AGENCE
DU NUMÉRIQUE
EN SANTÉ
La transformation commence ici

Elaboration et mise en œuvre d'une PSSI pour les structures des secteurs sanitaire, médico-social et social

Guide pratique organisationnel PGSSI-S

Publication : mai 2015 | *Classification : Publique* | *Version : v1.0*

Agence du Numérique en Santé
9, rue Georges Pitard – 75015 Paris
T. 01 58 45 32 50
esante.gouv.fr

SOMMAIRE

1. PREAMBULE

1.1. Objet du guide

Ce guide a été conçu pour aider les structures[1] des secteurs sanitaire, médico-social et social qui ne disposent pas encore d'approche formalisée pour la Sécurité de leur Système d'Information (SSI) à élaborer une Politique de Sécurité des Systèmes d'Information (PSSI) rapidement applicable.

Il propose une démarche qui permet :

- d'élaborer une PSSI pragmatique en s'appuyant sur un canevas et un contenu préparés spécifiquement pour les structures des secteurs sanitaire, médico-social et social,
- de la mettre en œuvre de manière progressive dans le temps, dans une optique d'amélioration continue de la sécurité.

Cette PSSI répond également à l'exigence de documentation de la politique de sécurité énoncée dans le cadre des différents programmes ou plans nationaux (ex. programme Hôpital Numérique, certification des établissements de santé HAS…).

☞ Ce guide se concentre sur la sécurité des SI et des données dématérialisées qu'ils manipulent.

Bien que certaines règles et mesures de sécurité proposées dans le canevas de PSSI puissent participer à la sécurisation des données sur support papier, ce sujet nécessite des dispositions spécifiques qui ne sont pas abordées dans ce guide.

Ce document fait partie des guides pratiques organisationnels de la Politique Générale de Sécurité des Systèmes d'Information de Santé [PGSSI-S].

1.2. A qui s'adresse ce guide ?

1.2.1. Quels lecteurs ?

Ce guide est particulièrement destiné :

- au responsable de la structure, pour comprendre les enjeux de sécurité, identifier la personne qui va porter le projet et être en mesure de mieux arbitrer les ressources humaines et matérielles nécessaires pour assurer la sécurité du système d'information de la structure ;
- aux personnes en charge de la définition, de la rédaction ou de la mise à jour de la PSSI de la structure ;
- aux personnes qui participent aux réflexions et aux travaux sur la PSSI.

Note : Ces rôles peuvent, bien entendu, être tenus par une seule et même personne.

[1] Par convention, le terme structure est utilisé dans le document pour désigner une structure d'exercice collectif du secteur sanitaire ou médico-social quel que soit son type (ex. hôpital, clinique, centre de santé, maison de santé, EHPAD…) prenant en charge des patients. Les structures d'exercice individuel de type cabinet libéral ne sont pas concernées par ce guide.

1.2.2. Quels types de structure ?

Le présent guide est destiné aux structures qui prennent en compte la nécessité de commencer une démarche sécurité et qui doivent la déployer de manière progressive et réaliste.

Il s'adresse également aux structures dont la PSSI est considérée comme obsolète, incomplète ou trop complexe à mettre en œuvre[2].

Le questionnaire suivant permet de déterminer rapidement si ce guide est adapté à la structure.

Afin de déterminer si ce document concerne votre structure, nous vous invitons à répondre aux questions ci-dessous :

Question	Oui	Non
Votre structure emploie un RSSI, ainsi qu'une équipe dédiée à la sécurité du SI ?		
Vous (ou quelqu'un de votre structure) êtes formé et familiarisé aux analyses de risques Sécurité (EBIOS, ISO 27005…) ?		
Vous (ou quelqu'un de votre structure) êtes familiarisé avec les règles inhérentes aux contraintes de sécurité des données de santé à caractère personnel ?		

Si vous avez répondu « Non » à au moins une de ces questions, ce guide concerne votre structure.

Si vous avez répondu « Oui » à l'ensemble des questions, ce guide n'est *a priori* pas adapté à votre structure. Nous vous invitons dans ce cas à vous reporter au chapitre 6 de ce guide.

Compte tenu de son périmètre, le guide est particulièrement adapté aux systèmes d'information « standard ».

Si le SI de votre structure comprend des éléments dits « spécifiques »[3], nous vous recommandons, une fois la PSSI de votre SI rédigée en suivant ce guide, de mettre rapidement en œuvre une démarche sécurité plus approfondie, afin de définir les règles relatives à ces éléments. Le chapitre 6 en fin de ce guide vous orientera vers des démarches et méthodes adaptées à ce type de situation.

1.2.3. Les structures ayant externalisé tout ou partie de leur SI sont-elles concernées ?

Une structure peut confier par contrat la gestion de tout ou partie de son SI à des tiers.

Les prestataires retenus doivent présenter des garanties suffisantes pour assurer la mise en œuvre des mesures de sécurité et de confidentialité définies dans le contrat conclu avec la structure, responsable du traitement[4] dès lors que des données à caractère personnel sont concernées. Le responsable du traitement a obligation de veiller à ce

[2] Le fait qu'une PSSI soit trop complexe pour être mise en œuvre n'indique pas forcément qu'elle est à rejeter comme inadaptée à la structure. Elle peut être conservée pour référence et/ou comme PSSI cible.

[3] C'est-à-dire qu'elle ne comprend pas uniquement des postes de travail de type ordinateur Windows ou Mac, des serveurs Windows, Mac ou Linux, un réseau TCP/IP, des accès internet, des progiciels « sur étagères », des dispositifs connectés… mais comprend aussi des applications développées spécifiquement pour votre structure (ex. : logiciel de gestion de la restauration patient) ou du matériel construit à façon (ex. chariot communiquant pour la distribution de médicaments aux patients hospitalisés).

[4] Au sens de la loi n°78-17 du 6 janvier 1978 dite « loi Informatique et Libertés » [L78-17] et du « Règlement Général sur la Protection des Données » [RGPD]

que chaque contrat qui le lie à un sous-traitant de données à caractère personnel intègre l'ensemble des dispositions requises par la législation[5]. De plus, si l'externalisation amène à confier des données de santé à caractère personnel à un prestataire, celui-ci doit être agréé comme hébergeur de données de santé[6].

☞ Dans le canevas de PSSI proposé (voir chapitre 1.3.1), un cartouche identifie les exigences et les règles de sécurité dont la responsabilité de mise en œuvre incombe a priori aux prestataires en charge du SI externalisé.

☞ **Point d'attention :**

Une externalisation, quel qu'en soit le type, n'exonère pas le responsable légal de la structure ni ses éventuels délégataires de toute responsabilité, en particulier pénale, pour les données de santé à caractère personnel collectées et conservées par la structure.

Toutefois, elle permet de confier l'exécution de règles de sécurité à des tiers dans le cadre d'une relation contractuelle définissant les responsabilités des deux parties engagées.

1.2.4. Faut-il des connaissances en sécurité des systèmes d'information pour utiliser ce guide ?

Ce guide peut être utilisé par des personnes qui connaissent le système d'information de leur structure mais qui n'ont pas nécessairement d'expertise particulière en sécurité des systèmes d'information (SSI).

Afin de rester d'un usage pratique et direct, le guide détaille la démarche d'élaboration de la PSSI en introduisant différents concepts de SSI sans toutefois s'appesantir sur ces points. Le lecteur, même novice en sécurité, peut ainsi acquérir les principes d'une démarche sécurité et se familiariser avec le vocabulaire de la SSI.

Le guide comporte également des paragraphes intitulés « pour aller plus loin » (identifiés par le pictogramme ) qui proposent, aux lecteurs qui le souhaitent, des explications plus approfondies et des références sur les sujets traités.

La sécurité n'est pas qu'une affaire de spécialistes techniques. Beaucoup de mesures de sécurité sont de nature organisationnelle et sont simples à mettre en œuvre à l'aide d'outils de sensibilisation et de formation des utilisateurs.

Cette approche de la sécurité et de son vocabulaire vous permettra, une fois acquise, de comprendre les experts en SSI lorsque qu'ils discuteront d'analyse de risque, ou de passer à des démarches plus approfondies après quelques temps d'utilisation de ce guide. Pour plus de détails sur la transition de la démarche proposée par ce guide vers une démarche approfondie, reportez-vous au chapitre 6 « Conclusion ».

[5] cf. article 28, relatif aux sous-traitants, du [RGPD]

[6] Tel que défini dans l'article L.1111-8 du code de la santé publique [CSP-L1111-8] et articles associés [CSP-R1111-8-8] et [CSP-R1111-9_11].

1.3. Comment utiliser ce guide ?

1.3.1. Guide PSSI et canevas de PSSI

Le guide PSSI est destiné à être utilisé conjointement au document « canevas de PSSI » [MOD PSSI] qui l'accompagne.

L'ensemble a été conçu pour proposer un maximum de contenu « prêt à l'emploi » afin de réduire autant que possible la charge de travail rédactionnel restant à réaliser :

- le guide expose la méthode à suivre pour préparer et élaborer la PSSI de la structure ;
- le canevas de PSSI constitue une PSSI générique, utilisable comme document de base à compléter et à adapter au contexte spécifique de la structure selon la méthode proposée par le guide ;
- les règles proposées dans le canevas de PSSI tiennent compte des exigences de la [PSSIE] à laquelle doivent se conformer les structures du secteur public, et permet de répondre à la très grande majorité de ces exigences. Le document [MOD PSSI COUV] annexé au canevas de PSSI fournit la traçabilité de la couverture des règles de la PSSIE par celles du canevas de PSSI ;
- différents modèles de documents utilisés au cours de la démarche ou utiles à la mise en application des règles de sécurité sont proposés en annexe du guide : tableau de recensement des moyens du SI, modèle de plan d'action sécurité, liste des premières règles à mettre en œuvre, modèle de charte d'usage du SI…

1.3.2. Quels chapitres lire en priorité ?

Les chapitres sont prévus pour être lus dans l'ordre dans lequel ils sont présentés afin d'avoir une vision cohérente de la démarche d'élaboration et de mise en œuvre d'une PSSI.

Après une première lecture de la méthode proposée, il est recommandé de prendre connaissance du canevas de PSSI et des notes « Guides de rédaction » qu'il comporte.

La lecture du canevas de PSSI, et notamment des exemples de contenu qui y sont présentés, permet de voir concrètement le type de résultat attendu.

Une fois cette prise de connaissance globale réalisée, la mise en application du guide peut être entamée.

1.3.3. Signalétique utilisée

Pour faciliter la lecture du guide, des pictogrammes sont utilisés pour signaler certains éléments particuliers :

	Résumé des spécificités des secteurs sanitaire et médico-social (points d'attention, même pour des personnes déjà familiarisées avec la SSI).
	Remarque, point à noter.
	Guide de rédaction : il s'agit d'indications sur le contenu de la PSSI qui sont positionnées aux endroits correspondants du canevas de PSSI. Ces guides de rédaction sont destinés à être supprimés du document PSSI dans sa phase de finalisation.
	Pour aller plus loin : explications complémentaires ou références pouvant être consultées pour approfondir le sujet.

1.3.4. Spécificité des secteurs sanitaire, médico-social et social

Les SI de structures des secteurs sanitaire, médico-social et social traitent souvent des données particulièrement sensibles (ex. : données de santé à caractère personnel, données sociales à caractère personnel…) et participent parfois directement à la prise en charge des usagers[7] (ex. : dispositifs médicaux comportant du logiciel). Ce contexte se traduit au niveau sécurité par des exigences ou des contraintes spécifiques qui modulent les exigences de sécurité « classiques » sans toutefois en augmenter la complexité.

1.4. Comment se positionne ce guide par rapport aux autres documents de référence ?

Des documents de diverse nature encadrent ou aident à la sécurisation des SI des structures des secteurs sanitaire, médico-social et social. On peut les répartir selon les catégories suivantes :

- un cadre légal définissant des obligations ;
- des guides, règles, référentiels, bonnes pratiques, etc., constituant l'« état de l'art » à connaitre et respecter.

Ces différents documents ont été pris en compte dans l'élaboration du présent guide et dans le choix des exigences et des exemples de règles de sécurité proposés dans le canevas de PSSI, que ce soit au titre de leur caractère d'obligation, de référentiel métier applicable ou de recommandation : voir Annexe 5.

2. POURQUOI UNE POLITIQUE DE SECURITE DES SYSTEMES D'INFORMATION ?

2.1. Les besoins de SSI dans les secteurs sanitaire, médico-social et social

La nature des données traitées par les structures des secteurs sanitaire, médico-social et social (données de santé à caractère personnel couvrant les notions d'informations médicales, d'informations de santé à caractère personnel ou relatives à la santé d'une personne, données médico-sociales à caractère personnel) imposent qu'elles soient particulièrement protégées.

Il est rappelé ci-dessous :

- les principaux besoins métiers des secteurs sanitaire, médico-social et social en matière de bon fonctionnement des dispositifs médicaux, de protection des données de santé à caractère personnel et de traçabilité des actes médicaux ;
- les besoins de sécurité « génériques » des SI, quel que soit le secteur d'activité ;
- les menaces qui pèsent sur la sécurité des données de santé à caractère personnel et les besoins de sécurisation des SI qui en découlent.

[7] Le terme « usager » recouvre, dans ce document, les notions de patient (sanitaire), de résident (EHPAD) et d'usager (handicap).

2.1.1. Les besoins métiers spécifiques des secteurs sanitaire, médico-social et social

La prise en charge d'un usager nécessite le recueil de données de santé à caractère personnel. Elle est optimale si elle est réalisée sur la base d'informations accessibles, vérifiées, à jour, précises, suffisantes et cohérentes. Elle nécessite des moyens informatiques adaptés et dont la continuité du service répond aux besoins métiers.

