Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Premier ministre

Agence nationale de la sécurité des systèmes d'information

Prestataires d'accompagnement et de conseil en sécurité des systèmes d'information (PACS)

Référentiel d'exigences

Version 0.3.0 du 5 novembre 2020

HISTORIQUE DES VERSIONS			
DATE	**VERSION**	**EVOLUTION DU DOCUMENT**	**REDACTEUR**
05/11/2020	0.3	*Version publiée pour appel à commentaire*	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 systèmes d'information des entreprises et organisations se transforment en profondeur, s'ouvrent vers l'extérieur et accueillent en continu des services innovants. Les entreprises et organisations doivent intégrer des technologies de plus en plus nombreuses (Big Data, Internet des Objets, Intelligence Artificielle, Industrie 4.0…) interagir avec de plus en plus d'acteurs (fournisseurs de services cloud, partenaires, sous-traitants, fournisseurs de produits, prestataires d'infogérance…) et faire face à une internationalisation de leur activité. A cela s'ajoutent une extension des périmètres applicables et un renforcement du niveau d'exigence des réglementations ([LPM], [NIS], [RGPD], [RGS], [EIDAS], [PSSIE], etc.) qui obligent les entreprises et organisations à mieux maitriser le niveau de sécurité de leurs systèmes d'information et à en élever le niveau.

Maintenir la confiance dans ces conditions représente un défi quotidien, notamment dans un contexte de menaces toujours plus actives et plus variées. Les organismes doivent mettre en place des dispositifs adaptés et proportionnés pour protéger leurs systèmes d'informations et répondre aux dispositions réglementaires. Tout d'abord, il s'agit d'identifier quelles mesures de sécurité (organisationnelles, physiques et techniques) mettre en place en priorité et définir la manière dont elles doivent être appliquées. Ceci passe par des démarches d'analyse de risque et de définition de plans d'action sécurité.

Face à cette évolution permanente des risques et des réglementations, il émerge un besoin des entreprises et organisations d'être soutenues dans leurs démarches de gestion des risques et de protection des systèmes d'information dont elles ont la responsabilité. Ces accompagnements sont parfois confiés à des prestataires externes afin de bénéficier de main d'œuvre et d'expertise souvent difficiles à réunir au sein même de l'organisme.

Ces activités de sécurisation des systèmes d'information viennent compléter d'autres types d'activités spécifiques de sécurité des systèmes d'information parmi lesquelles l'audit de sécurité des systèmes information, la détection et la réponse aux incidents de sécurité des systèmes d'information, respectivement objet des référentiels [PASSI], [PDIS] et [PRIS] également proposés par l'ANSSI.

I.1.2. Objet du document

Ce document constitue le référentiel d'exigences applicables à un prestataire d'accompagnement et de conseil en sécurité des systèmes d'information (PACS), ci-après dénommé « le prestataire ».

Il a vocation à permettre la qualification de cette famille de prestataires selon les modalités décrites au chapitre III.1.

Il permet au commanditaire d'une prestation de disposer de garanties sur les compétences du prestataire et de son personnel, sur la qualité des prestations et notamment l'application de démarches d'analyse adaptées, ainsi que sur la confiance que le commanditaire peut leur accorder, en particulier en matière de confidentialité des informations qui lui sont confiées.

Il ne se substitue ni à 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, ni à l'application des règles générales imposées aux prestataires en leur qualité de professionnels, notamment leur devoir de conseil vis-à-vis de leurs commanditaires.

I.1.3. Structure du document

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

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

Le chapitre III présente les modalités de la qualification permettant d'attester de la conformité des prestataires d'accompagnement et de conseil en sécurité des systèmes d'information aux exigences qui leur sont applicables.

Le chapitre IV présente les exigences relatives aux prestataires.

Le chapitre IV présente les exigences relatives aux consultants employés par le prestataire.

Le chapitre VI présente les exigences relatives au déroulement d'une prestation d'accompagnement et de conseil en sécurité des systèmes d'information.

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

L'Annexe 2 présente les missions et compétences attendues des consultants du prestataire.

L'Annexe 3 présente des recommandations aux commanditaires de prestations d'accompagnement et de conseil en sécurité des systèmes d'information.

L'Annexe 4 présente les prérequis minimums à fournir par les commanditaires dans le cadre d'une prestation d'accompagnement et de conseil en sécurité des systèmes d'information.

I.2. Identification du document

Le présent référentiel est dénommé « Prestataires d'accompagnement et de conseil en sécurité des systèmes d'information - 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 principaux acronymes utilisés dans le présent référentiel sont :

ANSSI	Agence nationale de la sécurité des systèmes d'information
CPC	Correspondant de la prestation chez le commanditaire
LID	Lutte informatique défensive
MCO	Maintien en condition opérationnelle
MCS	Maintien en condition de sécurité
OIV	Opérateur d'importance vitale
OSE	Opérateur de services essentiels
PACS	Prestataire d'accompagnement et de conseil en 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 d'incidents de sécurité
PRIS	Prestataire de réponse aux incidents de sécurité
PSSI	Politique de sécurité des systèmes d'information

I.3.2. Définitions

Les définitions ci-dessous s'appuient sur les normes de la suite ainsi que sur la stratégie nationale pour la sécurité du numérique.

Accompagnement et conseil en sécurité des systèmes d'information – Prestation intellectuelle liée à un périmètre défini ayant pour but d'accompagner le commanditaire dans la sécurisation de son système d'information. La démarche de conseil ne consistant pas à faire à la place du commanditaire, celui-ci conserve autonomie et responsabilité dans la sécurisation de son système d'information.

Commanditaire – entité faisant appel au service d'accompagnement et de conseil en sécurité des systèmes d'information.

Consultant - personne physique liée contractuellement avec le prestataire, disposant d'une attestation individuelle de compétence, amenée à intervenir dans le cadre de la prestation pour prendre en charge certaines ou toutes les activités identifiées au chapitre II du référentiel.

Convention de service – accord écrit entre un commanditaire et un prestataire pour la réalisation de la prestation.

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 de manière évidente. 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 d'origine réglementaire.

Expert – personne physique liée contractuellement avec le prestataire. L'expert est reconnu par le responsable d'équipe de la prestation comme ayant une ou plusieurs compétences spécifiques, nécessaires à l'appréhension du périmètre de la prestation et à l'exécution de certaines tâches nécessitant de telles compétences ou la maitrise d'un domaine d'expertise, et non nécessairement détenues par les consultants.

