Questions à considérer :

Question1/ Quels sont les actifs informationnels que la PSSI doit protéger ?

Actifs numériques de l'organisation comme ses logiciels, ses bases de données, son site web et ses infrastructures numériques.
Données sensibles de l'organisation, telles que les informations clients, les données financières ou encore les secrets commerciaux.

Question2/ Quels sont les systèmes et les technologies impliqués ?

Sont à prendre en compte, dans le périmètre de la SSI, les équipements de l'entité ou ceux gérés par le service informatique d'une tutelle, sur lesquels s'exécutent les fonctions essentielles comme la communication (serveur de messagerie, machines internes cibles de connexion depuis l'extérieur), la gestion financière et comptable, la modélisation (serveur de calcul), la publication (serveur web, serveur d'impression), le stockage, le traitement et l'interprétation des données (serveur de fichiers, pilotage/contrôle de manipulations). Par ailleurs, du fait de l'évolution des technologies, certains systèmes (téléphonie, visioconférence, photocopieur, vidéosurveillance), traditionnellement en dehors du champ de l'informatique, font désormais partie du périmètre.
La SSI intègre également les prestations externes telles que l'hébergement de serveurs et la sous-traitance dans leur incidence sur la sécurité interne des systèmes d'information.
Les usages liés à la mobilité (ordinateurs portables, connexions sans fil, assistants personnels, téléphones portables…) sont également à prendre en compte du fait que ces usages se pratiquent généralement en milieu non protégé.

Question3/ Quelles sont les parties prenantes concernées par cette PSSI ?

Parties prenantes (équipes techniques, responsables métiers, responsable communication…).

Employés : Les employés sont parmi les parties prenantes les plus directement concernées par la PSSI, car ils utilisent les systèmes d'information de l'organisation au quotidien. Ils doivent être sensibilisés aux bonnes pratiques de sécurité informatique et être formés pour reconnaître et éviter les menaces potentielles.

Partenaires : Les partenaires commerciaux, les sous-traitants et les autres entités avec lesquelles l'organisation travaille doivent également être pris en compte dans la PSSI. Cela peut inclure des accords contractuels spécifiques sur la sécurité des données et des systèmes d'information.

Fournisseurs : Les fournisseurs de services et de technologies informatiques, tels que les fournisseurs de cloud, les fournisseurs de logiciels, les fournisseurs de matériel, sont également des parties prenantes importantes. La PSSI peut impliquer des évaluations de sécurité des fournisseurs et la mise en place de mesures pour garantir la sécurité des produits et services fournis.

Clients : Les clients sont concernés par la PSSI car ils peuvent être affectés par les incidents de sécurité, tels que les violations de données, qui pourraient compromettre leurs informations personnelles ou financières. La confiance des clients dans la sécurité des systèmes d'information de l'organisation est essentielle pour maintenir des relations commerciales solides.

Actionnaires et investisseurs : Les actionnaires et les investisseurs ont un intérêt financier dans la sécurité des systèmes d'information de l'organisation, car les incidents de sécurité peuvent avoir un impact sur la valeur de l'entreprise et sur sa réputation sur le marché.

Autorités réglementaires et organismes de conformité : Les organismes gouvernementaux et les régulateurs peuvent également être considérés comme des parties prenantes dans la PSSI, car ils établissent souvent des exigences et des normes de sécurité que les organisations doivent respecter, notamment en matière de protection des données personnelles et de confidentialité.

Opinion publique : Enfin, l'opinion publique et le grand public peuvent être considérés comme des parties prenantes dans la mesure où les incidents de sécurité significatifs peuvent avoir un impact sur la perception de l'organisation et sur sa réputation auprès du public en général.

Question 4/ Comment les différents sites et emplacements géographiques affectent-ils le périmètre de la PSSI ?

La cartographie de l'administration du système d'informations représente le périmètre et le niveau de privilèges des administrateurs sur les ressources du parc informatique. Cela permet, en cas de compromission d'un compte d'administration, d'identifier le niveau de privilège de l'attaquant et la portion du parc potentiellement impactée.