Afin de répondre aux enjeux liés à une bonne prise en charge des usagers, il est nécessaire de garantir que :

- les données de santé à caractère personnel des usagers sont disponibles au sein des applications métiers et des dispositifs médicaux pilotés par un SI qui participent au traitement des usagers ;
- les données de santé à caractère personnel des usagers sont intègres[8] ;
- les applications métiers et les dispositifs médicaux pilotés par un SI qui participent au traitement des usagers sont eux-mêmes opérationnels ;
- la confidentialité des données sensibles[9] est assurée ;
- l'échange et le partage des données de santé à caractère personnel gérées dans le SI sont toujours maîtrisés ;
- la traçabilité des actes médicaux (dont les prescriptions médicales), des produits de santé dispensés ou administrés, des produits de santé utilisés ou implantés est assurée, ainsi que la conservation systématique de l'historique des antécédents médicaux et des comptes rendus médicaux, chaque fois que le SI est utilisé dans le cadre de ces activités.

Les principales spécificités des besoins SSI santé découlent de :

- l'impact possible d'une indisponibilité ou d'un manque d'intégrité des données sur la santé des usagers ;
- la spécificité des règles de partage et d'échange des données sociales et de santé à caractère personnel.

2.1.2. Les besoins de sécurité « génériques » des SI

Les besoins de sécurité d'un SI découlent de la nature des informations qu'il traite et de la nature de ces traitements. Par exemple, un SI traitant des données météorologiques statistiques a des besoins de sécurité différents d'un SI traitant les salaires au sein d'une entreprise.

En se plaçant à un niveau de description générique, il apparaît néanmoins un ensemble de besoins de sécurité communs à la majorité des SI d'organismes publics ou privés. Ces besoins « génériques », dont l'importance varie en fonction du contexte, sont également partagés par les structures des secteurs sanitaire, médico-social et social, en plus de leurs besoins spécifiques :

- les données utilisées dans des processus métiers non spécifiques à l'organisme ou à des processus supports potentiellement critiques (gestion de stock, comptabilité, paie, gestion des contrats, annuaire système des utilisateurs du SI…) doivent être disponibles au sein des applications qui les utilisent et ne doivent être modifiées que dans le cadre des processus prévus ;
- les applications métiers et les composants informatiques qui participent à ces mêmes processus doivent être opérationnels pendant les plages d'activité prévues de l'organisme ;

[8] C'est-à-dire qu'elles ne puissent pas être modifiées en dehors des procédures fixées (cf. encadré au 2.1.2)

[9] Données de santé à caractère personnel, données à caractère personnel, toutes autres données jugées sensibles dans le cadre d'une analyse de risque.

- certaines données, bien que non spécifiques, doivent rester confidentielles. C'est notamment le cas de toute donnée à caractère personnel : fichiers du personnel, salaires, traces générées par le SI et pouvant être rattachées à des personnes… ;
- les moyens informatiques ne doivent pas être détournés de leur usage prévu. En effet le SI risque, dans ce type de situation, de subir un ralentissement des traitements, une saturation des supports de stockage et des moyens de communication. La responsabilité de l'organisme peut être engagée quant à des utilisations illicites du SI : téléchargements illégaux de films, musiques, livres numériques ou logiciels, participation à des activités de commerce illégal (hébergement pirate de site illicite de vente de médicament en ligne…) ou au piratage d'autres systèmes informatiques…
- l'organisme doit disposer de traces, techniques ou fonctionnelles, des activités réalisées via son SI afin de pouvoir investiguer (ou permettre à la justice d'investiguer) en cas de dysfonctionnement ou d'utilisation malveillante du SI, soupçonnée ou avérée, et de préserver au mieux son activité et sa responsabilité.

Pour aller plus loin : Dans le domaine de la sécurité des systèmes d'information, quatre critères principaux sont utilisés pour qualifier les besoins de sécurité :

- **la disponibilité** des données ou des traitements : le fait que les données (annuaire des fournisseurs, dossier patient, inventaire de pharmacie…) ou les traitements (application, web service, composant logiciel…) soient accessibles au moment prévu pour leurs usages autorisés ;
- **l'intégrité** des donnée ou des traitements : le fait que les données ou les processus de traitement appliqués aux données ne puissent être modifiés que par les personnels habilités à le faire et qu'à défaut tout changement illégitime puisse être détecté ;
- **la confidentialité** des données : le fait que les données ne soient accessibles qu'aux utilisateurs habilités à les consulter ;
- **l'imputabilité** (ou traçabilité): le fait d'être capable de savoir quelles actions (connexion d'un utilisateur, consultation ou modification de donnée sensible, mise à jour d'un logiciel…) ont été réalisées au sein du SI, quand et par quel utilisateur.

Ces quatre critères de sécurité sont également utilisés pour qualifier les menaces qui pèsent sur le SI : par exemple, la menace « perte d'une clé USB » peut porter atteinte à la disponibilité et à la confidentialité des données stockées sur la clé USB.

2.1.3. La diversité des risques informatiques

De nombreux exemples, au sein de structures des secteurs sanitaire, médico-social et social, ont mis en lumière les impacts de la concrétisation des risques informatiques et la fragilité de moyens informatiques insuffisamment protégés :

- La **destruction** très rapide de volumes considérables de données ou la mise hors service d'un ordinateur, voire d'un SI, peuvent être provoquées par certains virus. Ces situations conduisent parfois à devoir réinstaller tout le parc informatique et reconstituer les données, avec un coût élevé pour un résultat souvent partiel.
- Les **vols** de matériels informatiques se multiplient et conduisent souvent à la perte de volumes conséquents de données de santé à caractère personnel. Les conséquences financières, de temps passé et de gêne professionnelle sont élevées, et des conséquences importantes en matière d'image et au niveau légal sont possibles, notamment en cas de divulgation publique de ces données.
- L'**altération** de données est fréquente (effacement par erreur, modifications indues…). Certaines de ces données sont essentielles au traitement d'un usager et leur altération peut impacter très significativement la qualité du suivi des soins et des diagnostics.

- Des **erreurs** de manipulation ou des **actes malveillants** peuvent aboutir à la publication non maîtrisée sur internet de dossiers d'usagers, ou à des menaces de publication de ces dossiers.

De manière générale et malgré les risques qui ont été présentés, l'informatisation des données de santé à caractère personnel les sécurise mieux que les dossiers papier dès lors qu'elle est accompagnée d'une réelle politique de gestion de risques.

Quelques exemples :

- le simple fait de disposer d'une sauvegarde journalière permet de préserver les données de santé à caractère personnel des patients avec leurs dernières mises à jour, alors qu'un sinistre quelconque (inondation, incendie dans un bureau) pourrait détruire son équivalent papier ;
- Un dossier papier peut être perdu ou simplement égaré pendant un certain temps, alors que sa version électronique reste conservée. Les dispositions de suivi des accès aux dossiers informatisés (les « traces » et les dispositifs de sceau électronique) facilitent l'identification des anomalies (suppression intempestive d'un élément du dossier) et permettent ainsi, le cas échéant, de déclencher la restauration de l'élément manquant depuis une version antérieure sauvegardée ;
- Ces mêmes dispositions de traces ont une valeur dissuasive contre les accès injustifiés à un dossier patient, l'utilisateur qui ne fait pas partie de l'équipe de soin étant informé que son accès laissera une trace et pourra conduire à ce qu'il rende des comptes à ce propos.

Certaines vulnérabilités et menaces informatiques auxquelles sont exposés les SI des structures des secteurs sanitaire et médico-social leur sont spécifiques :

- La combinaison de l'accueil de tiers (patients et visiteurs) et de situations d'urgence de production de soins peut rendre plus complexe la protection systématique des éléments informatiques (ex. : pour prendre en charge un patient en situation d'urgence, il n'y a pas toujours le temps de sécuriser son poste de travail malgré la présence de personnes étrangères au service) ;
- L'hétérogénéité des éléments informatiques (postes de travail, équipements bio-médicaux, terminaux mobiles…) en complexifie le maintien à jour ;
- La motivation des attaquants, qui peuvent être attirés par un impact médiatique, peut être élevée dans le cas de menaces liées à la santé des patients ou à la divulgation de données personnelles sensibles (médicales ou autres).

2.2. Définition et finalité d'une PSSI

Dans son *guide d'élaboration de politique de sécurité des systèmes d'information [GPSSI ANSSI],* l'ANSSI indique que :

« Une Politique de Sécurité des Systèmes d'Information (PSSI) reflète la vision stratégique de la direction de l'organisme (PME, PMI, industrie, administration...) en matière de sécurité des systèmes d'information (SSI) et de gestion de risques SSI. Elle décrit en effet les éléments stratégiques (enjeux, référentiel, principaux besoins de sécurité et menaces) et les règles de sécurité applicables à la protection du système d'information de l'organisme.

[…] La PSSI vise à informer la maîtrise d'ouvrage[10] et la maîtrise d'œuvre[11] des enjeux tout en l'éclairant sur ses choix en termes de gestion des risques et à susciter la confiance des utilisateurs et partenaires envers le système d'information. »

Ainsi, une PSSI est un document porté par la direction et qui regroupe les objectifs stratégiques de la structure en termes de SSI ainsi que les règles et mesures organisationnelles, fonctionnelles et techniques à mettre en œuvre pour y parvenir.

La PSSI n'est pas le seul document qui traite de SSI au sein de la structure. Cependant, par la vision synthétique qu'elle donne, c'est elle qui conditionne le reste de la documentation sécurité et permet de s'orienter dans cette documentation : procédures déclinant des règles de la PSSI au niveau opérationnel, règles métiers de définition des droits d'accès, spécifications des fonctions de sécurité du SI…

[10] La **maîtrise d'ouvrage** (ou **MOA**) porte le besoin, définit l'objectif du projet et son calendrier. La maîtrise d'ouvrage maîtrise la genèse du projet et représente, à ce titre, les utilisateurs finaux à qui l'ouvrage est destiné.

[11] La **maîtrise d'œuvre** (ou **MOE**) peut être chargée de la conception, de la réalisation et/ou de l'exploitation de SI, généralement pour le compte de la MOA.

2.3. Spécificité de la méthode d'élaboration de la PSSI proposée par ce guide

Comme indiqué en préambule, ce guide a été élaboré pour les structures des secteurs sanitaire et médico-social qui ne disposent pas encore d'approche formalisée pour la sécurité de leur système d'information.

La méthode proposée a été conçue pour :

- réduire autant que possible la charge de travail à fournir par chaque structure pour élaborer sa PSSI en fournissant un large ensemble d'éléments « prêts à l'emploi » pour tous les aspects potentiellement communs à la majorité de ces structures ;
- que la production de la PSSI et sa mise en application ne requièrent que des connaissances de base dans le domaine SSI ;
- que la PSSI produite permette d'atteindre rapidement un premier niveau de sécurité « sain » au vu des enjeux et des moyens de la structure ;
- que cette PSSI prévoie un renforcement progressif des mesures de sécurité jusqu'à un niveau conforme à l'état de l'art, dans une optique d'amélioration continue de la sécurité.

Ainsi, il ne s'agit pas d'identifier l'ensemble des règles et mesures qu'il faudrait idéalement mettre en place pour être au meilleur niveau de l'état de l'art, mais de lister les règles et mesures opérationnelles qui doivent et peuvent être mises en œuvre à court ou moyen terme pour atteindre un niveau de sécurité adapté aux enjeux de sécurité de la structure à un instant donné.

Seules ont été retenues les activités indispensables à la définition d'une PSSI et à la mise en œuvre rapide et efficace des mesures de sécurité adaptées permettant de couvrir les principaux risques de la structure à l'aide d'un Plan d'Action SSI.

Pour autant, l'élaboration du guide et du canevas de PSSI n'a pas fait abstraction des méthodes « classiques » d'analyse de la SSI et d'élaboration de PSSI. Bien qu'il n'apparaisse pas explicitement dans le guide, un travail d'analyse des enjeux, des menaces et des vulnérabilités SSI génériques dans les structures des secteurs sanitaire et médico-social a été mené en amont, dans la ligne de la norme ISO 27005 et de la méthodologie EBIOS [EBIOS 2010].

C'est de ce travail que découle la synthèse des risques génériques pour un établissement de santé présenté en Annexe 3.

Les aspects liés aux « biens essentiels » de la terminologie EBIOS sont ainsi pris en compte à un niveau générique et de façon implicite, une prise en compte explicite requérant une charge de travail de la part des structures pour l'appropriation de la méthode et pour la réalisation de l'inventaire des biens essentiels (informations et processus) incompatible avec les objectifs du guide.

L'Annexe 6 présente la correspondance entre les thématiques d'exigences utilisées par ce guide, les objectifs de sécurité fixés par la [PSSIE] et les articles ISO 27002.

3. COMMENT ELABORER LA POLITIQUE DE SECURITE DE VOTRE SI ?

3.1. Synthèse de la démarche

L'élaboration de la PSSI de votre structure se déroule en quatre étapes :

- « Cadrer » : Expliciter le contexte d'application de la PSSI ;
- « Inventorier » : Recenser les différentes catégories de moyens du SI ;
- « Analyser » : Qualifier les principaux risques auxquels est exposé le SI ;
- « Décider » : Choisir les mesures de sécurité nécessaires.

Afin d'alléger le travail de rédaction de la PSSI, un contenu générique adapté aux contextes des secteurs sanitaire, médico-social et social est d'ores et déjà intégré au canevas de PSSI qui accompagne ce guide.

Ainsi, pour chacune des étapes de la méthode, votre structure devra :

- mener les tâches de collecte d'information, d'analyse et de décision nécessaires à la personnalisation du canevas de PSSI ;
- compléter le canevas à l'aide des résultats de ces travaux ;
- le cas échéant, amender le contenu du canevas (ce contenu est un exemple générique) pour l'ajuster au contexte de votre structure et aux choix effectués ;
- supprimer les paragraphes « guide de rédaction » (encadrés introduits par le pictogramme ✍) qui, par définition, n'ont pas vocation à apparaître dans la PSSI finalisée.

> ☞ Le guide a été conçu pour que le travail requis pour ces tâches soit aussi limité que possible.
>
> En particulier, les exemples de contenu proposés dans le canevas de PSSI peuvent être presque intégralement conservés pour la PSSI de votre structure avec simplement quelques adaptations, quand cela est nécessaire, aux spécificités de votre contexte.
>
> Un sous-ensemble de règles de sécurité permettant de constituer rapidement un premier Plan d'Action SSI est également proposé en Annexe 4.

