'un outil de centralisation des évènements et d'alertes(SIEM)
- AD tiers (compartimentation de l'active directory en trois zones)

Outils / Documents clés

Politique de gestion des accès, politique de gestion des mots de passe

Outil de gestion de mot de passe

Siem, Bastion, SOC

Présentation de l'outil « *Plan d'Actions PGSSI-S* » (7/8)

❻ Acquérir des Equipements, Logiciels et services qui permettent la sécurité du SI

Objet de la thématique :
Intégrer dans l'acquisition des règles qui permettent de garantir le cadre de sécurité attendu.

Outils / Documents clés

Contrats adaptés

Actions prioritaires

Cadrer les relations avec les fournisseurs incluant :

- Des clauses de réversibilité dans les contrats
- Un cadre de sécurité régissant les accès externes au SI (VPN)
- Plan d'assurance qualité de prestataire

Niveau adéquat de conformité

Encadrer chaque changement par une analyse de risques et une mise à jour des documentations

Mise en place de log de suivi des accès externes

Gestion avancée

Mise en place d'un Bastion et d'un SIEM

Présentation de l'outil « *Plan d'Actions PGSSI-S* » (8/8)

❼ Limiter la survenue et les conséquences d'incidents de sécurité

Objet de la thématique :
Cette thématique a pour objet de se préparer à un accident de sécurité.

Actions prioritaires

- Tenir un registre des incidents de sécurité
- Mettre en place un outil de supervision et d'alerte
- Programmer un audit sécurité tous les ans
- Préparer la gestion de crise en cas d'incident (procédures, gouvernance)
- Mise en place d'un plan de sauvegarde et de tests de restauration

Niveau adéquat de conformité

- Prendre une assurance cyber
- Audit de sécurité réguliers sur les applications et sur le réseau
- Démarche d'amélioration continue sur les incidents de sécurité (RETEX)
- Fréquence mensuelle sur les tests de restauration
- Analyse de risques et définition du plan de continuité d'activité(PCA) et le tester

