Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Premier ministre

Agence nationale de la sécurité des systèmes d'information

Prestataires d'administration et de maintenance sécurisées

Référentiel d'exigences

Version 1.1 du 6 octobre 2022

HISTORIQUE DES VERSIONS			
DATE	**VERSION**	**ÉVOLUTION DU DOCUMENT**	**RÉDACTEUR**
30/09/2019	0.9	*Version publiée pour appel public à commentaires*	ANSSI
10/04/2020	1.0	*Version publiée pour la phase expérimentale*	ANSSI
06/10/2022	1.1	*Première version applicable*	ANSSI

Les commentaires sur le présent document sont à adresser à :

Agence nationale de la sécurité des systèmes d'information

SGDSN/ANSSI

51 boulevard de La Tour-Maubourg
75700 Paris 07 SP

qualification@ssi.gouv.fr

SOMMAIRE

I. Introduction

I.1. Présentation générale

I.1.1. Contexte

Les administrateurs et mainteneurs constituent un rouage essentiel de tout système d'information (SI), ayant non seulement vocation à assurer son bon fonctionnement, mais également à concourir à son maintien en condition de sécurité.

Selon les prérogatives qui lui sont accordées, un administrateur concentre ainsi des privilèges élevés sur son périmètre lui donnant notamment les capacités techniques d'accès aux informations métier de l'entité responsable du système d'information. Ceux-ci s'accompagnent nécessairement d'une responsabilité accrue, compte tenu des impacts considérables que peut avoir une utilisation indue de ces droits étendus. Par conséquent, le rôle d'administrateur requiert aussi bien des compétences techniques élevées qu'une faculté à conduire ses activités au sein d'un cadre clairement défini et sécurisé.

Si les administrateurs internes, c'est-à-dire employés par l'entité considérée, sont bien entendu concernés par ce constat, celui-ci est tout aussi valable dans le cadre de prestations d'administration externalisées. Ainsi, un prestataire d'administration et de maintenance sécurisées doit proposer à ses commanditaires un service à l'état de l'art, permettant aussi bien d'offrir des garanties face au risque de malveillance interne, que de se prémunir d'un scénario d'attaque pouvant conduire à la compromission du système d'information administré à travers les moyens d'administration qu'il met en œuvre.

Dès lors, l'instauration de cette indispensable relation de confiance entre un commanditaire et son prestataire passe notamment par le respect d'un cadre en matière de sécurité, permettant de couvrir les multiples cas d'usage envisageables pour l'administration et la maintenance d'un système d'information.

I.1.2. Objet du document

Ce document constitue le référentiel d'exigences applicables à un prestataire d'administration et de maintenance sécurisées (PAMS), ci-après dénommé « le prestataire ». Le prestataire délivre un service d'administration et de maintenance sécurisées. Dans le présent document, est entendu par « le service » l'ensemble des moyens techniques, organisationnels et humains mis en œuvre afin d'effectuer une prestation d'administration et maintenance sécurisées.

Il a vocation à permettre la qualification de cette famille de prestataires selon les modalités décrites au chapitre III.

Il permet à l'entité faisant appel à la prestation, ci-après dénommée « commanditaire » de disposer de garanties sur la capacité du prestataire à assurer un niveau de sécurité suffisant aux prestations d'administration et de maintenance réalisées.

Les exigences du référentiel permettent d'apporter une réponse aux besoins exprimés dans plusieurs réglementations telles que la loi n° 2018-133 du 26 février 2018 portant diverses dispositions d'adaptation au droit de l'Union européenne dans le domaine de la sécurité (issue de la transposition de la directive *Sécurité des réseaux et des systèmes d'information* dite « directive NIS »), les articles L. 1332-6-1 et suivants du code de la défense et la politique de sécurité des systèmes d'information de l'État [PSSIE]. Ainsi, recourir à un prestataire qualifié PAMS permet à un commanditaire de respecter une partie des exigences que ces réglementations imposent. Il peut également être utilisé, à titre de bonnes pratiques, en dehors de tout contexte réglementaire.

Il n'exclut ni l'application de la législation et de la réglementation nationale notamment en matière de protection des informations sensibles [II_901] et de protection du secret de la défense nationale [IGI_1300], ni l'application des règles générales imposées aux prestataires en leur qualité de professionnels et notamment leur devoir de conseil vis-à-vis de leurs commanditaires.

Les exigences du présent référentiel portent sur la sécurité de l'ensemble des systèmes d'information d'administration (interfaces d'administration incluses), quel que soit le système d'information administré (systèmes d'information bureautiques, systèmes d'information industriels, etc.). Par ailleurs, toute action nécessitant une interaction avec le système d'information administré depuis le système d'information d'administration grâce à l'utilisation de privilèges élevés est également couverte par le référentiel.
Le référentiel vise enfin à traiter les risques associés aux activités d'administration et de maintenance d'un système d'information conduites par le prestataire :

- compromission du système d'information d'administration par un attaquant externe ;
- compromission du système d'information administré, par un attaquant externe, par rebond sur le système d'information d'administration ;
- compromission du système d'information administré, par un attaquant externe, par rebond sur le système d'information administré appartenant à un autre commanditaire ;
- utilisation par un administrateur malveillant de ses privilèges.

I.1.3. Structure du présent document

Le chapitre I correspond à l'introduction du présent référentiel.

Le chapitre II décrit les activités visées par le présent référentiel.

Le chapitre III présente les modalités de la qualification, qui atteste de la conformité des prestataires d'administration et de maintenance aux exigences qui leur sont applicables.

Le chapitre IV présente les exigences que les prestataires qualifiés doivent respecter.

L'Annexe 1 présente les références des textes législatifs, réglementaires, normatifs et autres mentionnés dans le présent référentiel.

L'Annexe 2 présente les recommandations aux commanditaires de prestations d'administration et de maintenance sécurisées.

L'Annexe 3 présente les schémas illustratifs d'une architecture conforme au référentiel.

L'Annexe 4 présente une synthèse des exigences relatives aux zones d'interconnexion.

I.2. Identification du document

Le présent référentiel est dénommé « Prestataires d'administration et de maintenance sécurisées – Référentiel d'exigences ». Il peut être identifié par son nom, numéro de version et sa date de mise à jour.

I.3. Définitions et acronymes

I.3.1. Acronymes

Les acronymes utilisés dans le présent référentiel sont :

ANSSI	Agence nationale de la sécurité des systèmes d'information
PAMS	Prestataire d'administration et de maintenance sécurisées
PASSI	Prestataire d'audit de la sécurité des systèmes d'information
PDIS	Prestataire de détection des incidents de sécurité
PRIS	Prestataire de réponse aux incidents de sécurité

I.3.2. Définitions

Les définitions ci-dessous s'appuient sur les normes de la suite [ISO27000] ainsi que sur le guide de l'ANSSI relatif à l'administration sécurisée des systèmes d'information [G_ADMIN].

Action d'administration – installation, suppression, modification ou consultation d'une configuration d'un composant du système d'information, susceptibles de modifier le fonctionnement ou la sécurité de celui-ci.

Action de maintenance – réglage, vérification ou réparation des composants matériels ou logiciels du système d'information.

Actions de support – sous-ensemble des actions d'administration ne nécessitant pas les plus hauts niveaux de privilège et ne donnant pas accès, même indirectement, aux données du commanditaire.

Administrateur – personne physique disposant de droits privilégiés sur un système d'information, chargée des actions d'administration ou de maintenance sur celui-ci, responsable d'un ou plusieurs domaines techniques.

Administrateur du système d'information du service – se réfère à tout administrateur employé du prestataire administrant le ou les systèmes d'information permettant d'assurer le service pour le compte de ses commanditaires.

Administrateur PAMS – également mainteneur PAMS dans le cadre de ce référentiel, se réfère à tout administrateur employé du prestataire ou par le commanditaire (sous contrat direct dudit commanditaire ou via une prestation de mise à disposition de personnels) administrant le système d'information du commanditaire dans le cadre de la délivrance du service.

Administrateur tiers – se réfère à tout administrateur sous-traitant du prestataire ou du commanditaire intervenant sur le système d'information du commanditaire, hors administrateur PAMS.

Administration à distance – désigne l'administration d'un système d'information en dehors d'un périmètre de protection physique sous maîtrise directe ou indirecte, du prestataire ou du commanditaire. Ceci inclut l'administration en situation de nomadisme.

Administration sécurisée – ensemble des actions d'administration menées à l'état de l'art de la sécurité numérique.

Authentifiants d'administration – combinaison d'un identifiant et d'un ou plusieurs facteurs d'authentification (information connue, possédée, qui peut être montrée ou réalisée par l'administrateur) associés à un compte d'administration.

***Cloud computing* (informatique en nuage)** – modèle permettant un accès aisé, généralement à la demande, et au travers d'un réseau, à un ensemble de ressources informatiques partagées et configurables.

***Cloud* privé** – offre spécifique de *cloud computing* reposant sur des infrastructures dédiées à une entité et dont les outils d'administration peuvent ne pas être exposés sur Internet.

***Cloud* public –** offre générique de *cloud computing* reposant sur la mutualisation par défaut de l'infrastructure (capacité d'exécution, mémoire vive, stockage, etc.) au profit de différents clients et dont les outils d'administration sont exposés exclusivement sur Internet.

Commanditaire – entité faisant appel au service d'administration et de maintenance sécurisées.

Compte d'administration – compte disposant de privilèges nécessaires aux actions d'administration. Il peut être générique, individuel ou de service.

Compte de service – compte rattaché à un processus automatique (un programme, une application, un service, un script, etc.).

Connexion à distance – depuis un poste de travail, la connexion à distance consiste à se connecter sur un autre environnement (physique ou virtuel) afin d'y ouvrir une session graphique (au travers de protocoles tels que *Remote Desktop Protocol* ou *Independent Computing Architecture*) ou console (au travers de protocoles tels que *Secure Shell* ou des outils tels que PowerShell).

Console de programmation – terminal matériel, fixe ou portable, contenant les outils permettant de programmer, de configurer et de réaliser des actions d'administration ou de maintenance sur un automate industriel.

Convention de service – accord écrit entre un commanditaire et un prestataire pour la réalisation de la prestation. Dans le cas où le prestataire est un organisme privé, la convention de service inclut le contrat.

DNS – Système de résolution de nom.

DHCP – Protocole réseau configurant notamment les paramètres IP d'une machine.

État de l'art – ensemble publiquement accessible des bonnes pratiques, des technologies et des documents de référence relatifs à la sécurité des systèmes d'information, et des informations qui en découlent. Ces documents peuvent être mis en ligne sur Internet par la communauté de la sécurité des systèmes d'information, diffusés par des organismes de référence ou encore être d'origine réglementaire.

Flux d'administration – flux de communication, direct ou indirect vers une ressource administrée, pour la réalisation d'une action d'administration.

Hyperviseur – logiciel de virtualisation permettant d'exécuter un ou plusieurs systèmes d'exploitation dits « invités » ou « machines virtuelles » au sein d'un même système d'exploitation dit « hôte ». Dans ce cas, on parle généralement d'hyperviseur de type 2.

Infrastructures d'administration – serveurs d'infrastructure utiles au bon fonctionnement du système d'information d'administration (ex : ordonnanceurs, gestionnaire de certificats numériques, annuaires, etc.).

Interface d'administration – point d'entrée réseau, logique ou physique, sur la ressource administrée.

Maintenance sécurisée – ensemble des actions de maintenance menées à l'état de l'art de la sécurité numérique.

Mainteneur PAMS – cf. « Administrateur PAMS ».

Mainteneur tiers – cf. « Administrateur tiers ».

Nomadisme – Utilisation d'un poste d'administration ou de maintenance par un administrateur PAMS ou administrateur du système d'information du service depuis un lieu en dehors du réseau qualifié du prestataire.

Outils d'administration – outils techniques (consoles, utilitaires, etc.) utilisés pour accéder aux ressources administrées au travers des interfaces d'administration afin d'effectuer les actions d'administration.

Poste d'administration – terminal matériel, fixe ou portable, utilisé pour les actions d'administration.

Poste de maintenance – terminal matériel, fixe ou portable, utilisé pour les actions de maintenance.

Prestataire – entité proposant une offre de service d'administration et de maintenance conforme au référentiel.

Prestation qualifiée – service d'administration et de maintenance sécurisées conforme au référentiel, fourni à un commanditaire par un prestataire qualifié.

Rebond (serveur ou poste) – serveur ou poste permettant, après connexion, d'accéder directement ou indirectement à une ressource afin de l'administrer.

Réseau d'administration – réseau de communication faisant transiter les flux internes au système d'information d'administration et les flux d'administration.

Ressources administrées – ensemble des dispositifs physiques ou virtuels du système d'information administré qui nécessitent des actions d'administration.

Ressources d'administration – ensemble des dispositifs physiques ou virtuels du système d'information d'administration : postes d'administration, postes de maintenance, consoles de programmation, serveurs d'infrastructures d'administration, serveurs outils d'administration, équipements du réseau d'administration, etc.

Sous-traitance – opération par laquelle le prestataire confie sous sa responsabilité à une entité tout ou partie de l'exécution d'un contrat conclu avec le commanditaire.

Système d'information (SI) – ensemble organisé de ressources (matériel, logiciels, personnel, données et procédures) permettant de traiter, de stocker et de diffuser de l'information.

Système d'information administré – système d'information incluant les ressources administrées.

Système d'information d'administration – système d'information utilisé pour administrer des ressources qui sont présentes dans un autre système d'information dit système d'information administré.

Système d'information du service – système d'information permettant la délivrance du service et incluant son propre système d'information d'administration accessible à des administrateurs spécifiques (cf. « Administrateur du système d'information du service »).

Système de détection des incidents de sécurité – Dispositif technique destiné à repérer des activités anormales, suspectes ou malveillantes sur le périmètre supervisé.

Tiers – qualifie une personne ou une entité qui n'est ni le prestataire ni le commanditaire (ou leurs employés).

Utilisateur – personne physique disposant de droits non privilégiés sur un système d'information.

Zone de confiance – ensemble des ressources informatiques regroupées en fonction de l'homogénéité de facteurs divers, liés ou non à la sécurité (ex : exposition aux menaces, vulnérabilités résiduelles technologiques intrinsèques, localisation géographique, etc.).

II. Description générale des services d'administration et de maintenance sécurisées

II.1. Activités des services d'administration et de maintenance sécurisées

Le service d'administration est constitué de toutes les actions d'installation, de suppression, de modification et de consultation d'un système faisant partie du système d'information, et susceptible de modifier son fonctionnement ou sa sécurité. L'administration peut notamment comprendre :

- l'installation ou la désinstallation de composants ;
- la modification de la configuration ou du paramétrage ;
- la mise à jour des systèmes ou des composants ;
- la gestion de sauvegardes et des restaurations ;
- la gestion des droits d'accès des utilisateurs ;
- l'attribution de ressources informatiques.

Le service de maintenance comprend l'ensemble des activités réalisées afin de maintenir (maintenance préventive – voire prédictive – et maintenance corrective) ou de rétablir (maintenance curative) un système d'information afin que celui-ci délivre un service en adéquation avec les besoins exprimés par le commanditaire. La maintenance comprend notamment :

- le maintien en condition opérationnelle (MCO) ;
- le maintien en condition de sécurité (MCS) ;
- l'évolution du système d'information.

La tierce maintenance applicative (TMA) est un cas particulier de MCO/MCS.

Les activités de maintenance, contrairement aux activités d'administration, comprennent les actions physiques réalisées directement sur les systèmes administrés tels que le remplacement de matériels défectueux, dépoussiérage d'équipements, ajout de mémoire, etc.

Pour faciliter la lecture du référentiel, sauf mention explicite, les exigences portant sur le service d'administration sont applicables au service de maintenance.

II.2. Cas d'usage et architectures du système d'information dans le cadre d'un service d'administration et de maintenance

Le présent document s'attache à couvrir plusieurs implémentations possibles d'un système d'information associé à des activités d'administration et de maintenance. La prestation pourra s'appuyer sur n'importe lequel des cas d'usage décrits dans ce référentiel, tant que les exigences de ce dernier sont respectées.

La *Figure 1* est une représentation fonctionnelle type d'un service d'administration et de maintenance, donnée uniquement à titre d'illustration.

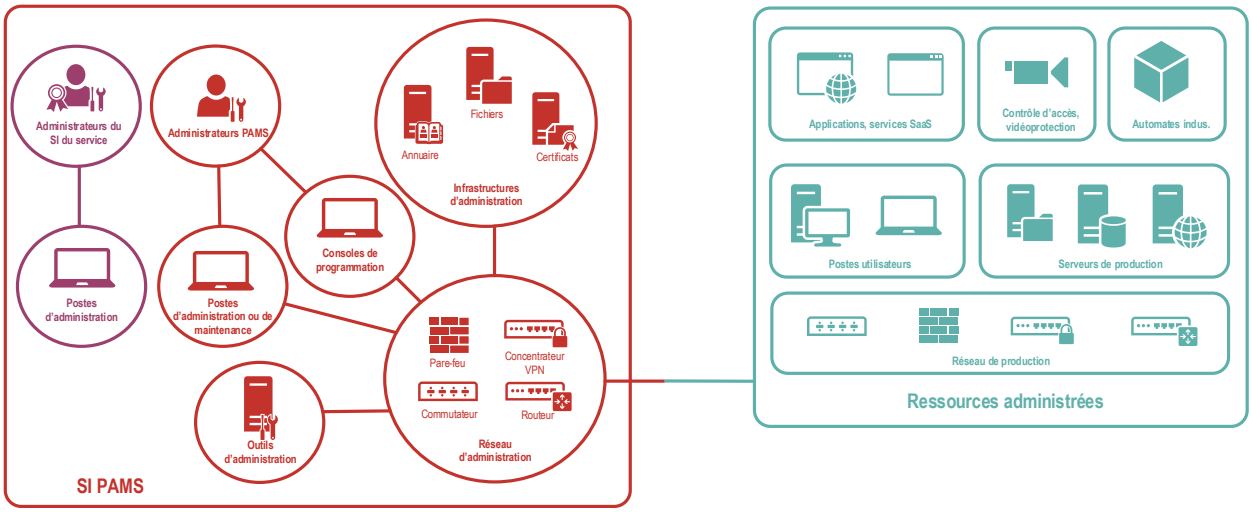


Figure 1 : Représentation fonctionnelle type d'un service d'administration et de maintenance sécurisées

Cette représentation décrit deux zones principales, cloisonnées l'une de l'autre :

- le système d'information du service (ou système d'information PAMS), intégrant l'ensemble des ressources nécessaires à l'administration du système d'information administré :
  - les administrateurs PAMS ;
  - les administrateurs du système d'information du service lui-même ;
  - les postes d'administration ou de maintenance ;
  - les consoles de programmation ;
  - les serveurs outils d'administration : serveurs hébergeant les outils d'administration ;
  - les infrastructures d'administration ;
  - le réseau d'administration.
- les ressources administrées, qui comprennent tous les dispositifs virtuels ou physiques (postes de travail, serveurs de production, composants réseaux, automates, applications, etc.) du système d'information administré (ex : système d'information bureautique ou système d'information industriel) nécessitant des actions d'administration, indépendamment de leur localisation.

Une prestation d'administration et de maintenance peut être caractérisée par les points suivants, pouvant éventuellement être combinés selon le contexte :

- l'administration du système d'information administré peut être réalisée depuis :
  - les locaux du prestataire ;
  - les locaux du commanditaire ;
  - les locaux d'un hébergeur tiers ;
  - en situation de nomadisme.
- les actions d'administration peuvent être menées par :
  - le prestataire ;
  - le commanditaire ;
  - un tiers, sous-traitant du commanditaire ou du prestataire.
- le système d'information administré peut être :
  - hébergé par le commanditaire ou un hébergeur tiers ;
  - administrable à distance ou non administrable à distance, nécessitant des interventions sur site.

Toutes les combinaisons peuvent être regroupées dans deux appellations, détaillées dans les sections suivantes :

- service externe d'administration ;
- service interne d'administration.

Un même prestataire peut réaliser des prestations qualifiées auprès de commanditaires distincts. Les conditions de mutualisation et de cloisonnement des ressources du prestataire entre prestations qualifiées et auprès de commanditaires distincts sont détaillées dans le présent référentiel.

II.2.1. Service externe d'administration

Le prestataire réalise les actions d'administration sur les ressources du commanditaire dans des conditions conformes au présent référentiel.

Il peut être amené à intervenir sur des ressources également administrées par le commanditaire ou un administrateur tiers.

Les ressources administrées peuvent se situer dans les locaux du commanditaire, dans les locaux du prestataire ou dans les locaux d'un hébergeur tiers (y compris des services d'informatique en nuage dit *cloud computing*).

Les actions d'administration sont réalisables en situation de nomadisme.

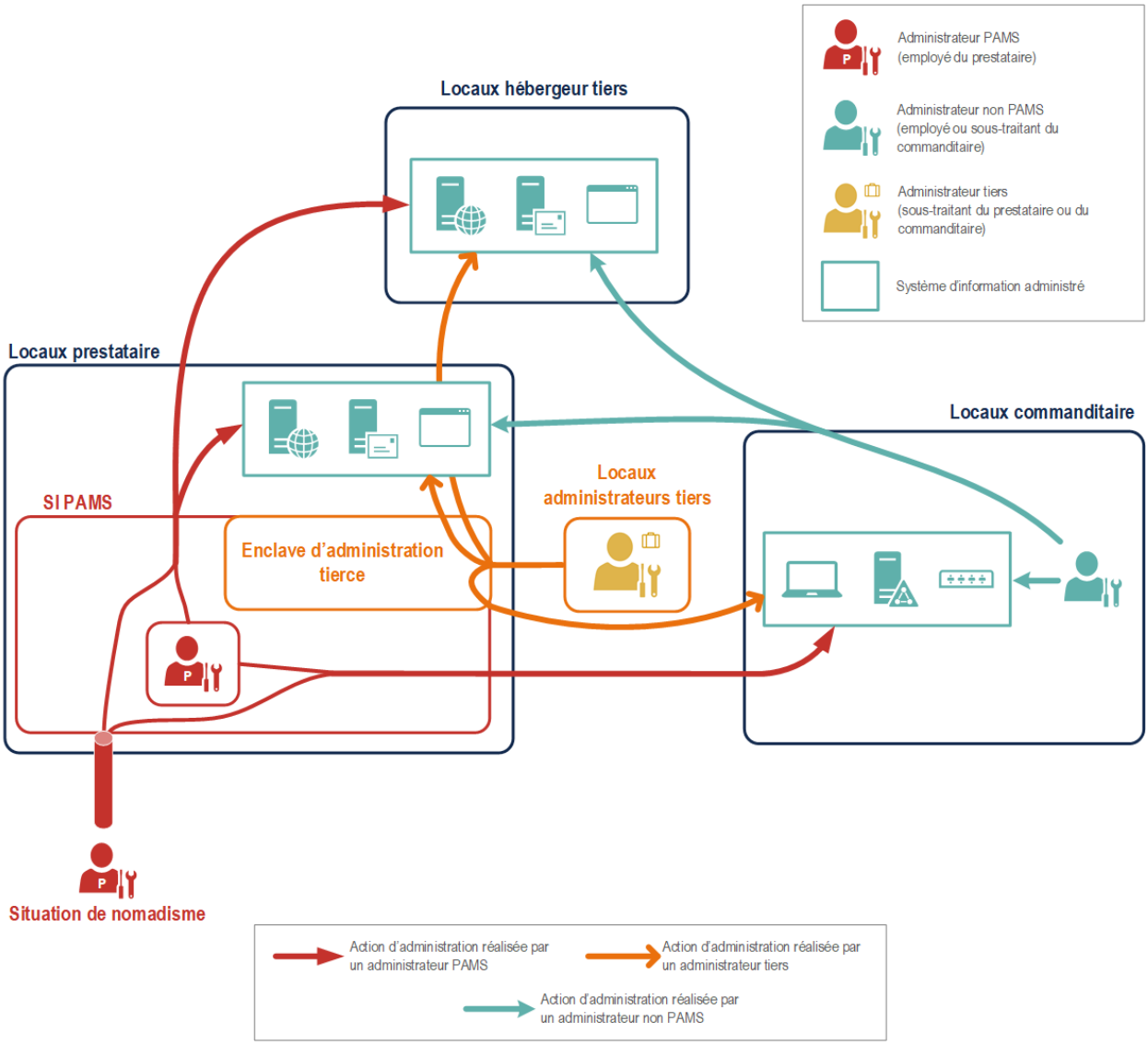


Figure 2 : Service externe d'administration

De plus, dans certains cas, le système d'information administré ne peut pas être administré à distance, la plupart du temps pour des raisons historiques, réglementaires, de criticité ou de nécessité technique. Ce cas est notamment rencontré sur les systèmes d'information de type industriel.

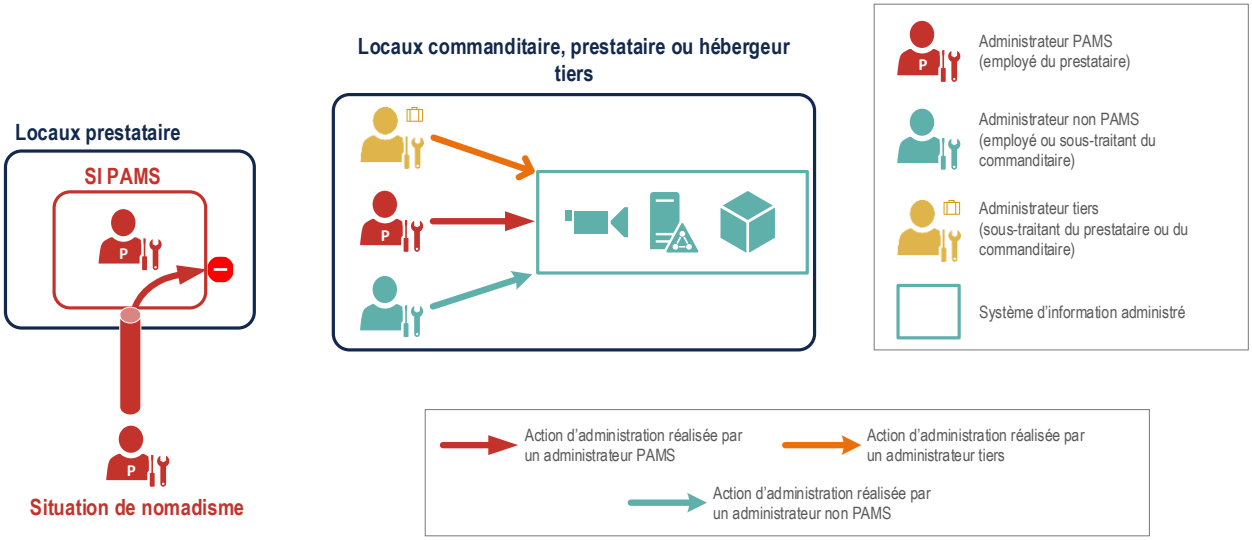


Figure 3 : Service d'administration de système d'information non administrable à distance (cas service externe)

II.2.2. Service interne d'administration

Le commanditaire réalise les actions d'administration sur ses ressources conformément au présent référentiel.