Chaque tâche de chaque étape est décrite par les éléments suivants :

- compétences nécessaires, qui peuvent éventuellement requérir la participation conjointe de plusieurs intervenants;
- détail des travaux à mener ;
- chapitres du canevas de PSSI qui doivent recueillir les résultats des travaux ou être adaptés en fonction de ces résultats.

Une fois la PSSI élaborée et validée par la direction, le Plan d'Action SSI doit être défini afin de fixer les objectifs, échelonnés dans le temps, de mise en œuvre des différentes mesures de sécurité. Cette phase est détaillée au chapitre 4 de ce guide.

3.2. Les acteurs de la PSSI

Qu'il s'agisse de la phase d'élaboration de la PSSI ou de sa mise en œuvre, différents acteurs sont susceptibles d'être mobilisés.

Outre les travaux opérationnels autour de la PSSI, il est essentiel que les acteurs qui ont en charge une partie des activités de la structure et qui seront concernés par la PSSI soient associés à la démarche, lors des réunions avec la direction sur le sujet, ou selon le cas au cours des réflexions sur la PSSI.

Afin de conserver une approche qui puisse être adaptée aux organisations variées des différentes structures des secteurs sanitaire, médico-social et social, le guide identifie ces acteurs par leur rôle. Des dénominations aussi génériques que possible sont utilisées, et on peut citer notamment :

- la direction générale de la structure ;
- les directions métiers, utilisatrices du SI ;
- les directions d'activités supports : RH, juridique, services généraux (dont sécurité des biens et des personnes) ;
- la direction de SI ou responsable informatique ;
- si cette fonction existe dans la structure, le Correspondant Informatique et Liberté (CIL) ;
- le Responsable Sécurité du SI (RSSI), ou le Référent Sécurité du SI.

3.3. Organisation du document PSSI

La démarche présentée ici permet à une structure d'élaborer la Politique de Sécurité du Système d'Information (PSSI) qui adopte l'organisation du document Canevas de PSSI.

La PSSI qui en découle comporte les chapitres suivants :

1. Préambule – Déclaration de la direction : description
2. Objet de la PSSI
3. Champs d'application
4. Contexte
5. Exigences de sécurité et règles applicables
6. Annexes

Ce plan constitue l'organisation préconisée pour la PSSI. Chaque structure peut toutefois décider d'adopter une organisation différente, par exemple en scindant le document unique en plusieurs documents :

- un document « chapeau » qui reprend les chapitres 1 à 4 du canevas (préambule, objet, champ d'application et contexte) ;
- un ou plusieurs documents pour les exigences et règles de sécurité, le cas échéant réparties par domaine de responsabilité en fonction des types de composants du SI auxquels elles s'appliquent (même si certaines règles peuvent alors apparaître en doublon dans les différents documents).

3.4. Etape 1 – « Cadrer » : expliciter le contexte

Cette première étape a pour objet :

- de fixer le périmètre du SI auquel doit s'appliquer la PSSI ;
- d'expliciter les enjeux associés à ce périmètre ;
- de vérifier que les conditions requises pour la définition et la mise en œuvre d'une PSSI sur ce périmètre sont réunies.

Les différentes tâches menées au cours de cette étape sont de :

1. Valider le projet avec la direction de la structure
2. Fixer l'objet de la PSSI
3. Définir le champ d'application de la PSSI
4. Préciser les enjeux de sécurité
5. Identifier les textes applicables

✍ La plupart de ces étapes se concluent par la formalisation de leur résultat dans le canevas de PSSI. Des conseils complémentaires sont proposés par les encadrés « guide de rédaction » des chapitres correspondants du canevas.

Un exemple de formulation est généralement proposé dans le canevas, et peut servir de base pour le texte final, une fois adapté au contexte de la structure.

3.4.1. Tâche 1.1 : Valider le projet avec la direction de la structure

☞ Compétences nécessaires pour cette étape : connaissance du SI, connaissance des métiers de la structure, communication avec la direction.

La définition et la mise en œuvre d'une PSSI constitue un véritable projet structurant pour le SI. Il est essentiel de vérifier que la direction de la structure en partage bien les objectifs et la démarche et que les moyens nécessaires à sa réalisation sont disponibles.

A cette fin, le porteur du projet peut préparer la réunion de validation en traitant, à un niveau macroscopique, les différentes tâches prévues par la démarche, à l'aide du contenu proposé dans le canevas de PSSI.

3.4.2. Tâche 1.2 : Fixer l'objet de la PSSI

☞ Compétences nécessaires pour cette étape : connaissance du SI, connaissance des métiers de la structure.

✍ L'objet de cette tâche est simplement de personnaliser le texte générique du chapitre 2 « Objet de la PSSI » proposé dans le canevas de PSSI.

3.4.3. Tâche 1.3 : Définir le champ d'application de la PSSI

☞ Compétences nécessaires pour cette étape : connaissance du SI, connaissance des métiers de la structure et de leur contexte règlementaire.

Le champ d'application de la PSSI se définit :

- du point de vue des activités métiers et des activités support d'une part ;
- du point de vue des moyens du SI d'autre part.

Cette tâche a pour objet de traiter le premier aspect, à savoir le périmètre auquel doit s'appliquer la PSSI du point de vue des activités. Le second aspect est traité au cours de l'étape 2 « Inventorier : recenser les moyens du SI ».

Il s'agit ici de dresser une rapide description de l'organisme et des activités qu'on souhaite inclure dans le périmètre. Il est important de préciser, le cas échéant, les activités qu'on souhaite exclure du périmètre (par exemple, de façon temporaire pour une première mise en œuvre de la PSSI uniquement).

Les activités supports qui sont nécessaires aux activités métiers doivent également être indiquées (ex : comptabilité, RH, informatique, logistique…).

La description nécessite le niveau de détail juste suffisant à garantir que le périmètre pris en compte est clair pour l'ensemble du personnel de la structure.

Le périmètre métier et support retenu conditionne notamment les enjeux de sécurité, les moyens du SI pris en compte et les risques liés au SI.

☞ Lors de la rédaction de la première version de la PSSI, un choix stratégique devra probablement être fait au sujet de son périmètre : soit prendre en compte les activités et le SI dans leur intégralité, soit en exclure certaines parties pour alléger l'élaboration initiale de la PSSI.

Dans le second cas, le périmètre de la PSSI pourra être étendu à l'occasion d'une version ultérieure de la PSSI.

☞ Ce guide et le canevas de PSSI associé se concentrent sur la sécurité des SI et des données dématérialisées qu'ils manipulent.

Bien que certaines exigences et règles de sécurité proposées dans le canevas de PSSI puissent participer à la sécurisation des données sur support papier, ce type de support d'information nécessite des dispositions spécifiques qui ne sont pas abordées dans le canevas de PSSI.

✍ La définition du champ d'application de la PSSI doit être reportée au chapitre 3 du canevas de PSSI.

3.4.4. Tâche 1.4 : Préciser les enjeux de sécurité

☞ Compétences nécessaires pour cette étape : connaissance du SI, connaissance des métiers de la structure et de leur contexte règlementaire.

L'objet de cette tâche est d'expliciter en quoi la sécurité du SI est importante pour la bonne réalisation des activités retenues pour le périmètre de la PSSI.

L'expression de ces enjeux fait typiquement ressortir l'importance du SI dans la réalisation des missions de la structure. Elle souligne les exigences qui pèsent sur le SI pour que ces activités puissent être réalisées conformément aux attentes. Les contraintes liées au contexte, aux obligations de la structure, à l'environnement, etc. peuvent également être mentionnées ici si elles sont susceptibles de conditionner les attentes en termes de SSI.

✍ Les enjeux de sécurité doivent être reportés au chapitre 4.1 du canevas de PSSI.

3.4.5. Tâche 1.5 : Identifier les textes applicables

☞ Compétences nécessaires pour cette étape : juridique, connaissance des métiers de la structure et de leur contexte règlementaire.

Cette tâche a pour finalité d'identifier les principaux textes qui imposent des contraintes à la structure quant à l'usage de son SI.

Ces contraintes peuvent, par exemple, être constituées :

- d'obligations de mise à disposition, dans des situations définies, de certaines informations à leurs propriétaires, aux autorités ;
- d'obligations de protection de la confidentialité et de l'intégrité de certaines données traitées ;
- de règles particulières d'échange de certaines données ;
- de limitations de durée de conservation de certaines données, de traces, … ;
- d'interdictions de certains traitements des données ;
- d'obligations de continuité de certaines activités de la structure, ou de délai maximal de production de certains résultats ;
- etc.

Il ne s'agit pas ici de lister ces contraintes, ni d'analyser la jurisprudence, mais d'identifier les textes qui fixent ces contraintes, afin que la direction, les responsables d'applications, les responsables du SI et de la sécurité du SI puissent les prendre en compte et s'y reporter quand nécessaire.

Outre les textes qui s'imposent (textes de nature législative ou règlementaire, circulaires ministérielles, …), la structure peut également identifier à ce stade les autres textes qu'elle considère comme applicables en termes de SSI (standards, référentiels de bonnes pratiques, …).

✍ La liste des textes applicables doit être intégrée au chapitre 4.2 du canevas de PSSI.

3.5. Etape 2 – « Inventorier » : recenser les moyens du SI

☞ Compétences nécessaires pour cette étape : connaissance des moyens technique et logistique relatifs au SI, connaissance de l'organisation de la structure.

Les moyens sur lesquels s'appuie le SI, également appelés « biens supports[12] » dans le cadre d'une analyse de risques, constituent le patrimoine matériel et organisationnel que les règles de la PSSI vont contribuer à protéger pour permettre à la structure de mener ses activités.

Pour que ces règles soient définies de manière pertinente, il est nécessaire :

- de connaître la nature des éléments auxquels chaque règle doit s'appliquer ;
- de savoir qui va être en charge de mettre chaque règle en application.

A cette fin, un inventaire des catégories de moyens (ou « biens supports ») du SI doit être réalisé.

Il ne s'agit pas ici de dresser un inventaire détaillé qui recenserait chaque composant du SI comme on le ferait pour une gestion de parc par exemple, mais d'identifier des groupes de biens supports homogènes et dont une même personne a la responsabilité (dont celle de mettre en œuvre les règles de la PSSI pour les biens supports en question).

Un modèle d'inventaire est proposé en Annexe 1. Il définit un premier niveau de catégorisation des biens supports, que vous pouvez adapter à votre contexte le cas échéant. Vous pouvez l'utiliser pour faire dresser l'inventaire des catégories de moyens du SI en créant une ligne supplémentaire pour chaque nouvelle entrée dans la catégorie ad-hoc pour :

- une catégorie de moyens homogènes (qui sera sommairement décrite dans la colonne « Dénomination de la catégorie de moyens »), qui est à la fois :
  - sous une même responsabilité technique (en charge de la mise en œuvre des règles de sécurité et qui sera identifiée dans la colonne « Fonction du responsable technique »),
  - et sous une même responsabilité métier (au sens demandeur/décideur côté utilisateurs, qui sera identifiée dans la colonne « Fonction du responsable métier»).

☞ Pour chaque catégorie, posez-vous la question « à qui sera confiée la mise en œuvre des règles de sécurité ? ». Si vous identifiez un contact unique (expert, chef d'équipe interne, prestataire ou fournisseur en charge d'une partie du SI externalisé), notez la fonction de cette personne dans la colonne « Fonction du responsable technique » et passez à la catégorie suivante.

S'il y a plusieurs contacts possibles, divisez la catégorie en ensembles plus détaillés pour lesquels le contact est unique. Par exemple, pour les périphériques de téléphonie, le contact pour les téléphones fixes peut être différent du contact pour les téléphones mobiles. A contrario, une même personne peut être contact pour plusieurs catégories.

Selon l'organisation de votre structure, la catégorisation la plus adaptée peut être fonctionnelle et non technique. Par exemple, les serveurs informatiques et ceux des équipements biomédicaux peuvent être les mêmes types de serveurs mais être gérés par deux équipes différentes.

[12] Bien sur lequel reposent les informations, les processus et les fonctions d'un SI. « On distingue notamment les systèmes informatiques, les organisations et les locaux. » [EBIOS 2010].

☞ Un exemple d'inventaire est présenté en Annexe 1bis.

L'inventaire des catégories de moyens du SI n'est pas destiné à être intégré au document « PSSI ». C'est néanmoins un document qui fait partie du corpus documentaire SSI de la structure et qui est référencé par d'autres documents (la PSSI, le Plan d'Action Sécurité…).

☞ L'inventaire des catégories de moyens doit aussi être l'occasion d'identifier les composants du SI susceptibles de recueillir ou de stocker des données de santé qui ne relèvent pas de la structure elle-même.

Par exemple, dans le cadre du partage des équipements médico-techniques (IRM, Scanner, laboratoire, pharmacie) entre deux ES publics, ou/et privé-public, les données sont stockées sur les modalités (IRM, Scanner, échographie) et les automates (laboratoire), voire sur des serveurs. L'ES qui héberge l'équipement ou/et la modalité héberge alors des données dont il n'est pas propriétaire.

Ce cas de figure appelle des dispositions particulières afin de se conformer au cadre légal et règlementaire (voir règles de la Thématique 1 et 6 du canevas de PSSI).

☞ Ce genre d'inventaire de haut niveau est relativement stable, les restructurations complètes du SI étant peu fréquentes. Toutefois, lorsque c'est le cas, il convient de mettre immédiatement l'inventaire en cohérence pour s'assurer que les règles de la PSSI sont appliquées à d'éventuels nouveaux éléments, même si ces changements interviennent en dehors d'une mise à jour planifiée de la PSSI.