Mesure de sécurité – ensemble des moyens techniques et non techniques de protection, permettant à l'entité responsable d'un un système d'information de réduire le risque d'atteinte à la sécurité de l'information ou des traitements.

Périmètre – environnement physique, logique et organisationnel dans lequel se trouve le système d'information ou la portion du système d'information, concerné par la prestation.

Prestataire – entité proposant une offre de service d'accompagnement et de conseil en sécurité des systèmes d'information conforme au référentiel.

Référentiel – le présent document.

Responsable d'équipe de prestations de conseil - personne responsable de la prestation d'accompagnement et de conseil en sécurité du système d'information et de la constitution de l'équipe de réalisation de la prestation, disposant d'une attestation individuelle de compétences. Ses missions sont détaillées dans l'Annexe 2.

Sécurité de l'information – préservation de la confidentialité, de l'intégrité et de la disponibilité de l'information.

Sécurité d'un système d'information – ensemble des moyens techniques et non-techniques de protection, prévention et récupération, permettant à un système d'information de résister à des évènements susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données, traitées ou transmises et des services connexes que ces systèmes offrent ou rendent accessibles.

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

Système d'information cible – sous-ensemble de système d'information concerné par la prestation. Il est inclus dans le périmètre.

Tiers – personne ou organisme indépendant du prestataire et du commanditaire.

II. Activités visées par le référentiel

Ce chapitre présente les différentes activités d'accompagnement et de conseil en sécurité des systèmes d'information traitées dans le référentiel.

Les activités couvertes par ce référentiel sont les suivantes :

- le conseil en homologation de sécurité des systèmes d'information ;
- le conseil en gestion des risques de sécurité des systèmes d'information ;
- le conseil en sécurité des architectures des systèmes d'information.

Dans toutes les activités visées, la démarche mise en œuvre ne consiste pas pour le prestataire à se substituer au commanditaire. Ce dernier doit, en effet, conserver autonomie et responsabilité dans la démarche de sécurisation de son système d'information et de son maintien dans le temps.

II.1. Conseil en homologation de sécurité des systèmes d'information

L'activité de conseil en homologation de sécurité des systèmes d'information consiste à accompagner le commanditaire dans les différentes étapes qui permettent de constituer le dossier d'homologation, d'aboutir à un rapport d'aide à la décision d'homologation puis de mettre en place les dispositifs de suivi de l'homologation et du processus de maintien en condition de sécurité du système d'information. Les différentes études réalisées dans le cadre de l'homologation (audit de sécurité, conseil en analyse de risque, conseil en architecture, etc.) n'entrent pas dans la définition de cette activité et peuvent être adressées via d'autres parties du présent référentiel ou via d'autres référentiels proposés par l'ANSSI.

II.2. Conseil en gestion des risques de sécurité des systèmes d'information

L'activité de conseil en gestion des risques de sécurité des systèmes d'information consiste à accompagner le commanditaire dans les différentes étapes qui permettent d'aboutir à une appréciation pertinente des risques pesant sur le système d'information cible et à la proposition d'un plan de traitement des risques associé.

Cet accompagnement intervient soit dans le cadre de la conception d'un système d'information, soit dans le cadre d'une revue d'un système d'information existant.

II.3. Conseil en sécurité des architectures des systèmes d'information

L'activité de conseil en sécurité des architectures des systèmes d'information consiste à accompagner le commanditaire dans la structuration des choix techniques et organisationnels de définition d'un système d'information en s'assurant de répondre à des exigences de sécurité adaptées au périmètre cible et au contexte d'activité du commanditaire. Ces choix doivent également prendre en compte les efforts de mise en œuvre et de maintien en condition associés ainsi que la maturité du commanditaire.

Les recommandations émises peuvent porter sur les architectures des systèmes d'information en tant que telles ainsi que sur les configurations des éléments composant l'architecture (systèmes, réseaux, applicatifs, etc.).

Cet accompagnement intervient soit dans le cadre de la conception d'un système d'information, soit dans le cadre d'une revue d'un système d'information existant.

III. Qualification des prestataires d'accompagnement et de conseil en sécurité des systèmes d'information

III.1. Modalités de la qualification

Le référentiel contient les exigences et les recommandations à destination des prestataires d'accompagnement et de conseil en sécurité des systèmes d'information.

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

Un organisme peut demander la qualification d'un service d'accompagnement et de conseil en sécurité des systèmes d'information interne, c'est-à-dire un service utilisé pour répondre à tout ou partie de ses propres besoins en la matière. Dans ce cas, le processus de qualification ainsi que les exigences applicables pour obtenir la qualification sont strictement identiques à ceux définis dans le présent référentiel. Le terme « prestataire » désigne donc indifféremment un organisme offrant des prestations d'accompagnement et de conseil en sécurité des systèmes d'information pour son propre compte ou pour le compte d'autres organismes.

Les exigences doivent être respectées par les prestataires pour obtenir la qualification.

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

Le référentiel donne également aux commanditaires des recommandations et la liste minimum des prérequis à fournir pour pouvoir réaliser une prestation qualifiée PACS, respectivement présentes dans l'Annexe 3 et l'Annexe 4 du présent référentiel. Ces recommandations et prérequis applicables au commanditaire ne font pas l'objet de vérification pour obtenir la qualification.

III.2. Portée de la qualification

Le prestataire d'accompagnement et de conseil en sécurité des systèmes d'information peut demander la qualification pour tout ou partie des activités décrites au chapitre II du présent référentiel :

- Conseil en homologation de sécurité des systèmes d'information (HOMOL)

- Conseil en gestion des risques de sécurité des systèmes d'information (RISQUE)

- Conseil en sécurité des architectures des systèmes d'information (ARCHI)

Toutefois, la qualification d'un prestataire d'accompagnement et de conseil en sécurité de systèmes d'information ne portant que sur l'activité de conseil en homologation de sécurité de systèmes d'information (HOMOL) n'est pas autorisée. Une telle qualification doit porter également sur l'activité de conseil en gestion des risques de sécurité des systèmes d'information (HOMOL + RISQUE) proposée dans le référentiel.

Les cinq portées de qualification ainsi définies sont les suivantes :

- RISQUE

- (HOMOL + RISQUE)

- ARCHI

- ARCHI + RISQUE

- ARCHI + (HOMOL +RISQUE).