Il peut être amené à intervenir sur des ressources également administrées par un administrateur tiers et peut par ailleurs confier une partie des actions d'administration à un prestataire opérant via une prestation de mise à disposition de personnels dans le cadre du service interne.

Les ressources administrées peuvent se situer dans les locaux du commanditaire ou dans les locaux d'un hébergeur tiers (y compris les services d'informatique en nuage dit *cloud computing*).

Les actions d'administration sont réalisables en situation de nomadisme.

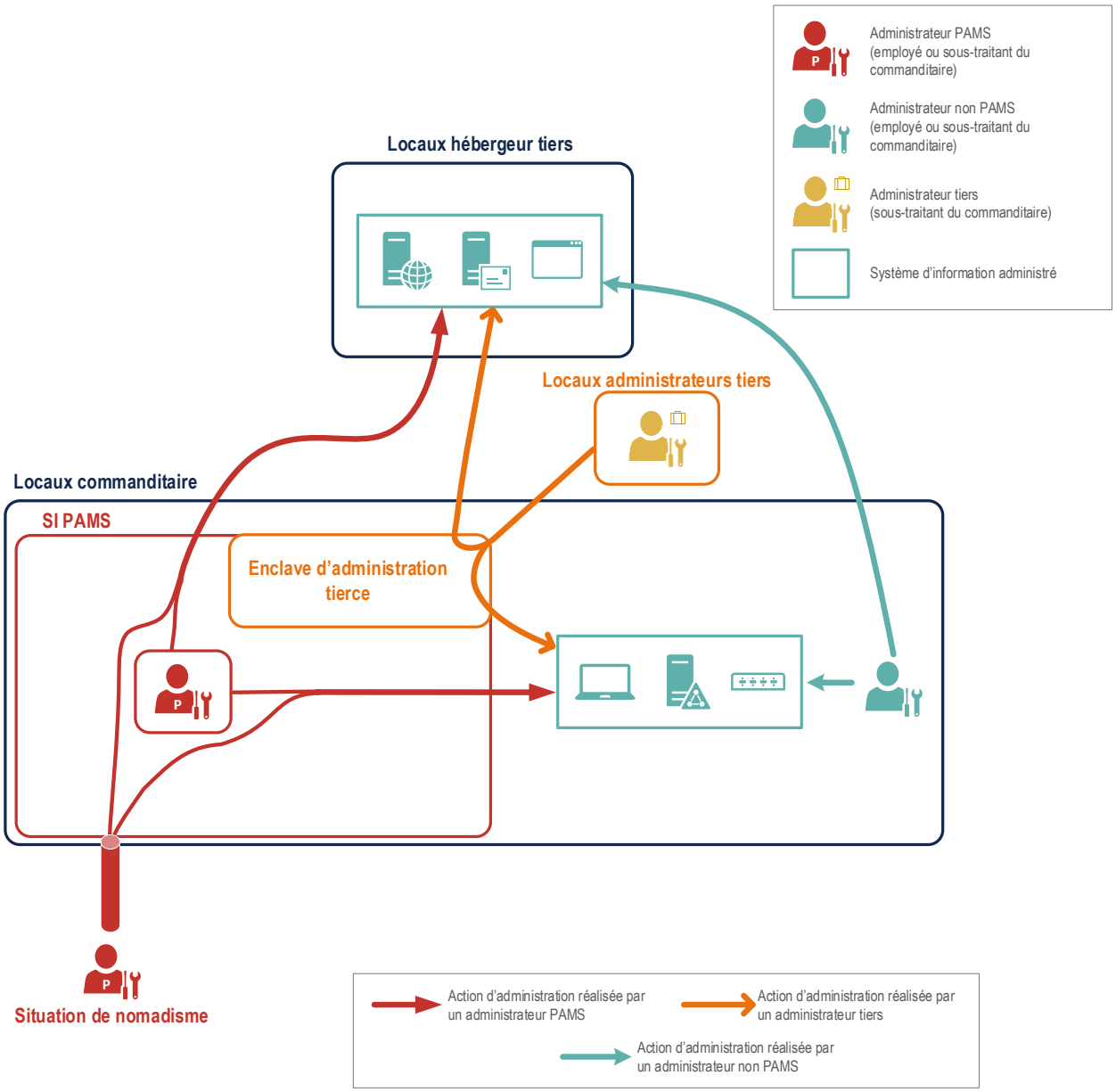


Figure 4 : Service interne d'administration

Dans certains cas, le commanditaire est amené à administrer un système d'information non administrable à distance. Ceci peut être dû à des raisons historiques, réglementaires, de criticité ou de nécessité technique. Ce cas est notamment rencontré sur les systèmes d'information de type industriel.

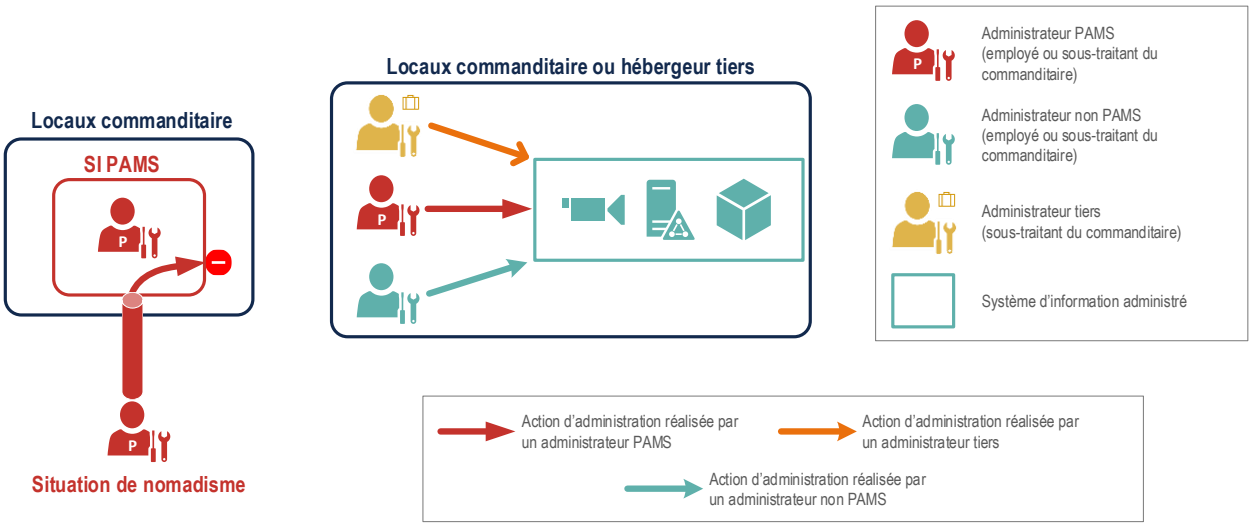


Figure 5 : Service d'administration de système d'information non administrable à distance (cas service interne)

II.3. Périmètre d'application des exigences du référentiel

Le chapitre IV.1 liste des exigences générales relatives aux obligations juridiques du prestataire, notamment ses devoirs vis-à-vis du commanditaire, ses garanties, etc.

Le chapitre IV.2 liste les exigences relatives à la protection de l'information, notamment la sécurité du réseau d'administration et son cloisonnement, la sécurité des postes et outils d'administration, ou encore les interconnexions et les systèmes d'échange sécurisés.

Le chapitre IV.3 liste les exigences relatives à l'organisation du prestataire et la gouvernance du service, notamment la mise en place d'une charte éthique et de recrutement, le contenu des comités opérationnels et stratégiques, etc.

III. Qualification des prestataires d'administration et de maintenance sécurisées

III.1. Modalités de la qualification

Le référentiel contient des exigences et des recommandations à destination des prestataires d'administration et de maintenance sécurisées.

La qualification d'un prestataire est réalisée conformément au processus de qualification d'un prestataire de service de confiance [QUAL_SERV_PROCESS] et permet d'attester de la conformité du prestataire aux exigences du référentiel.

Les exigences doivent être respectées par le prestataire pour obtenir la qualification.

Les recommandations aux prestataires sont données à titre de bonnes pratiques et ne font pas l'objet de vérification pour obtenir la qualification.

Le référentiel formule également des recommandations aux commanditaires dans l'Annexe 3. Ces recommandations ne font pas l'objet de vérification pour obtenir la qualification.

Un service d'administration et de maintenance sécurisées est dit « interne » dans les deux cas suivants[1] :

- s'il est offert exclusivement à un ou des commanditaires étant reconnus, au même titre que le prestataire qui l'opère, comme des filiales d'une même personne morale au sens des articles L. 233-l et suivants du Code de commerce ;
- s'il est offert à des commanditaires appartenant à la même autorité administrative que le prestataire qui l'opère, au sens de l'article I-1 de l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives.

Cette situation est représentée par la partie II.2.2 Service interne d'administration. Sinon le service d'administration et de maintenance sécurisées est dit « externe » et est représenté par la partie II.2.1 Service externe d'administration. Le service d'administration de système d'information non administrable à distance peut être interne ou externe.

Pour un service d'administration et de maintenance sécurisées interne, la qualification est octroyée :

- dans le premier cas, à la personne morale qui offre le service d'administration et de maintenance sécurisées à laquelle tous les commanditaires du service d'administration et de maintenance sécurisées sont liés juridiquement au sens des articles L. 233-l et suivants du Code de commerce ;
- dans le second cas, à l'autorité administrative, au sens de l'article I-1 de l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives à laquelle appartiennent tous les commanditaires du service d'administration et de maintenance sécurisées ainsi que le prestataire lui-même.

Pour un service d'administration et de maintenance sécurisées externe, la qualification ne peut être octroyée au prestataire que si les moyens humains, techniques et organisationnels nécessaires au respect des exigences du référentiel sont intégralement mis en œuvre par ledit prestataire et ses éventuels sous-traitants. Dans le cas où tout ou partie de ces moyens est mis en œuvre par un commanditaire, seul ledit commanditaire peut en effet prétendre à l'obtention de la qualification.

Que le service d'administration et de maintenance sécurisées soit interne ou externe, des sous-traitants peuvent être impliqués dans la mise en œuvre de tout ou partie des moyens humains, techniques et organisationnels nécessaires au respect des exigences de ce référentiel, pour fournir le service d'administration et de maintenance sécurisées du système d'information du commanditaire (ou pour

[1] Exemples : un service d'administration et de maintenance sécurisées créé par un commanditaire pour son usage propre, ou bien un service d'administration et de maintenance sécurisées offert par une filiale d'un groupe au profit d'autres filiales du même groupe.

l'administration du système d'information du service). Dans ce cas, ces sous-traitants sont évalués pour vérifier qu'ils respectent les exigences qui leur incombent, lors de l'évaluation du candidat à la qualification (prestataire ou commanditaire).

III.2. Portée de la qualification

Pour être qualifié, un prestataire doit répondre à toutes les exigences du présent référentiel.

Est considérée comme une prestation qualifiée au sens du référentiel, une prestation respectant toutes les exigences du présent référentiel.

Les prestataires qualifiés gardent la faculté de réaliser des prestations en dehors du périmètre pour lequel ils sont qualifiés, mais ne peuvent, dans ce cas, se prévaloir de la qualification sur ces prestations.

Une prestation d'administration et de maintenance sécurisées qualifiée peut être associée à d'autres prestations complémentaires non qualifiées (développement, intégration de produits de sécurité, etc.) sans perdre le bénéfice de la qualification.

Un prestataire d'administration et de maintenance sécurisées qualifié peut notamment être qualifié pour d'autres familles de prestataires de services de confiance (ex. : PDIS, SecNumCloud). Il est à noter que dans le cas où un prestataire d'administration et de maintenance sécurisées héberge certaines de ses ressources chez des prestataires de Cloud, la qualification ne pourra être octroyée que si le prestataire Cloud est qualifié SecNumCloud (en plus du respect des exigences du présent référentiel).

III.3. Avertissement

Une prestation d'administration et maintenance sécurisées non qualifiée, c'est-à-dire ne respectant pas intégralement les exigences du présent référentiel, peut potentiellement exposer le commanditaire à certains risques et notamment la fuite d'informations confidentielles, la compromission depuis un autre commanditaire du prestataire, la perte ou l'indisponibilité du service. Ainsi, dans le cas d'une prestation non qualifiée, il est recommandé au commanditaire d'exiger de la part de son prestataire un document listant l'ensemble des exigences de ce référentiel non couvertes dans le cadre de sa prestation, afin de connaître les risques auxquels il s'expose.

IV. Exigences à respecter par le prestataire

IV.1. Exigences générales

a) Le prestataire doit être une entité ou une partie d'une entité dotée de la personnalité morale de façon à pouvoir être tenu juridiquement responsable de sa prestation.

b) Le prestataire doit être soumis au droit d'un État membre de l'Union Européenne et respecter les droits et règlements qui lui sont applicables.

c) Le prestataire doit décrire l'organisation de son activité d'administration et de maintenance auprès du commanditaire.

d) Le prestataire a, en sa qualité de professionnel, un devoir de conseil vis-à-vis du commanditaire.

e) Le prestataire doit établir une convention de service avec le commanditaire. La convention de service doit être approuvée formellement, par écrit, par le commanditaire avant l'exécution de la prestation.

f) Le prestataire ou sous-traitant du prestataire doit assumer la responsabilité des activités qu'il réalise pour le compte respectivement du commanditaire et du prestataire dans le cadre de la prestation et en particulier les éventuels dommages causés au commanditaire. À ce titre, le prestataire doit préciser les modalités de partage des responsabilités dans la convention de service, en tenant compte de toutes les éventuelles activités sous-traitées.

g) Le prestataire doit souscrire une assurance couvrant les éventuels dommages causés au commanditaire et notamment à son système d'information dans le cadre de sa prestation.

h) Le prestataire doit s'assurer du consentement du commanditaire avant toute communication d'informations obtenues ou produites dans le cadre de sa prestation. Les modalités d'un tel consentement doivent être précisées dans la convention de service.

i) Le prestataire doit garantir que les informations qu'il fournit, y compris la publicité, ne sont ni fausses ni trompeuses.

j) Le prestataire doit apporter une preuve suffisante que les modalités de son fonctionnement, notamment financières, ne sont pas susceptibles de compromettre son impartialité et la qualité de sa prestation à l'égard du commanditaire ou de provoquer des conflits d'intérêts.

k) Le prestataire doit réaliser la prestation de manière impartiale, en toute bonne foi et dans le respect du commanditaire, de son personnel et de son infrastructure.

l) Le prestataire doit disposer des licences valides des outils (logiciels ou matériels) utilisés pour la réalisation de la prestation.

m) Le prestataire doit demander au commanditaire de lui communiquer les éventuelles exigences légales et réglementaires spécifiques auxquelles il est soumis et notamment celles liées à son secteur d'activité.

IV.2. Protection de l'information

IV.2.1. Maîtrise des risques et politique de sécurité des systèmes d'information

a) Le prestataire doit élaborer une appréciation des risques et le plan d'amélioration continue de la sécurité associé sur l'intégralité du périmètre du service. L'appréciation des risques et le plan d'amélioration continue de la sécurité doivent être validés formellement et par écrit auprès de la direction du prestataire.

b) L'appréciation des risques doit prévoir une liste d'incidents redoutés sur le périmètre du service. Cette liste doit intégrer au moins :
   - les tentatives d'intrusion sur le système d'information du service depuis une de ses interconnexions (cf. IV.2.9) ;
   - les tentatives de rebond entre les systèmes d'information de différents commanditaires via le système d'information du service ;
   - les tentatives illégitimes d'élévation de privilèges au-delà de leurs prérogatives par les administrateurs PAMS ;
   - la perte de communication avec un ou plusieurs équipements du service ;
   - les infections par des codes malveillants.

c) Le prestataire doit réviser l'appréciation des risques et le plan d'amélioration continue de la sécurité associé au minimum annuellement, et en cas de :
   - modifications structurantes du service, notamment celles concernant son hébergement, son infrastructure ou son architecture ;
   - en fonction des résultats de la veille effectuée (cf. IV.2.2.h)), des mises à jour et mesures de réduction des risques appliquées.

d) Le prestataire doit mettre le plan d'amélioration continue de la sécurité à disposition du commanditaire si ce dernier en fait la demande. Le prestataire doit indiquer au commanditaire les conditions de sécurité liées à la transmission et au stockage de ce plan d'amélioration continue de la sécurité.

e) Le prestataire doit définir et mettre en œuvre une politique de sécurité des systèmes d'information reposant sur l'appréciation des risques.

f) Le prestataire doit appliquer le guide d'hygiène informatique de l'ANSSI [HYGIENE] au système d'information du service.

g) Le prestataire doit homologuer le système d'information du service au minimum au *Niveau Standard* du guide d'hygiène informatique de l'ANSSI [HYGIENE].

h) Il est recommandé que le prestataire s'appuie sur le guide [HOMOLOGATION] de l'ANSSI pour l'homologation du système d'information du service.

i) Le prestataire doit tenir à jour l'inventaire de l'ensemble des équipements mettant en œuvre le service. Cet inventaire doit préciser pour chaque équipement :
   - les informations d'identification de l'équipement (nom, adresse IP, adresse MAC, etc.) ;
   - la fonction de l'équipement ;
   - le modèle de l'équipement ;
   - la localisation de l'équipement ;
   - le propriétaire de l'équipement ;
   - le besoin de sécurité des informations (disponibilité, intégrité et confidentialité) issu de l'appréciation des risques effectuées en IV.2.1.a).

j) Le prestataire doit tenir à jour l'inventaire de l'ensemble des administrateurs PAMS et administrateurs du système d'information du service et le tenir à disposition du commanditaire.

k) Le prestataire doit documenter et mettre en œuvre une procédure de restitution des postes d'administration et de maintenance permettant de s'assurer que chaque personne impliquée dans la fourniture du service restitue l'ensemble des actifs en sa possession à la fin de sa période d'emploi ou de son contrat.

l) Le prestataire doit documenter et mettre en œuvre des moyens permettant d'effacer de manière sécurisée tout support de données servant ou ayant servi au service.

m) Le prestataire doit documenter et mettre en œuvre une procédure de mise au rebut des actifs du système d'information du service. Pour les supports de stockage, cette procédure doit au minimum inclure la procédure d'effacement sécurisé (cf. IV.2.1.l)) ou de destruction physique par incinération ou déchiquetage.

n) Le prestataire doit s'assurer que lors de la sortie d'un actif du système d'information du service, l'actif en question ne contienne plus aucune information en clair relative au système d'information du service ou au système d'information du commanditaire.

o) Il est recommandé que le prestataire soit certifié [ISO27001] sur l'intégralité du périmètre du service.

p) Le prestataire doit documenter et mettre en œuvre un programme d'audit sur trois ans définissant le périmètre et la fréquence des audits en accord avec les politiques et les résultats de l'appréciation des risques.

q) Le prestataire doit inclure dans le programme d'audit un audit qualifié par an réalisé par un prestataire d'audit de la sécurité des systèmes d'information [PASSI] qualifié. L'ensemble du programme d'audit doit notamment couvrir :
   - L'audit de la configuration des serveurs et équipements réseau inclus dans le périmètre du service. Cet audit est réalisé par échantillonnage et doit inclure tous types d'équipements et de serveurs présents dans le système d'information su service ;
   - Si le service bénéficie de développements internes, l'audit de code source portant sur les fonctionnalités de sécurité implémentées.

r) Le prestataire doit formaliser une matrice de conformité des dispositifs du service devant être configurés en conformité avec les guides et notes techniques de l'ANSSI.

IV.2.2. Maintien en condition de sécurité

a) Le prestataire doit élaborer, tenir à jour et mettre en œuvre une procédure de maintien en condition de sécurité de toutes les ressources du service.

b) Le prestataire doit définir dans la procédure de maintien en condition de sécurité les délais d'application des mises à jour de sécurité en fonction du niveau de risque associé.

c) Le prestataire doit intégrer les cas d'urgence dans la procédure de maintien en condition de sécurité en précisant explicitement les motifs de déclenchement et les exceptions au cas nominal qui sont induites.

d) Le prestataire doit indiquer dans la procédure de maintien en condition de sécurité la marche à suivre dans le cas où l'application d'une mise à jour de sécurité échoue.

e) Le prestataire doit tenir à jour l'inventaire de l'ensemble des logiciels et micrologiciels mettant en œuvre le service. Cet inventaire doit identifier pour chaque logiciel, sa version et les équipements sur lesquels le logiciel est installé.

f) Le prestataire doit installer et maintenir les dispositifs du service dans des versions stables et à jour de leurs correctifs de sécurité. Les versions installées doivent être des versions supportées sauf si celles-ci empêchent la réalisation du service.

g) Le prestataire doit vérifier l'impact de l'installation des mises à jour sur le système d'information du service. Dans le cas où l'impact de l'installation ne permet pas la réalisation du service, le prestataire doit en documenter les raisons et, également, définir et mettre en œuvre des mesures de réduction des risques.

h) Le prestataire doit documenter et réaliser une veille sur les vulnérabilités, les mises à jour de sécurité et les mesures de réduction des risques concernant les ressources du système d'information du service.

i) Il est recommandé que le prestataire effectue une veille sur l'évolution des menaces concernant les ressources du système d'information du service ainsi que celles des systèmes d'information administrés du commanditaire.

j) Il est recommandé que le centre de veille, d'alerte aux attaques informatiques du prestataire soit référencé par le Centre gouvernemental français de veille, d'alerte et de réponse aux attaques informatiques (CERT-FR).

k) Le prestataire doit confirmer la pertinence des mesures de réduction des risques en place à chaque évolution de l'appréciation des risques et les faire évoluer le cas échéant.

l) Le prestataire doit s'assurer de l'authenticité et de l'intégrité des mises à jour téléchargées auprès des sources de mise à jour de confiance.

m) Le prestataire doit installer les mises à jour de sécurité ou mettre en œuvre les mesures de réduction des risques conformément à la procédure de maintien en condition de sécurité.

n) Le prestataire doit mettre en place, au sein du système d'information du service, une zone de mise à jour regroupant l'ensemble des dispositifs impliqués dans le processus de récupération et de mise à disposition des mises à jour des dispositifs du service.

o) Le prestataire doit produire les indicateurs suivants sur le périmètre du service et être en mesure de les fournir aux commanditaires :
   - le pourcentage et le nombre total de postes d'administration ou de maintenance dont les ressources système ou applicatives ne sont pas installées dans une version supportée par le fournisseur ou le fabricant ;
   - le pourcentage et le nombre total de serveurs du service dont les ressources système ou applicatives ne sont pas installées dans une version supportée par le fournisseur ou le fabricant ;
   - le pourcentage et le nombre total de postes d'administration ou de maintenance dont les ressources système ou applicatives ne sont pas mises à jour ou corrigées du point de vue de la sécurité au-delà du délai d'application défini par l'exigence IV.2.2.b) ;
   - le pourcentage et le nombre total de serveurs du service dont les ressources système ou applicatives ne sont pas mises à jour ou corrigées du point de vue de la sécurité au-delà du délai d'application défini par l'exigence IV.2.2.b).

IV.2.3. Sécurité physique

a) Le prestataire doit documenter et mettre en œuvre des périmètres de sécurité, incluant le marquage des zones physiques et les différents moyens de limitation et de contrôle des accès.

b) Le prestataire doit distinguer des zones publiques, des zones privées et des zones sensibles :

- Les zones publiques sont accessibles à tous dans les limites de la propriété du prestataire. Les zones de livraison et de chargement et les autres points par lesquels des personnes non autorisées peuvent pénétrer dans les locaux sans être accompagnées sont considérés comme des zones publiques ;
- Les zones privées (IV.2.3.1) peuvent héberger :
  - les postes d'administration ou de maintenance ;
  - les locaux à partir desquels le prestataire opère.
- Les zones sensibles (IV.2.3.2) sont réservées à l'hébergement du système d'information du service hors postes d'administration ou de maintenance.

c) Le prestataire ne doit héberger aucune ressource dévolue au service, ou permettant d'accéder à des composantes de celui-ci, dans les zones publiques.

d) Le prestataire doit isoler les points d'accès des zones de livraison vers les zones privées et sensibles, de façon à éviter les accès non autorisés, ou à défaut, implémenter des mesures compensatoires permettant d'assurer le même niveau de sécurité.

e) Le prestataire doit élaborer et tenir à jour la liste des personnes autorisées à accéder aux zones privées et sensibles.

f) Le prestataire doit documenter et mettre en œuvre une procédure de transfert hors site de données du commanditaire, équipements et logiciels. Cette procédure doit nécessiter que la direction du prestataire donne son autorisation écrite. Dans tous les cas, le prestataire doit mettre en œuvre les moyens permettant de garantir que le niveau de protection en confidentialité et en intégrité des actifs durant leur transport est équivalent à celui sur site.

g) Le prestataire doit documenter et mettre en œuvre une procédure de protection du matériel en attente d'utilisation.

h) Il est recommandé que le prestataire respecte l'ensemble des recommandations de l'ANSSI [G_CAVP].

i) Il est recommandé que le prestataire respecte l'ensemble des mesures et préconisations sur la sécurisation physique de [ISO27002].

IV.2.3.1. Contrôle d'accès physique aux zones privées

a) Le prestataire doit protéger les zones privées contre les accès non autorisés. Pour ce faire, il doit mettre en œuvre un contrôle d'accès physique reposant au moins sur un facteur personnel : la connaissance d'un secret, la détention d'un objet ou la biométrie.

b) Le prestataire doit définir et documenter des mesures d'accès physique dérogatoires en cas d'urgence.

c) Le prestataire doit afficher à l'entrée des zones privées un avertissement relatif aux limites et conditions d'accès à ces zones.

d) Le prestataire doit définir et documenter les plages horaires et conditions d'accès aux zones privées en fonction des profils des intervenants.

e) Le prestataire doit documenter et mettre en œuvre les moyens permettant de s'assurer que les visiteurs sont systématiquement accompagnés par le prestataire lors de leurs accès et séjours en zone privée.

f) Le prestataire doit mettre en œuvre des mécanismes de journalisation assurant la confidentialité et l'intégrité des journaux des accès aux zones privées.

g) Le prestataire doit conserver une trace de l'identité des visiteurs conformément à la législation et réglementation en vigueur.

h) Il est recommandé que le prestataire conserve la trace de l'identité des visiteurs pendant une durée de six mois, sous réserve du respect des exigences légales et réglementaires.

i) Le prestataire doit faire superviser (suivre, autoriser, interdire et questionner) les actions du tiers visiteur amené à intervenir en zone privée.

j) Le prestataire doit documenter et mettre en œuvre des mécanismes de surveillance et de détection des accès non autorisés aux zones privées.