Gestion avancée

- Mise en place d'un SOC externalisé ou d'un SIEM en interne

Outils / Documents clés

Stratégie de revue sécurité

Plan de gestion de crise

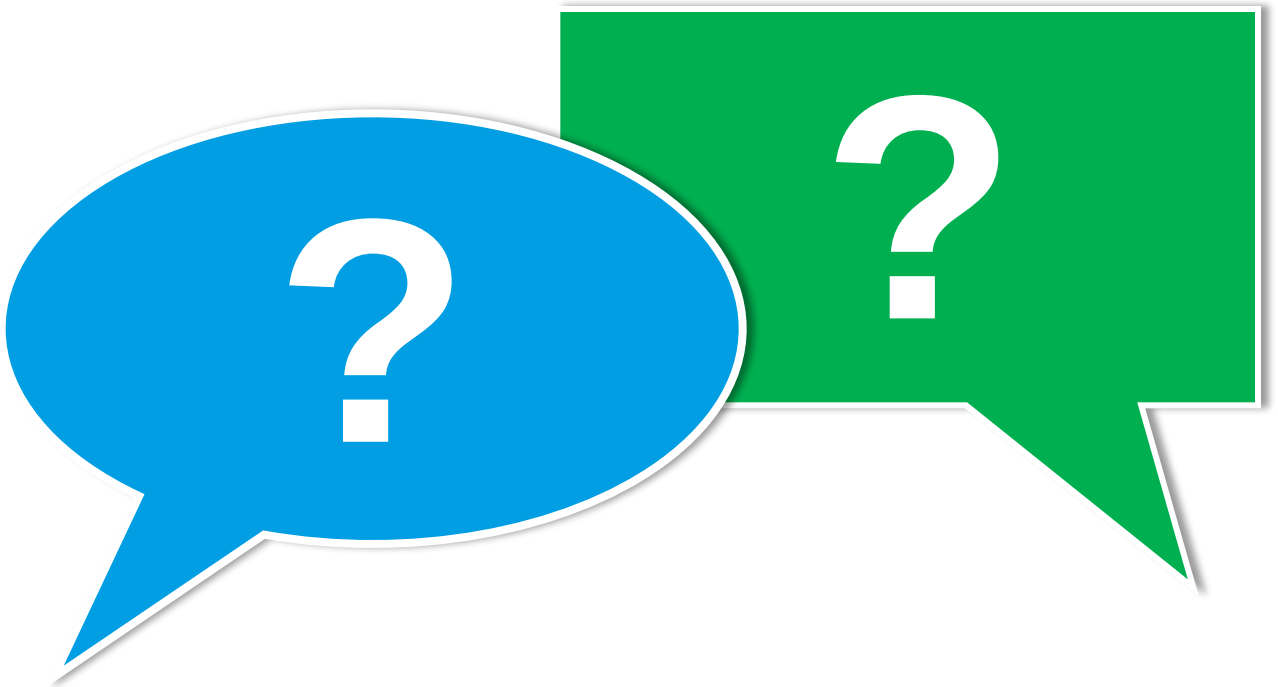
Analyse de risque

Plan de continuité d'activité

④

Questions / Réponses

Vos questions



⑤

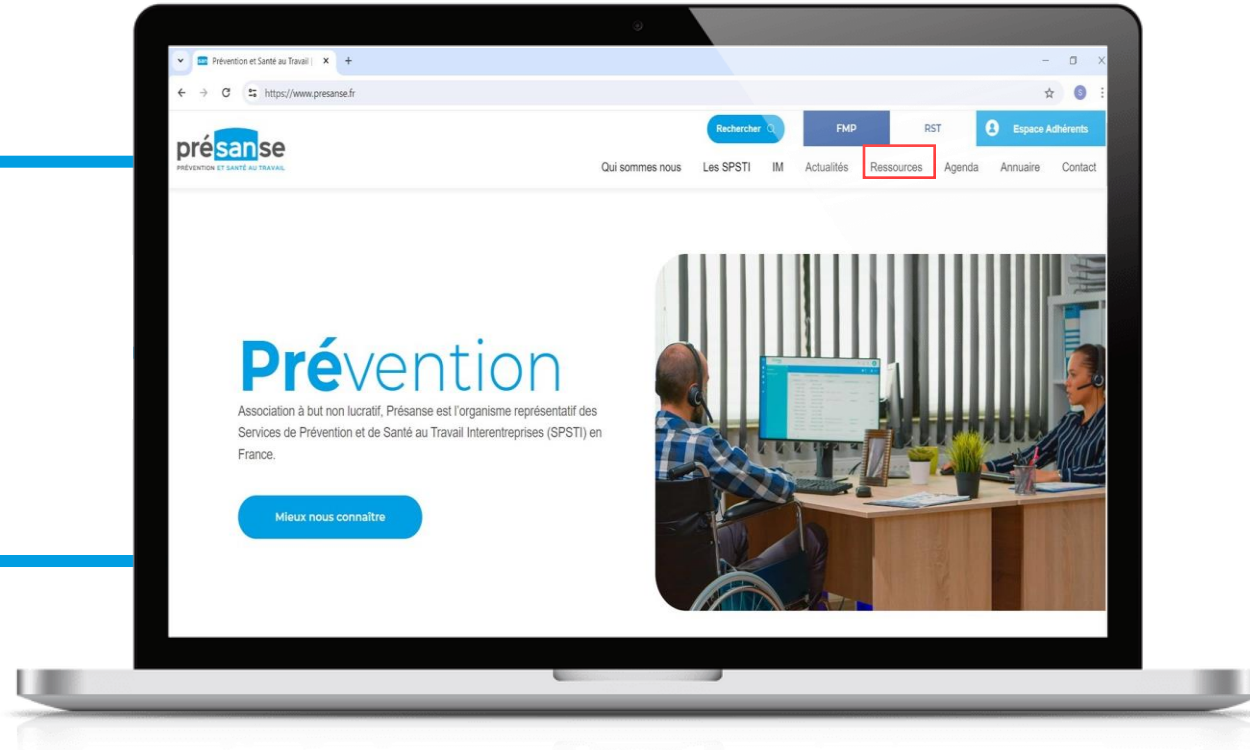
Conclusion et projets

Comment accéder aux supports sur le site de Présanse ?

Outil "*Plan d'Actions PGSSI-S*" En accès libre sur le site Internet de Présanse (espace Ressources)

www.presanse.fr

Accès aux autres ressources et documents produits ou mis à disposition par la Commission Système d'Information



Ressources utiles

AGENCE DU NUMÉRIQUE EN SANTÉ
La transformation commence ici

RÉPUBLIQUE FRANÇAISE
Liberté Égalité Fraternité

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION · ANSSI ·

Merci pour votre attention

Pour toute question :

c.letheux@presanse.fr