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

Est considérée comme une prestation qualifiée au sens du référentiel, une prestation respectant le déroulement décrit au chapitre VI, dont les activités sont réalisées par un ou plusieurs consultants évalués individuellement et reconnus compétents pour ces activités, conformément au chapitre IV et à l'Annexe 2 et travaillant pour un prestataire respectant les exigences du chapitre IV.

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

Une prestation d'accompagnement et de conseil en sécurité des systèmes d'information qualifiée peut être associée à la réalisation de prestations complémentaires (audit, développement, intégration de produits de sécurité, supervision et détection, etc.) sans perdre le bénéfice de la qualification. Un prestataire d'accompagnement et de conseil en sécurité des systèmes d'information qualifié peut notamment être qualifié pour d'autres familles de prestataires de services de confiance (PASSI, PDIS, PRIS, etc.).

III.3. Avertissement

Une prestation d'accompagnement et de conseil en sécurité des systèmes d'information 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, la perte ou l'indisponibilité de son système d'information.

Ainsi, dans le cas d'une prestation non qualifiée, il est recommandé au commanditaire de demander au prestataire un document listant l'ensemble des exigences de ce référentiel non couvertes dans le cadre de la prestation, afin de connaître les risques auxquels il s'expose. Le prestataire est tenu d'accéder favorablement à cette demande.

IV. Exigences relatives au prestataire d'accompagnement et de conseil en sécurité des systèmes d'information

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'accompagnement et de conseil en sécurité des systèmes d'information auprès du commanditaire.

d) 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.

e) 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.

f) 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.

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

h) Le prestataire doit apporter une preuve suffisante que son organisation, ses moyens mis en œuvre pour délivrer la prestation et 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.

i) 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.

j) Le prestataire doit réaliser sa prestation dans le cadre d'un accord de non-divulgation[1] et d'une convention de service d'accompagnement et de conseil en sécurité des systèmes d'information approuvée formellement et par écrit par le commanditaire, et conforme aux exigences du chapitre VI.2.

k) Le prestataire doit prévoir l'enregistrement et le traitement des réclamations portant sur sa prestation déposées par les commanditaires et les tiers (hébergeurs, sous-traitants, etc.).

l) 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.

[1] Pour les étapes de qualification préalable d'aptitude à la réalisation de la prestation (chapitre V.1) et d'élaboration d'une convention de service (chapitre VI.2).

IV.2. Charte d'éthique

a) Le prestataire doit disposer d'une charte d'éthique signée par chaque consultant du prestataire prévoyant notamment que :

- les prestations sont réalisées avec loyauté, discrétion et impartialité ;
- le prestataire s'assure que les consultants ne recourent qu'aux méthodes et outils validés par le lui-même ;
- le prestataire s'engage à ne pas divulguer d'informations à un tiers, même anonymisées et décontextualisées, obtenues ou générées dans le cadre de leurs activités, sauf autorisation écrite du commanditaire ;
- les consultants s'engagent à signaler au prestataire tout contenu manifestement illicite découvert durant la prestation ;
- le prestataire s'engage à respecter la législation et la réglementation nationale en vigueur ainsi que les bonnes pratiques liées à leurs activités d'accompagnement et de conseil en sécurité des systèmes d'information.

b) Le prestataire doit faire appliquer la charte d'éthique.

IV.3. Gestion des ressources et des compétences

a) Le prestataire doit s'assurer, pour chaque prestation, que les consultants désignés ont les qualités et les compétences requises. Chaque consultant[3] de l'équipe de réalisation[4] doit disposer d'une attestation individuelle de compétence[5] pour les activités qui lui sont affectées au cours de la prestation.

b) Le prestataire doit s'assurer du maintien à jour des compétences des consultants dans les activités pour lesquelles ils ont obtenu une attestation individuelle de compétence[2]. Pour cela, le prestataire doit disposer d'un processus de formation continue et permettre à ses consultants d'assurer une veille technologique.

c) Le prestataire doit, en matière de recrutement, procéder à une vérification, sauf impossibilité tracée, des formations, compétences et références professionnelles des consultants et de la véracité de leur curriculum vitae.

d) Le prestataire est responsable des méthodes et outils utilisés par ses consultants et de leur bonne utilisation pour la réalisation de la prestation. Pour cela, le prestataire doit assurer une veille technologique sur leur mise à jour et leur pertinence (efficacité et confiance).

e) Le prestataire doit justifier, au travers des consultants évalués au titre de la qualification du prestataire, qu'il dispose des compétences techniques, théoriques et pratiques, afférentes aux activités citées aux chapitres II.1 à II.3, couvrant les domaines détaillés en Annexe 2.

f) Le prestataire doit mettre en place un processus de sensibilisation des consultants à la réglementation en vigueur sur le territoire de l'Union Européenne et applicable à leurs missions.

g) Le prestataire doit s'assurer que les consultants ne font pas l'objet d'une inscription, qui n'est pas compatible 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.

[2] Le prestataire peut par exemple mettre en place une formation continue, des modules d'auto-formation, des séminaires internes, s'abonner à des revues spécialisées, ou toute autre méthode lui permettant d'assurer l'évolutivité de ses compétences ainsi que celles de ses consultants.

IV.4. Protection de l'information

a) Le prestataire doit respecter les prescriptions de l' [II 901] sur les systèmes d'information Diffusion Restreinte pour ses systèmes d'informations traitant les informations sensibles relatives à la prestation (documents sensibles transmis par le commanditaire, rapports de prestation, informations sensibles collectées, etc.).

b) Le prestataire doit homologuer au niveau Diffusion Restreinte le système d'information utilisé dans le cadre de ses prestations d'accompagnement et de conseil en sécurité des systèmes d'information. Si le commanditaire dispose d'un système d'information déjà homologué au niveau Diffusion Restreinte pour d'autres prestations, telles que celles relatives au référentiel [PASSI], ce dernier doit :

   - mettre en place un cloisonnement *a minima* logique du système d'information utilisé dans le cadre de ses prestations d'accompagnement et de conseil en sécurité des systèmes d'information ;
   - dédier un serveur physique au stockage des documents relatifs aux prestations d'accompagnement et de conseil en sécurité des systèmes d'information.

c) Le prestataire doit utiliser la démarche décrite dans le guide [G_HOMOLOGATION] pour homologuer son système d'information utilisé dans le cadre de ses prestations d'accompagnement et de conseil en sécurité des systèmes d'information.

d) Dans le cas où le commanditaire en fait la demande explicite, le prestataire doit être en mesure de stocker toutes les informations relatives à la prestation dans un espace logique[3] dédié à la prestation et accessible uniquement par les consultants participant à la prestation.