IV.2.3.2. Contrôle d'accès physique aux zones sensibles

a) Le prestataire doit protéger les zones sensibles contre les accès non autorisés. Pour ce faire, il doit mettre en œuvre un contrôle d'accès physique reposant au moins sur deux facteurs personnels : la connaissance d'un secret, la détention d'un objet ou la biométrie.

b) Le prestataire doit définir et documenter des mesures d'accès physique dérogatoires en cas d'urgence.

c) Le prestataire doit afficher à l'entrée des zones sensibles un avertissement relatif aux limites et conditions d'accès à ces zones.

d) Le prestataire doit définir et documenter les plages horaires et conditions d'accès aux zones sensibles en fonction des profils des intervenants.

e) Le prestataire doit documenter et mettre en œuvre les moyens permettant de s'assurer que les visiteurs sont systématiquement accompagnés par le prestataire lors de leurs accès et séjours en zone sensible.

f) Le prestataire doit conserver une trace de l'identité des visiteurs conformément à la législation et réglementation en vigueur.

g) Il est recommandé que le prestataire conserve la trace de l'identité des visiteurs pendant une durée de six mois, sous réserve du respect des exigences légales et réglementaires.

h) Le prestataire doit faire superviser (suivre, autoriser, interdire et questionner) les actions du tiers visiteur amené à intervenir en zone sensible.

i) Le prestataire doit documenter et mettre en œuvre des mécanismes de surveillance et de détection des accès non autorisés aux zones sensibles.

j) Le prestataire doit mettre en œuvre les moyens garantissant qu'aucun accès direct n'existe entre une zone publique et une zone sensible.

k) Le prestataire doit mettre en œuvre des mécanismes de journalisation assurant la confidentialité et l'intégrité des journaux des accès aux zones sensibles.

l) Le prestataire doit mettre en place une journalisation des accès physiques aux zones sensibles. Il doit effectuer une revue de ces journaux au moins mensuellement.

IV.2.3.3. Protection contre les menaces extérieures et environnementales

a) Le prestataire doit documenter et mettre en œuvre les moyens permettant de minimiser les risques inhérents aux sinistres physiques (incendie, dégât des eaux, etc.) et naturels (risques climatiques, inondations, séismes, etc.).

b) Le prestataire doit documenter et mettre en œuvre les mesures permettant de prévenir et limiter les conséquences d'une coupure d'alimentation électrique et permettre une reprise du service conforme aux exigences de disponibilité du service définies dans la convention de service.

c) Le prestataire doit documenter et mettre en œuvre les moyens permettant de maintenir des conditions de température et d'humidité adaptées aux équipements. De plus, il doit mettre en œuvre des mesures permettant de prévenir les pannes de climatisation et d'en limiter les conséquences.

d) Le prestataire doit documenter et mettre en œuvre des contrôles et tests réguliers des équipements de détection et de protection physique.

IV.2.3.4. Travail dans les zones privées et sensibles

a) Le prestataire doit intégrer les éléments de sécurité physique dans la politique de sécurité et l'appréciation des risques conformément au niveau de sécurité requis par la catégorie de la zone.

b) Le prestataire doit documenter et mettre en œuvre des procédures relatives au travail en zones privées et sensibles. Il doit communiquer ces procédures aux intervenants concernés

IV.2.3.5. Sécurité du câblage

a) Le prestataire doit documenter et mettre en œuvre des mesures permettant de protéger le câblage électrique et de télécommunication des dommages physiques et des possibilités d'interception.

b) Le prestataire doit établir et tenir à jour un plan de câblage.

c) Il est recommandé que le prestataire mette en œuvre des mesures permettant d'identifier les câbles (par exemple code couleur, étiquette, etc.) afin d'en faciliter l'exploitation et limiter les erreurs de manipulation.

IV.2.3.6. Maintenance des matériels

a) Le prestataire doit documenter et mettre en œuvre des mesures permettant de s'assurer que les conditions – matérielles et logicielles – d'installation, de maintenance et d'entretien des équipements du système d'information du service hébergés en zones privées et sensibles sont compatibles avec les exigences de confidentialité et de disponibilité du service définies dans la convention de service.

b) Le prestataire doit s'assurer que les supports ne peuvent être retournés à un tiers que si les données du commanditaire y sont stockées de manière chiffrée et non accompagnées du secret permettant le déchiffrement, ou ont préalablement été supprimées à l'aide d'un mécanisme d'effacement sécurisé conformément à IV.2.1.l).

c) Le prestataire doit documenter et mettre en œuvre des mesures permettant de s'assurer que les conditions d'installation, de maintenance et d'entretien des équipements consacrés à la gestion technique des bâtiments (alimentation électrique, climatisation, incendie, etc.) sont compatibles avec les exigences de disponibilité du service définies dans la convention de service.

IV.2.4. Sauvegardes

a) Le prestataire doit élaborer et mettre en œuvre un plan de sauvegarde et de restauration des dispositifs du service permettant un retour à un fonctionnement nominal du système d'information du service (le plan de sauvegarde pourra par exemple couvrir la sauvegarde des systèmes, des configurations, etc.).

b) Le prestataire doit tester le plan de sauvegarde et de restauration au minimum une fois par an.

c) Le prestataire doit mettre en œuvre les mesures permettant d'assurer la confidentialité et l'intégrité des sauvegardes stockées. En cas de stockage en dehors de la zone d'administration du système d'information du service, des mécanismes de chiffrement et d'authentification conformes à [CRYPTO_B1] doivent être utilisés.

d) Le prestataire doit dédier au système d'information du service les outils requis pour la sauvegarde du système d'information du service ; ceux-ci doivent être hébergés au sein de la zone d'administration.

e) Le prestataire doit définir et mettre en œuvre une procédure de sauvegarde. Cette procédure doit prévoir au minimum la réalisation des sauvegardes sur un dispositif de stockage physiquement déconnecté du système d'information du service (dispositif dit « hors-ligne ») à l'issue de l'opération de sauvegarde.

f) Le prestataire doit exporter les sauvegardes vers le ou les dispositifs de stockage hors-ligne à une fréquence cohérente avec les résultats de l'appréciation des risques, en particulier avec la perte de données maximale admissible.

g) Le prestataire doit localiser les sauvegardes à une distance suffisante des dispositifs principaux en cohérence avec les résultats de l'appréciation des risques et permettant de faire face à des sinistres majeurs. Les sauvegardes sont assujetties aux mêmes exigences de localisation (cf. IV.3.4.b)d)) que les données opérationnelles.

h) Le prestataire doit appliquer les exigences du paragraphe IV.2.3 aux sites de sauvegardes.

i) Le prestataire doit protéger les communications entre le site principal et le ou les sites de sauvegarde, par chiffrement conformément aux exigences du paragraphe IV.2.6.

j) Il est recommandé que le prestataire respecte l'ensemble des mesures et préconisations sur la sécurisation des sauvegardes de [ISO27002].

k) Il est recommandé que le prestataire conserve les sauvegardes pendant une durée minimale de deux mois sous réserve du respect des exigences légales et réglementaires.

IV.2.5. Journalisation, supervision de sécurité et détection des incidents de sécurité

a) Le prestataire doit mettre en œuvre des moyens de détection des incidents de sécurité pour le système d'information du service.

b) Le prestataire doit, sur la base de l'appréciation des risques et de la liste des événements redoutés associée telle que définie au IV.2.1b), élaborer une stratégie de collecte, une stratégie d'analyse, une stratégie de notification et une stratégie de réponse à incident.

c) Le prestataire doit journaliser l'ensemble des accès aux dispositifs du service ainsi que les actions réalisées sur le dispositif ou via les mécanismes du service.

d) Le prestataire doit conserver les événements issus de la journalisation pendant une durée minimale de six mois sous réserve du respect des exigences légales et réglementaires.

e) Le prestataire doit assurer un cloisonnement entre les moyens de détection et le reste du système d'information du service (séparation des moyens humains, techniques et organisationnels).

f) Le prestataire doit assurer l'intégrité des journaux lors de leur transfert, notamment conformément à la règle R12 de [NT_JOURNAL].

g) Le prestataire doit centraliser l'ensemble des journaux.

h) Le prestataire doit horodater l'ensemble des journaux.

i) Le prestataire doit synchroniser l'ensemble des événements à partir d'une ou plusieurs sources de temps internes cohérentes entre elles.

j) Le prestataire doit synchroniser sa ou ses sources de temps internes avec au moins 3 sources de temps indépendantes d'une précision supérieure ou égale à la seconde (par exemple, 3 sources de temps indépendantes sur Internet ou 2 sources de temps satellite et 1 source de temps sur Internet).

k) Le prestataire doit s'assurer que les canaux de synchronisation nominale et de secours ne sont pas dépendants l'un de l'autre.

l) Il est recommandé que le prestataire définisse une stratégie de collecte et une stratégie d'analyse pour la supervision sécurité du système d'information du service conformes au référentiel PDIS.

m) Il est recommandé de respecter la note technique de l'ANSSI pour la mise en œuvre d'un système de journalisation [NT_JOURNAL].

n) Il est recommandé que le prestataire informe les administrateurs de la traçabilité technique de leurs actions d'administration et la possibilité de contrôle et de supervision à laquelle ils sont soumis au titre de la politique de sécurité des systèmes d'information.

o) Il est recommandé que le prestataire déploie pour la détection d'incidents de sécurité une ou plusieurs sondes de détection qualifiées par l'ANSSI au niveau adéquat et utilisées conformément aux conditions de leur qualification sur le système d'information du service.

p) Il est recommandé que le prestataire fasse appel à un prestataire de détection en incidents de sécurité (PDIS) qualifié afin d'être conforme aux exigences ou aux recommandations IV.2.5.a), IV.2.5.e), IV.2.5.c), IV.2.5.l), IV.2.5.m).

q) Le prestataire doit mettre en place un processus de gestion de crise en cas de détection d'un incident de sécurité.

r) Le prestataire doit notifier le ou les commanditaires pouvant être affectés par un incident de sécurité. Lorsque le commanditaire est tenu par la réglementation de déclarer cet incident à une instance gouvernementale ou une autorité tierce, le prestataire doit l'accompagner dans cette démarche si ce dernier en fait la demande.

s) Il est recommandé que le prestataire fasse appel en cas d'incident à un prestataire de réponse aux incidents de sécurité (PRIS) qualifié afin de réaliser l'étude des fichiers suspects par une prestation d'investigation numérique sur périmètre restreint d'analyse de codes malveillants.

t) Le prestataire doit, sur demande du commanditaire, fournir les éléments techniques qui le concernent issus de la journalisation, de la supervision de sécurité ou de la détection des incidents de sécurité du système d'information du service, pouvant aider à la qualification d'un incident de sécurité sur le système d'information du commanditaire.

IV.2.6. Réseau d'administration, segmentation et cloisonnement du système d'information du service

a) Le prestataire doit segmenter le système d'information du service en plusieurs zones de confiance dans lesquelles sont répartis tous les dispositifs impliqués dans le service. La segmentation minimale comporte les zones de confiance suivantes :
   - *zone(s) d'exploitation*, regroupant les postes d'administration ou de maintenance utilisés par les administrateurs PAMS ;
   - *zone(s) de serveurs outils*, regroupant l'ensemble des serveurs hébergeant des outils d'administration pour les ressources administrées ;
   - *zone(s) d'administration* du système d'information du service, regroupant l'ensemble des outils d'administration du système d'information du service et les postes d'administration des administrateurs du système d'information du service ;
   - *zone(s) de mise à jour*, regroupant l'ensemble des dispositifs impliqués dans le processus de récupération et de mise à disposition des mises à jour des dispositifs du service ;
   - *zone(s) d'infrastructures* du système d'information du service, regroupant l'ensemble des serveurs d'infrastructure suivants : référentiel(s) d'identité, serveur(s) de temps, serveur(s) DHCP, serveur(s) DNS et infrastructure(s) de gestion de clés ;
   - *zone(s) de service interne* du système d'information du service, regroupant l'ensemble des services qui ne sont pas dans la ou le(s) zone(s) d'administration du système d'information du service et zone(s) d'infrastructure.

   Ainsi que les zones de confiance d'interconnexion suivantes :
   - *zone d'échange prestataire*, regroupant les dispositifs permettant l'échange de fichiers avec des systèmes d'information du prestataire extérieurs au système d'information du service ;
   - *zone d'accès à Internet*, regroupant l'ensemble des composants permettant un accès sécurisé à Internet, par exemple pour l'administration de systèmes dont les outils d'administration ne sont accessibles que par Internet (*cloud computing*, téléchargement de mises à jour, etc.) ;
   - *zone d'accès aux ressources administrées*, regroupant l'ensemble des dispositifs permettant un accès sécurisé aux interfaces d'administration des ressources du commanditaire (hors exposition sur Internet) administrées dans le cadre de la prestation ;
   - *zone d'échange commanditaire*, regroupant les ressources permettant à un commanditaire et au prestataire d'échanger de manière sécurisée les informations nécessaires à la réalisation et au suivi de la prestation qualifiée ;
   - *zone des enclaves d'administration tierce*, regroupant l'ensemble des dispositifs mis à disposition des administrateurs tiers à la prestation qualifiée en vue d'encadrer la sécurité de leurs interventions ;
   - *zone d'échange tiers*, regroupant les dispositifs permettant l'échange d'informations de façon sécurisée avec des tiers ;
   - *zone d'accès distants*, permettant aux administrateurs PAMS et aux administrateurs du système d'information du service en situation de nomadisme d'accéder au système d'information du service de manière sécurisée en vue de réaliser leurs actions.

b) Le prestataire doit mettre en œuvre des mesures garantissant le cloisonnement entre les différentes zones de confiance, notamment par des mécanismes de filtrage, d'authentification et de contrôle d'accès.

c) Le prestataire doit mettre en œuvre un ou plusieurs dispositifs de filtrage périmétrique aux interconnexions du système d'information du service.

d) Le prestataire doit mettre en œuvre soit des équipements de filtrage physiques dédiés au système d'information du service, soit des dispositifs de filtrage reposant sur un ou plusieurs socles physiques dédiés au filtrage pour le système d'information du service.

e) Le prestataire doit dissocier sur des équipements physiques ou socles physiques distincts, les dispositifs assurant le filtrage périmétrique et les dispositifs assurant le filtrage interne.

f) Le prestataire doit dédier des équipements physiques ou socles physiques distincts pour les dispositifs assurant le filtrage périmétrique des zones suivantes, au minimum comme suit :
   - un équipement ou un socle dédié aux zones suivantes : zone d'échange tiers (IV.2.9.3), zone d'accès à Internet (IV.2.9.4), zone d'accès distants (IV.2.9.6) et zone des enclaves d'administration tierce (IV.2.9.7) ;
   - un équipement ou un socle dédié à la zone d'échange prestataire (IV.2.9.1) ;
   - un équipement ou un socle dédié aux zones suivantes : zone d'échange commanditaire (IV.2.9.2) et zone d'accès aux ressources administrées (IV.2.9.5).

g) Il est recommandé que les dispositifs de filtrage périmétrique ou interne au système d'information du service soient des produits qualifiés par l'ANSSI et soient utilisés conformément aux conditions de leur qualification.

h) Le prestataire doit élaborer et tenir à jour une politique de filtrage associée à la matrice des flux de référence du service (définie en IV.2.6.u). La politique de filtrage doit n'autoriser que les flux strictement nécessaires au fonctionnement du service.

i) Le prestataire doit s'assurer que tous les flux en provenance ou à destination de l'extérieur du système d'information du service transitent par l'une des zones d'interconnexion mentionnées au IV.2.6.a).

j) Le prestataire doit mettre en œuvre des solutions de chiffrement et d'authentification des paquets IP entre deux ressources d'administration dès lors que les données échangées transitent par des réseaux de transport non dédiés physiquement au service ou dont la sécurité physique n'est pas assurée. Le prestataire doit mettre en œuvre ces solutions en conformité avec le guide [G_IPSEC].

k) Le prestataire doit mettre en œuvre, soit des équipements de chiffrement et d'authentification des paquets IP physiques dédiés au système d'information du service, soit des dispositifs de chiffrement et d'authentification des paquets IP reposant sur un ou plusieurs socles physiques dédiés au système d'information du service.

l) Le prestataire doit dédier des équipements physiques ou socles physiques distincts pour les dispositifs assurant le chiffrement et l'authentification des flux ou paquets IP pour les zones suivantes, au minimum comme suit :
   - équipement ou socle dédié aux zones d'échange tiers (IV.2.9.3) et zone des enclaves d'administration tierce (IV.2.9.7) ;
   - équipement ou socle dédié aux zones d'échange commanditaire (IV.2.9.2) et zone d'accès aux ressources administrées (IV.2.9.5) ;
   - équipement ou socle dédié à la zone d'accès distants (IV.2.9.6).

m) Le prestataire doit mettre en œuvre des serveurs physiquement dédiés au système d'information du service et, en cas de recours à la virtualisation, des serveurs d'hypervision physiquement dédiés au système d'information du service.

n) Le prestataire doit héberger les serveurs mis en œuvre dans la ou les zone(s) d'infrastructures du système d'information du service sur un ou plusieurs socles physiques dédiés.

o) Le prestataire doit appliquer un cloisonnement physique ou dédier un ou plusieurs systèmes d'exploitation pour chaque zone suivante :
   - Zone(s) de serveurs outils ;
   - Zone(s) de mise à jour ;
   - Zone(s) de service interne ;

- Zone d'accès à Internet ;
- Zone d'échange tiers ;
- Zone d'accès distants ;
- Zone d'accès aux ressources administrées ;
- Zone d'échange commanditaire ;
- Zone d'exploitation ;
- Zone d'échange prestataire.

p) Il est recommandé que le prestataire dédie des serveurs physiques pour chaque zone suivante :
- Zone(s) de serveurs outils ;
- Zone(s) de mise à jour ;
- Zone(s) de service interne ;
- Zone d'accès à Internet ;
- Zone d'échange tiers ;
- Zone d'accès distants ;
- Zone d'accès aux ressources administrées ;
- Zone d'échange commanditaire ;
- Zone d'exploitation ;
- Zone d'échange prestataire.

q) Le prestataire doit mettre en œuvre des infrastructures de stockage physiquement dédiées au système d'information du service.

r) Le prestataire doit mettre en œuvre une mesure de cloisonnement réseau pour que les postes d'administration ou de maintenance ne soient pas en mesure de communiquer directement entre eux.

s) Le prestataire doit durcir les configurations des équipements réseau et de sécurité mis en œuvre pour le système d'information du service.

t) Il est recommandé que le prestataire s'appuie sur les guides de durcissement de l'ANSSI pour le durcissement des configurations des équipements réseau et de sécurité du service, dont le guide de sécurisation d'un commutateur de desserte [NT_COMMUT].

u) Le prestataire doit établir et tenir à jour une cartographie du système d'information du service, en lien avec l'inventaire des actifs, comprenant au minimum les éléments suivants :
- la liste des ressources matérielles ou virtualisées ;
- les noms et fonctions des applications, supportant le service ;
- le schéma d'architecture réseau au niveau 3 du modèle OSI sur lequel les points névralgiques sont identifiés :
  - les zones d'interconnexions, notamment avec les réseaux tiers et publics ;
  - les réseaux, sous-réseaux, notamment les réseaux d'administration ;
  - les équipements assurant des fonctions de sécurité (filtrage, authentification, chiffrement, contrôle d'accès, traçabilité, etc.) ;
  - les serveurs hébergeant des données ou assurant des fonctions sensibles.
- la matrice des flux réseau autorisés en précisant :
  - leur description technique (sources, destinations, services, protocoles et ports) ;
  - la justification métier ou d'infrastructure ;
  - le cas échéant, lorsque des services, protocoles ou ports réputés non sûrs sont utilisés, les mesures compensatoires mises en place, dans la logique de défense en profondeur.

v) Le prestataire doit procéder à une revue au minimum annuelle de la cartographie afin de s'assurer que l'ensemble des modifications effectuées sur le système d'information du service et devant paraître dans la cartographie y figurent.

w) Il est recommandé que le prestataire s'appuie sur le guide de l'ANSSI [CARTO] dans l'élaboration de la cartographie du système d'information du service.

IV.2.7. Postes d'administration ou de maintenance

a) Le prestataire doit mettre à disposition des administrateurs PAMS des postes d'administration ou de maintenance dédiés exclusivement au service et sous sa maîtrise.

b) Il est recommandé de dédier un poste d'administration et de maintenance par administrateur PAMS.

c) Le prestataire doit mettre en œuvre une procédure pour la remise d'un poste d'administration ou de maintenance, incluant au minimum la mise à jour d'un inventaire et la sensibilisation de l'administrateur au caractère sensible du poste d'administration ou de maintenance et la responsabilité de ce dernier vis-à-vis de sa protection physique.

d) Il est recommandé de dédier un poste d'administration et de maintenance par niveau de sensibilité du système d'information administré.

e) Le prestataire doit, à la configuration initiale des postes d'administration ou de maintenance, procéder à un effacement sécurisé des supports de stockage dans leur intégralité, conformément à la procédure décrite en IV.2.1.l).

f) Le prestataire doit mettre en œuvre une procédure pour la restitution d'un poste d'administration ou de maintenance, incluant au minimum la mise à jour d'un inventaire et le reformatage complet du système.

g) Pour un poste d'administration ou de maintenance portable, le prestataire doit fournir un filtre de confidentialité et un dispositif de verrouillage physique adaptés au modèle du poste.

h) Le prestataire doit mettre en œuvre des mécanismes de chiffrement conformes à [CRYPTO_B1] pour la totalité du contenu des mémoires de masse des postes d'administration ou de maintenance.

i) Pour le chiffrement des mémoires de masse, il est recommandé d'utiliser une solution de chiffrement qualifiée par l'ANSSI et utilisée conformément aux conditions de sa qualification.

j) Le prestataire doit durcir les configurations système des postes d'administration ou de maintenance.

k) Il est recommandé que le prestataire s'appuie sur les guides de durcissement [G_LINUX] ou Windows [G_WINDOWS_1], [G_WINDOWS_2], [G_WINDOWS_3] de l'ANSSI pour le durcissement des configurations système des postes d'administration ou de maintenance.

l) Le prestataire doit s'assurer qu'un administrateur PAMS ne dispose pas des droits d'administration sur son poste d'administration ou de maintenance.

m) Le prestataire doit s'assurer que les postes d'administration ou de maintenance des administrateurs PAMS ne disposent que des logiciels et fonctions nécessaires au strict besoin opérationnel du service.

n) Le prestataire doit s'assurer que les postes d'administration ou de maintenance disposent d'un dispositif de filtrage réseau local activé et configuré pour n'autoriser que les connexions répondant strictement au besoin opérationnel du service.

o) Le prestataire doit s'assurer que les postes d'administration ou de maintenance des administrateurs PAMS n'ont aucun accès à Internet (hormis pour l'accès à un dispositif de chiffrement et d'authentification des paquets IP tel que défini dans le cadre du nomadisme, cf. IV.2.9.6). Cette exigence couvre, entre autres, la navigation Web ainsi que l'usage de messageries électroniques

connectées à Internet et s'applique même si ces services sont filtrés par des passerelles sécurisées d'accès Internet.

p) En cas de besoin d'accès à Internet ou à d'autres systèmes d'information (système d'information bureautique du prestataire par exemple) à d'autres fins que la réalisation d'actions d'administration, le prestataire doit mettre à disposition des administrateurs PAMS un équipement physiquement distinct de leur poste d'administration ou de maintenance, déployé en dehors du système d'information du service.

q) Le prestataire doit restreindre l'utilisation des systèmes de stockage amovibles au strict besoin opérationnel autorisé par la politique de sécurité des systèmes d'information.

Lorsque le prestataire doit héberger un hyperviseur sur un poste d'administration ou de maintenance pour des besoins opérationnels, les exigences suivantes doivent être appliquées :

r) Le prestataire doit s'assurer que la configuration de l'hyperviseur ne permet pas l'échange de données directement entre l'hôte et les machines virtuelles, ni entre machines virtuelles.

s) Le prestataire doit mettre en place des mesures interdisant aux administrateurs PAMS de déployer de nouvelles machines virtuelles, de supprimer une machine virtuelle déjà déployée ou d'en modifier la configuration.

t) Le prestataire doit s'assurer que les machines virtuelles utilisent une interface réseau dédiée distincte de l'interface réseau utilisée par l'hôte, via l'utilisation d'un adaptateur réseau externe physiquement dédié à cet usage et non utilisable par le système d'exploitation hôte.

Lorsque les postes d'administration ou de maintenance sont utilisés par plusieurs administrateurs, l'exigence suivante doit être appliquée :

u) Le prestataire doit s'assurer que les données déposées sur les postes d'administration ou de maintenance utilisés ne peuvent être accédées que par l'administrateur PAMS habilité en respectant le principe du besoin d'en connaître.

v) Il est recommandé de dédier un poste d'administration ou de maintenance par niveau de sensibilité du système d'information du commanditaire administré.

IV.2.8. Outils d'administration

a) Le prestataire doit s'assurer que le système hôte des postes d'administration ou de maintenance n'héberge que des clients de connexion légers, à l'exception des clients lourds indispensables à la réalisation du service (cf IV.2.8.q)).

b) Le prestataire doit installer les clients lourds ou outils d'administration sur des serveurs outils, notamment afin d'en faciliter le maintien en conditions opérationnelle et de sécurité.

c) Le prestataire doit s'assurer que les outils de gestion des configurations qu'il met en œuvre garantissent l'intégrité et la traçabilité des éléments qu'ils contiennent et suivant les besoins, la confidentialité.

d) Le prestataire doit s'assurer que les administrateurs PAMS ne disposent pas des droits d'administration sur les serveurs outils d'administration.

e) Le prestataire doit s'assurer que les serveurs outils d'administration sous sa responsabilité n'ont aucun accès à Internet (à la seule exception des éventuels serveurs de rebond utilisés pour l'accès aux outils d'administration exclusivement exposés sur Internet, cf. IV.2.12.1).

f) Le prestataire doit cloisonner les serveurs outils d'administration par commanditaire en dédiant les systèmes d'exploitation ou socle physique hébergeant les serveurs outils.

g) Le prestataire doit pouvoir, à la demande du commanditaire, héberger les serveurs outils de sa prestation qualifiée sur un ou plusieurs socles physiques qui lui sont dédiés.

h) Il est recommandé que le prestataire cloisonne les zones serveurs outils pour chaque commanditaire en fonction du niveau de criticité et d'exposition des systèmes d'information administrés.

i) Le prestataire doit accéder aux outils d'administration en utilisant des protocoles permettant l'authentification et le chiffrement au niveau applicatif en conformité avec les guides [G_TLS] ou [G_SSH] selon les protocoles utilisés, ou à défaut au niveau IP en conformité avec le guide [G_IPSEC].

j) Le prestataire doit accéder aux ressources administrées en utilisant des protocoles permettant l'authentification et le chiffrement au niveau applicatif ou, à défaut au niveau IP.

k) Il est recommandé que l'accès aux ressources administrées en utilisant des protocoles permettant l'authentification et le chiffrement au niveau applicatif ou IP soit en conformité avec les guides [G_TLS], [G_SSH] ou [G_IPSEC] selon les protocoles utilisés.

l) Dans le cas où l'administration d'une ressource administrée au moyen de protocoles permettant l'authentification et le chiffrement est techniquement impossible, il est recommandé que le prestataire mette en œuvre des mécanismes de chiffrement et d'authentification au niveau applicatif ou IP conformément à [G_TLS], [G_SSH] ou [G_IPSEC], selon les protocoles utilisés, pour l'accès au plus proche de cette ressource depuis le système d'information du service.

m) Le prestataire doit activer et configurer un dispositif de filtrage réseau local sur les serveurs outils d'administration pour n'autoriser que les connexions répondant strictement au besoin opérationnel du service.

n) Le prestataire doit durcir les configurations système et applicative des serveurs outils.

o) Il est recommandé que le prestataire s'appuie sur les guides de durcissement [G_LINUX] ou Windows [G_WINDOWS_1], [G_WINDOWS_2], [G_WINDOWS_3] de l'ANSSI pour le durcissement des configurations système des serveurs outils.

p) Le prestataire doit s'assurer que les serveurs outils d'administration ne disposent que des logiciels et fonctions nécessaires au strict besoin opérationnel du service.