Les différents sites et emplacements géographiques peuvent avoir un impact significatif sur le périmètre de la PSSI (Protection des Systèmes d'Information), car ils introduisent des défis uniques en termes de sécurité et de gestion des risques. Voici quelques façons dont les sites et emplacements géographiques peuvent affecter le périmètre de la PSSI :

1. **Étendue géographique** : Les organisations ayant des sites dispersés géographiquement doivent étendre leur périmètre de sécurité pour inclure tous ces sites. Cela signifie que la PSSI doit couvrir non seulement le siège social, mais également les bureaux régionaux, les succursales, les centres de données distants...
2. **Connectivité réseau** : Les sites géographiquement dispersés sont souvent connectés via des réseaux étendus, tels que des réseaux WAN (Wide Area Network) ou des réseaux VPN (Virtual Private Network). La sécurisation de ces connexions est essentielle pour éviter les intrusions et les fuites de données.
3. **Diversité des menaces** : Les sites géographiques peuvent être exposés à des menaces différentes en fonction de leur emplacement. Par exemple, les sites situés dans des zones à risque élevé de catastrophes naturelles peuvent être confrontés à des risques de perte de données dus à des événements tels que des tempêtes, des tremblements de terre...
4. **Conformité réglementaire** : Dans certaines régions, les lois et réglementations en matière de sécurité des données peuvent varier, ce qui oblige les organisations à adapter leur PSSI pour se conformer à ces exigences régionales spécifiques.
5. **Gestion des accès et des identités** : La gestion des accès et des identités peut devenir plus complexe dans le cas de sites géographiquement dispersés. Il est crucial de garantir que seules les personnes autorisées ont accès aux systèmes et aux données, quel que soit leur emplacement.
6. **Secours et reprise après sinistre** : Les sites géographiquement dispersés nécessitent des plans de secours et de reprise après sinistre spécifiques pour assurer la continuité des opérations en cas d'incident majeur, comme une panne de réseau ou une catastrophe naturelle affectant l'un des sites.
7. **Coûts opérationnels** : La gestion de la sécurité des sites dispersés géographiquement peut entraîner des coûts opérationnels supplémentaires, notamment en termes de personnel, d'infrastructure de sécurité et de maintenance.

En résumé, les sites et emplacements géographiques affectent le périmètre de la PSSI en introduisant des considérations spécifiques liées à la connectivité réseau, à la diversité des menaces, à la conformité réglementaire, à la gestion des accès et des identités, à la reprise après sinistre et aux coûts opérationnels. La PSSI doit donc être conçue de manière à tenir compte de ces facteurs et à assurer une protection efficace des systèmes d'information dans un contexte géographiquement distribué.

Question5/ Quels processus d'affaires doivent être inclus dans le périmètre de la PSSI ?

La PSSI doit englober tous les processus d'affaires critiques de l'organisation, de la conception des produits et services à la gestion des ventes, du support client à la gestion des ressources humaines, de la finance à la chaîne logistique, en passant par la conformité et la gouvernance. La protection de ces processus d'affaires est essentielle pour assurer la sécurité et la continuité des opérations de l'entreprise.

Question 6/ Comment la conformité réglementaire (GDPR, CCPA, etc.) influence-t-elle le périmètre de la PSSI ?

La conformité réglementaire, telle que le GDPR, le CCPA et d'autres lois similaires, étend le périmètre de la PSSI en imposant des exigences spécifiques en matière de sécurité des données personnelles, de gestion des consentements, de droits des individus sur leurs données, de notification des violations de données et de transferts internationaux de données. Les organisations doivent prendre en compte ces exigences lors de la conception et de la mise en œuvre de leur PSSI pour garantir une conformité totale et éviter les sanctions potentielles en cas de non-respect.

Activités :

1/ Identification des actifs

	Disponibilité	Intégrité	Confidentialité
Données sensibles ou confidentielles	X	XXX	XXX
Logiciels et applications	XXX	X	XX
Infrastructure physique	XX	XX	XXX
Identités et accès	X	XX	XXX
Ressources financières	X	XXX	XXX
Propriété intellectuelles	X	XX	X
Documentation interne	X	XX	XXX
Communication	X	X	X