[3] Par exemple, dossier avec implémentation d'un système de gestion des droits limitant l'accès aux consultants de la prestation.

V. Exigences relatives aux consultants

V.1. Aptitudes générales

a) Le consultant doit posséder les qualités personnelles identifiées au chapitre 7.2.2 de la norme [ISO19011].

b) Le responsable d'équipe de prestation de conseil doit posséder les qualités personnelles identifiées au chapitre 7.2.3.4 de la norme [ISO19011].

c) Le consultant doit être sensibilisé à la législation en vigueur sur le territoire français et applicable à ses missions.

d) Le responsable d'équipe de prestation de conseil doit maîtriser la législation en vigueur[4] sur le territoire français et applicable à ses missions ainsi qu'à celles des consultants qu'il encadre.

e) Le consultant doit disposer de qualités rédactionnelles, de rigueur et de synthèse et savoir s'exprimer à l'oral de façon claire et compréhensible.

f) Le consultant doit disposer de qualités d'écoute et de communication lui permettant d'engager un dialogue constructif avec les différents niveaux d'interlocuteur du commanditaire.

g) Le consultant doit régulièrement mettre à jour ses compétences conformément aux processus de formation et de veille du prestataire (voir chapitre IV.3) par une veille active sur les méthodologies et les outils utilisés dans le cadre de ses missions.

h) ⓘ Il est recommandé que les consultants participent à l'évolution de l'état de l'art par une contribution à des évènements professionnels de leurs domaines de compétence, à des travaux de recherche ou la publication d'articles.

V.2. Expérience

a) ⓘ Il est recommandé que le responsable d'équipe de prestation de conseil justifie d'au moins trois années d'expérience dans le domaine de la sécurité des systèmes d'information.

b) ⓘ Il est recommandé que le consultant en gestion des risques et conformité justifie :

- d'au moins deux années d'expérience dans le domaine de la sécurité des systèmes d'information ;
- d'au moins trois années d'expérience dans le domaine de la gestion du risque, incluant mais pas exclusivement le risque en sécurité des systèmes d'information.

c) ⓘ Il est recommandé que le consultant en sécurité des architectures des systèmes d'information justifie :

- d'au moins deux années d'expérience dans le domaine de la sécurité des systèmes d'information ;
- d'au moins trois années d'expérience dans le domaine des technologies des systèmes d'information ;
- d'au moins une année d'expérience dans le domaine de la sécurité des architectures des systèmes d'information.

V.3. Aptitudes et connaissances spécifiques aux activités

a) Le consultant doit être en mesure de réaliser la prestation conformément aux exigences du chapitre VI.

[4] Notamment les différents textes réglementaires listés dans la partie I.3 de l'Annexe 2.

b) Le consultant doit assurer les missions selon son profil, tel que défini dans l'Annexe 2.

c) Le consultant doit disposer des compétences requises par son profil, tel que défini dans l'Annexe 2.

d) ⓘ Il est recommandé que le consultant soit sensibilisé à l'ensemble des autres activités pour lesquelles le prestataire demande la qualification.

V.4. Engagements

a) Le consultant doit avoir une relation contractuelle avec le prestataire.

b) L'expert doit avoir une relation contractuelle avec le prestataire.

c) Le consultant doit avoir signé la charte d'éthique élaborée par le prestataire (voir chapitre IV.2).

d) L'expert intervenant doit avoir signé la charte d'éthique élaborée par le prestataire (voir chapitre IV.2).

VI. Exigences relatives au déroulement d'une prestation d'accompagnement et de conseil en sécurité des systèmes d'information

Dans la suite de ce chapitre, les exigences auxquelles doivent se conformer les prestataires sont regroupées dans les différentes étapes du déroulement d'une prestation d'accompagnement et de conseil en sécurité des systèmes d'information, à savoir :

- étape 1 : qualification préalable d'aptitude à la réalisation de la prestation ;
- étape 2 : établissement d'une convention de service ;
- étape 3 : préparation et déclenchement de la prestation ;
- étape 4 : exécution de la prestation ;
- étape 5 : restitution continue de la prestation ;
- étape 6 : élaboration du rapport de prestation ;
- étape 7 : clôture de la prestation.

VI.1. Étape 1 : qualification préalable d'aptitude à la réalisation de la prestation

a) Le prestataire doit vérifier que le commanditaire a identifié correctement le périmètre de la prestation.

b) Le prestataire doit s'assurer que la prestation est adaptée au contexte et aux objectifs visés par le commanditaire. A défaut, le prestataire notifie formellement le commanditaire préalablement à la prestation.

c) Le prestataire doit informer, dans la mesure du possible et à titre de conseil, le commanditaire des recommandations contenues dans l'Annexe 3.

d) L'Annexe 4 du présent document fournit la liste des prérequis nécessaires à la réalisation d'une prestation qualifiée. Le prestataire doit obtenir un engagement du commanditaire sur la fourniture de ces prérequis. Si le commanditaire est dans l'incapacité de fournir un ou plusieurs prérequis, le prestataire doit informer formellement le commanditaire que la prestation ne pourra pas être qualifiée.

e) Le prestataire doit demander au commanditaire, avant le début de la prestation, la fourniture d'un inventaire précis des prérequis disponibles et mobilisables (documentation, disponibilité des interlocuteurs du commanditaire, etc.), incluant pour chacun d'entre eux, dans la mesure du possible, le niveau d'utilisabilité estimé de ces prérequis (niveaux de structuration, d'actualité, d'exhaustivité et de validation du document).

f) Le prestataire doit demander au commanditaire, avant le début de la prestation :

- la fourniture d'un inventaire précis des prérequis disponibles (documentation, disponibilité des interlocuteurs du commanditaire, etc.), incluant pour chacun d'entre eux, dans la mesure du possible, le niveau d'utilisabilité estimé de ces prérequis (niveaux de structuration, d'actualité, d'exhaustivité et de validation du document) ;
- la liste des intervenants du commanditaire mobilisables durant la prestation.