Dans le cas où des clients lourds ou des outils d'administration doivent être présents sur un poste d'administration ou de maintenance pour des besoins opérationnels, les exigences suivantes doivent être respectées :

q) Le prestataire doit installer les clients lourds ou outils d'administration dans une ou plusieurs machines virtuelles, dédiées par commanditaire, hébergées par un hyperviseur tel que défini dans la section IV.2.7.

r) Les machines virtuelles hébergeant les clients lourds ou outils d'administration doivent respecter les exigences IV.2.7.n), IV.2.7.m), IV.2.7.j), IV.2.7.l), IV.2.7.o).

s) Dans le cas où l'exécution des clients lourds ou outils d'administration nécessite des privilèges d'administration, le prestataire doit s'assurer que l'administrateur PAMS utilise un compte de service dédié qui ne permet pas l'exécution interactive de commandes système.

IV.2.9. Interconnexions et systèmes d'échange sécurisés

IV.2.9.1. Zone d'échange prestataire

Pour le bon fonctionnement du service, le prestataire peut être amené à échanger des informations avec d'autres zones de son système d'information (extérieures au système d'information du service). La « zone d'échange prestataire » vise à garantir la sécurité de tels échanges. Elle ne constitue en aucun cas un espace de stockage partagé pérenne, mais bien un espace d'échanges où les données ne sont hébergées que de manière éphémère.

a) Le prestataire doit s'assurer que tous les flux entre le système d'information du service et les autres zones de son système d'information transitent par la zone d'échange prestataire.

b) Le prestataire doit s'assurer que seuls les flux correspondant au strict besoin opérationnel des échanges de fichiers ou de texte entre le système d'information du service et les autres zones du système d'information du prestataire (extérieures au système d'information du service) sont autorisés et transitent par les dispositifs de filtrage internes et périmétriques du système d'information du service.

c) Le prestataire doit dédier un ou plusieurs dispositifs de filtrage périmétrique à la zone d'échange prestataire.

d) Le prestataire doit mettre en œuvre des mécanismes ou dispositifs de chiffrement et d'authentification des flux pour l'accès à la zone d'échange prestataire. Le prestataire doit mettre en œuvre ces mécanismes ou dispositifs en conformité avec le guide [G_IPSEC], le guide [G_TLS] ou le guide [G_SSH].

e) Il est recommandé de dédier les dispositifs de chiffrement et d'authentification des flux à la zone d'échange prestataire.

f) Il est recommandé que les dispositifs de chiffrement et d'authentification des flux reposent sur un ou plusieurs socles physiques dédiés à la zone d'échange prestataire.

g) Il est recommandé que les dispositifs de chiffrement et d'authentification des paquets IP soient des produits qualifiés par l'ANSSI et soient utilisés conformément aux conditions de leur qualification.

h) Le prestataire doit restreindre l'accès à la zone d'échange prestataire aux seuls administrateurs PAMS et aux administrateurs du système d'information du service.

i) Le prestataire doit mettre en place un système d'échange sécurisé dédié au sein de la zone d'échange prestataire (dit « système d'échange prestataire »).

j) Le prestataire doit s'assurer que seuls les flux vers le système d'échange prestataire sont autorisés (le système d'échange prestataire ne peut être à l'origine des flux).

k) Le prestataire doit mettre en place des mécanismes d'authentification au niveau de la zone d'échange prestataire pour l'accès des administrateurs PAMS et des administrateurs du système d'information du service. Ces mécanismes reposent sur des comptes locaux ou un annuaire sans adhérence avec les annuaires des administrateurs PAMS, administrateurs du SI PAMS et les annuaires outils d'administration des commanditaires tels que définis dans le IV.2.10.c).

l) Le prestataire doit s'assurer au sein du système d'échange prestataire que chaque administrateur PAMS et chaque administrateur du système d'information du service ne peuvent accéder qu'aux données placées sous leur périmètre de responsabilité respectif.

m) Le prestataire doit s'assurer que les données sont supprimées du système d'échange prestataire au plus tard 24 heures après leur dépôt.

n) Il est recommandé que le prestataire s'assure de la suppression des données transitant par le système d'échange prestataire une fois le transfert effectué.

o) Le prestataire doit soumettre toutes les données transitant par le système d'échange prestataire à une analyse de contenu à la recherche de codes malveillants.

p) Le prestataire doit mettre en œuvre une traçabilité permettant de journaliser l'horaire de l'échange, l'identité de l'utilisateur du prestataire déposant le fichier ou texte, celle de l'utilisateur ayant les droits d'accès au fichier ou texte et la typologie de la donnée échangée.

q) Le prestataire doit s'assurer que les données, une fois déposées sur le système d'échange prestataire, ne peuvent être accédées que par l'émetteur et les destinataires qu'il aura choisis, en respectant le principe du besoin d'en connaître.

IV.2.9.2. Zone d'échange commanditaire

Pour le bon fonctionnement du service, le prestataire peut être amené à échanger des informations avec le commanditaire (ex. : partage de fichiers, accès à un portail de *ticketing*). La « zone d'échange commanditaire » vise à garantir la sécurité de tels échanges. Elle ne constitue en aucun cas un espace de stockage partagé pérenne, mais bien un espace d'échanges où les données ne sont hébergées que de manière éphémère.

a) Le prestataire doit s'assurer que tous les flux d'échanges entre le commanditaire et le prestataire transitent par la zone d'échange commanditaire (les flux d'administration ne sont pas considérés comme des flux d'échanges).

b) Le prestataire doit dédier un ou plusieurs dispositifs de filtrage périmétrique à la zone d'échange commanditaire.

c) Il est recommandé que le prestataire dédie un ou plusieurs dispositifs de filtrage périmétrique par commanditaire.

d) Le prestataire doit s'assurer que seuls les flux correspondant au strict besoin opérationnel des échanges de données entre le prestataire et le commanditaire sont autorisés et transitent par les dispositifs de filtrage internes et périmétriques du système d'information du service.

e) Le prestataire doit mettre en œuvre des mécanismes ou dispositifs de chiffrement et d'authentification des flux pour tout accès du commanditaire à la zone d'échange commanditaire. Le prestataire doit mettre en œuvre ces mécanismes ou dispositifs en conformité avec le guide [G_IPSEC], le guide [G_TLS] ou le guide [G_SSH].

f) Il est recommandé de dédier les dispositifs de chiffrement et d'authentification des flux à la zone d'échange commanditaire.

g) Il est recommandé que les dispositifs de chiffrement et d'authentification des flux reposent sur un ou plusieurs socles physiques dédiés à la zone d'échange commanditaire.

h) Il est recommandé que les dispositifs de chiffrement et d'authentification des flux soient des produits qualifiés par l'ANSSI et soient utilisés conformément aux conditions de leur qualification.

i) Le prestataire doit mettre en œuvre des mécanismes de rupture et d'analyse des flux au sein de la zone d'échange commanditaire pour les flux externes au système d'information du service accédant à la zone

d'échange commanditaire. Ces mécanismes doivent reposer sur un ou plusieurs socles physiques dédiés à la zone d'échange commanditaire.

j) Le prestataire doit dédier un ou plusieurs mécanismes de rupture et d'analyse des flux par commanditaire.

k) Le prestataire doit restreindre l'accès à la zone d'échange commanditaire aux seuls administrateurs PAMS ainsi qu'aux employés ou applicatifs du commanditaire autorisés selon la convention de service.

l) Le prestataire doit s'assurer que seuls les flux vers la zone d'échange commanditaire sont autorisés (la zone d'échange commanditaire ne peut être à l'origine des flux).

m) Le prestataire doit mettre en place des mécanismes d'authentification au niveau de la zone d'échange commanditaire pour l'accès des administrateurs PAMS et du commanditaire. Ces mécanismes reposent sur des comptes locaux ou un annuaire sans adhérence avec les annuaires des administrateurs PAMS, administrateurs du SI PAMS et les annuaires outils d'administration des commanditaires tels que définis dans le IV.2.10 c).

n) Le prestataire doit s'assurer que, au sein de la zone d'échange commanditaire, chaque administrateur PAMS et chaque employé ou applicatif du commanditaire autorisé ne peut accéder qu'aux données placées sous leur périmètre de responsabilité respectif.

Pour les échanges par fichier, les exigences suivantes doivent être appliquées et les recommandations suivantes peuvent être suivies :

o) Le prestataire doit mettre en place un système d'échange sécurisé dédié par commanditaire au sein de la zone d'échange commanditaire (dit « système d'échange commanditaire »).

p) Le prestataire doit s'assurer que seuls les flux vers les systèmes d'échange commanditaire sont autorisés (un système d'échange commanditaire ne peut être à l'origine des flux).

q) Le prestataire doit s'assurer que les données sont supprimées des systèmes d'échange commanditaire au plus tard 24 heures après leur dépôt.

r) Il est recommandé que le prestataire s'assure de la suppression des données transitant par les systèmes d'échange commanditaire une fois le transfert effectué.

s) Le prestataire doit soumettre toutes les données transitant par les systèmes d'échange commanditaire à une analyse de contenu à la recherche de codes malveillants.

t) Le prestataire doit mettre en œuvre une traçabilité permettant de journaliser l'horaire de l'échange, l'identité de l'utilisateur du commanditaire concerné, celle de l'administrateur PAMS concerné et la typologie de la donnée échangée.

u) Le prestataire doit s'assurer que les données, une fois déposées sur les systèmes d'échange commanditaire, ne peuvent être accédées que par l'émetteur et les destinataires qu'il aura choisis, en respectant le principe du besoin d'en connaître.

IV.2.9.3. Zone d'échange tiers

Pour le bon fonctionnement du service, le prestataire peut être amené à échanger des informations avec des tiers. La « zone d'échange tiers » vise à garantir la sécurité de tels échanges. Elle ne constitue en aucun cas un espace de stockage partagé pérenne, mais bien un espace d'échanges où les données ne sont hébergées que de manière éphémère.

a) Le prestataire doit s'assurer que tous les flux d'échanges entre le système d'information du service et les tiers transitent par la zone d'échange tiers (les flux d'administration ne sont pas considérés comme des flux d'échanges).

b) Le prestataire doit dédier un ou plusieurs dispositifs de filtrage périmétrique à la zone d'échange tiers.

c) Le prestataire doit s'assurer que seuls les flux correspondant au strict besoin opérationnel des échanges de données (fichier, texte, flux vidéo) entre le système d'information du service et le tiers sont autorisés et transitent par les dispositifs de filtrages internes et périmétriques du système d'information du service.

d) Le prestataire doit mettre en œuvre des mécanismes ou dispositifs de chiffrement et d'authentification des flux pour tout accès des tiers à la zone d'échange tiers. Le prestataire doit mettre en œuvre ces mécanismes ou dispositifs en conformité avec le guide [G_IPSEC], le guide [G_TLS] ou le guide [G_SSH].

e) Il est recommandé de dédier les dispositifs de chiffrement et d'authentification des flux pour l'accès à la zone d'échange tiers.

f) Il est recommandé que le dispositif de chiffrement et d'authentification des flux repose sur un ou plusieurs socles physiques dédiés à la zone d'échange tiers.

g) Il est recommandé que les dispositifs de chiffrement et d'authentification des flux soient des produits qualifiés par l'ANSSI et soient utilisés conformément aux conditions de leur qualification.

h) Le prestataire doit mettre en œuvre des mécanismes de rupture et d'analyse des flux au sein de la zone d'échange tiers pour les flux externes au système d'information du service accédant à la zone d'échange tiers.

i) Le prestataire doit dédier les mécanismes de rupture et d'analyse des flux à la zone d'échange tiers. Les mécanismes doivent reposer sur un ou plusieurs socles physiques dédiés à la zone d'échange tiers ou prendre la forme d'une instance dédiée sur un socle physique commun avec les mécanismes de rupture et d'analyse de flux de la zone d'accès à Internet.

j) Il est recommandé que les mécanismes de rupture et d'analyse protocolaire reposent sur un ou plusieurs socles physiques dédiés à la zone d'échange tiers.

k) Le prestataire doit restreindre l'accès à la zone d'échange tiers aux administrateurs PAMS, administrateurs du système d'information du service ainsi qu'aux tiers autorisés selon les conventions de service.

l) Le prestataire doit mettre en place des mécanismes d'authentification au niveau de la zone d'échange tiers pour l'accès des administrateurs PAMS, administrateurs du système d'information du service et des tiers autorisés. Ces mécanismes reposent sur des comptes locaux ou un annuaire dédié aux zones d'échange tiers et d'enclaves d'administration tierces.

m) Le prestataire doit renouveler les secrets d'authentification des tiers à l'issue de chaque accès ou à une fréquence au minimum mensuelle et ne communiquer les nouveaux secrets que lorsqu'un accès à la zone est requis par le tiers concerné.

n) Le prestataire doit mettre en place un système d'échange sécurisé dédié au sein de la zone d'échange tiers (dit « système d'échange tiers »).

o) Le prestataire doit s'assurer que seuls les flux vers le système d'échange tiers sont autorisés (le système d'échange tiers ne peut être à l'origine des flux).

p) Le prestataire doit s'assurer au sein du système d'échange tiers que chaque administrateur PAMS, administrateur du système d'information du service ou tiers authentifiés ne peuvent accéder qu'aux données sous leur périmètre de responsabilité respectif.

q) Le prestataire doit s'assurer que les données sont supprimées du système d'échange tiers au plus tard 24 heures après leur dépôt.

r) Il est recommandé que le prestataire s'assure de la suppression des données transitant par le système d'échange tiers une fois le transfert effectué.

s) Le prestataire doit soumettre toutes les données transitant par le système d'échange tiers à une analyse de contenu à la recherche de codes malveillants.

t) Le prestataire doit mettre en œuvre une traçabilité permettant de journaliser l'horaire de l'échange, l'identité du tiers concerné (personne physique ou entité), l'administrateur concerné et la typologie de la donnée échangée.

u) Le prestataire doit s'assurer que les données, une fois déposées sur le système d'échange tiers, ne peuvent être accédées que par l'émetteur et les destinataires qu'il aura choisis, en respectant le principe du besoin d'en connaître.

IV.2.9.4. Zone d'accès à Internet

Pour le bon fonctionnement du service, le prestataire peut être amené à télécharger des mises à jour depuis les sites des éditeurs sur Internet ou à réaliser des prestations d'administration de système d'information dans le *cloud* public. La « zone d'accès à Internet » vise à garantir la sécurité de tels échanges.

a) Le prestataire doit s'assurer que tous les flux depuis le système d'information du service et à destination d'Internet transitent par la zone d'accès à Internet.

b) Le prestataire doit dédier un ou plusieurs dispositifs de filtrage périmétrique à la zone d'accès à Internet.

c) Le prestataire doit s'assurer que les flux transitant par la zone d'accès à Internet sont initialisés depuis les zones du système d'information du service pour lesquels le besoin opérationnel le justifie.

d) Le prestataire doit s'assurer que seuls les flux sortants de la zone d'accès à Internet vers Internet et correspondant au strict besoin opérationnel du service sont autorisés et transitent par un dispositif de filtrage périmétrique du système d'information du service.

e) Le prestataire doit mettre en place des mécanismes d'authentification pour les accès à la zone d'accès à Internet. Ces mécanismes reposent sur des comptes locaux ou un annuaire sans adhérence avec les annuaires des administrateurs PAMS, administrateurs du SI PAMS et les annuaires outils d'administration des commanditaires tels que définis dans le IV.2.10 c).

f) Le prestataire doit mettre en œuvre des mécanismes de rupture et d'analyse des flux au sein de la zone d'accès à Internet.

g) Le prestataire doit dédier les mécanismes de rupture et d'analyse des flux à la zone d'accès à Internet. Les mécanismes doivent reposer sur un ou plusieurs socles physiques dédiés à la zone d'accès à Internet ou prendre la forme d'une instance dédiée sur un socle physique commun avec les mécanismes de rupture et d'analyse des flux de la zone d'échange tiers.

h) Le prestataire doit analyser les flux de moindre confiance transitant par la zone d'accès à Internet en vue de détecter des codes malveillants et de s'assurer de la conformité protocolaire des échanges.

L'évaluation du niveau de confiance accordé à chaque flux s'appuie sur les résultats issus de l'appréciation des risques (IV.2.1.a)).

i) Le prestataire doit mettre en œuvre des mécanismes de filtrage applicatif sortant par liste blanche.

j) Le prestataire doit dédier les mécanismes de filtrage applicatif à la zone d'accès à Internet.

k) Le prestataire doit élaborer et tenir à jour la liste blanche de sorte à n'autoriser que l'accès aux ressources Web correspondant au strict besoin opérationnel du service.

l) Il est recommandé que le prestataire respecte les recommandations de l'ANSSI [G_INTERNET] pour la mise en œuvre de la zone d'accès à Internet.

IV.2.9.5. Zone d'accès aux ressources administrées

Le prestataire peut être amené à administrer des ressources du commanditaire hébergées dans ses locaux ou à distance. Les flux d'administration pourraient transiter par des réseaux de transport tiers dont la sécurité n'est maîtrisée ni par le prestataire ni par le commanditaire. La « zone d'accès aux ressources administrées » vise à assurer l'interconnexion avec les ressources administrées et *in fine* à garantir la sécurité de tels échanges.

a) Le prestataire doit s'assurer que tous les flux entre le système d'information du service et les ressources administrées (hors ressources dont les outils d'administration sont exclusivement exposés sur Internet ou ressources non administrables à distance) transitent par la zone d'accès aux ressources administrées.

b) Le prestataire doit s'assurer que seuls des flux entre le système d'information du service et les ressources administrées transitent par la zone d'accès aux ressources administrées.

c) Le prestataire doit dédier un ou plusieurs dispositifs de filtrage périmétrique à la zone d'accès aux ressources administrées.

d) Le prestataire doit s'assurer que les flux transitant par la zone d'accès aux ressources administrées sont initialisés depuis les zones du système d'information du service pour lesquelles le besoin opérationnel le justifie.

e) Le prestataire doit s'assurer que seuls les flux entre la zone d'accès aux ressources administrées et le système d'information administré du commanditaire correspondant au strict besoin opérationnel du service sont autorisés et transitent par un dispositif de filtrage périmétrique du système d'information du service.

Pour les accès à distance aux ressources administrées à travers un réseau tiers, les exigences suivantes doivent être appliquées et les recommandations suivantes peuvent être suivies :

f) Le prestataire doit mettre en œuvre dans le SI PAMS des dispositifs de chiffrement et d'authentification des paquets IP pour l'accès aux ressources administrées. Le prestataire doit mettre en œuvre ces dispositifs en conformité avec le guide [G_IPSEC].

g) A la demande du commanditaire, le prestataire doit pouvoir être en mesure de mettre en œuvre un socle physique dédié par niveau de sensibilité des systèmes d'information administrés pour les dispositifs de chiffrement et d'authentification des paquets IP.

h) Le prestataire doit dédier par commanditaire des dispositifs de chiffrement et d'authentification des paquets IP.

i) Il est recommandé que les dispositifs de chiffrement et d'authentification des paquets IP reposent sur un ou plusieurs socles physiques dédiés à la zone d'accès aux ressources administrées.

j) Il est recommandé que les dispositifs de chiffrement et d'authentification des paquets IP soient des produits qualifiés par l'ANSSI et soient utilisés conformément aux conditions de leur qualification.

IV.2.9.6. Zone d'accès distants

Pour le bon fonctionnement du service, le prestataire peut être amené à effectuer des actions d'administration en situation de nomadisme selon les modalités précisées en IV.2.11. La « zone d'accès distants » vise à réduire les risques inhérents aux accès des administrateurs PAMS ou administrateurs du système d'information du service en situation de nomadisme.

a) Le prestataire doit dédier la zone d'accès distants pour l'accès exclusif des postes d'administration ou de maintenance en situation de nomadisme.

b) Le prestataire doit s'assurer que tous les accès des administrateurs PAMS ou administrateurs du système d'information du service en situation de nomadisme transitent par la zone d'accès distants.

c) Le prestataire doit dédier un ou plusieurs dispositifs de filtrage périmétrique à la zone d'accès distants.

d) Le prestataire doit s'assurer que seuls les flux correspondant aux accès des postes d'administration ou de maintenance en situation de nomadisme sont autorisés et transitent par un dispositif de filtrage périmétrique du système d'information du service.

e) Le prestataire doit cloisonner les accès distants des administrateurs PAMS d'une part et les accès distants des administrateurs du système d'information du service d'autre part.

f) Le prestataire doit mettre en œuvre des dispositifs de chiffrement et d'authentification des paquets IP pour l'accès des postes d'administration ou de maintenance en situation de nomadisme à la zone d'accès distants. Le prestataire doit mettre en œuvre ces dispositifs en conformité avec le guide [G_IPSEC].

g) Il est recommandé que les dispositifs de chiffrement et d'authentification des paquets IP soient des produits qualifiés par l'ANSSI et soient utilisés conformément aux conditions de leur qualification.

h) En situation de nomadisme, le prestataire doit mettre en place des mécanismes d'authentification dédiés au dispositif de chiffrement et d'authentification des paquets IP, sans adhérence avec les annuaires des administrateurs PAMS, administrateurs du SI PAMS et les annuaires outils d'administration des commanditaires tels que définis dans le IV.2.10 c).

i) Il est recommandé que les mécanismes d'authentification reposent sur des certificats électroniques délivrés par l'infrastructure définie en IV.2.10.n).

j) Il est recommandé que les mécanismes d'authentification reposent sur des certificats électroniques délivrés par des prestataires de services de certification électronique qualifiés par l'ANSSI [CRYPTO_A7].

k) Le prestataire doit mettre en place une journalisation des accès à la zone d'accès distants. Il doit effectuer une revue mensuelle des accès (comptes autorisés et journaux d'accès) à la zone d'accès distants.

IV.2.9.7. Zone des enclaves d'administration tierce

Pour le bon fonctionnement du service, le commanditaire peut être amené à solliciter l'intervention exceptionnelle d'administrateurs tiers sur son système d'information (par exemple un support éditeur) et

souhaiter encadrer la sécurité de cette intervention en s'appuyant sur son prestataire d'administration et de maintenance sécurisées. Il peut en être de même pour le prestataire s'agissant de l'administration du système d'information du service. La zone des enclaves d'administration tierce vise à réduire les risques inhérents à de telles interventions.

a) Le prestataire doit mettre en œuvre des serveurs physiquement dédiés à la zone des enclaves d'administration tierce et, en cas de recours à la virtualisation, des serveurs d'hypervision physiquement dédiés à la zone des enclaves d'administration tierce. Les dispositifs de filtrage (IV.2.6.f)) et les dispositifs de chiffrement et authentification des paquets IP (IV.2.6.l)) font l'objet d'exigences et recommandations spécifiques et ne sont donc pas traités par la présente exigence.

b) Le prestataire doit dédier un ou plusieurs dispositifs de filtrage périmétrique à la zone des enclaves d'administration tierce.

c) Le prestataire doit mettre en œuvre des infrastructures de stockage physiquement dédiées à la zone des enclaves d'administration tierce.

d) Le prestataire doit dédier une enclave d'administration tierce à chaque commanditaire ayant demandé la mise à disposition d'une enclave d'administration tierce (dite « enclave d'administration tierce commanditaire »).

e) Le prestataire doit dédier une enclave d'administration tierce pour les administrateurs tiers intervenant sur le système d'information du service (dite « enclave d'administration tierce prestataire »).

f) Le prestataire doit mettre en œuvre avec le commanditaire une procédure organisationnelle encadrant l'accès des administrateurs tiers à l'enclave d'administration tierce commanditaire et *in fine* aux ressources administrées du commanditaire.

g) Le prestataire doit mettre en œuvre une procédure organisationnelle encadrant l'accès des administrateurs tiers à l'enclave d'administration tierce prestataire et *in fine* aux ressources administrées du système d'information du service.

h) Le prestataire doit s'assurer que seuls les flux correspondant à l'accès d'administrateurs tiers aux enclaves d'administration tierce sont autorisés et transitent par un dispositif de filtrage périmétrique du système d'information du service.

i) Le prestataire doit mettre en œuvre des dispositifs de chiffrement et d'authentification des paquets IP pour l'accès aux enclaves d'administration tierce. Le prestataire doit mettre en œuvre ces dispositifs en conformité avec le guide [G_IPSEC], le guide [G_TLS] ou le guide [G_SSH].

j) Le prestataire doit dédier un dispositif de chiffrement et d'authentification des paquets IP à chaque enclave d'administration tierce.

k) Il est recommandé que le prestataire mette en œuvre un ou plusieurs dispositifs de chiffrement et d'authentification des paquets IP dédiés physiquement à la zone des enclaves d'administration tierce.

l) Il est recommandé que les dispositifs de chiffrement et d'authentification des paquets IP soient des produits qualifiés par l'ANSSI et soient utilisés conformément aux conditions de leur qualification.

m) Le prestataire doit mettre en place des mécanismes d'authentification au niveau de la zone des enclaves d'administration tierce pour l'accès des administrateurs tiers. Ces mécanismes reposent sur des comptes locaux ou un annuaire dédié aux zones d'échange tiers et d'enclaves d'administration tierces.

n) Le prestataire doit mettre en œuvre une traçabilité nominative pour les accès des administrateurs tiers, que les comptes utilisés soient individuels (associés à une unique personne physique) ou génériques.

o) Le prestataire doit activer à la demande les comptes des administrateurs tiers pour la connexion à chaque enclave d'administration tierce. Le prestataire doit désactiver ces comptes à la fin de chaque intervention.

p) Le prestataire doit mettre en œuvre une supervision des comptes des administrateurs tiers afin de détecter et alerter en cas de compte actif pendant une durée supérieure à 24 heures.

q) Il est recommandé de mettre en œuvre une authentification double facteur pour l'accès des administrateurs tiers.

r) Le prestataire doit renouveler les secrets d'authentification des tiers, au moins tous les sept jours dans le cas d'une authentification simple facteur et dans un délai défini formellement dans le cas d'une authentification double facteur. Ces secrets renouvelés ne sont communiqués aux tiers que lors de leur prochaine intervention.

s) Le prestataire doit mettre en œuvre un rebond au sein de la chaîne d'accès aux ressources administrées. Ce rebond doit être dédié à chaque enclave d'administration tierce et doit y être hébergé.

t) Le prestataire doit s'assurer de la suppression du rebond à l'issue de l'intervention, puis de sa nouvelle instanciation dans sa configuration initiale dès que nécessaire.

u) Le prestataire doit assurer une traçabilité des accès aux ressources administrées réalisés au travers de chaque enclave d'administration tierce.

v) Le prestataire doit s'assurer que les actions d'administration de l'administrateur tiers respectent les exigences de la partie IV.2.12.