La structuration des catégories proposée dans le modèle en Annexe 1 se base sur la classification des biens supports du guide méthodologique EBIOS [EBIOS 2010 BDC]. Cette classification a cependant été subdivisée afin de correspondre plus facilement à l'organisation des responsabilités des moyens du SI généralement rencontrée. Le lien avec la classification proposée par [EBIOS 2010 BDC] peut être établi

3.6. Etape 3 – « Analyser » : qualifier les principaux risques du SI

3.6.1. Tâche 3.1 : Identifier les principaux risques liés au SI

☞ Compétences nécessaires pour cette étape : connaissance des enjeux métiers de la structure et éventuellement connaissance du SI.

Il est important de comprendre les principaux risques susceptibles d'être applicables à votre structure pour vous assurer que les exigences et les règles de sécurité proposées dans le canevas de PSSI sont adaptées à votre contexte.

Pour vous éviter de mener vous-même une analyse de risque complète, il a été établi une cartographie générique des risques pesant sur les SI de structures des secteurs sanitaire, médico-social et social.

Le tableau récapitulatif de la cartographie des risques est présenté ci-dessous.

La finalité de cette cartographie est de lister les principaux risques qui pèsent sur le SI, hiérarchisés par niveau de risque, afin de pouvoir définir les priorités de mise en œuvre des règles de sécurité.

Le niveau associé à chaque risque (scénario combinant un évènement redouté avec un ou plusieurs scénarios de menace) découle de la gravité de l'évènement redouté et de la vraisemblance des scénarios de menace.

La règle de combinaison du niveau de gravité et du niveau de vraisemblance pour obtenir le niveau de risque est détaillée en Annexe 2.

Le détail du niveau de gravité et du niveau de vraisemblance pour chaque risque identifié est donné en Annexe 3.

Le niveau de risque indiqué correspond au risque « brut », c'est-à-dire en présence de l'ensemble des vulnérabilités potentielles, et avant qu'aucune mesure de sécurité du SI ne soit mise en œuvre.

Evènement redouté	Scénarios de menaces	Réf. risque	Niveau de risque
Indisponibilité de fonctions (application médicale, dispositif connecté, …) ou d'informations (données de santé à caractère personnel ou données personnelles d'un usager) pouvant entrainer une désorganisation du service, un impact d'image négatif auprès des usagers et ou un risque usager	▶ code malveillant (virus, cheval de Troie) ; ▶ dégradation ou interruption du réseau (réseau local, accès WAN et Internet, réseau Wifi) ; ▶ défaillance de l'alimentation électrique ; ▶ défaillance de la climatisation des salles serveurs ; ▶ erreur de manipulation de la part du personnel en charge du SI ; ▶ manque de maintenance ; ▶ défaillance de matériel.	R-01	Fort
	▶ saturation des applications ; ▶ modification non maîtrisée d'un logiciel	R-02	Modéré
	▶ détérioration de matériel informatique (incendie, dégât des eaux, …) ; ▶ indisponibilité du personnel (pandémie, crise sanitaire, difficultés d'accès aux bâtiments…).	R-03	Fort
Altération de fonctions (application médicale, dispositif connecté, …) ou d'informations (par exemple, les données de santé à caractère personnel ou données personnelles d'un usager) pouvant entrainer une désorganisation du service, un impact d'image négatif auprès des usagers et ou un risque patient	▶ code malveillant (virus, cheval de Troie) ; ▶ erreur de saisie ou de commande d'un utilisateur du SI ; ▶ manque de maintenance ; ▶ défaillance de matériel.	R-04	Fort
	▶ modification non maîtrisée d'un logiciel (mise à jour de logiciel ou du paramétrage/configuration) ; ▶ détournement de l'usage prévu d'un logiciel (abus de droits systèmes ou applicatifs, accès direct aux données des applications, …).	R-05	Modéré
	▶ intrusion informatique	R-06	Modéré
Altération des éléments de preuves générés et stockés par le SI (par ex. traces applicatifs …)	▶ détournement de l'usage prévu d'un logiciel (abus de droits systèmes ou applicatifs, accès direct aux données des applications, …).	R-07	Modéré

Evènement redouté	Scénarios de menaces	Réf. risque	Niveau de risque
pouvant augmenter le risque juridique pour la structure en cas de contentieux	► intrusion informatique	R-08	Modéré
Accès aux données de santé à caractère personnel ou personnelles d'un patient par un Tiers non autorisé constituant une atteinte à la vie privée et/ou au secret professionnel	► perte ou sortie non contrôlée d'un matériel (ordinateur portable, support de stockage amovible, …).	R-09	Fort
	► détournement de l'usage prévu d'un logiciel (abus de droits systèmes ou applicatifs, accès direct aux données d'un logiciel).	R-10	Modéré
	► intrusion informatique.	R-11	Modéré

Ce tableau sert de base de travail pour adapter si nécessaire ces éléments génériques, les préciser ou en retirer.

A ce niveau macroscopique, les évènements redoutés sont similaires aux évènements redoutés « classiques » utilisés en SSI. En revanche, certains impacts sont spécifiques aux secteurs sanitaire et médico-social dans le cas de données de santé à caractère personnel dont l'altération ou l'indisponibilité pourrait avoir des conséquences sur la santé du patient.

Le tableau des risques permet également de sensibiliser les acteurs du SI aux situations qui peuvent porter atteinte au SI et à l'activité de la structure, et tend à améliorer leur vigilance vis-à-vis des principales menaces identifiées.

Dans certains cas de figure, il peut s'avérer :

- que, d'après votre expérience, le niveau de risque indiqué vous semble surévalué ou sous-évalué pour un ou plusieurs scénarios de risque ;
- que des évènements redoutés et/ou des scénarios de menaces spécifiques à votre structure ne sont pas couverts par les scénarios de risques proposés et doivent être ajoutés.

Ces modifications ne peuvent être prises en compte de manière simple dans le cadre du présent guide. En effet, une analyse de risque spécifique doit être menée pour traiter ces cas particuliers.

Deux options s'offrent alors :

- soit mettre en œuvre la méthode d'analyse plus approfondie pour les scénarios en question (voir chapitre 6) ;
- soit confier à un expert SSI l'analyse des scénarios de risques supplémentaires ou modifiés, tout en conservant le formalisme simplifié, les métriques et l'Annexe 3 de ce guide. L'analyse d'un petit nombre de scénarios avec ce formalisme simplifié constitue une tâche simple pour un expert SSI.

Dans les deux cas, l'analyse de risque doit permettre de déterminer si des exigences de sécurité supplémentaires sont nécessaires, et de définir dans ce cas les règles de sécurité qui permettent d'y répondre.

Il n'en reste pas moins que les exigences de sécurité proposées dans le canevas et les règles de sécurité associées permettent de réduire de manière significative les risques nouvellement identifiés. La prise en compte des risques spécifiques ne remet donc pas en cause la mise en œuvre de la démarche proposée ici, même s'il est nécessaire de la compléter dans certains cas.

✍ Les modifications qui découleraient d'une éventuelle analyse de risque complémentaire doivent être reportées dans le tableau des risques au chapitre 4.3.2 et en Annexes 4 et 5 du canevas de PSSI. Les exigences et règles supplémentaires éventuellement nécessaires dans ce cas doivent être ajoutées dans les thématiques idoines du chapitre 5 et de l'Annexe 5 du canevas de PSSI.

☞ L'analyse de risque générique qui a été menée, et les exigences et règles de sécurité qui en découlent, prennent en compte les origines potentielles de menaces « basiques » : personnel interne et sous-traitants, patients et visiteurs, cybercriminels ne visant pas spécifiquement la structure, délinquants « classiques » (vols, vandalisme), catastrophes naturelles, catastrophes industrielles d'ampleur locale, …

Elles ne prennent que partiellement en compte les risques liés à des menaces qui seraient d'origine étatique ou qui seraient spécifiquement ciblées sur la structure, par exemple dans le cadre d'enjeux de recherche sur des domaines très concurrentiels d'un point de vue économique.

Si l'origine de tels risques devait être intégralement prise en compte, une analyse de risques complémentaire spécifique devrait être menée. Le chapitre 4.3.1 du canevas de PSSI devrait alors également être modifié en conséquence.

3.6.2. Tâche 3.2 : Préciser la stratégie de traitement des risques

☞ Compétences nécessaires pour cette étape : connaissance des enjeux métiers de la structure et éventuellement connaissance du SI.

Une fois les principaux risques identifiés, il reste à confirmer la manière dont ils doivent être traités. C'est l'objet de cette tâche.

Pour chaque risque, il s'offre quatre options de traitement[13]. Les deux premières sont le plus souvent adoptées :

- réduire le risque : mettre en œuvre des mesures de sécurité pour diminuer la vraisemblance du risque ou son impact (ou les deux), pour que le risque se limite à un niveau acceptable ;
- transférer ou partager le risque : partager les pertes avec d'autres acteurs en cas de sinistre (par exemple avec une compagnie d'assurance), faire assumer la responsabilité par un tiers…

Les deux dernières peuvent être retenues vis-à-vis de certains risques, dans des situations particulières :

- éviter (ou refuser) le risque : modifier des éléments du contexte du SI afin qu'il n'existe plus d'exposition à ce risque. Par exemple, pour une application, ne plus l'autoriser qu'au personnel interne authentifié au lieu de la laisser en libre accès à toute personne à l'intérieur de la structure comme initialement souhaité, ou encore renoncer complètement à une application car le coût des mesures nécessaires pour la sécuriser n'est pas acceptable en regard des services attendus de cette application ;
- prendre (ou « maintenir ») le risque : accepter le risque tel quel et assumer ses conséquences sans prendre de mesure de sécurité supplémentaire ;

[13] Source EBIOS [EBIOS 2010], valable également pour ISO27005

Il est possible de choisir plusieurs options pour un même risque, par exemple réduire partiellement le risque par des mesures de sécurité et recourir à une assurance pour couvrir les frais en cas de réalisation du risque résiduel.

La stratégie de traitement des risques peut être exprimée de manière générale dans la PSSI sous forme de principe de base, puis explicitée pour chaque risque identifié.

✍ Une stratégie de traitement des risques générique est énoncée au chapitre 4.3.3 du canevas de PSSI, à la suite du tableau des risques. Elle consiste à réduire l'ensemble des risques identifiés à un niveau acceptable.

3.7. Etape 4 – « Décider » : choisir les mesures de sécurité

A ce stade de la démarche :

- les éléments constitutifs du SI ont été identifiés ;
- les risques qui peuvent y être associés ont été cartographiés ;
- la stratégie de traitement de chaque risque a été fixée.

La tâche suivante (tâche 4.1) consiste, pour chaque risque qu'il a été décidé de réduire à un niveau acceptable, à déterminer les exigences de sécurité[14] qui doivent être imposées au SI pour atteindre cet objectif.

Ces exigences de sécurité peuvent être de nature à éviter la survenance du risque (il s'agit alors de prévention) ou à en limiter les impacts lorsqu'ils donnent lieu à des incidents (il s'agit alors de réaction à l'incident). Elles sont généralement exprimées sous une forme fonctionnelle, générique et peu technique. C'est sur la base de ces exigences que seront élaborées, au cours de la tâche 4.2, les règles opérationnelles concrètes qui répondent à ces exigences.

3.7.1. Organisation des exigences et des règles

Suivant la même logique que le reste du guide, le chapitre 5 du canevas de PSSI propose un ensemble d'exigences et de règles de sécurité présélectionnées pour le contexte de structures des secteurs sanitaire, médico-social et social.

Les exigences et les règles sont organisées en 7 thématiques :

- Thématique 1 : Répondre aux obligations légales
- Thématique 2 : Promouvoir et organiser la sécurité
- Thématique 3 : Assurer la sécurité physique des équipements informatiques du SI
- Thématique 4 : Protéger les infrastructures informatiques
- Thématique 5 : Maîtriser les accès aux informations
- Thématique 6 : Acquérir des équipements, logiciels et services
- Thématique 7 : Limiter la survenue et les conséquences d'incidents de sécurité

[14] En ingénierie, les **exigences** sont l'expression documentée de ce qu'un produit ou un service particulier doit être ou faire. Dans le cadre de la sécurité du système d'information d'un établissement de santé, elles sont l'expression du besoin de l'établissement concernant la sécurité de ses locaux, de ses données et du traitement de ces données.

Cette structuration en 7 thématiques s'est appuyée sur les thèmes utilisés par l'ISO 27002:2013. Certains de ces thèmes ont cependant été regroupés pour mieux se rapprocher de l'organisation quotidienne des structures. Cet aménagement a pour finalité de vous permettre d'identifier plus aisément les contextes sur lesquels portent les exigences afin d'en apporter une déclinaison adaptée aux populations qui doivent les mettre en œuvre.

Ainsi la thématique 3 « Assurer la sécurité physique des équipements informatiques du SI » concerne plus particulièrement les services généraux de votre structure, tandis que la thématique 1 « Répondre aux obligations légales » concerne plus particulièrement le personnel prenant en charge les patients ainsi que le service juridique.

L'Annexe 6 présente la correspondance entre les thématiques d'exigences et de règles utilisées par ce guide, et :

- les objectifs de sécurité fixés par la Politique de Sécurité des Systèmes d'Information de l'Etat [PSSIE], applicable à toute structure qui relève du service public ;
- les articles de l'ISO 27002:2013.

3.7.2. Tâche 4.1 - Fixer les exigences de sécurité applicables

Compétences nécessaires pour cette étape : connaissance des enjeux métiers de la structure, connaissance du SI.

Les exigences de sécurité proposées au chapitre 5 du canevas de PSSI ont été choisies, conformément au cadre légal et à la stratégie de traitement des risques adoptée, afin de :

- réduire les risques génériques identifiés dans le tableau de la cartographie des risques (cf. chapitre 3.6.1) ;
- répondre aux principales obligations légales en matière de sécurité des SI de structures du secteur sanitaire ou médico-social.

Elles sont issues :

- de l'ensemble des référentiels techniques et guides pratiques de la PGSSI-S [PGSSI-S] ;
- du Programme Hôpital Numérique [HN- BAO] ;
- de la [PSSIE] ;
- des bonnes pratiques en sécurité des SI : norme [ISO27002:2013] (« Technologies de l'information – Techniques de sécurité – Systèmes de gestion de sécurité de l'information – Exigences »), normes ISO suivantes du même domaine, guides ANSSI, guides élaborés par la DGOS [GP SSI ES]...