2/ Cartographie des systèmes et technologies

- Réseau : Connexions VPN sécurisées, pare-feu.
- Infrastructure Cloud : AWS pour l'hébergement de services, stockage de données.
- Applications : CRM pour la gestion des relations clients, systèmes de gestion de projet, et plateformes de développement logiciel.
- Prévention des pertes de données (DLP): Les systèmes de prévention des pertes de données surveillent les postes de travail, les serveurs et les réseaux afin de veiller à ce que les données sensibles ne soient pas effacées, supprimées, déplacées ou copiées. Elles surveillent également qui utilise et transmet des données, en vue de repérer les utilisations non autorisées.
- Systèmes de détection et de prévention des intrusions (IDS/IPS): Les systèmes de détection des intrusions (IDS) et de prévention des intrusions (IPS) effectuent une inspection des paquets sur le trafic réseau et enregistrent les activités potentiellement malveillantes. Un IDS peut être configuré pour évaluer les journaux d'événements du système, examiner les activités réseau suspectes et émettre des alertes sur les sessions qui semblent violer les paramètres de sécurité. Un IPS offre des capacités de détection et peut mettre fin à des sessions jugées malveillantes. Il y a presque toujours une étape analytique entre l'alerte et l'action – les administrateurs sécurité évaluent si l'alerte est une menace, si cette menace les concerne et s'ils peuvent faire quelque chose pour y remédier. Les IPS et IDS sont utiles en matière de protection des données car ils peuvent empêcher les pirates de pénétrer dans vos serveurs de fichiers à l'aide d'exploits et de logiciels malveillants. Toutefois, ces solutions nécessitent un bon réglage et une analyse approfondie avant de prendre une décision de fermeture de session sur une alerte entrante.
- Gestion des informations et des événements de sécurité (SIEM): Les solutions de gestion des informations et des événements de sécurité (SIEM) fournissent une analyse en temps réel des journaux de sécurité qui sont enregistrés par les équipements réseau, les serveurs et les applications logicielles. Les SIEM agrègent et mettent en corrélation les événements entrants, elles peuvent également effectuer une déduplication des événements: supprimer des rapports multiples sur une même instance et agir ensuite en fonction de critères d'alerte et de déclenchement. En général, elles fournissent également une panoplie d'outils d'analyse qui vous permettent de ne trouver que les événements qui vous intéressent, par exemple les événements liés à la sécurité des données. Les solutions SIEM sont essentielles pour les enquêtes relatives à la sécurité des données.
- Bases de données : Serveurs de bases de données SQL, et NoSQL pour le big data, pour stocker les données clients et opérationnelles.

- Systèmes de sauvegarde : Solutions de sauvegarde en ligne et hors ligne pour la récupération des données en cas de sinistre.
- Endpoints : Ordinateurs portables des employés, smartphones et tablettes équipés de solutions de gestion des appareils mobiles.

Question 3/ Analyse des parties prenantes

PARTIE PRENANTE	EXTERNE	INTERNE	RÔLES
EMPLOYÉS		X	Collaborer et applications de la sécurité
PARTENAIRES	X		Sécuriser les données Confidentialité des données
FOURNISSEURS	X		Sécuriser l'infrastructure, Mettre à jour les équipements
CLIENTS	X		Formation aux applications
AUTORITÉ RÉGULATRICE	X		Auditer, vérifier, informer et certifier

- Employés : Personnel de développement, marketing, vente, support client, et gestion administrative. Les employés ont pour tâche de collaborer pour une cybersécurité renforcée en entreprise.
- Partenaires : Autres entreprises technologiques, fournisseurs de services cloud, agences de marketing.
- Les prestataires de services de sécurité : pour une sécurité renforcée
- Les entreprises de conseil en sécurité sont des partenaires pour les entreprises, agissant souvent comme un œil externe objectif. Elles disposent d'une expertise spécialisée pour évaluer, orienter et recommander les meilleures stratégies de cybersécurité à adopter.
- Les fournisseurs de solutions de sécurité proposent une large panoplie d'outils pour renforcer la sécurité numérique. Ils offrent une gamme de produits et services, allant des antivirus et pare-feux à des solutions de sécurité avancées comme les systèmes de protection des données et de défense contre les intrusions.
- Les entreprises de réponse à incidents possèdent une expertise spécifique en matière de gestion de crises liées à la sécurité numérique. Elles interviennent lorsqu'une violation de données se produit, pour contenir l'incident, minimiser l'impact et restaurer les services.
- Les services de gestion des identités et des accès jouent un rôle clé dans la prévention des accès non autorisés aux ressources de l'entreprise. Ils assurent que seules les personnes appropriées ont accès aux ressources numériques.
- Fournisseurs : Fournisseurs d'accès Internet, de matériel informatique, et de logiciels: leur rôle est de fournir une ***Disponibilité*** d'accès à internet.
- Clients : Entreprises utilisant les applications de notre entreprise DataSecureTech pour sécuriser leurs propres données.
- Autorités régulatrices : Organismes de conformité qui régulent la protection des données personnelles.
- Les organismes de réglementation et de conformité sont les gardiens des normes de sécurité. Les organismes de réglementation et de conformité :Rôle de surveillance de la conformité aux normes. Les organismes de réglementation et de conformité assurent la protection des données sensibles à un niveau macroscopique. Ils établissent des directives et normes de sécurité que les entreprises sont tenues de suivre. Ces normes visent à garantir la sécurité, l'intégrité et la disponibilité des données. Ces organismes sont également chargés de surveiller la conformité aux réglementations en vigueur. Par le biais d'inspections et d'audits, ils vérifient que les entreprises respectent les lois et règles. Ils ont le pouvoir de