IV.2.10. Identification, authentification et droits d'administration

a) Le prestataire doit mettre en place, au sein de la ou les zone(s) d'infrastructure, au minimum un annuaire centralisé et dédié à l'authentification des administrateurs PAMS et des administrateurs du système d'information du service, permettant en particulier l'authentification sur l'ensemble des ressources du système d'information du service dont les postes d'administration ou de maintenance.

b) Le prestataire doit assurer un cloisonnement logique des populations administrateurs PAMS et administrateurs du système d'information du service au sein de l'annuaire centralisé, pour l'authentification, et la gestion des autorisations.

c) Le prestataire doit mettre en place des mécanismes d'authentification pour l'authentification des administrateurs PAMS sur les outils d'administration dont il maîtrise le référentiel d'identité. Ces mécanismes reposent sur des comptes locaux ou un annuaire sans adhérence avec :
   - L'annuaire centralisé utilisé pour l'authentification des administrateurs PAMS et administrateurs du SI du service ;
   - Les annuaires des autres commanditaires, utilisés pour l'administration du système d'information du commanditaire.

d) Le prestataire doit s'assurer que les administrateurs PAMS et les administrateurs du système d'information du service n'ont les droits d'accès qu'aux ressources utiles (par exemple : postes de rebonds, serveurs outils d'administration, répertoires partagés, etc.) dans le cadre de leur prestation.

e) Le prestataire doit attribuer de façon individuelle les comptes aux administrateurs PAMS et administrateurs du système d'information du service. Toute exception doit être assortie d'un mécanisme de journalisation permettant d'associer à chaque instant et sans ambiguïté un compte générique et une personne physique.

f) Le prestataire doit s'assurer que les comptes de service ne sont utilisés que pour répondre à un besoin opérationnel spécifique et sont effectifs sur le seul périmètre associé à ce besoin.

g) Le prestataire doit identifier pour chaque compte de service un administrateur ou une équipe d'administrateurs responsable de son cycle de vie.

h) Le prestataire doit s'assurer que l'authentification d'un administrateur PAMS ou d'un administrateur du système d'information du service sur un poste d'administration ou de maintenance est réalisée via une authentification double facteur.

i) Le prestataire doit déployer un outil de gestion sécurisée des mots de passe sur les postes d'administration ou de maintenance.

j) Il est recommandé que l'outil de gestion sécurisée des mots de passe dispose d'un visa de sécurité de l'ANSSI.

k) Le prestataire doit s'assurer que les mots de passe portés à la connaissance des administrateurs sont stockés exclusivement dans un outil de gestion sécurisée des mots de passe.

l) Il est recommandé de cloisonner par commanditaire les mots de passe stockés dans un outil de gestion sécurisée des mots de passe.

m) Le prestataire doit modifier les secrets par défaut des équipements ou services utilisés au sein du système d'information du service au moment de l'installation.

n) Le prestataire doit mettre en œuvre une infrastructure de gestion de clés hébergée dans la zone d'infrastructure du système d'information du service ou avoir recours à un prestataire de service de certification électronique qualifié par l'ANSSI [CRYPTO_A7] pour la réalisation de l'authentification à base de certificats au sein du système d'information du service.

o) Il est recommandé que l'infrastructure de gestion de clés soit dédiée au système d'information du service.

p) Le prestataire doit configurer la génération des certificats selon les exigences de l'ANSSI [CRYPTO_B1], [CRYPTO_B2].

q) Il est recommandé que le prestataire mette en place et utilise un outil, dédié au service, permettant la gestion centralisée de l'ensemble des annuaires dont il a la responsabilité.

Les exigences suivantes sont à appliquer à tous les annuaires dont le prestataire a la responsabilité :

r) Le prestataire doit désactiver les comptes dès le départ ou la suspension d'un administrateur PAMS ou d'un administrateur du système d'information du service ; puis ces comptes doivent être supprimés au terme d'un délai raisonnable à définir formellement dans le respect de la réglementation et des besoins opérationnels de réponse aux incidents de sécurité.

s) Il est recommandé que les comptes désactivés soient retirés des groupes à privilèges dont ils faisaient partie et qu'un mot de passe long déterminé aléatoirement lui soit attribué.

t) Le prestataire doit mettre en place un processus de gestion des secrets d'authentification conformément à la politique de sécurité du système d'information du service.

u) Le prestataire doit générer des secrets d'authentification conformes aux recommandations de l'ANSSI [CRYPTO_B3].

v) Le prestataire doit garantir que les secrets utilisés sont à destination unique et ne peuvent en aucun cas être mutualisés, notamment d'un annuaire à l'autre.

IV.2.11. Situation de nomadisme

a) Le prestataire doit mettre en œuvre et tenir à jour une liste des administrateurs PAMS et des administrateurs du système d'information du service possédant un poste d'administration ou de maintenance nomade.

b) Le prestataire doit sensibiliser aux bonnes pratiques de sécurité liées au nomadisme les administrateurs possédant un poste d'administration ou de maintenance nomade.

c) Le prestataire doit interdire toute activité d'administration ou de maintenance de systèmes d'information d'importance vitale en situation de nomadisme. Cette interdiction peut faire l'objet d'un processus dérogatoire validé par le commanditaire.

d) Le prestataire doit, par défaut, interdire tout accès à la zone d'infrastructure par les administrateurs du système d'information du service en situation de nomadisme. Cette interdiction de principe pourra faire l'objet de dérogations lors de situations exceptionnelles et temporaires.

e) Le prestataire doit mettre en œuvre des mesures techniques et organisationnelles permettant de s'assurer que les opérations d'administration en situation de nomadisme sont réalisées uniquement depuis le domicile de l'administrateur ou bien depuis un lieu privé non ouvert au public et autorisé explicitement par le client. Une procédure de contrôle régulier doit être établie par le prestataire.

f) Le prestataire doit mettre en œuvre un mécanisme d'alerte lorsque des serveurs de la zone d'infrastructure sont accédés par des administrateurs du système d'information du service en dehors des locaux du prestataire.

g) Le prestataire doit être en mesure de bloquer l'accès du poste d'administration ou de maintenance nomade au reste du système d'information du service au plus tard deux heures après sa déclaration de perte ou de vol.

h) Dans l'hypothèse où un poste déclaré perdu ou volé est retrouvé, le prestataire doit réinitialiser le poste conformément à l'exigence IV.2.7.e) dès qu'il y a suspicion d'altération de son intégrité.

i) Il est recommandé qu'un poste déclaré perdu ou volé, retrouvé et pour lequel il y a suspicion d'altération de son intégrité soit désengagé du système d'information du service.

j) Le prestataire doit s'assurer qu'en dehors de ses locaux (zones privées ou sensibles définies en IV.2.3), les postes d'administration ou de maintenance nomades ne peuvent communiquer qu'avec la zone d'accès distants ; les postes doivent être configurés pour ne pouvoir communiquer qu'avec le dispositif dédié de chiffrement et d'authentification des paquets IP de la zone d'accès distants, via un tunnel IPsec (IV.2.9.6.f)).

IV.2.12. Accès aux ressources administrées

IV.2.12.1. Système d'information du commanditaire dont les outils d'administration sont exclusivement exposés sur Internet

Dans le cas où les ressources administrées ne possèdent que des outils d'administration exposés sur Internet (ex : consoles d'administration de services en *cloud* public) :

a) Il est recommandé de mettre en œuvre un dispositif d'authentification et de chiffrement des paquets IP pour la sécurisation des flux d'administration des ressources dont les outils d'administration sont exclusivement exposés sur Internet.Dans ce cas, ces dispositifs doivent mettre en œuvre un tunnel IPsec conforme avec le guide [G_IPSEC].

b) Le prestataire doit mettre en œuvre une infrastructure de postes de rebond dédiés à l'accès aux ressources administrées. Cette infrastructure est hébergée dans une zone de serveurs outils dédiée.

c) Le prestataire doit s'assurer que toutes les actions d'administration à destination d'outils d'administration exclusivement exposés sur Internet sont effectuées via la zone d'accès à Internet, depuis les postes de rebond.

d) Le prestataire doit s'assurer au minimum de façon quotidienne de la suppression et de la nouvelle instanciation dans la configuration initiale des postes de rebond utilisés pour l'administration de systèmes d'information dont les outils d'administration sont exposés sur Internet.

e) Le prestataire doit assurer une traçabilité nominative des accès aux ressources administrées et actions d'administration réalisés au travers de la zone d'accès à Internet.

IV.2.12.2. Système d'information du commanditaire non administrable à distance

Dans le cas où les ressources administrées ne sont pas administrables à distance et nécessitent un accès physique aux ressources :

a) Le prestataire doit tracer formellement l'ensemble des actions d'administration ou de maintenance réalisées.

Lorsque le prestataire utilise un ou plusieurs systèmes de stockage amovibles pour ses actions d'administration ou de maintenance, les exigences suivantes doivent être appliquées et la recommandation suivante peut être suivie :

b) Le prestataire doit dédier physiquement, par commanditaire, un ou plusieurs systèmes de stockage amovibles.

c) Le prestataire doit décontaminer tout système de stockage amovible au travers d'une station de décontamination, à chaque connexion dudit système sur le système d'information du commanditaire.

d) Le prestataire doit maintenir à jour la station de décontamination et toutes les briques logicielles qui la composent.

e) Le prestataire doit héberger la station de décontamination au sein d'une zone privée.

f) Il est recommandé de limiter au strict minimum l'emploi des systèmes de stockage amovibles.

Afin de traiter le cas dans lequel le prestataire fournit le poste utilisé pour réaliser les actions d'administration ou de maintenance, le prestataire doit respecter les exigences suivantes :

g) Le prestataire doit s'assurer que le poste d'administration ou de maintenance utilisé pour l'administration des systèmes d'information non administrables à distance répond aux exigences des sections IV.2.7 et IV.2.8.q), IV.2.8.r), IV.2.8.s).

h) Dans le cas où des clients lourds ou des outils d'administration doivent être présents sur un poste d'administration ou de maintenance pour des besoins opérationnels, le prestataire doit s'assurer que les administrateurs PAMS, entre chaque intervention, restaurent à leur état d'origine les machines virtuelles utilisées pour réaliser les actions d'administration ou de maintenance. Il est à noter que l'administration ou la maintenance de deux composants isolés pour le compte d'un même commanditaire correspond à deux interventions distinctes.

IV.2.12.3. Système d'information du commanditaire administrable à distance (hors cloud computing)

Dans les cas non couverts par les paragraphes IV.2.12.1 et IV.2.12.2 :

a) Le prestataire doit s'assurer que toute action d'administration d'un système d'information du commanditaire administrable à distance est effectuée via la zone d'accès aux ressources administrées.

b) Le prestataire doit assurer une traçabilité nominative des accès aux ressources administrées et actions d'administration réalisés au travers de la zone d'accès aux ressources administrées.

IV.2.13. Administration du système d'information du service

a) Le prestataire doit mettre à disposition des administrateurs du système d'information du service des postes d'administration sous sa maîtrise et dédiés exclusivement aux actions d'administration et de maintenance du système d'information du service. Ces postes doivent être conformes aux exigences de la section IV.2.7.

b) Le prestataire doit héberger les serveurs de la zone d'administration du système d'information du service sur un ou plusieurs socles physiques dédiés.

c) Le prestataire doit mettre en œuvre des serveurs outils d'administration dédiés à l'administration du système d'information du service.

d) Le prestataire doit accéder aux outils d'administration du système d'information du service en utilisant des protocoles permettant l'authentification et le chiffrement au niveau applicatif en conformité avec les guides [G_TLS] ou [G_SSH] selon les protocoles utilisés, ou à défaut au niveau IP en conformité avec le guide [G_IPSEC].

e) Le prestataire doit accéder aux ressources administrées du système d'information du service en utilisant des protocoles permettant l'authentification et le chiffrement applicatif ou, à défaut au niveau IP.

f) Le prestataire doit activer et configurer un mécanisme de filtrage réseau local sur les serveurs outils d'administration pour n'autoriser que les connexions répondant strictement au besoin opérationnel des actions d'administration ou de maintenance du système d'information du service.

g) Il est recommandé que le prestataire cloisonne physiquement le réseau d'administration du système d'information du service.

h) Le prestataire doit déployer sur les serveurs outils d'administration les logiciels et fonctions nécessaires au strict besoin opérationnel des actions d'administration ou de maintenance du système d'information du service.

i) Le prestataire doit durcir les configurations système et applicative des serveurs outils d'administration du système d'information du service.

j) Si le prestataire héberge tout ou partie du système d'information du service dans un *cloud* public, alors ce cloud public doit être qualifié SecNumCloud[2] [SecNumCloud].

k) Il est recommandé que le prestataire s'appuie sur les guides de durcissement [G_LINUX] ou Windows [G_WINDOWS_1], [G_WINDOWS_2], [G_WINDOWS_3] de l'ANSSI pour le durcissement des configurations système des serveurs outils d'administration du système d'information du service.

l) Il est recommandé que les administrateurs du système d'information du service n'opèrent pas d'actions d'administration ou de maintenance sur les systèmes d'information des commanditaires.

IV.2.14. Territorialité du service

a) Le prestataire doit héberger et traiter les données relatives au service d'administration et de maintenance sécurisées exclusivement au sein d'un État de l'Union Européenne.

b) Le prestataire doit exploiter et administrer le service d'administration et de maintenance sécurisées exclusivement depuis un État de l'Union Européenne.

c) Le prestataire doit documenter et communiquer à la demande du commanditaire la localisation du stockage et du traitement de ses données à sa disposition (documents d'architecture, éléments de configuration, informations d'authentification, etc.).

IV.2.15. Sécurité des actions de support effectuées depuis un État en dehors de l'Union Européenne

Le prestataire peut réaliser des actions de support pour les systèmes d'information administrés des commanditaires depuis un État hors de l'Union Européenne.

a) Le prestataire doit documenter la liste des actions de support qui peuvent être effectuées par des administrateurs PAMS depuis un État en dehors de l'Union Européenne, et les mécanismes permettant d'en assurer le contrôle d'accès et la supervision depuis un État de l'Union Européenne.

IV.2.15.1. Scripts de support

a) Le prestataire doit mettre en œuvre des scripts de support pour la réalisation de chacune des actions de support par des administrateurs PAMS depuis un État en dehors de l'Union Européenne.

b) Le prestataire doit s'assurer que les scripts de support sont validés formellement par un personnel du prestataire localisé dans un État de l'Union Européenne.

c) Le prestataire doit s'assurer que les scripts de support ne permettent pas, même indirectement, de transférer des données du commanditaire à l'extérieur d'un État de l'Union Européenne.

d) Le prestataire doit réaliser un audit du code des scripts de support à chaque mise à jour majeure, afin de s'assurer de sa sécurité et de la pertinence de ses actions.

[2] Le catalogue des prestataires de service d'informatique en nuage (SecNumCloud) qualifiés par l'ANSSI est publié sur le site Web de l'ANSSI.

IV.2.15.2. Conditions de réalisation des actions de support

a) Le prestataire doit mettre à disposition un poste d'administration ou de maintenance nomade pour les administrateurs PAMS intervenant depuis un État hors de l'Union Européenne, et ce pour la réalisation exclusive des actions de support.

b) Le prestataire doit s'assurer que les scripts de support sont exécutés sur les infrastructures du service hébergées dans un État de l'Union Européenne.

c) Le prestataire doit mettre en œuvre des moyens de s'assurer :
   - que les scripts de support sont le moyen exclusif de réalisation des actions de support ;
   - qu'aucun accès interactif avec les ressources administrées n'est autorisé aux administrateurs PAMS intervenant depuis un État en dehors de l'Union Européenne.

d) Le prestataire doit s'assurer que les administrateurs PAMS intervenant depuis un État en dehors de l'Union Européenne ne peuvent pas modifier les scripts de support.

IV.2.15.3. Journalisation des actions de support

a) Le prestataire doit s'assurer que les actions de support réalisées par les scripts de support sont journalisées. Les événements journalisés doivent inclure :
   - le compte ayant lancé le script de support ;
   - les comptes ayant exécuté les actions de support ;
   - l'horodatage des actions de support ;
   - les ressources administrées concernées par les scripts de support ;
   - la description des actions de support réalisées et les résultats du script de support.

b) Le prestataire doit s'assurer que les journaux sont signés avec une autorité de certification et que leur sauvegarde est hébergée dans le système d'information du service. Le prestataire doit s'assurer que les journaux respectent les exigences IV.2.5.c), IV.2.5.f), IV.2.5.g), IV.2.5.h), IV.2.5.i), IV.2.5.m), IV.2.5.n).

c) Le prestataire doit s'assurer que la durée de rétention des journaux est la durée maximum autorisée par la législation (IV.2.5.c).

IV.3. Organisation du prestataire et gouvernance

IV.3.1. Charte éthique et recrutement

a) Le prestataire doit procéder à une vérification des formations, qualifications, références professionnelles des candidats pour le service et de la véracité de leur curriculum vitae préalablement à leur embauche.

b) Le prestataire doit demander aux candidats pour le service de lui fournir une preuve qu'ils ne font pas l'objet d'une inscription, qui n'est pas incompatible avec l'exercice de ses fonctions, au bulletin n°3 du casier judiciaire français ou un extrait de casier judiciaire étranger pour les candidats résidant hors du territoire français.

c) Les administrateurs PAMS et les administrateurs du système d'information du service doivent être liés contractuellement avec le prestataire ou avec un de ses sous-traitants dans le cas de la sous-traitance d'une partie de son activité.

d) Le prestataire doit disposer d'une charte d'éthique intégrée, prévoyant notamment que :
   - les prestations sont réalisées avec loyauté, discrétion, impartialité et dans des conditions de confidentialité des informations traitées ;
   - les personnels ne recourent qu'aux méthodes, outils et techniques validés par le prestataire ;
   - les personnels s'engagent à ne pas divulguer d'informations à un tiers, même anonymisées et décontextualisées, obtenues ou générées dans le cadre de la prestation sauf autorisation définie dans le cadre de la convention de service ;
   - les personnels s'engagent à signaler au prestataire tout contenu manifestement illicite découvert pendant la prestation ;
   - les personnels s'engagent à respecter la législation et la réglementation IV.3.4.e) en vigueur et les bonnes pratiques liées à leurs activités.

e) Le prestataire doit faire signer à l'ensemble des personnes impliquées dans la fourniture du service la charte d'éthique prévue à l'exigence précédente et préalablement à la réalisation de la prestation.

f) Le prestataire doit documenter et mettre en œuvre un processus disciplinaire applicable à l'ensemble des personnes impliquées dans la fourniture du service ayant enfreint la politique de sécurité.

g) Le prestataire doit, sur demande d'un commanditaire, lui rendre accessibles les sanctions encourues en cas d'infraction à la politique de sécurité.

h) Le prestataire doit élaborer et mettre en œuvre un plan de sensibilisation de son personnel à la sécurité des systèmes d'information et des mesures de sécurité associées.

IV.3.2. Organisation et gestion des compétences

a) Le prestataire doit disposer d'une équipe :
   - permettant la réalisation du service ;
   - disposant des compétences associées à ses missions.

b) Le prestataire doit définir et formaliser la liste exhaustive :
   - des différents rôles d'administrateur PAMS et des missions associées ;
   - des différents rôles d'administrateurs du système d'information du service et des missions associées.

   Les rôles définis doivent respecter les principes du moindre privilège et du besoin d'en connaître.

c) Le prestataire doit documenter et mettre en œuvre un plan de formation concernant la sécurité de l'information adapté au service et aux missions des personnels.

d) Il est recommandé que la formation à destination des administrateurs PAMS de systèmes industriels soit conforme au guide pour une formation sur la cybersécurité des systèmes industriels [FORMATION_SI_INDUS].

e) Le responsable de la sécurité des systèmes d'information du prestataire doit valider formellement le plan de formation concernant la sécurité de l'information.

f) Le prestataire doit élaborer et mettre à disposition des administrateurs PAMS les guides d'exploitation des zones du système d'information du service (IV.2.6.a).

g) Le prestataire doit élaborer et mettre à disposition des administrateurs du service les guides d'administration des dispositifs du service.

h) Le prestataire doit élaborer et mettre à disposition des administrateurs PAMS les guides d'administration des dispositifs des systèmes d'information administrés dans le cadre de la délivrance du service.

i) Le prestataire doit inclure dans les plans de formation des administrateurs les guides d'administration des dispositifs des systèmes d'information qui les concernent (conformément aux IV.3.2 g) et h)).

j) Le prestataire doit documenter et réaliser une veille sur les vulnérabilités, les mises à jour de sécurité et les mesures de réduction des risques concernant les ressources des systèmes d'information administrés dans le cadre de la délivrance du service.

k) Il est recommandé que le prestataire mette en place des astreintes lui permettant la mobilisation d'administrateurs du système d'information du service en dehors des heures ouvrées.

l) Le prestataire doit désigner un référent opérationnel pour le commanditaire. Il est l'interlocuteur privilégié concernant le fonctionnement opérationnel du service. Le prestataire doit informer le commanditaire de tout changement de l'interlocuteur opérationnel pour le service.

m) Les référents opérationnels doivent participer aux comités opérationnels et stratégiques définis dans le chapitre IV.3.3.

IV.3.3. Comités opérationnels et stratégiques

IV.3.3.1. Comité opérationnel

a) Le prestataire doit mettre en place et animer en présence du commanditaire un comité opérationnel, au minimum une fois par trimestre.

b) Il est recommandé que le prestataire organise un comité opérationnel une fois par mois.

c) Le comité opérationnel doit traiter au minimum des sujets suivants :
- périmètre du service :
  - revue du contexte du commanditaire ;
  - revue des changements concernant le système d'information administré du commanditaire ;
  - présentation des projets d'évolutions impactant le périmètre du service.
- suivi des engagements de sécurité pris dans le cadre de la prestation :

- suivi des indicateurs relatifs au maintien en condition de sécurité du système d'information du service, exposés en IV.2.2.o) ;
- suivi des incidents de sécurité détectés sur le service, des impacts pour le commanditaire et de leur plan de traitement ;
- suivi des exceptions et de leur plan de traitement ;
- liste des administrateurs tiers ayant utilisé l'enclave d'administration tierce commanditaire depuis le dernier comité ;
- liste des tiers ayant eu accès à la zone d'échange tiers depuis le dernier comité.

d) Le prestataire doit rédiger un compte rendu à la suite de chaque comité opérationnel et le transmettre au commanditaire pour validation. Ce compte rendu doit contenir au minimum la liste des participants, les décisions prises en comité et le plan d'action associé.

e) Le prestataire doit protéger les comptes-rendus du comité opérationnel qu'il détient ou transmet, en particulier en matière de confidentialité, en tenant compte du niveau de sensibilité ou de classification de son contenu.

f) Le prestataire doit stocker et archiver les supports des comités opérationnels et comptes rendus associés dans un espace spécifique au sein de l'infrastructure du service, avec un cloisonnement des données au minimum logique entre les commanditaires.

IV.3.3.2. Comité stratégique

a) Le prestataire doit mettre en place et animer en présence de représentants de la direction du commanditaire un comité stratégique, au minimum une fois par an.

b) Il est recommandé que le prestataire organise un comité stratégique une fois par semestre.

c) Le comité stratégique doit traiter au minimum des sujets suivants :
- revue de la convention de service ;
- revue du plan de réversibilité ;
- revue du périmètre de la prestation.

d) Le prestataire doit rédiger un compte rendu à la suite de chaque comité stratégique et le transmettre au commanditaire pour validation. Ce compte rendu doit contenir au minimum les participants et les décisions prises en comité.

e) Le prestataire doit protéger les comptes-rendus du comité stratégique qu'il détient ou transmet, en particulier en matière de confidentialité, en tenant compte du niveau de sensibilité ou de classification de son contenu.

f) Le prestataire doit stocker et archiver les supports des comités stratégiques et comptes rendus associés dans un espace spécifique au sein de l'infrastructure du service, avec un cloisonnement des données au minimum logique entre les commanditaires.

IV.3.4. Convention de service

a) Le prestataire doit établir une convention de service avec chacun des commanditaires du service. Toute modification de la convention de service doit être soumise à acceptation du commanditaire.

b) Le prestataire doit préciser dans la convention de service le périmètre couvert par le service. Ce périmètre est une liste de systèmes d'information ou éléments de systèmes d'information.

c) Le prestataire doit décrire dans la convention de service les activités de maintien en condition de sécurité qu'il s'engage à réaliser sur le périmètre couvert par le service, en particulier les activités de surveillance et de veille en vulnérabilités.

d) Le prestataire doit identifier dans la convention de service :
   - les obligations, droits et responsabilités de chacune des parties : prestataire et tiers impliqués dans la fourniture du service, commanditaires, etc. ;
   - les éléments explicitement exclus des responsabilités du prestataire dans la limite de ce que prévoient les exigences légales et réglementaires en vigueur, notamment l'article 28 du [RGPD] ;
   - la localisation du service. La localisation des actions de support doit être précisée lorsqu'elles sont réalisées depuis un État hors de l'Union Européenne ;
   - la liste des actions de support réalisées depuis un État en dehors de l'Union Européenne.

e) Le prestataire doit proposer une convention de service appliquant le droit d'un État membre de l'Union Européenne. Le droit applicable doit être identifié dans la convention de service.

f) Le prestataire doit décrire dans la convention de service les moyens techniques et organisationnels qu'il met en œuvre pour assurer le respect du droit applicable.

g) Le prestataire doit inclure dans la convention de service une clause de révision de la convention prévoyant notamment une résiliation sans pénalité pour le commanditaire en cas de perte de la qualification octroyée au service.

h) Le prestataire doit inclure dans la convention de service une clause de réversibilité permettant au commanditaire de récupérer l'ensemble de ses données (fournies directement par le commanditaire ou produites dans le cadre du service à partir des données ou des actions du commanditaire).

i) Le prestataire doit assurer cette réversibilité au minimum via l'une des modalités techniques suivantes :
   - la mise à disposition de fichiers suivant un ou plusieurs formats documentés et exploitables en dehors du service fourni par le prestataire ;
   - la mise en place d'interfaces techniques permettant l'accès aux données suivant un schéma documenté et exploitable (API, format pivot, etc.). Les modalités techniques de la réversibilité figurent dans la convention de service.

j) Le prestataire doit indiquer dans la convention de service le niveau de disponibilité du service.

k) Le prestataire doit indiquer dans la convention de service qu'il ne peut disposer des données transmises et générées par le commanditaire, leur disposition étant réservée au commanditaire.

l) Le prestataire doit indiquer dans la convention de service qu'il ne divulgue aucune information relative à la prestation à des tiers, sauf autorisation formelle et écrite du commanditaire.

m) Le prestataire doit indiquer dans la convention de service qu'il met en place une liste des informations transmises aux tiers autorisés ; cette dernière précise pour chaque information le tiers auquel elle a été transmise. Cette liste est maintenue à jour et mise à disposition du commanditaire lorsque ce dernier en fait la demande.

n) Le prestataire doit indiquer dans la convention de service qu'il protège les données transmises à des tiers, en confidentialité, conformément à leur niveau de sensibilité ou de classification.

o) Le prestataire doit indiquer dans la convention de service qu'il détruit l'ensemble des informations relatives au commanditaire à l'issue de la prestation ou à la date d'échéance de la durée de conservation, au premier terme échu, à l'exception de celles pour lesquelles il a reçu une autorisation de conservation

de la part du commanditaire. Il doit s'assurer que ses éventuels sous-traitants sont tenus aux mêmes obligations.

p) Le prestataire doit indiquer dans la convention de service s'il autorise l'accès distant pour des actions d'administration ou de support au système d'information du service.

q) Le prestataire doit préciser dans la convention de service que :
   - le service est qualifié et inclure l'attestation de qualification ;
   - le commanditaire peut déposer une réclamation relative au service qualifié auprès de l'ANSSI.

r) Le prestataire doit préciser dans la convention de service qu'il s'engage à mettre à disposition toutes les informations nécessaires à la réalisation d'audits de conformité menés par le commanditaire ou un tiers mandaté.

s) Il est recommandé que le tiers mandaté pour les audits soit un prestataire d'audit de la sécurité des systèmes d'information [PASSI] qualifié.