VI.2. Étape 2 : établissement d'une convention de service

a) Le prestataire doit établir une convention de service avec le commanditaire avant l'exécution de la prestation.

b) La convention de service doit être signée par un représentant légal du commanditaire et du prestataire. Toute modification de la convention de service doit être soumise à acceptation du commanditaire.

VI.2.1. Modalités de la prestation

La convention de service doit :

a) décrire le périmètre de la prestation, la démarche générale d'accompagnement et de conseil en sécurité des systèmes d'information, les activités et les modalités de la prestation (objectifs, jalons, livrables attendus en entrée, prérequis, etc.), le lieu d'exécution de la prestation (pays) ;

b) préciser que la prestation est qualifiée ou non ;

c) préciser les prérequis attendus en entrée du commanditaire, dont la liste minimum pour la réalisation d'une prestation qualifiée est fournie en Annexe 4 ;

d) préciser les livrables attendus, les réunions d'ouverture et de clôture, les publics destinataires, le niveau de sensibilité ou de classification des systèmes impactés et les modalités de protection de l'information associées ;

e) décrire les moyens techniques (matériel et outils) et organisationnels mis en œuvre par le prestataire dans le cadre de sa prestation ;

f) décrire les méthodes de communication qui seront employées lors de la prestation entre le prestataire, et le commanditaire ;

g) prévoir les moyens logistiques devant être mis à disposition du prestataire par le commanditaire (moyens matériels, humains, techniques, etc.) ;

h) définir les règles de titularité des éléments protégés par la propriété intellectuelle tels que les outils développés spécifiquement par le prestataire dans le cadre de la prestation, les bases de connaissance ou le rapport de prestation ;

i) préciser les traitements qui ne peuvent être menés sur les informations collectées sans autorisation expresse du commanditaire et éventuellement accord ou présence de celui-ci, ainsi que les modalités associées (mise en œuvre, personnes présentes, durée, plage horaire, exécutant, description des données sensibles et des actions autorisées, etc.).

VI.2.2. Organisation

La convention de service doit :

a) préciser le nom du correspondant de la prestation chez le commanditaire (CPC) en charge, de mettre en relation le prestataire avec les différents correspondants impliqués ;

b) préciser les noms, rôles, responsabilités ainsi que les droits et besoin d'en connaître des personnes désignées par le prestataire et le commanditaire ;

c) le cas échant, prévoir et prendre en compte les modalités de collaboration avec les prestataires tiers concernés (sous-traitants du commanditaire, etc.) ;

d) spécifier que le prestataire ne recourt pas à des consultants n'ayant pas de relation contractuelle avec lui, n'ayant pas signé sa charte d'éthique, n'ayant pas obtenu une attestation individuelle de compétence[5] ou ayant fait l'objet d'une inscription au bulletin n°3 du casier judiciaire ;

e) spécifier les instances de gouvernance de la prestation mises en place et leur fréquence de réunion (réunions, comités de pilotage, etc.).

VI.2.3. Responsabilités

La convention de service doit :

[5] Voir [PROCESS_QUALIF].

a) spécifier que le prestataire informe le commanditaire en cas de manquement à la convention et réciproquement ;

b) spécifier que le prestataire s'engage à ce que les tâches réalisées dans le cadre de la prestation restent strictement en adéquation avec les objectifs de la prestation ;

c) spécifier que le commanditaire et le prestataire remplissent toutes les obligations légales et réglementaires applicables aux activités menées dans le cadre de la prestation ;

d) définir les responsabilités et les précautions d'usage à respecter par l'ensemble des parties concernant les risques potentiels liés à la prestation, notamment en matière de confidentialité des informations collectées et analysées ;

e) spécifier que le prestataire dispose d'une assurance professionnelle couvrant les éventuels dommages causés lors de la réalisation des activités d'accompagnement et de conseil et préciser la couverture de celle-ci ainsi qu'inclure l'attestation d'assurance.

VI.2.4. Confidentialité

La convention de service doit :

a) indiquer que le prestataire ne peut disposer des données transmises et générées par le commanditaire, leur disposition étant réservée au commanditaire.

b) indiquer que le prestataire, ses consultants et experts ne divulguent aucune information relative à la prestation à des tiers, sauf autorisation écrite du commanditaire.

c) indiquer que le prestataire 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.

d) indiquer que le prestataire protège les données transmises à des tiers, en confidentialité, conformément à leur niveau de sensibilité ou de classification.

e) indiquer que le prestataire 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.

La convention de service doit :

f) préciser que le prestataire garantit la confidentialité des informations confidentielles échangées ou produites dans le cadre de la prestation, et s'assure de la non divulgation à un tiers par ses consultants et ses experts de ces informations, sauf autorisation écrite du commanditaire

g) spécifier que le prestataire peut, sauf refus formel et écrit du commanditaire, conserver certains types d'informations liées à la prestation une fois celle-ci terminée. Le prestataire doit identifier ces types d'informations dans la convention (ex : livrables, informations, documents, etc.) et préciser, le cas échéant, la durée et les modalités de conservation des informations confidentielles échangées ou produites dans le cadre de la prestation ;

h) spécifier que le prestataire anonymise et décontextualise (suppression de toute information permettant d'identifier le commanditaire, de toute information à caractère personnel, etc.) l'ensemble des informations que le commanditaire l'autorise à conserver ;

i) spécifier que le prestataire détruit l'ensemble des informations relatives au commanditaire à l'issue de la prestation, selon un délai convenu entre le prestataire et le commanditaire et défini dans la convention de service, à l'exception de celles pour lesquelles il a reçu une autorisation de conservation de la part du commanditaire ;

j) préciser les modalités (contenu, forme, etc.) de rédaction des livrables.

VI.2.5. Lois et réglementations

La convention de service doit :

a) identifier et appliquer le droit d'un Etat membre de l'Union Européenne ;

b) préciser les moyens techniques et organisationnels mis en œuvre par le prestataire pour le respect de la législation applicable [6]notamment ceux concernant :

- les données à caractère personnel ;
- l'abus de confiance ;
- le secret des correspondances privées ;
- le secret médical ;
- l'atteinte à la vie privée ;
- l'accès ou le maintien frauduleux à un système d'information ;
- le secret professionnel.

c) identifier les éventuelles exigences légales et réglementaires spécifiques auxquelles est soumis le système d'information cible ; préciser, le cas échéant, les exigences légales et réglementaires spécifiques auxquelles est soumis le commanditaire et notamment celles liées à son secteur d'activité.