Par conséquent, l'ensemble de ces exigences est, a priori, applicable à une structure du secteur sanitaire ou médico-social.

Pour plus de détails sur la correspondance entre les risques et les exigences, vous pouvez vous reporter au tableau de synthèse de la couverture des risques par les exigences figurant en Annexe 5 du canevas de PSSI, qui indique quelles exigences participent à la réduction de chaque risque.

Chaque sous-thème des thématiques du chapitre 5 du canevas de PSSI comporte une ou plusieurs exigences de sécurité.

Ces propositions d'exigences ont été élaborées en dehors de tout contexte spécifique. Il peut donc être nécessaire de reformuler chacune d'elles afin de l'adapter à votre contexte (SI, organisation de la structure, répartition des tâches par équipe…).

✍ Au chapitre 5 du canevas de PSSI, personnaliser le cas échéant la formulation des exigences pour chaque sous-thématique.

3.7.3. Tâche 4.2 - Décliner les exigences de sécurité en règles

☞ Compétences nécessaires pour cette étape : connaissance du SI, connaissance de l'organisation de la structure.

Une fois les exigences de sécurité établies, il convient de déterminer les mesures de sécurité qui permettront de satisfaire chacune d'elles.

Ces mesures sont présentées sous forme de règles, de consignes à mettre en œuvre par les utilisateurs du SI, les employés et/ou les prestataires de la structure. Le canevas de PSSI propose un ensemble d'exemples de règles qui répondent aux exigences prédéfinies dans le canevas. Là encore, ces exemples ont été élaborés afin de pouvoir être presque directement utilisés comme règle pour la PSSI de votre structure.

A cette fin, les opérations à mener au cours de cette tâche sont, pour chaque exemple de règle proposé :

- vérifier que la règle s'applique à des catégories de moyens de SI effectivement présentes dans le SI de votre structure. Pour cela, il convient de se demander sur quel(s) élément(s) du SI va porter la règle et comment le(s) responsable(s) de cet/ces élément(s) vont la satisfaire. Si vous êtes certain que cette règle ne s'applique à aucun moyen de votre SI, elle peut être supprimée. Les catégories de moyens auxquelles la règle est susceptible de s'appliquer sont indiquées pour chaque règle du chapitre 5 du canevas de PSSI.
- si la règle est applicable à au moins un moyen du SI, la contextualiser pour votre structure, son organisation et son SI, si nécessaire ;
- le cas échéant, adapter la dénomination des catégories de moyens du SI auxquelles s'applique la règle, pour que ces noms correspondent à ceux effectivement utilisés dans votre inventaire des moyens du SI (cf. Etape 2 de la méthode).

✍ Dans le canevas de PSSI, des blocs « guide de rédaction » peuvent, pour certaines thématiques d'exigences, fournir des indications sur la déclinaison des exigences en règles et vous aider ainsi à personnaliser les règles proposées.

☞ Il peut s'avérer que, pour une thématique donnée, aucune des règles de sécurité ne soit applicable dans le contexte de votre structure, ces règles s'appliquant à des moyens qui n'existent pas dans votre SI. Par exemple, si le SI ne dispose d'aucune infrastructure d'accès sans fil (Wifi ou autre), aucune règle de la thématique T4-4 « gérer les connexions sans fils » n'a lieu d'être appliquée.

Dans ce cas, il est légitime de supprimer toutes les règles de sécurité correspondantes (pour les deux sous-thématiques dans l'exemple donné), qui n'ont pas d'objet.

En revanche, il est important de conserver les thématiques concernées et les exigences de sécurité associées au sein de la PSSI. En effet, de cette manière, si des moyens concernés par ces thématiques viennent à être mis en œuvre ultérieurement, les exigences correspondantes ne seront pas oubliées. Les règles associées, qui avaient été retirées, pourront être réintégrées à partir du canevas de PSSI dès qu'il y en aura besoin, par exemple quand la mise en œuvre d'un réseau Wifi sera étudiée, pour que ces règles soient prises en compte dès le début du projet.

✍ Modifications à apporter éventuellement au chapitre 5 du canevas de PSSI :

- le cas échéant, personnaliser la formulation de chaque règle de sécurité et l'indication des catégories de moyens du SI concernées par sa mise en application ;
- uniquement s'il est certain qu'une règle ne peut s'appliquer à aucun composant du SI de la structure, la supprimer.

3.7.4. Par quelles règles commencer ?

Pour un établissement abordant pour la première fois la sécurisation du système d'information, le choix des premières règles est important. Il doit permettre de traiter les fondamentaux de la sécurisation tout en constituant une marche réaliste eu égard à la nouveauté de la démarche. Cette marche constitue également un support à la mise en place d'un cycle d'amélioration continue. Ce cycle permettra d'améliorer la sécurisation par passes successives afin d'atteindre un objectif de sécurisation conforme à la PSSI et adapté aux enjeux de l'organisation.

Pour ces établissements, il est proposé une liste des mesures essentielles propres à constituer cette première marche (cf. Annexe 4), qui peut être utilisée dans le cadre du chapitre suivant.

4. COMMENT METTRE EN ŒUVRE LA PSSI : LE PLAN D'ACTION SSI

Une fois la PSSI élaborée et validée par la direction de la structure, il reste à la mettre en application.

Toutes les règles énoncées au chapitre 5 de la PSSI étant applicables à votre structure, une démarche naturelle consisterait à mettre en œuvre toutes ces règles au plus vite.

Pourtant, vous avez pu constater en élaborant la PSSI que les règles sont nombreuses, et même si certaines d'entre elles sont peut-être déjà en vigueur dans votre structure, la prise en compte de l'intégralité de ces règles constitue un effort important aussi bien pour les services en charge du soutien (logistique, SI, services généraux…) que pour les utilisateurs eux-mêmes. Si certains logiciels ou équipements complémentaires doivent être déployés pour se conformer à certaines règles, le budget correspondant devra également être mobilisé.

Pour ces différentes raisons, une mise en œuvre « exhaustive » de prime abord risquerait d'aboutir rapidement à un essoufflement des volontés comme des moyens. Au final, la PSSI risquerait de ne jamais être réellement mise en application : elle serait décrédibilisée car perçue par les équipes SI comme « déconnectée » de la réalité et d'une applicabilité improbable.

Pour éviter cet écueil majeur, il est essentiel de séquencer la mise en œuvre de la PSSI. Ce séquencement est formalisé dans un « Plan d'Action Sécurité des Systèmes d'Information » (Plan d'Action SSI[15]) dont les étapes identifient les règles à appliquer à différentes échéances réalistes, en fonction des moyens dont dispose la structure et des spécificités de son SI et de son organisation.

Le Plan d'Action SSI est l'outil qui :

- fixe le périmètre des règles qui doivent être en application effective à des échéances déterminées ;
- constate, à chaque échéance, le degré d'atteinte des objectifs qui avaient été fixés et permet de présenter de manière synthétique l'état d'avancement réel de la mise en œuvre des règles de la PSSI ;
- est révisé chaque fois que nécessaire pour prendre en compte l'avancée constatée du déploiement des règles de la PSSI et prendre en compte les freins ou les opportunités qui se présentent pour la mise en œuvre de ces règles.

☞ Un modèle de Plan d'Action SSI sous forme de feuille de calcul (tableur) est proposé conjointement à ce guide : « Modèle de Plan d'Action Sécurité » [MOD PAS]. Il permet de fixer les objectifs du déploiement des mesures de sécurité échelonné dans le temps.

Pour chaque étape de la démarche d'élaboration du Plan d'Action SSI, un encadré indique comment utiliser le modèle proposé.

L'utilisation de ce modèle nécessite des connaissances de base dans l'usage d'un tableur (feuille de calcul).

[15] Le sigle PASSI ne sera pas utilisé, étant déjà utilisé pour la désignation des *Prestataires d'audit de la sécurité des systèmes d'information*

4.1. Elaborer le Plan d'Action SSI

☞ Compétences nécessaires pour cette étape : connaissance technique du SI, évaluation des coûts et des charges pour les mesures de sécurité.

L'élaboration du *Plan d'Action SSI* permet de préparer :

- la diffusion des règles à mettre en œuvre pour les biens supports sur lesquels elles doivent s'appliquer ;
- le suivi formel de la mise en œuvre des règles sur les différents biens supports.

Le *Plan d'Action SSI* est construit en 4 étapes :

1. identifier les personnes en charge de la mise en application de chaque règle de sécurité ;
2. estimer l'effort nécessaire à la mise en œuvre de chaque règle ;
3. fixer les priorités, et de là, les objectifs de déploiement des règles échelonnés dans le temps ;
4. obtenir la validation de la direction sur la PSSI et le *Plan d'Action SSI* élaborés, et mobiliser les moyens nécessaires à la mise en œuvre planifiée.

✍ **Utilisation du modèle de Plan d'Action SSI** : l'onglet « Plan et suivi » du modèle est celui utilisé pour l'ensemble des étapes de l'élaboration du Plan d'Action SSI.

4.1.1. Etape 1 : Identifier les personnes en charge de l'application de chaque règle

Il s'agit tout d'abord, pour chaque règle de sécurité fixée par la PSSI, d'identifier les personnes qui seront responsables de sa mise en application.

La méthode est simple :

- pour chaque règle de sécurité de votre PSSI (chapitre 5 de la PSSI) sont indiquées les catégories de moyens du SI concernées, liste de catégories que vous avez éventuellement adaptée au contexte de votre structure (lors de l'étape 4.2 du guide) ;
- l'inventaire des moyens du SI (établi à l'étape 2 de la démarche) vous permet de retrouver, pour chacune de ces catégories de moyens, le responsable technique qui, a priori, sera en charge de la mise en œuvre de la règle de sécurité.

✍ **Réalisation de cette étape à l'aide du modèle de Plan d'Action SSI** : le modèle est pré-renseigné avec la liste complète des règles de sécurité, organisées en thématiques et sous-thématiques conformément à la PSSI.

- copiez et insérez intégralement chaque ligne de règle autant de fois que nécessaire afin que la règle soit déclinée pour chaque catégorie de moyens associée ;
- indiquez, pour chaque ligne, la catégorie de moyens concernée dans la colonne « Moyens du SI » et renseignez le nom ou la fonction de la personne en charge de l'application de la règle pour cette catégorie de moyens dans la colonne « Resp. mise en œuvre ».

4.1.2. Etape 2 : Estimer l'effort nécessaire à la mise en œuvre de chaque règle

Afin d'alimenter les choix d'ordre de mise en œuvre des règles de sécurité, il est nécessaire de dresser une estimation de l'effort nécessaire au déploiement de chaque règle pour chaque catégorie de moyens du SI concernée.

Pour cela, il faut tout d'abord communiquer les règles de sécurité à l'ensemble des contacts identifiés à l'étape précédente, ainsi que l'indication des règles qui concernent spécifiquement chacun d'eux. Les contacts pourront ainsi :

- prendre connaissance des règles qui concernent leur périmètre de responsabilité ;
- déterminer dans quelle mesure chaque règle est déjà mise en œuvre sur le périmètre cible qui les concerne ;
- déterminer l'effort nécessaire, en charge de travail et en coût (achats éventuels notamment) pour la mise en œuvre de chaque règle sur l'ensemble du périmètre cible qui les concerne.
- retourner ces informations au coordonnateur de l'élaboration du *Plan d'Action SSI*.

Selon le même principe que celui proposé au chapitre suivant, ce travail peut, dans un premier temps, être restreint aux règles dont la priorité est 1 dans le modèle de *Plan d'Action SSI* fourni (colonne « Prio »), voire aux règles listées par l'Annexe 4. Cette approche permet d'aboutir dans un délai plus court à un premier *Plan d'Action SSI* qui vise essentiellement les règles de priorité 1.

✍ **Réalisation de cette étape à l'aide du modèle de Plan d'Action SSI** : le document Plan d'Action SSI ainsi que la PSSI peuvent être communiqués aux différentes personnes concernées, si possible après une rapide réunion de présentation de ces documents et des objectifs poursuivis.

- chaque responsable d'une ou plusieurs catégories de moyens du SI retrouve dans le Plan d'Action SSI les lignes qui le concernent, et consulte dans la PSSI les règles de sécurité correspondantes ;
- après qu'il a fait le point sur les mesures de sécurité déjà en place, il peut renseigner, pour les lignes qui le concernent, les trois colonnes de « situation initiale » :
  - « % déjà en œuvre » doit estimer le pourcentage des composants appartenant à la catégorie de moyen en question pour lesquels la règle étudiée est déjà effectivement et intégralement appliquée,
  - Les colonnes « charge » et « coût » du « reste à faire » doivent recueillir les informations correspondantes, dans les unités indiquées (à adapter le cas échéant avant diffusion du Plan d'Action SSI) ;
- le coordonnateur de l'élaboration du Plan d'Action SSI rassemble les informations retournées dans la version consolidée du document.

☞ Il peut être utile de souligner, à l'attention des différents responsables de catégories de moyens, que l'objet du Plan d'Action SSI est bien d'échelonner dans le temps la mise en œuvre des règles de sécurité, et non pas de tout appliquer d'un coup, et que l'estimation de l'effort à fournir participe à ce choix d'échelonnement.

4.1.3. Etape 3 : Fixer les objectifs de déploiement des règles

C'est au cours de cette étape que sont fixés les objectifs de déploiement des règles de sécurité pour la première échéance du *Plan d'Action SSI* et éventuellement pour l'échéance suivante.

Les objectifs de déploiement de la mise en œuvre des règles sont déterminés selon les principes suivants :

- les règles doivent être mises en œuvre en respectant l'indication de priorité mentionnée pour chacune d'elle à la colonne « Prio » (Priorité) du modèle de *Plan d'Action SSI* fourni. Les règles de priorité 1 doivent être mises en œuvre avant celles de priorité 2, et celles de priorité 2 avant celles de priorité 3.