Annexe 1 Références documentaires

I. Codes, textes législatifs et réglementaires

Renvoi	Document
[IGI_1300]	Arrêté du 13 novembre 2020 portant approbation de l'instruction générale interministérielle n° 1300 sur la protection du secret de la défense nationale. Disponible sur https://www.legifrance.gouv.fr
[II_901]	Instruction interministérielle n°910/SGDSN/ANSSI du 22 octobre 2013 relative à la protection des systèmes d'information sensibles. Disponible sur https://www.circulaire.legifrance.gouv.fr
[II_910]	Instruction interministérielle relative aux articles contrôlés de la sécurité des systèmes d'information (ACSSI), n°910/SGDSN/ANSSI, 22 octobre 2013. Disponible sur http://www.legifrance.gouv.fr
[PSSIE]	Politique de sécurité des systèmes d'information de l'Etat. Dernière version en vigueur. Disponible sur https://www.ssi.gouv.fr
[RGPD]	Règlement (UE) 2016/679 du parlement européen et du conseil du 27 avril 2016 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. Disponible sur https://eur-lex.europa.eu

II. Normes et documents techniques

Renvoi	Document
[CARTO]	Cartographie du système d'information, Guide d'élaboration en 5 étapes, ANSSI. Dernière version en vigueur. Disponible sur https://www.ssi.gouv.fr
[CRYPTO_A7]	Politique de Certification Type Authentification, ANSSI. Dernière version en vigueur. Disponible sur https://www.ssi.gouv.fr
[CRYPTO_B1]	Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, ANSSI. Dernière version en vigueur. Disponible sur https://www.ssi.gouv.fr
[CRYPTO_B2]	Règles et recommandations concernant la gestion des clés utilisées dans les mécanismes cryptographiques, ANSSI. Dernière version en vigueur. Disponible sur https://www.ssi.gouv.fr
[CRYPTO_B3]	Règles et recommandations concernant les mécanismes d'authentification, ANSSI. Dernière version en vigueur. Disponible sur https://www.ssi.gouv.fr
[G_ADMIN]	Recommandations relatives à l'administration sécurisée des systèmes d'information, ANSSI. Dernière version en vigueur. Disponible sur https://www.ssi.gouv.fr
[G_CAVP]	Recommandations sur la sécurisation des systèmes de contrôle d'accès physique et de vidéoprotection. Dernière version en vigueur. Disponible sur https://www.ssi.gouv.fr

Renvoi	Document
[G_INTERNET]	Recommandations relatives à l'interconnexion d'un SI à Internet. Dernière version en vigueur. Disponible sur https://www.ssi.gouv.fr
[G_IPSEC]	Recommandations de sécurité relatives à IPsec pour la protection des flux réseau, ANSSI. Dernière version en vigueur. Disponible sur https://www.ssi.gouv.fr
[G_LINUX]	Recommandations de configuration d'un système GNU/LINUX, ANSSI. Dernière version en vigueur. Disponible sur https://www.ssi.gouv.fr
[G_SSH]	Recommandations pour un usage sécurisé d'(Open)SSH, ANSSI. Dernière version en vigueur. Disponible sur https://www.ssi.gouv.fr
[G_TLS]	Recommandations de sécurité relatives à TLS, ANSSI. Dernière version en vigueur. Disponible sur https://www.ssi.gouv.fr
[G_WINDOWS_1]	Recommandations pour la mise en œuvre d'une politique de restrictions logicielles sous Windows. Dernière version en vigueur. Disponible sur https://www.ssi.gouv.fr
[G_WINDOWS_2]	Préoccupations relatives au respect de la vie privée et à la confidentialité des données sous Windows 10. Dernière version en vigueur. Disponible sur https://www.ssi.gouv.fr
[G_WINDOWS_3]	Mise en œuvre des fonctionnalités de sécurité de Windows 10 reposant sur la virtualisation. Dernière version en vigueur. Disponible sur https://www.ssi.gouv.fr
[HOMOLOGATION]	L'homologation de sécurité en neuf étapes simples, ANSSI. Dernière version en vigueur. Disponible sur https://www.ssi.gouv.fr
[HYGIENE]	Guide d'hygiène informatique, ANSSI. Dernière version en vigueur. Disponible sur https://www.ssi.gouv.fr
[ISO27000]	Norme internationale ISO/IEC 27000 - Technologies de l'information – Techniques de sécurité – Systèmes de gestion de la sécurité de l'information – vue d'ensemble et vocabulaire. Dernière version en vigueur. Disponible sur https://www.iso.org
[ISO27001]	Norme internationale ISO/IEC 27001 - Technologies de l'information – Techniques de sécurité – Systèmes de management de la sécurité de l'information – Exigences. Dernière version en vigueur. Disponible sur https://www.iso.org
[ISO27002]	Norme internationale ISO/IEC 27002 – Technologies de l'information – Techniques de sécurité – Code de bonne pratique pour le management de la sécurité de l'information. Dernière version en vigueur. Disponible sur https://www.iso.org

Renvoi	Document
[ISO27005]	Norme internationale ISO/IEC 27005 – Technologies de l'information – Techniques de sécurité – Gestion des risques liés à la sécurité de l'information. Dernière version en vigueur. Disponible sur https://www.iso.org
[ISO27035]	Norme internationale ISO/IEC 27035 – Technologies de l'information – Techniques de sécurité – Gestion des incidents de sécurité de l'information. Dernière version en vigueur. Disponible sur https://www.iso.org
[NT_COMMUT]	Recommandations pour la sécurisation d'un commutateur de desserte, ANSSI. Dernière version en vigueur. Disponible sur https://www.ssi.gouv.fr
[NT_JOURNAL]	Recommandations de sécurité pour la mise en œuvre d'un système de journalisation, ANSSI. Dernière version en vigueur. Disponible sur https://www.ssi.gouv.fr
[NT_JOURNAL_W]	Recommandations de sécurité pour la journalisation des systèmes Microsoft Windows en environnement Active Directory. Dernière version en vigueur. Disponible sur https://www.ssi.gouv.fr
[PASSI]	Référentiel d'exigences applicables à un prestataire d'audit de la sécurité des systèmes d'information, ANSSI. Dernière version en vigueur. Disponible sur https://www.ssi.gouv.fr
[SecNumCloud]	Prestataires de services d'informatique en nuage (SecNumCloud), référentiel d'exigences, ANSSI. Dernière version en vigueur. Disponible sur https://www.ssi.gouv.fr

III. Autres références documentaires

Renvoi	Document
[FORMATION_SI_INDUS]	Guide pour une formation sur la cybersécurité des systèmes industriels, ANSSI. Dernière version en vigueur. Disponible sur https://www.ssi.gouv.fr
[GUIDE_ACHAT]	Guide d'achat de produits de sécurité et de services de confiance qualifiés, ANSSI. Dernière version en vigueur. Disponible sur http://www.ssi.gouv.fr
[QUAL_SERV_PROCESS]	Processus de qualification d'un service, ANSSI. Dernière version en vigueur. Disponible sur https://www.ssi.gouv.fr

Annexe 2 Recommandations aux commanditaires

Cette annexe liste les recommandations de l'ANSSI aux commanditaires de prestations qualifiées d'administration et de maintenance sécurisées.

I. Qualification

a) Le commanditaire peut, lorsqu'il est une autorité administrative ou un opérateur d'importance vitale, demander à l'ANSSI de participer à la définition du cahier des charges faisant l'objet d'un appel d'offres ou d'un contrat.

b) Il est recommandé que le commanditaire choisisse son prestataire dans le catalogue des prestataires qualifiés publié sur le site Web de l'ANSSI ; la qualification d'un prestataire d'administration et de maintenance sécurisées atteste de sa conformité à l'ensemble des exigences du présent référentiel.

c) Pour bénéficier d'une prestation qualifiée, c'est-à-dire conforme à l'ensemble des exigences du présent référentiel, le commanditaire doit :
   - choisir le prestataire dans le catalogue des prestataires qualifiés publié sur le site Web de l'ANSSI ;
   - exiger du prestataire de stipuler dans la convention de service que la prestation réalisée est une prestation qualifiée.

   En effet, un prestataire qualifié garde la faculté de réaliser des prestations non qualifiées. Le recours à un prestataire issu du catalogue des prestataires qualifiés est donc une condition nécessaire mais pas suffisante pour bénéficier d'une prestation qualifiée ; le commanditaire doit donc également exiger une prestation qualifiée.

d) Il est recommandé que le commanditaire qui recourt à un prestataire qualifié pour la réalisation d'une prestation non qualifiée demande la liste des exigences du présent référentiel que le prestataire ne respectera pas pour la prestation.

e) Il est recommandé que le commanditaire utilise le guide d'achat des produits de sécurité et des services de confiance [GUIDE_ACHAT] qui a vocation à accompagner la fonction achat des commanditaires lors des appels d'offres.

f) Il est recommandé que le commanditaire demande au prestataire de lui transmettre son attestation de qualification. Cette attestation identifie notamment les activités pour lesquelles le prestataire est qualifié ainsi que la date de validité de la qualification.

g) Le commanditaire peut, conformément au processus de qualification des prestataires de service de confiance [QUAL_SERV_PROCESS], déposer auprès de l'ANSSI une réclamation contre un prestataire qualifié pour lequel il estime que ce dernier n'a pas respecté une ou plusieurs exigences du présent référentiel dans le cadre d'une prestation qualifiée. S'il s'avère après instruction de la réclamation que le prestataire n'a pas respecté une ou plusieurs exigences du présent référentiel dans le cadre d'une prestation qualifiée, et selon la gravité, la qualification du prestataire peut être suspendue, retirée ou sa portée de qualification réduite.

h) La qualification d'un prestataire n'atteste pas de sa capacité à accéder ou à détenir des informations classifiées de défense [IGI_1300] et par conséquent ne se substitue pas à une habilitation de défense. Il est possible pour un commanditaire de recourir à un prestataire qualifié après s'être assuré que ce dernier dispose des habilitations de défense adéquates si nécessaire.

i) La qualification d'un prestataire n'atteste pas de sa capacité à accéder ou à détenir des articles contrôlés de la sécurité des systèmes d'information (ACSSI) [II_910]. Un commanditaire peut recourir à un

prestataire qualifié après s'être assuré que ce dernier dispose au minimum des décisions d'accès aux ACSSI (DACSSI) adéquates pour les ACSSI classifiés ou des attestations de formation à la manipulation des ACSSI pour les ACSSI non classifiés.

II. Avant la prestation

a) Il est recommandé que le commanditaire désigne, dans son organisation, un référent opérationnel chargé d'être l'interlocuteur privilégié avec le prestataire concernant le fonctionnement opérationnel du service.

b) Il est recommandé que le commanditaire communique au prestataire :
   - les tiers autorisés à accéder à l'enclave d'administration tierce commanditaire ;
   - les types d'informations que peut communiquer le prestataire à un tiers ;
   - l'état de la menace sur le système d'information administré par le prestataire.

c) Il est recommandé que le commanditaire exige du prestataire de lui dédier un ou plusieurs socles physiques pour l'hébergement de la zone d'accès aux ressources administrées.

d) Il est recommandé que le commanditaire mette en œuvre un ou plusieurs dispositifs de chiffrement et d'authentification des paquets IP sur le système d'information administré pour l'accès du prestataire au réseau d'administration.

e) Il est recommandé que le commanditaire exige du prestataire de lui dédier un ou plusieurs socles physiques pour l'hébergement de la zone d'échange commanditaire.

f) Il est recommandé que le commanditaire définisse avec le prestataire les modalités d'accès à l'enclave d'administration tierce commanditaire.

g) Il est recommandé que le commanditaire cloisonne le réseau d'administration à partir duquel le prestataire va réaliser les actions d'administration ou de maintenance du reste du système d'information.

h) Il est recommandé que le réseau d'administration du commanditaire repose sur un ou plusieurs socles physiques dédiés.

i) Il est recommandé que le commanditaire exige du prestataire de cloisonner les outils d'administration en cohérence avec le cloisonnement effectué au sein du ou des systèmes d'information administrés.

j) Il est recommandé que le commanditaire définisse une politique de maintien en condition de sécurité de son système d'information administré avec le prestataire.

k) Il est recommandé que le commanditaire dispose des licences valides des outils (logiciels ou matériels) utilisés pour la réalisation de la prestation.

l) Il est recommandé que le commanditaire demande au prestataire de lui fournir les résultats de la veille réalisée sur le système d'information administrée telle que définie dans l'exigence IV.3.2.j).

m) Il est recommandé que le commanditaire identifie dans la convention de service les éventuelles exigences légales et réglementaires spécifiques auxquelles il est soumis et notamment celles liées à son secteur d'activité.

n) Il est recommandé que la fréquence des comités opérationnels (voir chapitre IV.3.3.1) devant être définie dans la convention de service soit mensuelle.

o) Il est recommandé que la fréquence des comités stratégiques (voir chapitre IV.3.3.2) devant être définie dans la convention de service soit semestrielle.

III. Pendant la prestation

a) Il est recommandé que le commanditaire informe le prestataire de tout projet d'évolution de son système d'information pouvant impacter l'efficacité du service.

b) Il est recommandé que le commanditaire mette en place un processus de gestion des changements lui permettant d'informer en continu le prestataire de toute modification sur son système d'information administré (configuration, paramètres, versions logicielles, etc.).

c) Il est recommandé que le commanditaire recoure à une prestation qualifiée réalisée par un prestataire de réponse aux incidents de sécurité (PRIS)[3] en cas d'incident de sécurité suspecté ou avéré.

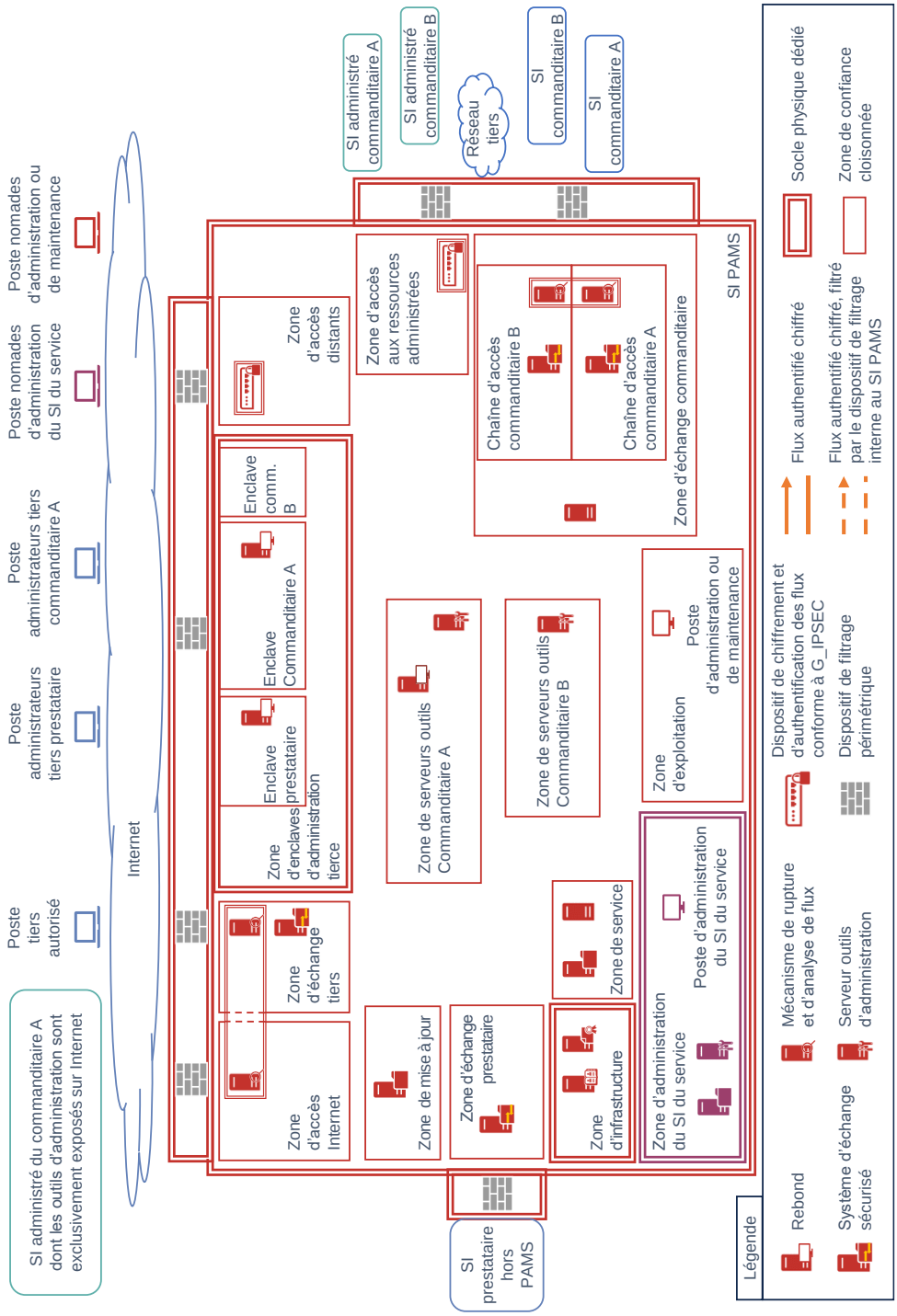
d) Il est recommandé que le commanditaire, en cas d'occurrence d'incidents de sécurité sur son système d'information administré par le prestataire, fasse appel au prestataire pour les efforts d'investigation.

[3] Le catalogue des prestataires de réponse aux incidents de sécurité (PRIS) qualifiés par l'ANSSI est publié sur le site Web de l'ANSSI.

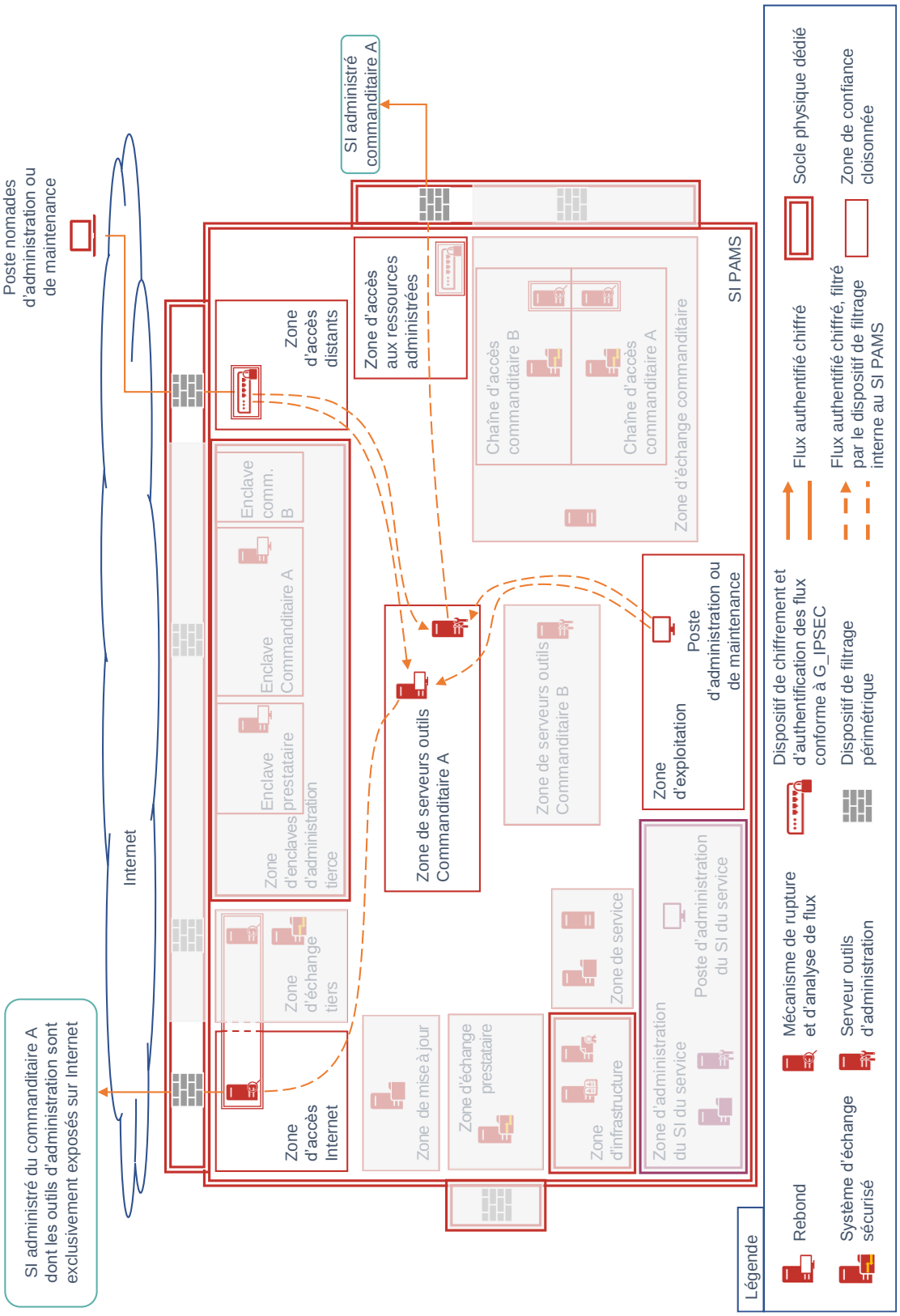
Annexe 3 Schémas illustratifs d'une architecture de système d'information du service et des flux associés

Les schémas ci-dessous sont une représentation d'une architecture possible pour le système d'information du service ainsi que les flux autorisés dans des cas d'usages associés. Ces schémas sont donnés uniquement à titre d'illustration pour faciliter la compréhension du référentiel et n'excluent pas la mise en place d'autres architectures.

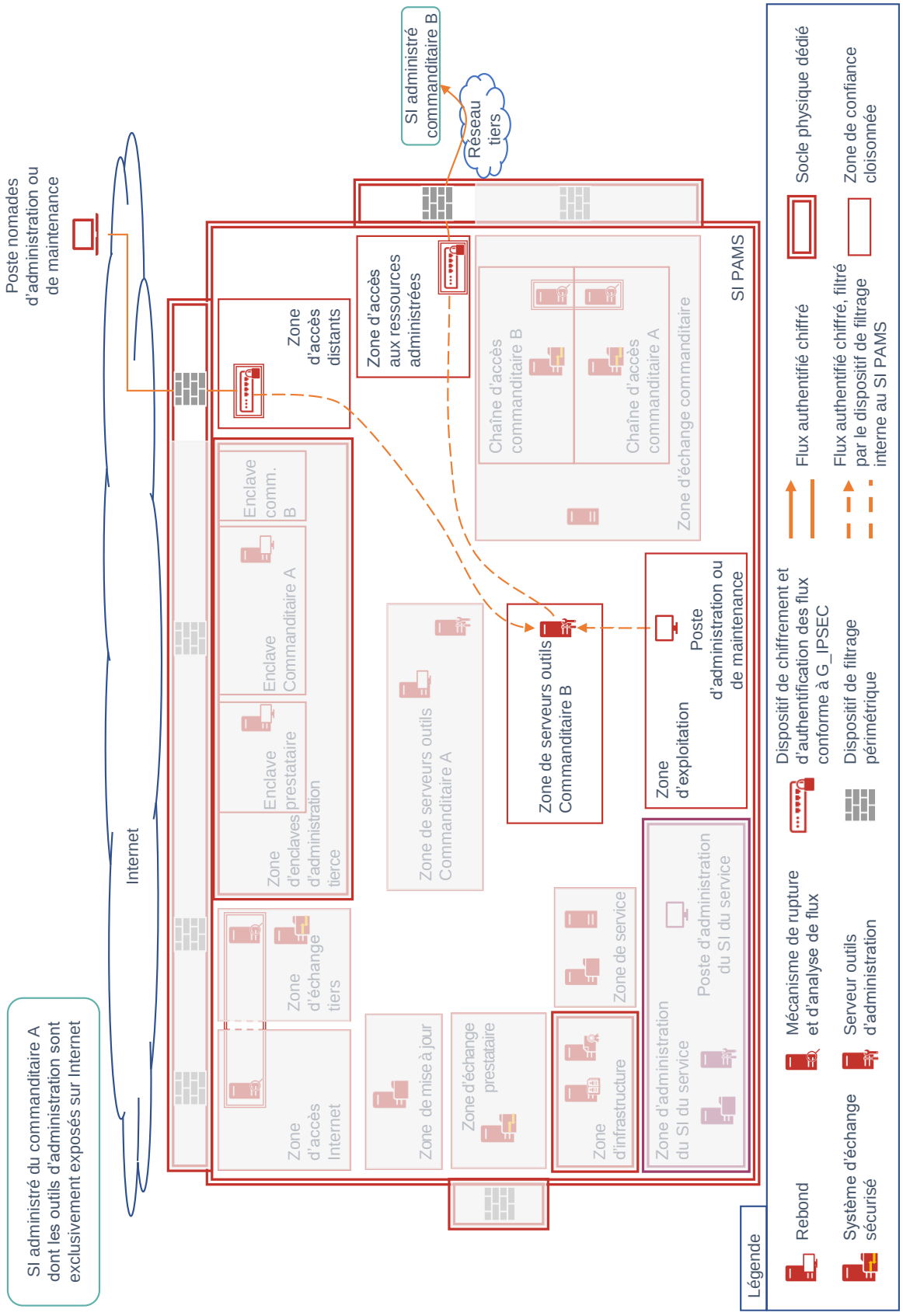
I. Zones, interconnexions et écosystème du système d'information du service