VI.2.6. Sous-traitance

La convention de service doit :

a) préciser que le prestataire peut faire intervenir un expert sur une partie des activités, pour des besoins en compétences spécifiques et non couverts par les consultants, sous réserve que :

- il existe une convention ou un cadre contractuel documenté entre le prestataire et l'expert ;
- le recours est connu et formellement accepté par écrit par le commanditaire ;
- l'expert est dûment encadré par le responsable d'équipe de la prestation.

b) préciser que le prestataire peut sous-traiter une partie de cette expertise à un autre prestataire conformément aux exigences du référentiel qui lui sont applicables sous réserve que :

- il existe une convention ou un cadre contractuel documenté entre le prestataire et son sous-traitant ;
- le recours à la sous-traitance est connu et formellement accepté par écrit par le commanditaire.

VI.2.7. Livrables

a) La convention de service doit préciser les modalités (contenu, forme, langue, etc.) de rédaction des livrables produits par le prestataire au titre de la prestation.

VI.2.8. Qualification

La convention de service doit :

b) indiquer que la prestation réalisée est :

- une prestation qualifiée et inclure l'attestation de qualification du prestataire[7] ;
- une prestation non qualifiée. Dans ce cas, le prestataire doit sensibiliser le commanditaire aux risques de ne pas exiger une prestation qualifiée.

[6] Dans le cas de la législation française se référer à [LOI_IL], [CP_ART_314-1], [CP_ART_226-15], [CSP_ART_L1110-4], [CP_ART_226-1], [CP_ART_323-1], [CP_ART_226-13] (le cas échéant sans préjudice de l'application de l'article 40 alinéa 2 du Code de procédure pénale relatif au signalement à une autorité judiciaire).

[7] Voir [PROCESS_QUALIF].

c) indiquer que les consultants disposent d'une attestation individuelle de compétence[8] pour les activités de la prestation et inclure ces attestations.

VI.3. Étape 3 : préparation et déclenchement de la prestation

a) Le prestataire doit nommer un responsable d'équipe de la prestation pour toute prestation qu'il effectue.

b) Le responsable d'équipe de la prestation doit identifier le niveau d'habilitation requis du personnel, en fonction de la sensibilité du système d'information concerné et de la réglementation associée.

c) Le responsable d'équipe de la prestation doit constituer une équipe de consultants ayant les compétences adaptées à la nature de la prestation. Le responsable d'équipe de la prestation peut, s'il dispose des compétences suffisantes et que le périmètre de la prestation le permet, réaliser la prestation lui-même et seul.

d) Le responsable d'équipe de la prestation doit, dès le début de la préparation de la prestation, établir un contact avec le CPC. Ce contact, formel ou informel, a notamment pour objectif de mettre en place les circuits de communication et de décision et de préciser les modalités d'exécution de la prestation. Le responsable d'équipe de la prestation doit également obtenir du CPC la liste des points de contact nécessaires à la réalisation de la prestation.

e) Le responsable d'équipe de la prestation s'assure auprès du commanditaire que les représentants légaux des entités impactées par la prestation ont été préalablement avertis et qu'ils ont donné leur accord.

f) Le responsable d'équipe de la prestation élabore un plan de la prestation. Ce plan couvre en particulier les points suivants : les objectifs, champs et critères de la prestation, le périmètre technique et organisationnel de la prestation, les dates et lieux où seront menées les activités et notamment celles éventuellement menées chez le commanditaire, les informations générales sur les réunions d'ouverture et de clôture de la prestation, les noms des consultants et experts qui constituent l'équipe, le niveau de sensibilité des données récupérées et l'anonymisation des constats et des résultats.

g) Les objectifs, le périmètre, les critères et le planning de la prestation doivent être définis entre le prestataire et le commanditaire. Ces éléments doivent figurer dans la convention de service ou dans le plan de la prestation.

h) En fonction de l'objet de la prestation, l'équipe du prestataire doit obtenir du commanditaire, au préalable, toute la documentation existante (exemples : politique de sécurité, analyse de risque, procédures d'exploitation de la sécurité, cartographie du système d'information, schémas d'architecture, etc.), relative au périmètre dans l'objectif d'acquérir une compréhension suffisante du système d'information cible. Il doit ainsi, le cas échéant, demander au commanditaire des compléments d'informations par rapport à ceux déjà transmis lors de l'élaboration de la proposition de service répondant à la demande du commanditaire.

i) La prestation ne doit débuter qu'après une réunion formelle, la réunion d'ouverture, au cours de laquelle les représentants habilités du prestataire et ceux du commanditaire confirment leur accord sur l'ensemble des modalités de la prestation.

   ⓘ Il est recommandé que cette réunion implique au minimum :

   - le futur responsable d'équipe de la prestation chez le prestataire ;
   - un consultant qualifié pour chaque activité demandée chez le prestataire ;
   - un responsable projet du périmètre objet de la prestation ;
   - un représentant métier du périmètre de la prestation ;

[8] Voir [PROCESS_QUALIF].

- au moins un architecte fonctionnel ou technique ayant une compréhension du système d'information cible ;
- un responsable technique du système ;
- un acteur en charge du MCO ;
- un acteur en charge du MCS ;
- un interlocuteur des équipes responsables de la sécurité des systèmes d'information ;
- le cas échéant, un représentant de chaque partie prenante (partenaire, éditeurs ou sous-traitants du commanditaire).

Un même interlocuteur peut cumuler plusieurs profils de la liste ci-dessus.

j) Afin de garantir la confidentialité des échanges, la réunion d'ouverture doit se dérouler en présentiel, sauf accord explicite du commanditaire. Dans le cas où cette réunion se déroule à distance, les modalités de sécurisation des informations échangées pendant cette réunion doivent être convenues en amont entre le commanditaire et le prestataire.

VI.4. Étape 4 : exécution de la prestation

VI.4.1. Exigences générales

a) Les prestations doivent être réalisées dans le respect des personnels et des infrastructures physiques et logiques du commanditaire.

b) Le prestataire et ses consultants doivent prendre toutes les précautions utiles pour préserver la confidentialité des documents et informations relatives au commanditaire.

VI.4.2. Exigences spécifiques à une activité

Lorsqu'elles sont demandées par le commanditaire, les activités d'accompagnement et de conseil réalisées par le prestataire doivent être conformes aux exigences précisées dans les chapitres VI.4.2.2 à VI.4.2.3.