- Ces trois niveaux de priorité ont été définis pour tenir compte à la fois des dépendances entre les différentes mesures de sécurité, des gains en sécurité qu'on est en droit d'attendre de l'application de chaque règle et de l'effort *a priori* nécessaire pour mettre en œuvre chaque règle (ce dernier point restant difficile à estimer de manière précise car dépendant fortement du contexte de chaque structure) ;
- ce premier classement doit ensuite être affiné en fonction de l'effort estimé par les responsables concernés (à l'étape précédente) qui tient compte cette fois des spécificités de la structure et de son SI ;
- des ajustements du classement obtenu peuvent encore être apportés de manière « opportuniste ». Par exemple, une règle peut être « remontée » dans le classement pour favoriser un déploiement anticipé :
  - si une mesure a priori reléguée à une mise en application ultérieure peut être mise en œuvre très facilement dans le contexte de la structure,
  - si une mesure proche était déjà en cours de déploiement et que son ajustement et sa finalisation pour répondre à l'une des règles demande un effort mineur,
  - si une règle répond à une problématique urgente (notamment si elle répond à une exigence liée, dans l'analyse des risques, à un risque « Fort » - cf. Annexe 3 de la PSSI pour le lien entre exigences et risques),
- d'autres ajustements peuvent également être réalisés selon la situation, par exemple pour tenir compte de l'impact de ces règles sur les utilisateurs et les métiers, qu'elles induisent certaines contraintes ou qu'elles simplifient l'utilisation du SI (les deux cas sont parfois combinés),
- en dehors des actions « opportunistes », il est inutile de passer du temps à classer les règles de priorité 2 ou 3 tant que des règles de priorité 1 restent à déployer (même principe pour les règles de priorité 3 tant qu'il en reste de priorités 2, lors de la mise à jour du *Plan d'Action SSI*)
- il faut alors sélectionner les règles en tête du classement obtenu et dont l'effort cumulé de mise en œuvre correspond à ce que la structure peut consacrer jusqu'à la première échéance de mise en œuvre souhaitée.
- Il est recommandé de viser une première échéance à 6 mois pour les actions qui pourront être rapidement mises en application, et de planifier également une seconde échéance à 12 mois afin de donner une visibilité suffisante sur les objectifs et, à échéance, sur les résultats obtenus.

☞ Il est recommandé que les règles listées en Annexe 4 soient systématiquement sélectionnées parmi les premières règles à mettre en application au sein de la structure, quitte à se limiter à cet ensemble dans un premier temps.

☞ L'objectif de déploiement d'une règle sur une catégorie de moyens donnée peut être un objectif de déploiement partiel à l'échéance fixée (ex : 50%), puis complet à l'échéance suivante, selon les moyens affectés et la disponibilité des personnes en charge des opérations correspondantes.

Ce type de déploiement « partiel » peut répondre, par exemple, au souhait de réaliser un « pilote » pour la mise en œuvre d'une ou plusieurs règles de sécurité sur un périmètre limité à fin de validation avant un déploiement généralisé.

Ça peut également être le cas quand il est souhaité que la règle soit mise en œuvre en priorité sur un sous-ensemble particulièrement sensible du périmètre potentiel, bien que dans une telle situation il serait probablement justifié d'identifier ce sous-ensemble comme une catégorie de moyens spécifique dans l'inventaire des moyens du SI afin d'en faire apparaître les particularités.

✍ **Réalisation de cette étape à l'aide du modèle de Plan d'Action SSI** : pour travailler sur le classement des règles à mettre en œuvre, il est recommandé d'utiliser une copie du fichier tableau Plan d'Action SSI élaboré jusque-là, afin que les opérations de tri et de sélection ne le désorganisent pas. Sauf mention contraire, c'est toujours cette copie qui est utilisée pour cette étape :

- utiliser les fonctions de tri de données pour trier les règles par ordre de Priorité croissante (colonne « Prio »), puis de charge et/ou de coût décroissante (NB : ne pas se préoccuper d'erreurs de formules éventuelles qui apparaîtraient suite au tri : les formules intégrées au modèle ne sont pas utilisées ici) ;
- changer manuellement l'ordre des lignes de règles pour prendre en compte les moyens nécessaires, les éventuelles actions « opportunistes » et les autres facteurs pertinents ;
- sélectionner le groupe de tête du classement dont le besoin cumulé de moyens correspond aux ressources disponibles jusqu'à l'échéance fixées ;
- optionnellement, sélectionner le groupe de règle qui suit dans le classement pour donner de la visibilité sur l'échéance suivante ;
- dans le document Plan d'Action SSI consolidé (et non plus dans la copie utilisée pour le tri), reporter dans la zone « déploiement » :
  - la date de l'échéance à droite de la première cellule « date »,
  - pour chaque règle sélectionnée, indiquer le taux de déploiement cible attendu à l'échéance dans la première colonne « % cible »,
  - optionnellement, indiquer la date de l'échéance suivante à droite de la seconde cellule « date », et pour chaque règle envisagée pour cette seconde échéance, indiquer le taux de déploiement cible dans la seconde colonne « % cible ».

4.1.4. Etape 4 : Faire valider la PSSI et le Plan d'Action SSI par la direction

La validation par la direction de la PSSI et du *Plan d'Action SSI* proposés, et son soutien affiché sont évidemment nécessaires à l'exécution du Plan d'Action Sécurité et à la mobilisation des moyens requis.

Une présentation synthétique des enjeux, des principaux risques et des choix de mise en œuvre prioritaire des règles formalisées dans le *Plan d'Action SSI*, doit être effectuée à la direction de la structure et aux principaux acteurs métiers.

Les premiers chapitres de la PSSI (objet, champ d'application, enjeux, principaux risques, stratégie de traitement) constituent une bonne base pour une telle présentation, à compléter par les principales actions prévues au *Plan d'Action SSI* et moyens nécessaires associés.

Une fois la PSSI et le *Plan d'Action SSI* validés, la PSSI peut être communiquée à l'ensemble des utilisateurs du SI, tel que le prévoit certainement la PSSI elle-même. L'exécution du *Plan d'Action SSI* peut alors être lancée.

☞ Dans l'absolu, la PSSI pourrait être validée par la direction de la structure avant que ne soit entamée l'élaboration du Plan d'Action SSI.

Il vous est proposé ici de faire valider les deux documents en même temps, afin de fournir à la direction des éléments opérationnels et concrets sur lesquels se positionner (moyens nécessaires mis en regard de la proposition des règles de sécurité déployées) en plus des objectifs, éléments d'analyses et règles de sécurité énoncés par la PSSI.

4.1.5. Comment prendre en compte les parties externalisées du SI dans le Plan d'Action SSI ?

La validation par la direction de la PSSI et du *Plan d'Action SSI* proposés, et son soutien affiché sont évidemment

La prise en compte des parties externalisées du SI dépend du contrat d'externalisation. Il doit y avoir un accord sur les exigences de sécurité figurant au contrat, celles-ci devant être alignées sur les exigences de la PGSSI-S.

C'est alors au fournisseur de vérifier que les règles qu'il met en œuvre répondent aux exigences contractualisées. Selon le contrat, la structure peut avoir un droit de regard sur les règles prévues par le fournisseur, voire avoir un droit d'audit (ce qui reste généralement complexe et coûteux à appliquer).

Dans tous les cas, il est souhaitable que la conformité -au moins revendiquée, sinon vérifiée- du fournisseur aux exigences de sécurité énoncées dans la PSSI soit matérialisée pour chaque exigence (et non pour chaque règle) dans le *Plan d'Action SSI*. De la même manière qu'en interne, le fournisseur peut communiquer sa conformité initiale, et proposer un échéancier de mise en conformité qui sera suivi de la même manière que le reste du *Plan d'Action SSI*.

4.2. Suivre et mettre à jour le Plan d'Action SSI

A l'échéance prévue dans le *Plan d'Action SSI*, un bilan doit être dressé par chaque responsable de la mise en œuvre des règles prévues au *Plan d'Action SSI* et éventuellement de celles qu'il n'était pas prévu de déployer mais qui l'ont tout de même été (il peut s'agir d'un « effet de bord » d'une autre action par exemple).

Il est recommandé de procéder à une revue des actions avec les différents responsables afin d'en retirer les enseignements sur les succès et les écueils rencontrés, de constater l'avancement global, et de préparer la phase suivante du *Plan d'Action SSI*.

✍ **Réalisation de ces tâches à l'aide du modèle de Plan d'Action SSI** : dans l'onglet « Plan et suivi » du fichier Plan d'Action SSI, chaque responsable de mise en œuvre de règles de sécurité renseigne le taux d'avancement effectif des déploiements dont il a la charge dans la colonne « % atteint ».

La méthode d'élaboration du *Plan d'Action SSI* peut alors être réitérée (à partir de l'étape 2), en considérant la situation à l'échéance comme « situation initiale ». La finalisation des actions qui n'ont pas été terminées à l'échéance prévue est replanifiée, et la mise en œuvre de nouvelles règles est préparée.

Les résultats de l'exécution du *Plan d'Action SSI* précédent peuvent être exposés à la direction conjointement à la présentation du nouveau *Plan d'Action SSI* pour validation.

Ce cycle « planification, présentation/validation, mise en œuvre, bilan » se répète ainsi dans un intervalle de 6 mois au départ, puis plus probablement avec une périodicité annuelle ensuite, quand les actions restant à mener sont plus longues à mettre en place, jusqu'à la mise en œuvre de l'ensemble des règles de sécurité sur le périmètre complet prévu par la PSSI.

Ces itérations se poursuivent ensuite, pour :

- vérifier que les mesures de sécurité restent toujours appliquées comme exigé par la PSSI ;
- prendre en compte les évolutions du SI et de la PSSI, dont le périmètre est susceptible d'évoluer.

✍ **Réalisation de ces tâches à l'aide du modèle de Plan d'Action SSI** : pour chaque nouvelle itération du plan d'action, un nouveau document Plan d'Action SSI peut être créé par copie du document en cours (afin de conserver les désignations des catégories de moyens et des responsables de mise en œuvre) :

- les dates d'échéance sont mises à jour ;
- les valeurs de la colonne « % atteint » sont reportées dans la colonne « % déjà atteint », puis les valeurs de la colonne « % atteint » sont effacées ;
- les valeurs des colonnes « % cibles » sont mises à jour selon les nouveaux objectifs fixés, ainsi que les colonnes du « Reste à faire », selon la méthode indiquée précédemment.

5. FAIRE VIVRE LA PSSI

Le contexte de sécurité du SI de votre structure évolue naturellement dans le temps. Par exemple :

- les activités de la structure peuvent varier ;
- il peut être décidé d'élargir le périmètre auquel s'applique la PSSI, par exemple pour prendre en compte des activités métiers qui utilisent de nouveaux dispositifs informatiques, ou parce que la version initiale de la PSSI avait volontairement été restreinte à un périmètre « pilote » réduit ;
- la règlementation peut évoluer et modifier les contraintes qui s'appliquent au SI ;
- de nouvelles menaces spécifiques ou non aux secteurs sanitaire et médicosocial peuvent émerger ;
- l'amélioration de la sensibilisation des utilisateurs à la sécurité du SI peut rendre acceptable et donc envisageable la mise en œuvre de mesures de sécurité plus efficaces ;
- les incidents survenus peuvent avoir révélé des risques qui n'avaient pas été clairement identifiés à leur juste niveau jusque-là, ou la nécessité de renforcer certaines mesures de sécurité ;
- les retours d'expérience sur la mise en œuvre des règles de sécurité peuvent amener à les améliorer, à les adapter encore plus spécifiquement à la structure, à ajuster leur périmètre d'application…

Il est normal -et souhaitable- que ces éléments donnent lieu à une évolution de la PSSI dès lors qu'ils peuvent avoir un impact notable sur la sécurité du SI, ou qu'ils révèlent un besoin d'amélioration de certains aspects de la PSSI.

Une bonne pratique est de procéder à une revue collégiale régulière, par exemple annuelle, de la PSSI, après transmission des remarques des responsables concernés par la mise en œuvre de la PSSI à la personne en charge de sa maintenance.

☞ Ce processus de retours d'expériences, de revue régulière et de mise à jour des documentations et des pratiques de sécurité du SI peut probablement être comparé (avec les limites de toute comparaison) avec le processus de vigilance sanitaire en vigueur dans de nombreuses structures.

La mise à jour de la PSSI se fait selon les mêmes principes que ceux qui président à sa rédaction initiale. Vous pouvez donc vous reporter aux parties de ce guide qui correspondent aux chapitres de la PSSI que vous devez mettre à jour.

Le Plan d'Action Sécurité est susceptible de devoir être mis à jour suite à la revue de la PSSI. Cette opération peut être menée :

- dans la foulée si les changements doivent être pris en compte en urgence au niveau opérationnel ou si ils sont susceptibles de remettre en cause des actions SSI qui sont en cours ;
- à l'occasion du prochain point de suivi du *Plan d'Action SSI* planifié dans les autres cas.

Cette démarche de revue et de mise à jour de la PSSI s'inscrit dans le schéma de système de management de la sécurité de l'information (SMSI) décrit par la norme ISO 27001 « Technologies de l'information - Techniques de sécurité - Systèmes de gestion de sécurité de l'information – Exigences ». Elle permet une amélioration continue de la gestion de la SSI au sein de votre structure, et facilitera l'évolution ultérieure vers une sécurité du SI encore mieux maîtrisée en adoptant progressivement des méthodes de sécurité plus approfondies comme celles présentées au chapitre 6.

Cette démarche d'amélioration continue permet de fixer à la structure un objectif initial réaliste, puis d'évoluer lorsque c'est nécessaire. Elle permet d'augmenter le niveau de maturité SSI tout en assurant une adéquation des mesures au contexte actualisé.

6. CONCLUSION

La définition de la PSSI de votre structure à l'aide de la méthode proposée, puis la mise en application progressive de cette PSSI, permettent de réduire à un niveau acceptable les risques liés au système d'information.