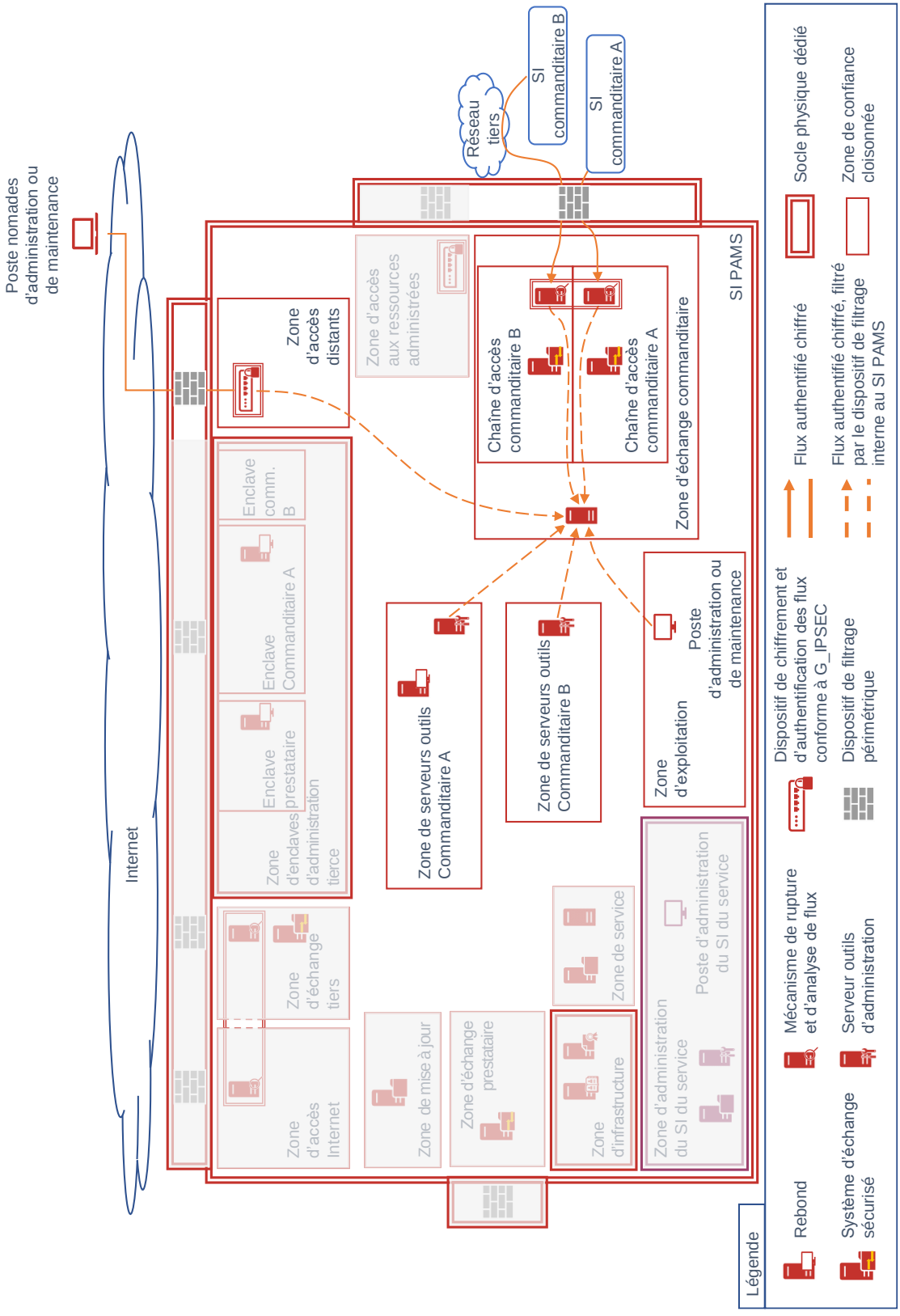
II. Flux d'administration du SI administré d'un commanditaire avec des outils d'administration exposés sur Internet et des ressources administrées accessibles sans passage par un réseau tiers



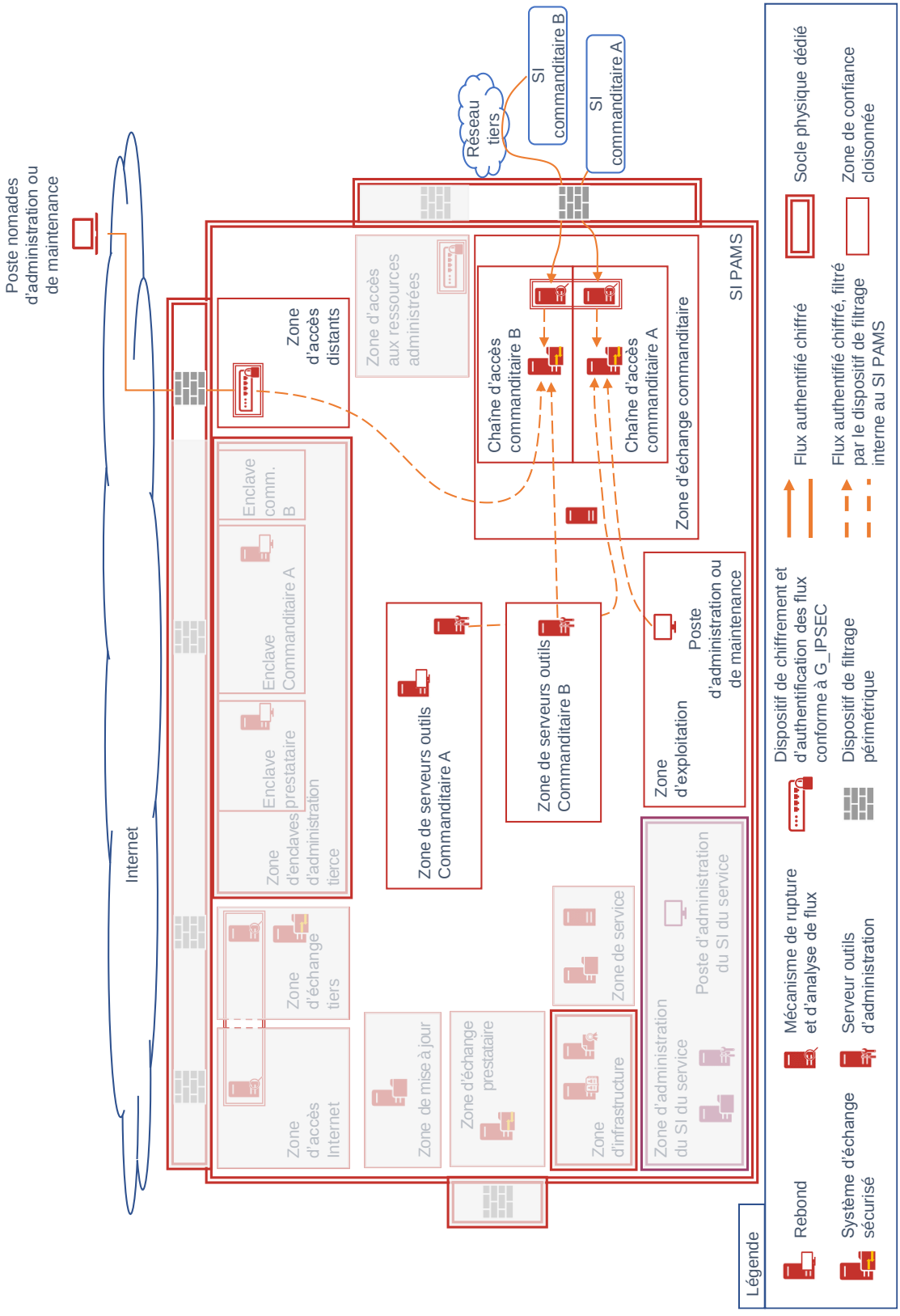
III. Flux d'administration du SI administré d'un commanditaire avec passage par un réseau tiers



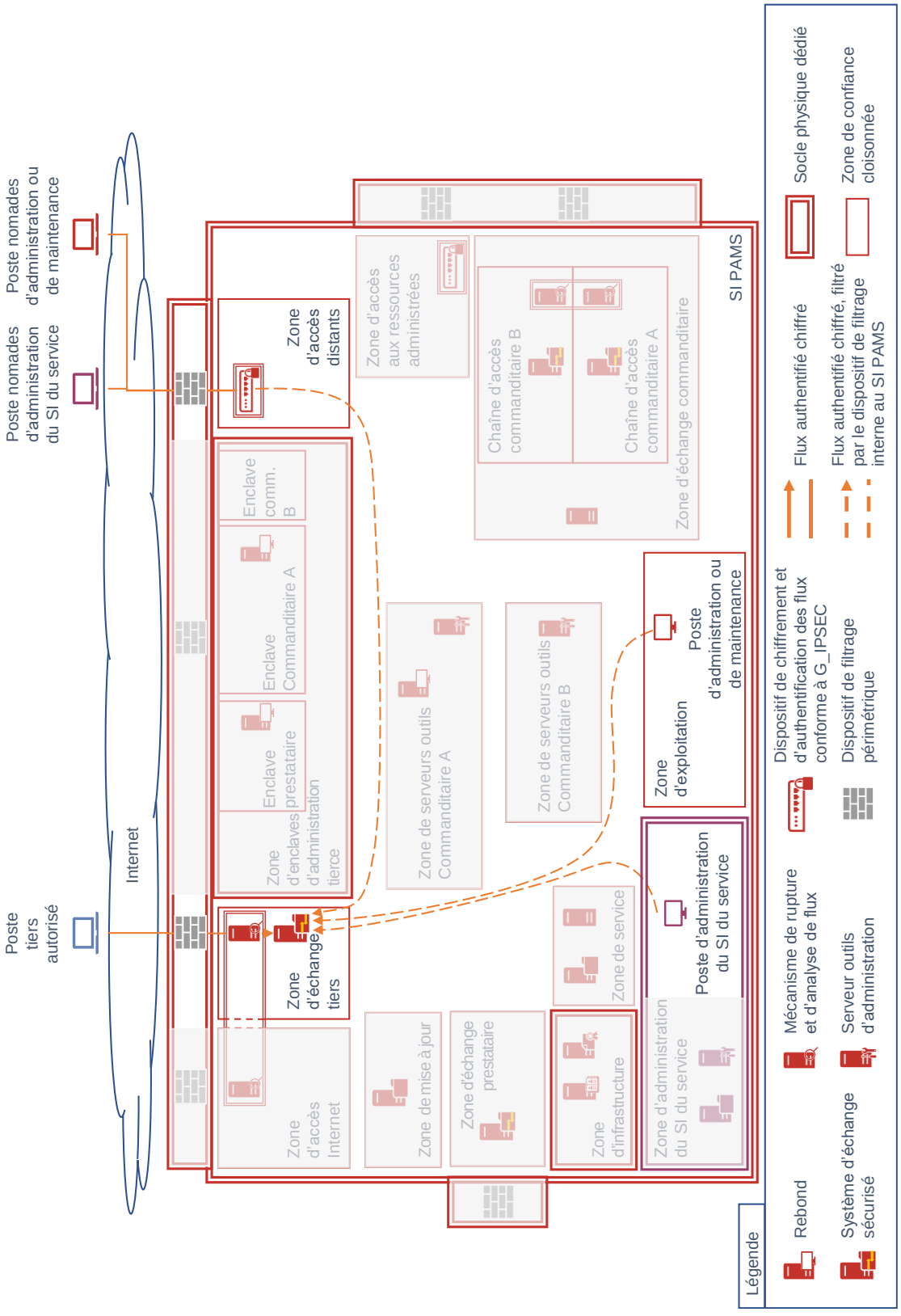
IV. Flux d'échanges machine à machine avec les commanditaires



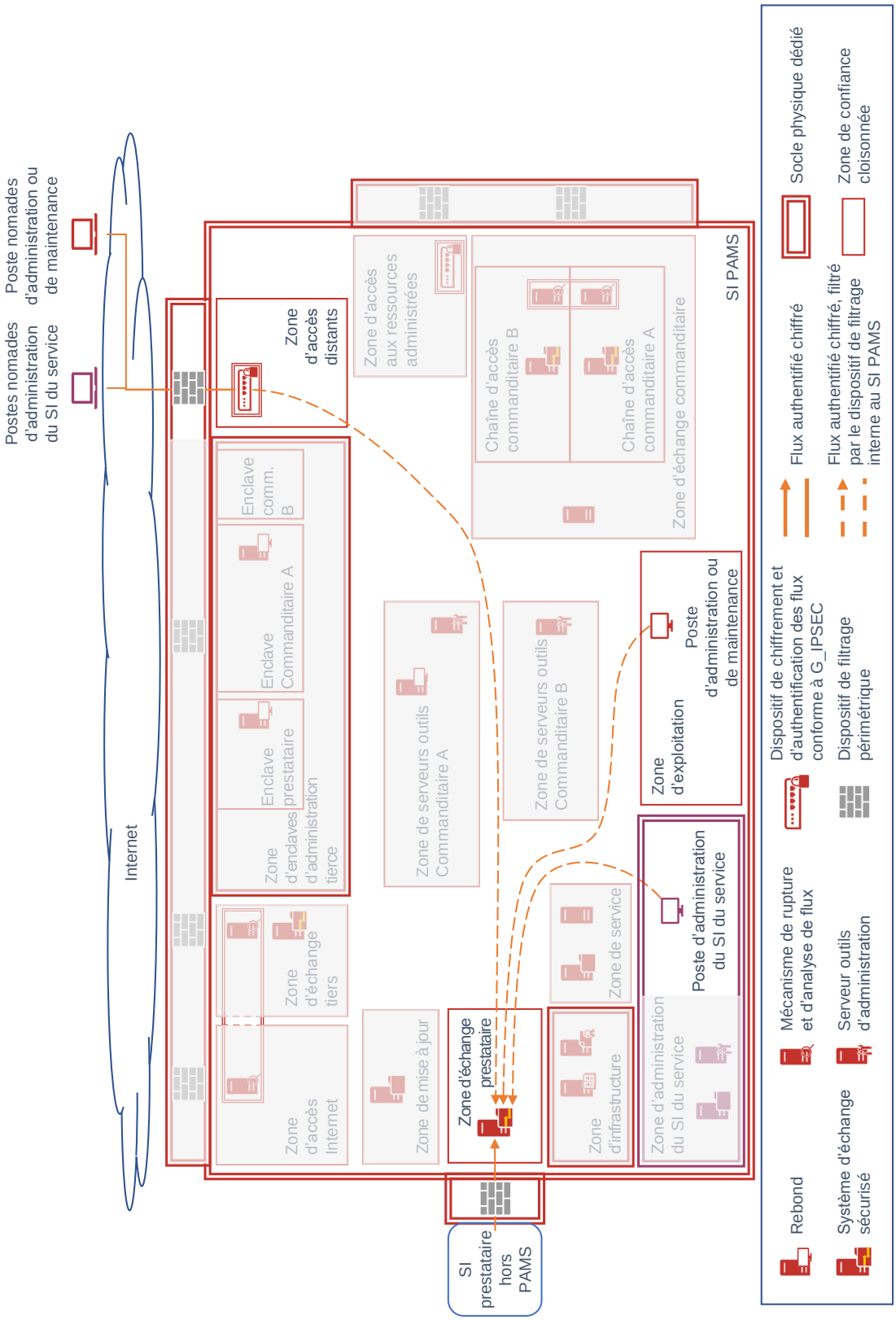
V. **Flux d'échanges de fichiers avec les commanditaires**



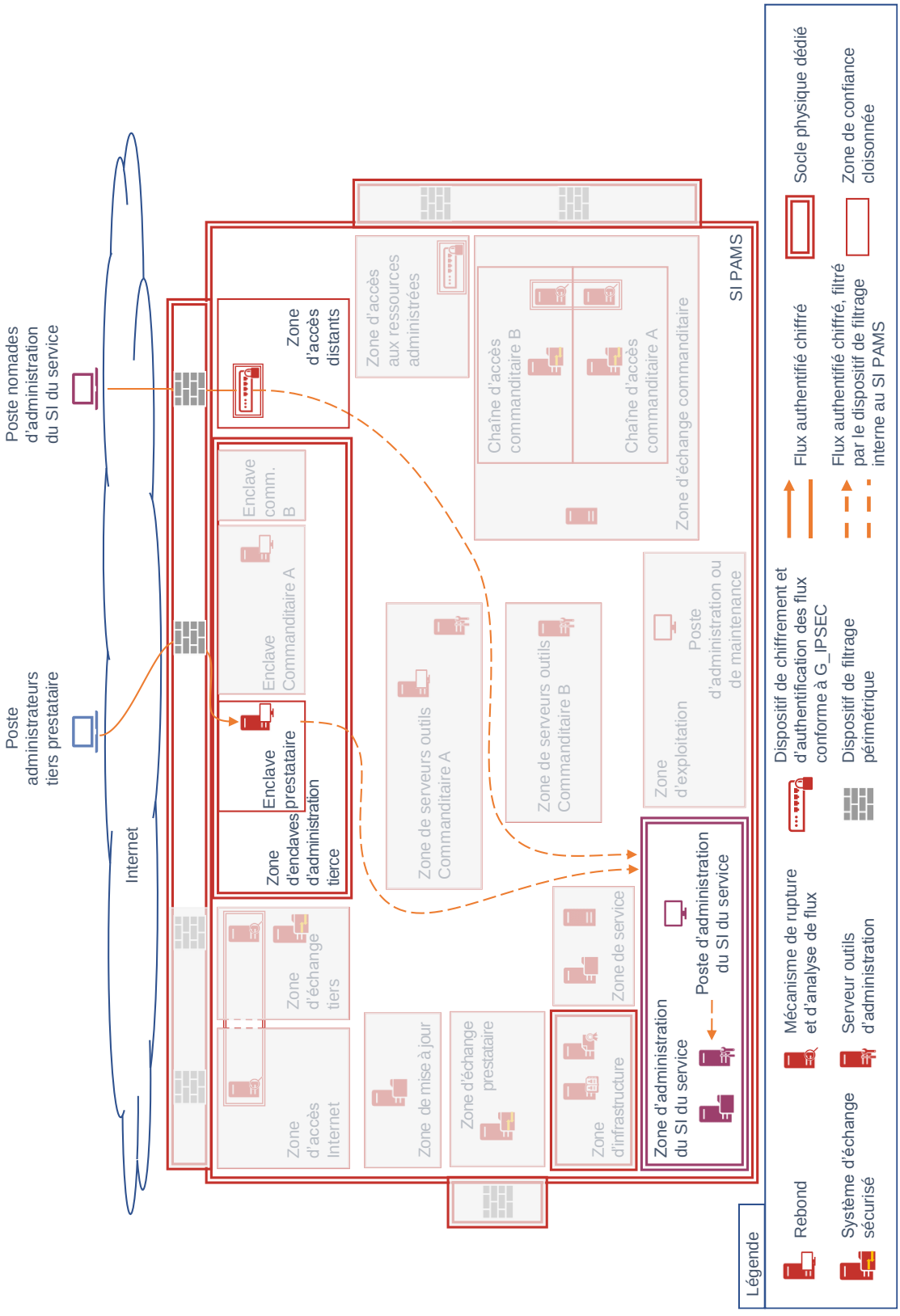
VI. Flux d'échanges de fichiers avec un tiers autorisé



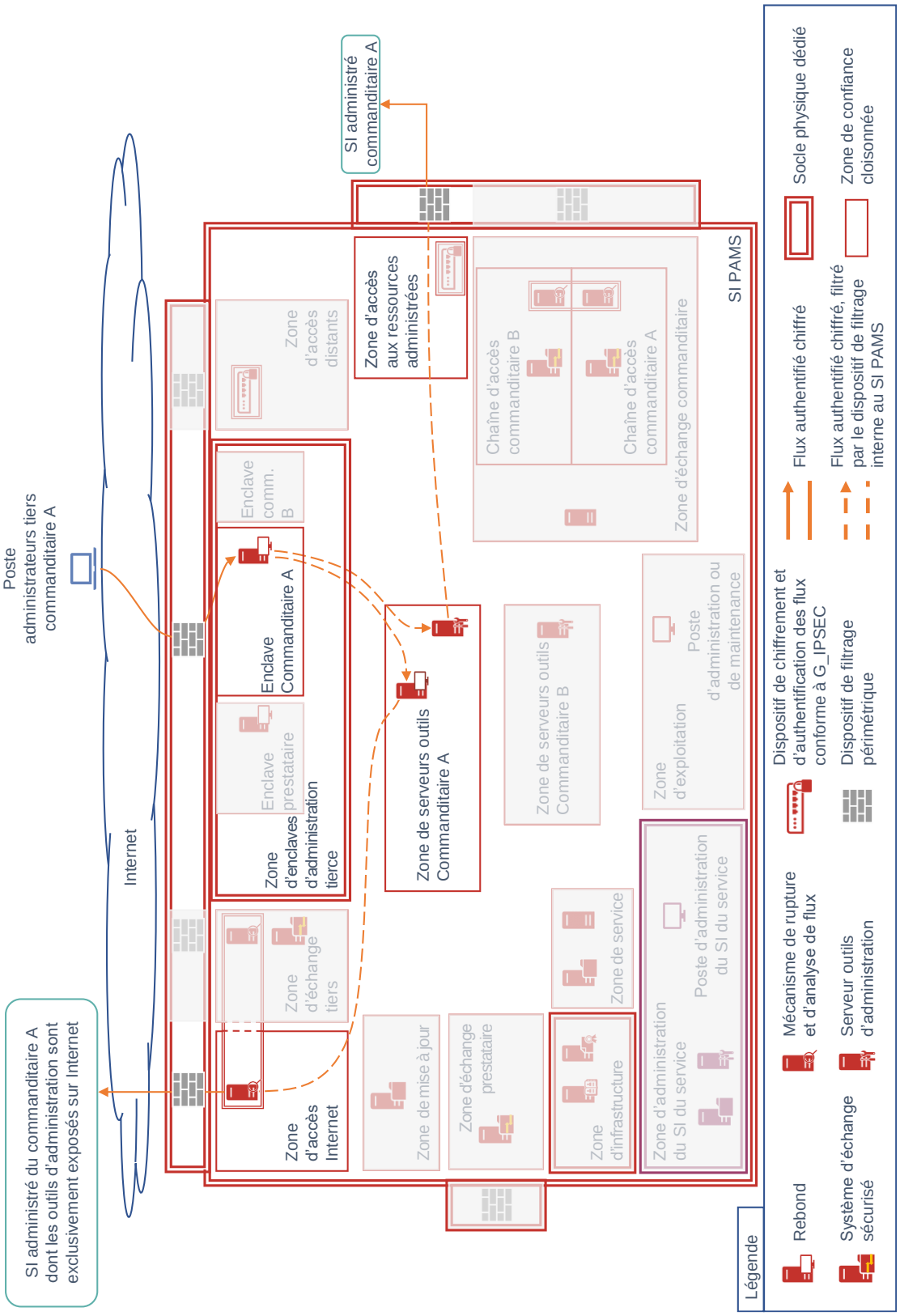
VII. Flux d'échanges de texte avec le SI prestataire hors PAMS (ex : SI bureautique)



VIII. **Flux d'administration du SI du service**



IX. Flux d'administration du SI administré d'un commanditaire à travers l'enclave d'administration tierce commanditaire



Annexe 4 Tableaux de synthèse des exigences relatives aux zones d'interconnexion

Les tableaux suivants rassemblent l'ensemble des exigences de la partie IV.2.9 concernant les interconnexions et les systèmes d'échanges sécurisés. Les exigences ont été regroupées en fonction des thèmes et objectifs de sécurité. Pour certaines zones et thèmes, aucune exigence n'est formulée au sein de la partie IV.2.9, les pratiques sont, dans ce cas, couvertes par d'autres exigences de la section IV.

Cette annexe est un outil de synthèse donné à titre indicatif ; les exigences de la partie IV font référence en cas d'écart.

I. Exigences relatives aux zones d'échanges

	IV.2.9.1. Zone d'échange prestataire	**IV.2.9.2. Zone d'échange commanditaire**	**IV.2.9.3. Zone d'échange tiers**
Objet de la zone	Pour le bon fonctionnement du service, le prestataire peut être amené à échanger des informations avec d'autres zones de son système d'information (extérieures au système d'information du service). La « zone d'échange prestataire » vise à garantir la sécurité de tels échanges. Elle ne constitue en aucun cas un espace de stockage partagé pérenne, mais bien un espace d'échanges où les données ne sont hébergées que de manière éphémère.	Pour le bon fonctionnement du service, le prestataire peut être amené à échanger des informations avec le commanditaire (ex. : partage de fichiers, accès à un portail de *ticketing*). La « zone d'échange commanditaire » vise à garantir la sécurité de tels échanges. Elle ne constitue en aucun cas un espace de stockage partagé pérenne, mais bien un espace d'échanges où les données ne sont hébergées que de manière éphémère.	Pour le bon fonctionnement du service, le prestataire peut être amené à échanger des informations avec des tiers. La « zone d'échange tiers » vise à garantir la sécurité de tels échanges. Elle ne constitue en aucun cas un espace de stockage partagé pérenne, mais bien un espace d'échanges où les données ne sont hébergées que de manière éphémère.
Cloisonnement physique de la zone	*Thématique traitée de manière plus globale au sein de la partie IV.2*		
Cloisonnement intra-zone	*Thématique traitée de manière plus globale au sein de la partie IV.2*		
Zones périphériques concernées	a) Le prestataire doit s'assurer que tous les flux entre le système d'information du service et les autres zones de son système d'information transitent par la zone d'échange prestataire.	a) Le prestataire doit s'assurer que tous les flux d'échanges entre le commanditaire et le prestataire transitent par la zone d'échange commanditaire (les flux d'administration ne sont pas considérés comme des flux d'échanges).	a) Le prestataire doit s'assurer que tous les flux d'échanges entre le système d'information du service et les tiers transitent par la zone d'échange tiers (les flux d'administration ne sont pas considérés comme des flux d'échanges).

	IV.2.9.1. Zone d'échange prestataire	IV.2.9.2. Zone d'échange commanditaire	IV.2.9.3. Zone d'échange tiers
Source des flux	j) Le prestataire doit s'assurer que seuls les flux vers le système d'échange prestataire sont autorisés (le système d'échange prestataire ne peut être à l'origine des flux).	l) Le prestataire doit s'assurer que seuls les flux vers la zone d'échange commanditaire sont autorisés (la zone d'échange commanditaire ne peut être à l'origine des flux).	p) Le prestataire doit s'assurer que seuls les flux vers le système d'échange tiers sont autorisés (le système d'échange tiers ne peut être à l'origine des flux).
Exclusivité des flux et besoins opérationnels	b) Le prestataire doit s'assurer que seuls les flux correspondant au strict besoin opérationnel des échanges de fichiers ou de texte entre le système d'information du service et les autres zones du système d'information du prestataire (extérieures au système d'information du service) sont autorisés et transitent par les dispositifs de filtrage internes et périmétriques du système d'information du service.	d) Le prestataire doit s'assurer que seuls les flux correspondant au strict besoin opérationnel des échanges de données entre le prestataire et le commanditaire sont autorisés et transitent par les dispositifs de filtrage internes et périmétriques du système d'information du service.	c) Le prestataire doit s'assurer que seuls les flux correspondant au strict besoin opérationnel des échanges de données (fichier, texte, flux vidéo) entre le système d'information du service et le tiers sont autorisés et transitent par les dispositifs de filtrages internes et périmétriques du système d'information du service.
Dispositifs de filtrage périmétrique	c) Le prestataire doit dédier un ou plusieurs dispositifs de filtrage périmétrique à la zone d'échange prestataire.	b) Le prestataire doit dédier un ou plusieurs dispositifs de filtrage périmétrique à la zone d'échange commanditaire. c) Il est recommandé que le prestataire dédie un ou plusieurs dispositifs de filtrage périmétrique par commanditaire.	b) Le prestataire doit dédier un ou plusieurs dispositifs de filtrage périmétrique à la zone d'échange tiers.
Dispositifs de chiffrement des flux	d) Le prestataire doit mettre en œuvre des mécanismes ou dispositifs de chiffrement et d'authentification des flux pour l'accès à la zone d'échange prestataire. Le prestataire doit mettre en œuvre ces mécanismes ou dispositifs en conformité avec le guide [G_IPSEC], le guide [G_TLS] ou le guide [G_SSH].	e) Le prestataire doit mettre en œuvre des mécanismes ou dispositifs de chiffrement et d'authentification des flux pour tout accès du commanditaire à la zone d'échange commanditaire. Le prestataire doit mettre en œuvre ces mécanismes ou dispositifs en conformité avec le guide [G_IPSEC], le guide [G_TLS] ou le guide [G_SSH].	d) Le prestataire doit mettre en œuvre des mécanismes ou dispositifs de chiffrement et d'authentification des flux pour tout accès des tiers à la zone d'échange tiers. Le prestataire doit mettre en œuvre ces mécanismes ou dispositifs en conformité avec le guide [G_IPSEC], le guide [G_TLS] ou le guide [G_SSH].
Contraintes de mutualisation des dispositifs de chiffrement des flux	e) Il est recommandé de dédier les dispositifs de chiffrement et d'authentification des flux à la zone d'échange prestataire. f) Il est recommandé que les dispositifs de chiffrement et d'authentification des flux reposent sur un ou plusieurs socles physiques dédiés à la zone d'échange prestataire.	f) Il est recommandé de dédier les dispositifs de chiffrement et d'authentification des flux à la zone d'échange commanditaire. g) Il est recommandé que les dispositifs de chiffrement et d'authentification des flux reposent sur un ou plusieurs socles physiques dédiés à la zone d'échange commanditaire.	e) il est recommandé de dédier les dispositifs de chiffrement et d'authentification des flux pour l'accès à la zone d'échange tiers. f) Il est recommandé que le dispositif de chiffrement et d'authentification des flux repose sur un ou plusieurs socles physiques dédiés à la zone d'échange tiers.