Remarque : *Les énumérations listées dans les chapitres* VI.4.2.2 à VI.4.2.3 *sont données à titre indicatif et ne sont pas exhaustives. Par ailleurs, elles ne doivent être réalisées que lorsqu'elles sont applicables au périmètre de la prestation.*

VI.4.2.1. Exécution des activités de conseil en homologation de sécurité des systèmes d'information

a) Le prestataire doit guider et accompagner le commanditaire dans son projet d'homologation selon les principes de la démarche d'homologation décrits dans [G_HOMOLOGATION].

b) Le prestataire doit être capable d'organiser des entretiens avec les différents acteurs de l'homologation décrits dans [G_HOMOLOGATION] (maîtrise d'ouvrage, responsable de la sécurité des systèmes d'information, responsable d'exploitation système, etc.).

c) Le prestataire doit procéder à la revue des documents identifiés dans la convention de service.

d) Le prestataire doit s'assurer de la complétude du dossier d'homologation à l'issue de la prestation. Celui-ci doit inclure au minimum les éléments suivants :

- la stratégie d'homologation ;
- un rapport d'analyse de risques de sécurité des systèmes d'information du périmètre ;
- la PSSI incluant les mesures de MCS et de LID ;
- un rapport d'audit de sécurité sur le périmètre ;
- un plan d'amélioration continue de la sécurité ;
- les procédures d'exploitation de la sécurité sur le périmètre ;
- le document d'analyse de risque, incluant notamment la liste des risques résiduels.

e) Le prestataire doit accompagner le commanditaire dans la collecte de l'ensemble des éléments constitutifs du dossier d'homologation. Il doit fournir un avis motivé sur la pertinence des éléments collectés au regard des objectifs de la prestation. Le cas échéant, le prestataire doit faire part au commanditaire du besoin de déclencher la rédaction ou la mise à jour des éléments manquants.

VI.4.2.2. Exécution des activités de conseil en gestion des risques de sécurité des systèmes d'information

a) Le prestataire doit utiliser une méthode d'analyse de risque éprouvée, maintenue, pérenne et respectant la norme [ISO27005].

b) Le prestataire doit préconiser auprès du commanditaire l'utilisation de la méthode [EBIOS RM] dans le cadre de l'accompagnement à l'analyse de risque d'un système d'information, sauf si le commanditaire a fait le choix d'une autre méthode d'analyse de risque satisfaisant l'exigence VI.4.2.2 a).

c) Le prestataire doit proposer au commanditaire des réunions de validation intermédiaire à chaque étape de la méthode d'analyse de risque.

d) Le prestataire doit identifier les différents interlocuteurs pertinents pour la réalisation de l'analyse de risques à rencontrer et préconiser l'organisation d'entretiens avec ces derniers.

e) Le prestataire et le commanditaire doivent s'accorder sur les échelles et métriques utilisées dans le cadre de la prestation en début de la prestation.

f) Le prestataire doit procéder à la revue des documents et organiser la rencontre des interlocuteurs identifiés dans la convention de service.

VI.4.2.3. Exécution des activités de conseil en sécurité des architectures des systèmes d'information

a) Le prestataire doit être capable d'organiser des entretiens avec le personnel concerné par la définition, la mise en place, le maintien en condition opérationnelle (MCO) et le maintien en condition de sécurité (MCS) de toutes les briques des systèmes d'information impliquées dans la mise en place et le fonctionnement du système d'information cible.

b) Le prestataire doit procéder à la revue des documents et organiser la rencontre des interlocuteurs identifiés dans la convention de service.

c) Le prestataire doit baser ses recommandations sur des standards éprouvés, maintenus, pérennes, respectant les principes des textes et guides de sécurisation techniques publiés par l'ANSSI ou reconnus comme conformes aux normes existantes en matière d'architecture des systèmes d'information sécurisés. Le prestataire doit justifier ses recommandations et mettre en avant les écarts avec l'état de l'art pour toute recommandation alternative.

VI.5. Étape 5 : restitution continue de la prestation

a) Le prestataire doit organiser des points de suivi selon les modalités définies dans la convention de service. Ces points de suivi doivent notamment permettre de discuter des sujets suivants :

- avancement de la prestation ;
- difficultés rencontrées ;
- nouveaux besoins de documentation ou de rencontre avec des interlocuteurs chez le commanditaire ;
- tout changement dans les consultants réalisant la prestation au sein de d'équipe du prestataire ;
- tout autre changement de modalité de la prestation.

b) Dès la fin de l'étape 3, et sans attendre que le rapport de prestation soit achevé, le responsable d'équipe de prestation de conseil doit informer le commanditaire des constats et des premières conclusions de la prestation.

c) Le cas échéant, le responsable d'équipe doit signaler formellement les risques et vulnérabilités potentiels majeurs et critiques qui nécessiteraient une action rapide et, dans la mesure du possible, décrit les recommandations associées.

VI.6. Étape 6 : élaboration du rapport de prestation

a) Le prestataire doit, pour toute prestation, élaborer un rapport global de prestation et le transmettre au commanditaire.

b) Dans le cas où la prestation comporte plusieurs activités telles que définies au chapitre II, chacune des activités doit faire l'objet d'un rapport ou d'une partie de rapport de prestation spécifique en complément du rapport global de prestation.

c) Le rapport global de prestation doit mentionner explicitement s'il s'agit d'une prestation qualifiée et préciser les activités d'accompagnement et de conseil en sécurité des systèmes d'information concernées.

d) Le rapport de prestation doit contenir en particulier une synthèse, compréhensible par des non experts, qui précise :

- le contexte, dont une analyse de la menace, le périmètre et les objectifs de la prestation ;
- les différentes étapes menées, les entretiens réalisés et les documents analysés dans le cadre de la prestation ;
- les principaux résultats des différentes activités d'accompagnement et conseil en sécurité des systèmes d'information réalisées dans le cadre de la prestation.

e) Le rapport de prestation doit mentionner les réserves relatives à l'exhaustivité du périmètre de l'analyse (liées aux délais alloués, à la disponibilité des informations demandées, à la collaboration du commanditaire, au budget de la prestation, etc.) ou à la pertinence de l'objectif de la prestation.

f) Le rapport de prestation doit mentionner les noms et coordonnées des experts, consultants, responsables d'équipe et commanditaires de la prestation.