sanctionner les entreprises en cas de non-conformité. Le rôle de ces organismes est de veiller à ce que les entreprises prennent la sécurité informatique au sérieux.

4/ Évaluation des exigences de conformité

La norme ISO 27001:2022 fournit des lignes directrices complètes sur la manière dont la gestion des risques peut être mise en œuvre dans le contexte de la sécurité de l'information.
La norme 27002 reprend les différents point traités dans les questions précédentes notamment le chapitre no°6 de la norme: organisation de la sécurité de l'information:

- Répartition des rôles et responsabilités: une mesure conseille de répartir clairement les rôles et responsabilités en matière de sécurité. Il est également possible d'identifier les responsables pour les principaux actifs. Les parties prenantes auront un rôle déterminés pour assurer la sécurité su SI.
- Séparation des tâches: la norme recommande la séparation des tâches dans le but de prévenir les risques de fraude et/ou de modifications illicites. Cette recommandation est utile dans le domaine financier, et s'appliquera au processus de DataSecureTech relevant de ce domaine.
- Relations avec les groupes de travail spécialisés: Permet de coordonner les différentes parties prenantes et services de l'entreprise DataSecureTech, cela permet d'échanger les expériences et d'améliorer le niveau général de sécurité.
- Mobilité et télétravail: cette mesure aborde les questions de la mobilité malgré son aspect technique. Cette mesure a pris de l'importance avec le développement des parcs mobiles (smartphones, tablettes), ce point relève des Endpoints vu au chapitre précédent dans la cartographie du SI, notamment des portables des employés.

Le chapitre n°7 de L'ISO 27002 traite de la sécurité liée au ressources humaines. Ce chapitre concerne dans le processus de DataSecureTech la gestion administrative.
Il existe un certain nombre de mesures de sécurité à prendre auprès du personnel avant son embauche, pendant sa présence dans l'organisme, puis à son départ:

- Avant l'embauche: il est souhaitable de préciser des critères de sélection avant l'embauche en matière de compétences en sécurité nécessaire pour chaque poste. La norme conseille, de plus, de formaliser dans les contrats de travail les engagements du futur salarié en matière de sécurité.
- Pendant la durée du contrat: la direction doit faire en sorte que tout le monde adopte un comportement adéquat par rapport à la sécurité de l'information notamment par la publication d'une charte destinée aux utilisateurs, partie prenante indispensable au SI.
- Au départ du personnel: la norme conseille de clarifier autant que possible les règles de sécurité qui seront applicables au salarié, même quand il aura quitté l'entreprise en matière de ***Confidentialité***.
- S'appuyer sur une norme permet de mieux faire passer les messages de sensibilisation, notamment auprès des populations techniques

Le chapitre n°8 porte sur la gestion des actifs donc sur ce que l'on a vu dans l'activité 1, soit notamment sur les actifs informationnels qui nécessitent protection. Il aborde les actifs d'information au sens large du terme comme les supports physiques.

- Responsabilités relatives aux actifs: la norme recommande de dresser un inventaire des actifs d'information. Elle conseille ensuite de préciser, pour chaque actif, quelle est son utilisation. (vu à la partie 1).
- Classification de l'information: cette partie recommande de classifier l'information. Cela met en évidence les actifs les plus sensibles, dans le but de mieux les protéger.
- Manipulation des supports: cette mesure rappelle qu'il est prudent de bien penser les procédures de manipulation des supports amovibles. La norme rappelle qu'il convient de

prévoir une procédure de destruction ou d'effacement des données lorsque les supports amovibles sont en fin de vie afin d'assurer la ***Confidentialité***.