	IV.2.9.1. Zone d'échange prestataire	IV.2.9.2. Zone d'échange commanditaire	IV.2.9.3. Zone d'échange tiers
Qualification des dispositifs de chiffrement des flux	g) Il est recommandé que les dispositifs de chiffrement et d'authentification des paquets IP soient des produits qualifiés par l'ANSSI et soient utilisés conformément aux conditions de leur qualification.	h) Il est recommandé que les dispositifs de chiffrement et d'authentification des flux soient des produits qualifiés par l'ANSSI et soient utilisés conformément aux conditions de leur qualification.	g) Il est recommandé que les dispositifs de chiffrement et d'authentification des flux soient des produits qualifiés par l'ANSSI et soient utilisés conformément aux conditions de leur qualification.
Mécanismes de rupture et analyse des flux		i) Le prestataire doit mettre en œuvre des mécanismes de rupture et d'analyse des flux au sein de la zone d'échange commanditaire pour les flux externes au système d'information du service accédant à la zone d'échange commanditaire. Ces mécanismes doivent reposer sur un ou plusieurs socles physiques dédiés à la zone d'échange commanditaire. j) Le prestataire doit dédier un ou plusieurs mécanismes de rupture et d'analyse des flux par commanditaire.	h) Le prestataire doit mettre en œuvre des mécanismes de rupture et d'analyse des flux au sein de la zone d'échange tiers pour les flux externes au système d'information du service accédant à la zone d'échange tiers. i) Le prestataire doit dédier les mécanismes de rupture et d'analyse des flux à la zone d'échange tiers. Les mécanismes doivent reposer sur un ou plusieurs socles physiques dédiés à la zone d'échange tiers ou prendre la forme d'une instance dédiée sur un socle physique commun avec les mécanismes de rupture et d'analyse de flux de la zone d'accès à Internet. j) Il est recommandé que les mécanismes de rupture et d'analyse protocolaire reposent sur un ou plusieurs socles physiques dédiés à la zone d'échange tiers.
Mécanismes d'authentification, Annuaire et Gestion des comptes	k) Le prestataire doit mettre en place des mécanismes d'authentification au niveau de la zone d'échange prestataire pour l'accès des administrateurs PAMS et des administrateurs du système d'information du service. Ces mécanismes reposent sur un annuaire sans adhérence avec les annuaires stockant des comptes d'administration. l) Il est recommandé de dédier un annuaire à la zone d'échange prestataire.	m) Le prestataire doit mettre en place des mécanismes d'authentification au niveau de la zone d'échange commanditaire pour l'accès des administrateurs PAMS et du commanditaire. Ces mécanismes reposent sur un annuaire sans adhérence avec les annuaires stockant des comptes d'administration. n) Il est recommandé de dédier un annuaire à la zone d'échange commanditaire.	l) Le prestataire doit mettre en place des mécanismes d'authentification au niveau de la zone d'échange tiers pour l'accès des administrateurs PAMS, administrateurs du système d'information du service et des tiers autorisés. Ces mécanismes reposent sur un annuaire sans adhérence avec les annuaires stockant des comptes d'administration. m) Il est recommandé de dédier un annuaire à la zone d'échange tiers.
Gouvernance des accès	*Thématique traitée au sein de la partie IV.2 et IV.3*		

	IV.2.9.1. Zone d'échange prestataire	IV.2.9.2. Zone d'échange commanditaire	IV.2.9.3. Zone d'échange tiers
Gestion des secrets	-	-	n) Le prestataire doit renouveler les secrets d'authentification des tiers à l'issue de chaque accès ou à une fréquence au minimum mensuelle et ne communiquer les nouveaux secrets que lorsqu'un accès à la zone est requis par le tiers concerné.
Respect des exigences sur les actions d'admin.	*Non applicable*		
Traçabilité	q) Le prestataire doit mettre en œuvre une traçabilité permettant de journaliser l'horaire de l'échange, l'identité de l'utilisateur du prestataire déposant le fichier ou texte, celle de l'utilisateur ayant les droits d'accès au fichier ou texte et la typologie de la donnée échangée.	u) Le prestataire doit mettre en œuvre une traçabilité permettant de journaliser l'horaire de l'échange, l'identité de l'utilisateur du commanditaire concerné, celle de l'administrateur PAMS concerné et la typologie de la donnée échangée.	u) Le prestataire doit mettre en œuvre une traçabilité permettant de journaliser l'horaire de l'échange, l'identité du tiers concerné (personne physique ou entité), l'administrateur concerné et la typologie de la donnée échangée.
Supervision	*Thématique traitée de manière plus globale au sein de la partie IV.2*		
Systèmes d'échange	i) Le prestataire doit mettre en place un système d'échange sécurisé dédié au sein de la zone d'échange prestataire (dit « système d'échange prestataire »).	p) Le prestataire doit mettre en place un système d'échange sécurisé dédié par commanditaire au sein de la zone d'échange commanditaire (dit « système d'échange commanditaire »). q) Le prestataire doit s'assurer que seuls les flux vers les systèmes d'échange commanditaire sont autorisés (un système d'échange commanditaire ne peut être à l'origine des flux).	o) Le prestataire doit mettre en place un système d'échange sécurisé dédié au sein de la zone d'échange tiers (dit « système d'échange tiers »).
Restriction d'accès utilisateurs	h) Le prestataire doit restreindre l'accès à la zone d'échange prestataire aux seuls administrateurs PAMS et aux administrateurs du système d'information du service.	k) Le prestataire doit restreindre l'accès à la zone d'échange commanditaire aux seuls administrateurs PAMS ainsi qu'aux employés ou applicatifs du commanditaire autorisés selon la convention de service.	k) Le prestataire doit restreindre l'accès à la zone d'échange tiers aux administrateurs PAMS, administrateurs du système d'information du service ainsi qu'aux tiers autorisés selon les conventions de service.

	IV.2.9.1. Zone d'échange prestataire	IV.2.9.2. Zone d'échange commanditaire	IV.2.9.3. Zone d'échange tiers
Suppression des données	n) Le prestataire doit s'assurer que les données sont supprimées du système d'échange prestataire au plus tard 24 heures après leur dépôt. o) Il est recommandé que le prestataire s'assure de la suppression des données transitant par le système d'échange prestataire une fois le transfert effectué.	r) Le prestataire doit s'assurer que les données sont supprimées des systèmes d'échange commanditaire au plus tard 24 heures après leur dépôt. s) Il est recommandé que le prestataire s'assure de la suppression des données transitant par les systèmes d'échange commanditaire une fois le transfert effectué.	r) Le prestataire doit s'assurer que les données sont supprimées du système d'échange tiers au plus tard 24 heures après leur dépôt. s) Il est recommandé que le prestataire s'assure de la suppression des données transitant par le système d'échange tiers une fois le transfert effectué.
Analyse des contenus	p) Le prestataire doit soumettre toutes les données transitant par le système d'échange prestataire à une analyse de contenu à la recherche de codes malveillants.	t) Le prestataire doit soumettre toutes les données transitant par les systèmes d'échange commanditaire à une analyse de contenu à la recherche de codes malveillants.	t) Le prestataire doit soumettre toutes les données transitant par le système d'échange tiers à une analyse de contenu à la recherche de codes malveillants.
Droits d'accès	m) Le prestataire doit s'assurer au sein du système d'échange prestataire que chaque administrateur PAMS et chaque administrateur du système d'information du service ne peuvent accéder qu'aux données placées sous leur périmètre de responsabilité respectif. r) Le prestataire doit s'assurer que les données, une fois déposées sur le système d'échange prestataire, ne peuvent être accédées que par l'émetteur et les destinataires qu'il aura choisis, en respectant le principe du besoin d'en connaître.	o) Le prestataire doit s'assurer que, au sein de la zone d'échange commanditaire, chaque administrateur PAMS et chaque employé ou applicatif du commanditaire autorisés ne peuvent accéder qu'aux données placées sous leur périmètre de responsabilité respectif. v) Le prestataire doit s'assurer que les données, une fois déposées sur les systèmes d'échange commanditaire, ne peuvent être accédées que par l'émetteur et les destinataires qu'il aura choisis, en respectant le principe du besoin d'en connaître.	q) Le prestataire doit s'assurer au sein du système d'échange tiers que chaque administrateur PAMS, administrateur du système d'information du service ou tiers authentifiés ne peuvent accéder qu'aux données sous leur périmètre de responsabilité respectif. v) Le prestataire doit s'assurer que les données, une fois déposées sur le système d'échange tiers, ne peuvent être accédées que par l'émetteur et les destinataires qu'il aura choisis, en respectant le principe du besoin d'en connaître.

II. Exigences relatives aux zones d'accès et la zone des enclaves d'administration tierce

	IV.2.9.4. Zone d'accès à Internet	IV.2.9.5. Zone d'accès aux ressources administrées	IV.2.9.6. Zone d'accès distants	IV.2.9.7. Zone des enclaves d'administration tierce
Objet de la zone	Pour le bon fonctionnement du service, le prestataire peut être amené à télécharger des mises à jour depuis les sites des éditeurs sur Internet à réaliser des prestations d'administration de système d'information dans le cloud public. La « zone d'accès à Internet » vise à garantir la sécurité de tels échanges.	Le prestataire peut être amené à administrer des ressources du commanditaire hébergées dans ses locaux ou à distance. Les flux d'administration pourraient transiter par des réseaux de transport tiers dont la sécurité n'est maîtrisée ni par le prestataire ni par le commanditaire. La « zone d'accès aux ressources administrées » vise à assurer l'interconnexion avec les ressources administrées à distance et *in fine* à garantir la sécurité de tels échanges.	Pour le bon fonctionnement du service, le prestataire peut être amené à effectuer des actions d'administration en situation de nomadisme selon les modalités précisées en IV.2.11. La « zone d'accès distants » vise à réduire les risques inhérents aux accès des administrateurs PAMS ou administrateurs du système d'information du service en situation de nomadisme.	Pour le bon fonctionnement du service, le commanditaire peut être amené à solliciter l'intervention exceptionnelle d'administrateurs tiers sur son système d'information (par exemple un support éditeur) et souhaiter encadrer la sécurité de cette intervention en s'appuyant sur son prestataire d'administration et de maintenance sécurisées. Il peut en être de même pour le prestataire s'agissant de l'administration du système d'information du service. La zone des enclaves d'administration tierce vise à garantir la sécurité de telles interventions.

	IV.2.9.4. Zone d'accès à Internet	IV.2.9.5. Zone d'accès aux ressources administrées	IV.2.9.6. Zone d'accès distants	IV.2.9.7. Zone des enclaves d'administration tierce
Cloisonnement physique de la zone	*Thématique traitée de manière plus globale au sein de la partie IV.2*			a) Le prestataire doit mettre en œuvre des serveurs physiquement dédiés à la zone des enclaves d'administration tierce et, en cas de recours à la virtualisation, des serveurs d'hypervision physiquement dédiés à la zone des enclaves d'administration tierce. Les dispositifs de filtrage (IV.2.6.f)) et les dispositifs de chiffrement et authentification des paquets IP (IV.2.6.l)) font l'objet d'exigences et recommandations spécifiques et ne sont donc pas traités par la présente exigence. c) Le prestataire doit mettre en œuvre des infrastructures de stockage physiquement dédiées à la zone des enclaves d'administration tierce.

	IV.2.9.4. Zone d'accès à Internet	IV.2.9.5. Zone d'accès aux ressources administrées	IV.2.9.6. Zone d'accès distants	IV.2.9.7. Zone des enclaves d'administration tierce
Cloisonnement intra-zone	-	*Thématique traitée de manière plus globale au sein de la partie IV.2*	e) Le prestataire doit cloisonner les accès distants des administrateurs PAMS d'une part et les accès distants des administrateurs du système d'information du service d'autre part.	d) Le prestataire doit dédier une enclave d'administration tierce à chaque commanditaire ayant demandé la mise à disposition d'une enclave d'administration tierce (dite « enclave d'administration tierce commanditaire »). e) Le prestataire doit dédier une enclave d'administration tierce pour les administrateurs tiers intervenant sur le système d'information du service (dite « enclave d'administration tierce prestataire »). t) Le prestataire doit mettre en œuvre un rebond au sein de la chaîne d'accès aux ressources administrées. Ce rebond doit être dédié à chaque enclave d'administration tierce et doit y être hébergé. u) Le prestataire doit s'assurer de la suppression du rebond à l'issue de l'intervention, puis de sa nouvelle instanciation dans sa configuration initiale dès que nécessaire.

	IV.2.9.4. Zone d'accès à Internet	IV.2.9.5. Zone d'accès aux ressources administrées	IV.2.9.6. Zone d'accès distants	IV.2.9.7. Zone des enclaves d'administration tierce
Zones périphériques concernées	a) Le prestataire doit s'assurer que tous les flux depuis le système d'information du service et à destination d'Internet transitent par la zone d'accès à Internet.	a) Le prestataire doit s'assurer que tous les flux entre le système d'information du service et les ressources administrées (hors ressources dont les outils d'administration sont exclusivement exposés sur Internet ou ressources non administrables à distance) transitent par la zone d'accès aux ressources administrées.	a) Le prestataire doit dédier la zone d'accès distants pour l'accès exclusif des postes d'administration ou de maintenance en situation de nomadisme. b) Le prestataire doit s'assurer que tous les accès des administrateurs PAMS ou administrateurs du système d'information du service en situation de nomadisme transitent par la zone d'accès distants.	*Non applicable*
Source des flux	c) Le prestataire doit s'assurer que les flux transitant par la zone d'accès à Internet sont initialisés depuis les zones du système d'information du service pour lesquels le besoin opérationnel le justifie.	d) Le prestataire doit s'assurer que les flux transitant par la zone d'accès aux ressources administrées sont initialisés depuis les zones du système d'information du service pour lesquelles le besoin opérationnel le justifie.	*Thématique traitée de manière plus globale au sein de la partie IV.2*	*Thématique traitée de manière plus globale au sein de la partie IV.2*
Exclusivité des flux et besoins opérationnels	d) Le prestataire doit s'assurer que seuls les flux sortants de la zone d'accès à Internet vers Internet et correspondant au strict besoin opérationnel du service sont autorisés et transitent par un dispositif de filtrage périmétrique du système d'information du service.	b) Le prestataire doit s'assurer que seuls des flux entre le système d'information du service et les ressources administrées transitent par la zone d'accès aux ressources administrées. e) Le prestataire doit s'assurer que seuls les flux entre la zone d'accès aux ressources administrées et le système d'information administré du commanditaire correspondant au strict besoin opérationnel du service sont autorisés et transitent par un dispositif de filtrage périmétrique du système d'information du service.	d) Le prestataire doit s'assurer que seuls les flux correspondant aux accès des postes d'administration ou de maintenance en situation de nomadisme sont autorisés et transitent par un dispositif de filtrage périmétrique du système d'information du service.	h) Le prestataire doit s'assurer que seuls les flux correspondant à l'accès d'administrateurs tiers aux enclaves d'administration tierce sont autorisés et transitent par un dispositif de filtrage périmétrique du système d'information du service.

	IV.2.9.4. Zone d'accès à Internet	IV.2.9.5. Zone d'accès aux ressources administrées	IV.2.9.6. Zone d'accès distants	IV.2.9.7. Zone des enclaves d'administration tierce
Dispositifs de filtrage périmétrique	b) Le prestataire doit dédier un ou plusieurs dispositifs de filtrage périmétrique à la zone d'accès à Internet. k) Le prestataire doit mettre en œuvre des mécanismes de filtrage applicatif sortant par liste blanche. l) Le prestataire doit dédier les mécanismes de filtrage applicatif à la zone d'accès à Internet. m) Le prestataire doit élaborer et tenir à jour la liste blanche de sorte à n'autoriser que l'accès aux ressources Web correspondant au strict besoin opérationnel du service.	c) Le prestataire doit dédier un ou plusieurs dispositifs de filtrage périmétrique à la zone d'accès aux ressources administrées.	c) Le prestataire doit dédier un ou plusieurs dispositifs de filtrage périmétrique à la zone d'accès distants.	b) Le prestataire doit dédier un ou plusieurs dispositifs de filtrage périmétrique à la zone des enclaves d'administration tierce.
Dispositifs de chiffrement des flux	*Thématique traitée de manière plus globale au sein de la partie IV.2*	f) Le prestataire doit mettre en œuvre des dispositifs de chiffrement et d'authentification des paquets IP pour l'accès aux ressources administrées. Le prestataire doit mettre en œuvre ces dispositifs en conformité avec le guide [G_IPSEC].	f) Le prestataire doit mettre en œuvre des dispositifs de chiffrement et d'authentification des paquets IP pour l'accès des postes d'administration ou de maintenance en situation de nomadisme à la zone d'accès distants. Le prestataire doit mettre en œuvre ces dispositifs en conformité avec le guide [G_IPSEC].	i) Le prestataire doit mettre en œuvre des dispositifs de chiffrement et d'authentification des paquets IP pour l'accès aux enclaves d'administration tierce. Le prestataire doit mettre en œuvre ces dispositifs en conformité avec le guide [G_IPSEC], le guide [G_TLS] ou le guide [G_SSH].

	IV.2.9.4. Zone d'accès à Internet	IV.2.9.5. Zone d'accès aux ressources administrées	IV.2.9.6. Zone d'accès distants	IV.2.9.7. Zone des enclaves d'administration tierce
Contraintes de mutualisation des dispositifs de chiffrement des flux	*Non applicable*	g) Le prestataire doit dédier par commanditaire des dispositifs de chiffrement et d'authentification des paquets IP. h) Il est recommandé que les dispositifs de chiffrement et d'authentification des paquets IP reposent sur un ou plusieurs socles physiques dédiés à la zone d'accès aux ressources administrées. i) Il est recommandé que les dispositifs de chiffrement et d'authentification des paquets IP reposent sur un ou plusieurs socles physiques dédiés par commanditaire et à la zone d'accès aux ressources administrées.	*Non applicable*	j) Le prestataire doit dédier un dispositif de chiffrement et d'authentification des paquets IP à chaque enclave d'administration tierce. k) Il est recommandé que le prestataire mette en œuvre un ou plusieurs dispositifs de chiffrement et d'authentification des paquets IP dédiés physiquement à la zone des enclaves d'administration tierce.
Qualification des dispositifs de chiffrement des flux		j) Il est recommandé que les dispositifs de chiffrement et d'authentification des paquets IP soient des produits qualifiés par l'ANSSI et soient utilisés conformément aux conditions de leur qualification.	g) Il est recommandé que les dispositifs de chiffrement et d'authentification des paquets IP soient des produits qualifiés par l'ANSSI et soient utilisés conformément aux conditions de leur qualification.	l) Il est recommandé que les dispositifs de chiffrement et d'authentification des paquets IP soient des produits qualifiés par l'ANSSI et soient utilisés conformément aux conditions de leur qualification.

	IV.2.9.4. Zone d'accès à Internet	IV.2.9.5. Zone d'accès aux ressources administrées	IV.2.9.6. Zone d'accès distants	IV.2.9.7. Zone des enclaves d'administration tierce
Mécanismes de rupture et analyse des flux	g) Le prestataire doit mettre en œuvre des mécanismes de rupture et d'analyse des flux au sein de la zone d'accès à Internet. h) Le prestataire doit dédier les mécanismes de rupture et d'analyse des flux à la zone d'accès à Internet. Les mécanismes doivent reposer sur un ou plusieurs socles physiques dédiés à la zone d'accès à Internet ou prendre la forme d'une instance dédiée sur un socle physique commun avec les mécanismes de rupture et d'analyse des flux de la zone d'échange tiers. i) Il est recommandé que les mécanismes de rupture et d'analyse protocolaire reposent sur un ou plusieurs socles physiques dédiés à la zone d'accès à Internet. j) Le prestataire doit analyser les flux de moindre confiance transitant par la zone d'accès à Internet en vue de détecter des codes malveillants et de s'assurer de la conformité protocolaire des échanges. L'évaluation du niveau de confiance accordé à chaque flux s'appuie sur les résultats issus de l'appréciation des risques (IV.2.1.a)).	*Non applicable*		*Thématique traitée de manière plus globale au sein de la partie IV.2*

	IV.2.9.4. Zone d'accès à Internet	IV.2.9.5. Zone d'accès aux ressources administrées	IV.2.9.6. Zone d'accès distants	IV.2.9.7. Zone des enclaves d'administration tierce
Mécanismes d'authentification, Annuaire et Gestion des comptes	e) Le prestataire doit mettre en place des mécanismes d'authentification pour les accès à la zone d'accès à Internet en s'appuyant sur un annuaire sans adhérence avec les annuaires stockant des comptes d'administration. f) Il est recommandé de dédier un annuaire à la zone d'accès à Internet.	*Non applicable*	h) Le prestataire doit mettre en place des mécanismes d'authentification du poste, de l'administrateur PAMS et de l'administrateur du système d'information du service en situation de nomadisme, en s'appuyant sur un annuaire sans adhérence avec les annuaires stockant des comptes d'administration. i) Il est recommandé de dédier un annuaire à la zone d'accès distants. j) Il est recommandé que les mécanismes d'authentification reposent sur des certificats électroniques délivrés par l'infrastructure définie en IV.2.10.n). k) Il est recommandé que les mécanismes d'authentification reposent sur des certificats électroniques délivrés par des prestataires de services de certification électronique qualifiés par l'ANSSI [CRYPTO_A7].	m) Le prestataire doit mettre en place des mécanismes d'authentification au niveau de la zone des enclaves d'administration tierce pour l'accès des administrateurs tiers. Ces mécanismes reposent sur un annuaire sans adhérence avec les annuaires hébergeant des comptes d'administration. n) Le prestataire doit dédier un annuaire à la zone des enclaves d'administration tierce. p) Le prestataire doit activer à la demande les comptes des administrateurs tiers pour la connexion à chaque enclave d'administration tierce. Le prestataire doit désactiver ces comptes à la fin de chaque intervention.
Gouvernance des accès	*Thématique traitée de manière plus globale au sein de la partie IV.2*		f) Le prestataire doit mettre en œuvre avec le commanditaire une procédure organisationnelle encadrant l'accès des administrateurs tiers à l'enclave d'administration tierce commanditaire et in fine aux ressources administrées du commanditaire. g) Le prestataire doit mettre en œuvre une procédure organisationnelle encadrant l'accès des administrateurs tiers à l'enclave d'administration tierce prestataire et in fine aux ressources administrées du système d'information du service.	

<table>
<tr><th></th><th>IV.2.9.4. Zone d'accès à Internet</th><th>IV.2.9.5. Zone d'accès aux ressources administrées</th><th>IV.2.9.6. Zone d'accès distants</th><th>IV.2.9.7. Zone des enclaves d'administration tierce</th></tr>
<tr><td>Gestion des secrets</td><td colspan="2">Non applicable</td><td colspan="2">r) Il est recommandé de mettre en œuvre une authentification double facteur pour l’accès des administrateurs tiers.

s) Le prestataire doit renouveler les secrets d’authentification des tiers, au moins tous les sept jours dans le cas d’une authentification simple facteur et dans un délai défini formellement dans le cas d’une authentification double facteur. Ces secrets renouvelés ne sont communiqués aux tiers que lors de leur prochaine intervention.</td></tr>
<tr><td>Respect des exigences sur les actions d'admin.</td><td>Thématique traitée de manière plus globale au sein de la partie IV.2</td><td colspan="2">Non applicable</td><td>w) Le prestataire doit s’assurer que les actions d’administration de l’administrateur tiers respectent les exigences de la partie IV.2.12.</td></tr>
<tr><td>Traçabilité</td><td colspan="2">Thématique traitée de manière plus globale au sein de la partie IV.2</td><td colspan="2">o) Le prestataire doit mettre en œuvre une traçabilité nominative pour les accès des administrateurs tiers, que les comptes utilisés soient individuels (associés à une unique personne physique) ou génériques.

v) Le prestataire doit assurer une traçabilité des accès aux ressources administrées réalisés au travers de chaque enclave d’administration tierce.</td></tr>
<tr><td>Supervision</td><td>Thématique traitée de manière plus globale au sein de la partie IV.2</td><td colspan="2">l) Le prestataire doit mettre en place une journalisation des accès à la zone d’accès distants. Il doit effectuer une revue mensuelle des accès (comptes autorisés et journaux d’accès) à la zone d’accès distants.</td><td>q) Le prestataire doit mettre en œuvre une supervision des comptes des administrateurs tiers afin de détecter et alerter en cas de compte actif pendant une durée supérieure à vingt-quatre heures.</td></tr>
<tr><td>Systèmes d'échange</td><td colspan="4">Non applicable</td></tr>
<tr><td>Restriction d'accès utilisateurs</td><td colspan="4">Thématique traitée au sein de la partie IV.2</td></tr>
<tr><td>Suppression des données</td><td colspan="2">Non applicable</td><td colspan="2">Thématique traitée au sein de la partie IV.2-</td></tr>
<tr><td>Analyse des contenus</td><td colspan="4">Non applicable</td></tr>
<tr><td>Droits d'accès</td><td colspan="4">Thématique traitée au sein de la partie IV.2 et IV.3</td></tr>
<tr><td>Guide de mise en œuvre de la zone</td><td>n) Il est recommandé que le prestataire respecte les recommandations de l’ANSSI [G_INTERNET] pour la mise en œuvre de la zone d’accès à Internet.</td><td colspan="3">Non applicable</td></tr>
</table>