Il se peut que la maturité que votre structure aura acquise dans la gestion de la sécurité du SI au cours de vos travaux sur la PSSI révèle des besoins d'élargissement de la démarche. Voici quelques situations symptomatiques du besoin d'aller au-delà de ce que ce guide propose :

- vous avez déjà mené un ou plusieurs cycles de mise à jour de la PSSI et de revue du *Plan d'Action SSI* et vous pensez avoir épuisé ce que ce guide peut vous apporter, car vous identifiez des axes d'amélioration de la sécurité qu'il n'évoque pas ;
- vous êtes confronté à des menaces qui ne sont pas identifiées dans ce guide et qui sont maintenant les menaces les plus importantes à prendre en compte dans votre contexte, toutes les autres étant déjà intégrées à votre PSSI ;
- des incidents du SI que les règles proposées dans ce guide ne permettent pas d'éviter sont survenus.

Dans ces différents cas, il est nécessaire d'aller au-delà de ce que ce guide peut vous apporter : il est nécessaire de mener une analyse de risque détaillée qui permette de prendre en compte toutes les spécificités de votre SI. L'expérience acquise avec la mise en œuvre de ce guide et la mise en application de la PSSI que vous avez élaborée vous permettent désormais de mener cette analyse de sécurité approfondie et d'échanger sur les risques avec un expert sécurité.

Nous vous conseillons alors de vous référer aux démarches et méthodes suivantes :

- Norme NF ISO/CEI 27005 « Technologies de l'information - Techniques de sécurité - Gestion des risques liés à la sécurité de l'information » [ISO27005:2013] qui fixe en cadre normatif complet et générique pour les analyses de risques SSI ;
- EBIOS « Méthode de gestion des risques » [EBIOS 2010], qui se conforme à l'ISO 27005 tout en proposant une démarche modulaire et guidée, ainsi que des référentiels pouvant être utilisés directement ou être adaptés à chaque contexte spécifique (cette dernière option étant fortement recommandée).

Annexe 1 : Modèle d'inventaire des moyens du SI

Locaux

Locaux d'hébergement du SI

Locaux hébergeant une partie ou la totalité des composants d'un SI

Dénomination de la catégorie de moyens	Fonction responsable technique	Fonction responsable métier (si applicable)

Locaux donnant accès au SI

Locaux depuis lesquels les utilisateurs accèdent au SI

Dénomination de la catégorie de moyens	Fonction responsable technique	Fonction responsable métier (si applicable)

Equipements d'infrastructure système et réseaux

Composants centraux constitués de matériel, logiciel ou élément de réseau, qui stockent et traitent des informations ou réalisent des fonctions du SI. Ces équipements et logiciels sont généralement opérés par le personnel informatique et principalement localisés dans les locaux d'hébergement du SI.

Matériels

Dénomination de la catégorie de moyens	Fonction responsable technique	Fonction responsable métier (si applicable)

Logiciels

Dénomination de la catégorie de moyens	Fonction responsable technique	Fonction responsable métier (si applicable)

Réseaux

Dénomination de la catégorie de moyens	Fonction responsable technique	Fonction responsable métier (si applicable)

Téléphonie et télécommunications

Dénomination de la catégorie de moyens	Fonction responsable technique	Fonction responsable métier (si applicable)

GTC-GTB (Gestion Technique Centralisée – Gestion Technique du Bâtiment)

Dénomination de la catégorie de moyens	Fonction responsable technique	Fonction responsable métier (si applicable)

Equipements utilisateurs

Composants employés par les utilisateurs du SI pour accéder aux fonctions qu'il offre. Il s'agit des terminaux (poste de travail fixe ou nomade, mobile, tablette PC etc.), périphériques locaux (imprimante, scanneur, photocopieur etc.) et logiciels qui permettent d'accéder aux fonctions et informations du SI. Ces équipements et logiciels sont directement opérés par les utilisateurs du SI et principalement localisés dans les locaux donnant accès au SI (ils sont également utilisés par le personnel informatique et potentiellement présents dans les locaux d'hébergement du SI pour permettre son exploitation).

Terminaux

Dénomination de la catégorie de moyens	Fonction responsable technique	Fonction responsable métier (si applicable)

Périphériques informatiques

Dénomination de la catégorie de moyens	Fonction responsable technique	Fonction responsable métier (si applicable)

Support de données amovibles

Dénomination de la catégorie de moyens	Fonction responsable technique	Fonction responsable métier (si applicable)

Logiciels des postes de travail

Dénomination de la catégorie de moyens	Fonction responsable technique	Fonction responsable métier (si applicable)

Equipements biomédicaux associés au SI

Système à finalité médicale, fixe ou mobile, connecté au SI, qui permet de traiter automatiquement des données et qui intègre les organes nécessaires à son fonctionnement autonome, ses interfaces de communication et ses périphériques indispensables.

Dénomination de la catégorie de moyens	Fonction responsable technique	Fonction responsable métier (si applicable)

Téléphonie

Dénomination de la catégorie de moyens	Fonction responsable technique	Fonction responsable métier (si applicable)

Organisations

Services

Transposition de l'organisation de la structure.

Dénomination du service	Fonction responsable technique	Fonction responsable métier (si applicable)

Catégories de personnel

Catégories de personnel utiles à la gestion de la sécurité du SI

Dénomination de la catégorie de personnel	Fonction responsable technique	Fonction responsable métier (si applicable)

Annexe 1bis : Exemple d'inventaire des moyens du SI

☞ Cet inventaire des catégories de moyens du SI d'une structure imaginaire est donné à titre d'exemple pour illustrer le type de contenu et la granularité possible d'un tel inventaire.

Locaux

Locaux d'hébergement du SI

Locaux hébergeant une partie ou la totalité des composants d'un SI

Dénomination de la catégorie de moyens	Fonction responsable technique	Fonction responsable métier (si applicable)
Salle serveur principale	Responsable services généraux	Responsable serveurs
Locaux techniques d'étage	Responsable services généraux	Responsable réseau
Local point d'accès Wifi invité	Responsable services généraux	Responsable réseau
Locaux de l'hébergeur de données de santé « H »	Hébergeur de données de santé	Direction

Locaux donnant accès au SI

Locaux depuis lesquels les utilisateurs accèdent au SI

Dénomination de la catégorie de moyens	Fonction responsable technique	Fonction responsable métier (si applicable)
Bâtiment d'accueil	Responsable services généraux	Responsable administratif
Chambres	Responsable services généraux	Chef de service A
Chambres maternité	Responsable services généraux	Chef de service maternité
Bloc chirurgie	Responsable services généraux	Chef de service B
Locaux de radiologie	Responsable services généraux	Chef de service radiologie

Equipements d'infrastructure système et réseaux

Composants centraux constitués de matériel, logiciel ou élément de réseau, qui stockent et traitent des informations ou réalisent des fonctions du SI. Ces équipements et logiciels sont généralement opérés par le personnel informatique et principalement localisés dans les locaux d'hébergement du SI.

Matériels

Dénomination de la catégorie de moyens	Fonction responsable technique	Fonction responsable métier (si applicable)
Serveurs bureautique	Responsable serveurs	n/a (transverse)

Dénomination de la catégorie de moyens	Fonction responsable technique	Fonction responsable métier (si applicable)
Serveurs dédiés progiciels médicaux	Responsable serveurs	Directeur de l'Information Médicale (DIM)
Serveurs dédiés gestion	Responsable serveurs	Responsable administratif
Serveurs dédiés Dossier patient informatisé (hébergement externe)	Hébergeur de données de santé	DIM
Serveurs de bases de données	Responsable serveurs	Responsable informatique
Baies de disques	Responsable serveurs	Responsable informatique
Serveurs de messagerie, passerelles Internet	Responsable serveurs	Responsable informatique
Serveur portail Internet	Responsable serveurs	Responsable de la communication
Serveurs d'administration du SI	Responsable serveurs	Responsable informatique
Equipements de sécurité du SI	Responsable sécurité informatique	Responsable SSI
Système de sauvegarde	Responsable serveurs	Responsable SSI
Modem de télémaintenance des baies de disque	Responsable serveurs	Responsable SSI

Logiciels

Dénomination de la catégorie de moyens	Fonction responsable technique	Fonction responsable métier (si applicable)
<système d'exploitation linux pour serveurs>	Responsable serveurs	Responsable informatique
<système d'exploitation propriétaire pour serveurs>	Responsable serveurs	Responsable informatique
<logiciel serveur web>	Responsable serveurs	Responsable de la communication
<logiciel serveur de messagerie>	Responsable serveurs	Responsable de la communication
<logiciel proxy web>	Responsable serveurs	Responsable de la communication
<SGBDR propriétaire>	Responsable serveurs	Responsable informatique
<suite progiciel de gestion propriétaire>	Responsable serveurs	Responsable administratif
Service Dossier patient informatisé (hébergement externe)	Hébergeur de données de santé	DIM
<progiciel médical A>	Responsable serveurs	Chef de service A
<progiciel médical B>	Responsable serveurs	Chef de service B
<antivirus serveur>	Responsable sécurité informatique	Responsable SSI

Réseaux

Dénomination de la catégorie de moyens	Fonction responsable technique	Fonction responsable métier (si applicable)
Commutateurs cœur de réseau	Responsable réseau	Responsable informatique
Commutateurs distribution réseau	Responsable réseau	Responsable informatique
Routeur d'accès Internet	Responsable réseau	Responsable informatique
Routeurs de liaison avec bâtiment annexe	Responsable réseau	Responsable informatique
Pare-feu	Responsable sécurité informatique	Responsable SSI
Points d'accès Wifi interne	Responsable réseau	Responsable informatique
Point d'accès Wifi invité	Responsable réseau	Responsable informatique

Téléphonie et télécommunications

Dénomination de la catégorie de moyens	Fonction responsable technique	Fonction responsable métier (si applicable)
Serveur et passerelles téléphonie IP	Responsable réseau	Responsable informatique
Téléphones IP	Responsable réseau	Responsable informatique
Autocom historique (bâtiment annexe)	Responsable services généraux	Responsable informatique
Téléphones classiques	Responsable services généraux	Responsable informatique
Téléphones portables (hors smartphones)	Responsable services généraux	Responsable informatique
Liaison d'accès Internet + secours	Responsable réseau	Responsable informatique
Faisceau téléphonie	Responsable réseau	Responsable informatique
LS historique (liaison avec bâtiment annexe)	Responsable réseau	Responsable informatique

GTC-GTB (Gestion Technique Centralisée – Gestion Technique du Bâtiment)

Dénomination de la catégorie de moyens	Fonction responsable technique	Fonction responsable métier (si applicable)
Système GTC (Chauffage, climatisation, incendie)	Responsable services généraux	Responsable de la sécurité des personnes et des biens
Système d'alarme intrusion	Responsable services généraux	Responsable de la sécurité des personnes et des biens
Serveur de contrôle d'accès (portes à ouverture par badge ou par code)	Responsable services généraux	Responsable de la sécurité des personnes et des biens
Serveur de vidéo-protection	Responsable services généraux	Responsable de la sécurité des personnes et des biens

Dénomination de la catégorie de moyens	Fonction responsable technique	Fonction responsable métier (si applicable)
Caméras de vidéo-protection	Responsable services généraux	Responsable de la sécurité des personnes et des biens

Equipements utilisateurs

Composants employés par les utilisateurs du SI pour accéder aux fonctions qu'il offre. Il s'agit des terminaux (poste de travail fixe ou nomade, mobile, tablette PC etc.), périphériques locaux (imprimante, scanneur, photocopieur etc.) et logiciels qui permettent d'accéder aux fonctions et informations du SI. Ces équipements et logiciels sont directement opérés par les utilisateurs du SI et principalement localisés dans les locaux donnant accès au SI (ils sont également utilisés par le personnel informatique et potentiellement présents dans les locaux d'hébergement du SI pour permettre son exploitation).

Terminaux

Dénomination de la catégorie de moyens	Fonction responsable technique	Fonction responsable métier (si applicable)
Poste de travail fixe standard	Responsable postes de travail	Chef de service concerné
Poste de travail fixe Imagerie médicale	Responsable postes de travail	Chef de service concerné
Ordinateur portable standard	Responsable postes de travail	Chef de service concerné
Tablette	Responsable postes de travail	Chef de service concerné
Smartphone	Responsable postes de travail	Chef de service concerné
Equipement nomade d'usager ou visiteur (tout type possible)	-	-

Périphériques informatiques

Dénomination de la catégorie de moyens	Fonction responsable technique	Fonction responsable métier (si applicable)
Imprimante laser N/B	Responsable postes de travail	Chef de service concerné
Imprimante/Photocopieur laser Couleur	Responsable postes de travail	Chef de service concerné
Scanner de documents couleur	Responsable postes de travail	Chef de service concerné

Support de données amovibles

Dénomination de la catégorie de moyens	Fonction responsable technique	Fonction responsable métier (si applicable)
CD-Rom d'installation des logiciels	Selon les logiciels	Responsable informatique
Clés USB standard pour usage interne	Responsable postes de travail	Chef de service concerné

Dénomination de la catégorie de moyens	Fonction responsable technique	Fonction responsable métier (si applicable)
Clés USB sécurisées pour transport de données sensibles	Responsable sécurité informatique	Chef de service concerné
Disque dur amovible pour sauvegarde de postes spécifiques	Responsable sécurité informatique	Chef de service concerné

Logiciels des postes de travail

Dénomination de la catégorie de moyens	Fonction responsable technique	Fonction responsable métier (si applicable)
<système d'exploitation pour postes de travail>	Responsable postes de travail	Chef de service concerné
<suite bureautique>	Responsable postes de travail	Chef de service concerné
<navigateur web>	Responsable postes de travail	Chef de service concerné
<logiciel client de messagerie>	Responsable postes de travail	Chef de service concerné
<progiciel d'accès au Dossier patient informatisé>	Responsable postes de travail	DIM
<antivirus poste de travail>	Responsable postes de travail	Chef de service concerné
<logiciel de téléphonie IP sur poste de travail>	Responsable postes de travail	Chef de service concerné

Equipements biomédicaux associés au SI

Système à finalité médicale, fixe ou mobile, connecté au SI, qui permet de traiter automatiquement des données et qui intègre les organes nécessaires à son fonctionnement autonome, ses interfaces de communication et ses périphériques indispensables.