Le chapitre n°9 concerne le Contrôle d'accès.
L'objectif de cette catégorie est de contrôler l'accès aux informations des installations de traitement, d'information et des processus commerciaux. Dans le processus de l'entreprise DataSecureTech il concerne le processus Ventes de l'entreprise. Celui-ci doit réguler comment les fournisseurs et clients doivent accéder aux informations et lesquelles.

Le chapitre n°11 concernant la sécurité physique et environnementale, se rapporte notamment à la partie cartographie du SI. Ce chapitre traite des mesures physiques qui doivent être mise en place selon la géographie des lieux dont dépend les activités de DataSecureTech.

- Mesure de sécurité des salles machines et des autres locaux de l'organisme:
    - Les salles machines doivent être conçues dans les règles de l'art
    - Contrôle d'accès physique doit interdire l'accès à toute personne non habilitée
    - Protections contre les désastres naturels, contre les attaques malveillantes ainsi que contre les accidents
- Sécurité des équipements:
    - Les services généraux doivent être exploités conformément aux spécifications du fabricant. Le câblage réseau doit être posé de telle sorte qu'il soit difficile d'intercepter les flux
    - Le matériel doit être maintenu régulièrement afin de prévenir des pannes, pour garantir la ***Disponibilité*** et de prévoir des procédures appropriées en vue de la mise au rebut, en fin de vie
    - Les équipements laissés sans surveillance doivent être protégés et les postes de travail doivent être automatiquement verrouillés

Le chapitre n°13 traitant de la sécurité des communications traite des mesures relatives à la sécurité des réseaux, concerne l'actif informationnel: Communication et également la partie réseaux dans la cartographie du SI. (vu en partie 1 et 2)

- De là dépend la sécurité des services: Cette mesure recommande de spécifier avec l'entité qui fournit le service réseau les propriétés du service rendu. Cela concerne entre autres la capacité des réseaux, leur dispositif de continuité de service (***Disponibilité***), mais également les services supplémentaires comme le filtrage, le chiffrement(***Confidentialité***)…
- Cloisonnement des réseaux: Le cloisonnement des différents domaines de réseau est recommandé (poste de travail, serveurs, DMZ…)
- Transferts d'information: Il est recommandé de prendre des dispositions techniques et organisationnelles pour sécuriser les échanges d'information. Une des mesures recommande au personnel de ne pas tenir de conversations *confidentielles* dans les lieux publics. Une autre mesure évoque les précautions à prendre dans la messagerie électronique
- Engagement de ***Confidentialité***: Il est conseillé de disposer d'engagement de confidentialité

Le chapitre n°15 traite des relations avec les fournisseurs, il concerne donc la partie prenante «fournisseurs».

- Relations avec les fournisseurs: Il est conseillé de rédiger une politique de sécurité destinée aux fournisseurs, d'insérer des articles relatifs à la sécurité des SI dans les contrats pour que les fournisseurs s'engagent dans le domaine de la sécurité
- Gestion de la prestation de service: Le fournisseur doit être en mesure d'apporter la preuve qu'il respecte ses engagements en matière de sécurité

5/ Définition des processus critiques

Il faut pour cela s’appuyer sur le chapitre n°17: Aspects de la sécurité de l’information dans la gestion de la continuité de l’activité.
Les processus critiques doivent être pris en compte pour le PCA afin d’identifier et formaliser les besoins de continuité, gérer les risques prioritaires, et ainsi définir la stratégie de continuité.
Il est recommandé de réaliser un plan de continuité (PCA) ou de reprise (PRA), qui doit être testé et mis à jour.

Les processus critiques sont souvent communs à plusieurs activités de DataSecureTechet, ils sont associés au système d’information, la cartographie des systèmes d’informations aide à les identifier (Partie 2 cartographie des SI). Les flux concernent les échanges en entrée ou sortie des systèmes d’information.

Les processus critiques sont ceux qui sont essentiels pour le maintien de l’activité. Ce travail d’identification doit être réalisé à partir d’entretiens avec les responsables des métiers et des processus. L’analyse des processus doit comprendre l’identification des interfaces (prestataires etc...). La cartographie des processus critiques doit être validée par la direction.
Il est recommandé de cartographier les processus de l’organisation. Il est recommandé de cartographier les flux entre les systèmes d’information supportant les différents processus de l’organisation ; cette cartographie est nécessaire pour la détermination des impacts qui devront être traités par le plan de continuité informatique. Elle se décline assez naturellement à partir de la cartographie des processus.