Dénomination de la catégorie de moyens	Fonction responsable technique	Fonction responsable métier (si applicable)
Système IRM	Technicien IRM	Chef de service concerné
Système radiothérapie	Technicien radiothérapie	Chef de service concerné

Téléphonie

Dénomination de la catégorie de moyens	Fonction responsable technique	Fonction responsable métier (si applicable)
Téléphones IP	Responsable réseau	Chef de service concerné
Téléphones classiques	Responsable services généraux	Chef de service concerné
Téléphones portables (hors smartphones)	Responsable services généraux	Chef de service concerné
FAX	Responsable services généraux	Chef de service concerné

Organisations

Services

Transposition de l'organisation de la structure.

Dénomination du service	Fonction responsable technique	Fonction responsable métier (si applicable)
Service d'accueil	-	Responsable administratif
Service des urgences	-	Chef du service des urgences
Direction de l'Information Médicale	-	Directeur de l'Information Médicale
Service informatique	-	Responsable informatique

Catégories de personnel

Catégories de personnel utiles à la gestion de la sécurité du SI

Dénomination de la catégorie de personnel	Fonction responsable technique	Fonction responsable métier (si applicable)
Professionnel de santé	-	
Personnel administratif	-	Responsable administratif
Personnel de soutien de l'hébergement du SI : Agents techniques assurant la maintenance, l'exploitation, l'administration technique ou de sécurité des composants informatiques du SI (administrateur informatique d'une structure, prestataire informatique, personnel d'un hébergeur etc.).	-	Responsable informatique
Personnel de soutien des moyens d'accès au SI : Agents techniques assurant la maintenance, l'exploitation, l'administration ou de sécurité des moyens d'accès au SI (prestataire informatique, professionnel de santé lui-même etc.).	-	Responsable informatique
Patients	-	-
Visiteurs	-	-

Annexe 2 : Métriques d'analyse de risques

Échelle de niveaux de vraisemblance

La vraisemblance est l'estimation de la possibilité qu'un scénario de menace ou un risque, se produise. Elle représente sa force d'occurrence.

Niveau	Libellé	Description
1	Exceptionnel	Théoriquement possible, pas de cas rencontré par ailleurs, ou réalisable dans des conditions particulières, très difficiles à obtenir, nécessitant des moyens et compétences très importants. Evènement très rare s'il s'agit d'un accident (une occurrence sur une période de plusieurs dizaines d'années).
2	Peu probable	Cas déjà rencontré une ou plusieurs fois, rarement (une occurrence sur une période d'une dizaine d'années) pour un incident d'origine involontaire, ou réalisable dans des conditions difficiles pour une malveillance, avec nécessité de personnes organisées, très compétentes et disposant de moyens importants, ou malveillance présentant peu d'intérêt pour son auteur.
3	Plausible	Cas rencontré assez fréquemment (une occurrence sur une période d'une à plusieurs années) par ailleurs, pouvant se produire avec probabilité pour un incident d'origine involontaire, ou réalisable dans des conditions occasionnelles pour une malveillance, par des personnes ou organisations dotées de moyens limités.
4	Quasi certain	Cas auquel le système est de toute façon confronté, fréquent (plusieurs fois par an), s'il s'agit d'un incident d'origine principalement involontaire ou réalisable facilement et avec un intérêt évident s'il s'agit d'une malveillance.

les conditions de la mise en œuvre de la SSI et sont très utiles pour sensibiliser les directions de structure aux efforts nécessaire à la mise en œuvre d'une démarche SSI. En particulier, le document DGOS *Introduction à la sécurité des systèmes d'information – Guide pour les directeurs d'établissement de santé* [GP SSI ES], explique l'importance d'une démarche sécurité dans une structure ainsi que les prérequis à sa mise en œuvre. Il constitue une bonne introduction et mise en perspective de ce guide.

Annexe 6 : Correspondance entre thématiques PSSI, PSSIE et ISO27002:2013

Correspondance entre thématiques PSSI et objectifs de sécurité PSSIE

Thématique PSSI	**Objectifs de sécurité PSSIE – Version 1.0** (voir [PSSIE])
T1 - Répondre aux obligations légales	Obj. 2, 4, 10, 19
T2 - Promouvoir et organiser la sécurité	Obj. 1, 2, 4, 5, 6, 10, 19, 21, 22, 23, 24, 33
T3 - Assurer la sécurité physique des équipements informatiques du SI	Obj. 9, 10, 19, 22, 23, 24, 25
T4 - Protéger les infrastructures informatiques	Obj. 2, 3, 4, 6, 4, 9, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 30, 31, 33
T5 - Maîtriser les accès aux informations	Obj. 2, 12, 16, 19, 21, 22, 23, 24, 25, 30
T6 - Acquérir des équipements, logiciels et services qui préservent la sécurité du SI	Obj. 5, 6, 7, 8, 10, 14, 19, 22, 24, 29, 30, 31
T7 - Limiter la survenue et les conséquences d'incidents de sécurité	Obj. 10, 16, 20, 21, 22, 23, 24, 25, 32, 33, 34

Ces correspondances sont détaillées :

- jusqu'au niveau des sous-thématiques de règles du canevas de PSSI dans l'Annexe 6 du « Canevas de PSSI » [MOD PSSI] ;
- jusqu'au niveau individuel des règles du canevas de PSSI et des règles de la PSSIE dans le document « Annexe au canevas de PSSI pour les structures des secteurs sanitaire et médico-social : Couverture des règles de la PSSIE par les règles du canevas de PSSI » [MOD PSSI COUV].

Correspondance entre thématiques PSSI et articles ISO 27002:2013

Thématique PSSI	**Articles NF ISO/CEI 27002 – janvier 2014 (ISO 27002:2013)**
T1 - Répondre aux obligations légales	18 - Conformité
T2 - Promouvoir et organiser la sécurité	5 - Politiques de sécurité de l'information
	6 - Organisation de la sécurité de l'information
	7 - La sécurité des ressources humaines
T3 - Assurer la sécurité physique des équipements informatiques du SI	11 - Sécurité physique et environnementale
T4 - Protéger les infrastructures informatiques	8 - Gestion des actifs
	12 - Sécurité liée à l'exploitation

Thématique PSSI	Articles NF ISO/CEI 27002 – janvier 2014 (ISO 27002:2013)
	13 - Sécurité des communications
T5 - Maîtriser les accès aux informations	9 - Contrôle d'accès
	10 - Cryptographie
T6 - Acquérir des équipements, logiciels et services qui préservent la sécurité du SI	14 - Acquisition, développement et maintenance des systèmes d'information
	15 - Relations avec les fournisseurs
T7 - Limiter la survenue et les conséquences d'incidents de sécurité	16 - Gestion des incidents liés à la sécurité de l'information
	17 - Aspects de la sécurité de l'information dans la gestion de la continuité de l'activité

Annexe 7 : Documents cités en référence

Réglementation

Renvoi	Document
[CSP]	Code de la santé publique https://www.legifrance.gouv.fr/codes/id/LEGITEXT000006072665/
[CSP-L1111-8]	Article L1111-8 du code de la santé publique, modifié par l'ordonnance n°2017-27 du 12 janvier 2017 - art. 1. https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000033862549/
[CSP-R1111-8-8]	Article R1111-8-8 du code de la santé publique, créé par le décret n°2018-137 du 26 février 2018 - art. 2 « Dispositions générales relatives à l'hébergement de données de santé à caractère personnel » https://www.legifrance.gouv.fr/codes/section_lc/LEGITEXT000006072665/LEGISCTA000036656497/
[CSP-R1111-9_11]	Articles R1111-9 à R1111-11 du code de la santé publique, modifiés par le décret n°2018-137 du 26 février 2018 - art. 2 « Hébergement des données de santé à caractère personnel sur support numérique soumis à certification » https://www.legifrance.gouv.fr/codes/section_lc/LEGITEXT000006072665/LEGISCTA000006196138/
[L78-17]	Loi n° 78-17 du 6 janvier 1978 modifiée, relative à l'informatique, aux fichiers et aux libertés, dite « loi informatique et libertés »
[PSSI-MCAS]	PSSI – MCAS : Politique de Sécurité des Systèmes d'Information pour les Ministères Chargés des Affaires Sociales https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000031386468
[PSSIE]	PSSIE - Politique de Sécurité des Systèmes d'Information de l'Etat (ANSSI). https://www.ssi.gouv.fr/administration/reglementation/protection-des-systemes-informations/la-politique-de-securite-des-systemes-dinformation-de-letat-pssie/
[RGPD]	Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 (« règlement général sur la protection des données »), relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE et Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32016R0679
[RGS]	Référentiel Général de Sécurité - Version 2.0 https://www.ssi.gouv.fr/administration/reglementation/confiance-numerique/le-referentiel-general-de-securite-rgs/

Documents techniques

Renvoi	Document
[ANSSI-MDP]	Recommandations relatives à l'authentification multifacteur et aux mots de passe - V2.0 – octobre 2021 - Guide ANSSI https://www.ssi.gouv.fr/guide/recommandations-relatives-a-lauthentification-multifacteur-et-aux-mots-de-passe/
[EBIOS 2010]	EBIOS – Méthode de gestion des risques – 25 janvier 2010 (ANSSI)
[EBIOS 2010 BDC]	EBIOS – Base de connaissances – 2010 (ANSSI)
[EBIOS RM]	EBIOS Risk Manager https://www.ssi.gouv.fr/administration/management-du-risque/la-methode-ebios-risk-manager/#
[GEXT ANSSI]	Guide « Maîtriser les risques de l'infogérance - Externalisation des systèmes d'information » (ANSSI) https://www.ssi.gouv.fr/guide/externalisation-et-securite-des-systemes-dinformation-un-guide-pour-maitriser-les-risques/
[GP SSI ES]	Introduction à la sécurité des systèmes d'information – Guide pour les directeurs d'établissement de santé (DGOS) https://solidarites-sante.gouv.fr/IMG/pdf/Guide_-_Introduction_a_la_securite_du_Systeme_d_Information_-_DGOS_-_091213.pdf
[GM AUDIT SI]	Guide méthodologique pour l'auditabilité des SI – Fiches pratiques (DGOS) https://solidarites-sante.gouv.fr/IMG/pdf/dgos_guide_auditabilite_systemes_information.pdf
[GP SSI ES]	Introduction à la sécurité des systèmes d'information – Guide pour les directeurs d'établissement de santé (DGOS) https://solidarites-sante.gouv.fr/IMG/pdf/Guide_-_Introduction_a_la_securite_du_Systeme_d_Information_-_DGOS_-_091213.pdf
[GPSSI ANSSI]	Guide d'élaboration de politiques de sécurité des systèmes d'information (ANSSI) https://www.ssi.gouv.fr/guide/pssi-guide-delaboration-de-politiques-de-securite-des-systemes-dinformation/
[HN-BAO]	Programme Hôpital numérique - Boite à outils pour l'atteinte des pré-requis - Fiches pratiques https://solidarites-sante.gouv.fr/IMG/pdf/HN_-_Boite_a_outils_pre-requis_-_Fiches_pratiques_-_Octobre_2012.pdf
[ISO27002:2013]	Norme NF ISO/IEC 27002:2013 – octobre 2013 « Technologies de l'information - Techniques de sécurité - Code de bonne pratique pour le management de la sécurité de l'information »
[ISO27005:2013]	Norme NF ISO/IEC 27005 – avril 2013 « Technologies de l'information - Techniques de sécurité - Gestion des risques liés à la sécurité de l'information » (AFNOR)
[MOD CHARTE SI]	Modèle de charte d'accès et d'usage du SI, disponible dans l'espace de publication de la PGSSI-S https://esante.gouv.fr/produits-services/pgssi-s/corpus-documentaire
[MOD CHARTE IT]	Modèle de charte sécurité pour les personnels IT, disponible dans l'espace de publication de la PGSSI-S https://esante.gouv.fr/produits-services/pgssi-s/corpus-documentaire

[MOD PAS]	Modèle de Plan d'Action SSI, disponible dans l'espace de publication de la PGSSI-S https://esante.gouv.fr/produits-services/pgssi-s/corpus-documentaire
[MOD PSSI]	Canevas de PSSI pour les structures des secteurs sanitaire, médico-social et social, disponible dans l'espace de publication de la PGSSI-S https://esante.gouv.fr/produits-services/pgssi-s/corpus-documentaire
[MOD PSSI COUV]	Annexe au canevas de PSSI pour les structures des secteurs sanitaire, médico-social et social : Couverture des règles de la PSSIE par les règles du canevas de PSSI, disponible dans l'espace de publication de la PGSSI-S https://esante.gouv.fr/produits-services/pgssi-s/corpus-documentaire
[PGSSI-S]	Politique générale de sécurité des systèmes d'information de santé https://esante.gouv.fr/produits-services/pgssi-s Corpus documentaire de la Politique générale de sécurité des systèmes d'information de santé https://esante.gouv.fr/produits-services/pgssi-s/corpus-documentaire

Annexe 8 : Glossaire

Sigle / Acronyme	Signification
ANAP	Agence Nationale d'Appui à la Performance des établissements de santé et médico-sociaux
ANS	Agence du Numérique en Santé
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
CNIL	Commission Nationale de l'Informatique et des Libertés
DGOS	Direction générale de l'offre de soins
DMP	Dossier Médical Personnel
DP	Dossier Pharmaceutique
EBIOS	Expression des Besoins et Identification des Objectifs de Sécurité
GT	Groupe de Travail
PGSSI-S	Politique Générale de Sécurité des Systèmes d'Information de Santé
Plan d'Action SSI	Plan d'Action Sécurité du Système d'Information
PS	Professionnel de Santé
PSSI	Politique de Sécurité des Systèmes d'Information
RSSI	Responsable de la Sécurité des Systèmes d'Information
SI	Système d'information
SIS	Système d'Information de Santé
SMSI	Système de Management de la Sécurité de l'Information
SSI	Sécurité des Systèmes d'Information
TCP/IP	Transmission Control Protocol / Internet Protocol
USB	Universal Serial Bus