VI.6.1. Rapport de prestation de conseil en homologation de sécurité des systèmes d'information

a) Le rapport de prestation concernant les activités de conseil en homologation de sécurité des systèmes d'information doit comprendre, en complément des éléments requis dans le cadre du rapport global de prestation, les éléments suivants :

- la stratégie d'homologation comme décrite dans l'annexe 3 de [G_HOMOLOGATION] ;
- le journal de bord de l'homologation comme décrit dans l'annexe 3 de [G_HOMOLOGATION] ;
- le support de présentation de la commission d'homologation, incluant les éléments suivants :

    i. l'ordre du jour de la réunion, un rappel de l'objectif d'homologation et des différents acteurs et autorités concernés ;

    ii. un rappel du contexte métier, du système et de son écosystème, du référentiel dans lequel s'inscrit la démarche, de la démarche d'homologation adoptée ainsi que du corpus documentaire constitutif du dossier d'homologation ;

iii. le socle de sécurité[9] appliqué au système (objectifs de sécurité et niveau de conformité attendu), en lien avec le cadre réglementaire et les PSSI de référence, ainsi qu'une synthèse des écarts les plus significatifs et des mesures palliatives proposées ;

iv. la synthèse de l'analyse de risque, la politique de sécurité spécifique appliquée au système d'information cible, la synthèse des audits et travaux de certification menés et la synthèse des risques résiduels ;

v. le plan d'amélioration continue de la sécurité, incluant les actions en cours et prévues pour corriger les vulnérabilités constatées et maintenir la sécurité dans un cadre d'amélioration continue, et prévoyant l'évolution de la cartographie des risques résiduels associée ;

vi. l'organisation du management du risque mise en place pour assurer l'exploitation sécurisée du système d'information cible et l'avancement du plan d'amélioration continue de la sécurité.

VI.6.2. Rapport de prestation de conseil en gestion des risques de sécurité des systèmes d'information

a) Le rapport de prestation concernant les activités de conseil en gestion des risques de sécurité des systèmes d'information doit inclure, en complément des éléments requis dans le cadre du rapport global de prestation, les éléments spécifiques suivants :

- une synthèse, incluant les conclusions de l'analyse de risque ;
- les objectifs et le périmètre de l'analyse et la cartographie de l'écosystème ;
- les limites de l'analyse, les hypothèses utilisées ainsi que leur justification ;
- la méthodologie d'analyse appliquée ;
- les personnes ayant participé à l'analyse ainsi que leurs fonctions respectives ;
- les résultats des grandes phases de l'analyse ;
- le plan de traitement des risques préconisé, hiérarchisant la liste des mesures de sécurité pour les risques réduits ;
- la cartographie des risques avant et après traitement par les mesures préconisées ;
- la cartographie des risques résiduels après traitement par les mesures de sécurité préconisées ;
- les références documentaires.

b) Les résultats des analyses de risques doivent y être exprimés en termes compréhensibles.

c) Le prestataire doit expliquer en langage compréhensible les points forts, les limites des différentes mesures de risques et les incertitudes qui entourent les estimations du risque.

d) Le prestataire doit rappeler la nécessité de mise en œuvre par le commanditaire d'un processus de gestion des risques résiduels.

e) Le rapport de prestation peut également présenter des recommandations générales non associées à des risques et destinées à conseiller le commanditaire sur des actions complémentaires (déjà identifiées ou non par le commanditaire) qui seraient pertinentes pour améliorer la sécurité du système d'information.

[9] Le socle de sécurité sous-entend la liste des référentiels applicables, l'état d'application et l'identification et justification des écarts.

VI.6.3. Rapport de prestation de conseil en sécurité des architectures des systèmes d'information

a) Le rapport de prestation concernant les activités de conseil en sécurité des architectures des systèmes d'information doit comprendre, en complément des éléments requis dans le cadre du rapport global de prestation, les éléments spécifiques suivants :

- un rappel des objectifs de la prestation, du périmètre et la cartographie du système d'information cible ;
- un rappel des objectifs de sécurité à couvrir (conformité à un référentiel réglementaire ou à un guide de standards et de bonnes pratiques, application d'un plan de remédiation suite à un audit, etc.) ;
- une analyse listant les écarts aux objectifs de sécurité identifiés et les vulnérabilités à traiter, et fournissant un avis de sécurité sur l'architecture soumise par le commanditaire, pouvant être regroupés par thématiques de sécurité de systèmes d'information, incluant notamment les thématiques suivantes :
    - PSSI ;
    - Cartographie / Documentation ;
    - Maintien en condition opérationnelle (MCO) / Maintien en condition de sécurité (MCS) ;
    - Journalisation ;
    - Détection ;
    - Traitement des incidents de sécurité et gestion de crise (SOC – Security Operation Center) ;
    - Identification (utilisateurs/processus) ;
    - Authentification (utilisateurs/processus) ;
    - Gestion des droits d'accès ;
    - Gestion des comptes à privilèges ;
    - Administration sécurisée ;
    - Cloisonnement réseau et chiffrement des données en transit ;
    - Cloisonnement système et chiffrement des données au repos ;
    - Filtrage des flux ;
    - Accès à distance (nomadisme, partenaires) ;
    - Sécurité physique et contrôle d'accès / vidéo-protection ;
    - Sauvegardes et PRA/PCA (Plan de Reprise/Continuité d'Activité) ;
    - Stockage et hébergement.

  Ces thématiques sont à adapter en fonction du périmètre et des objectifs de la prestation.
- un ou plusieurs scénarios, adaptés au contexte du commanditaire, permettant d'atteindre les objectifs de sécurité du commanditaire, incluant une analyse des avantages et limites ainsi qu'une appréciation des efforts (mise en œuvre et maintien en condition opérationnelle et de sécurité) associés, pour chaque scénario proposé ;
- une liste de recommandations priorisée pour chaque scénario, permettant d'atteindre les objectifs de sécurité du commanditaire, avec des indicateurs de priorité et d'effort de mise en œuvre pour chacune d'entre elles ;
- une liste d'écarts et vulnérabilités résiduels pour chaque scénario, si l'atteinte des objectifs de sécurité est jugée impossible par le prestataire, à la suite de l'analyse ;
- une synthèse à l'attention de la direction du commanditaire, reprenant les axes principaux de l'analyse, un résumé des différents scénarios proposés, les écarts et vulnérabilités résiduels les plus critiques pour chacun d'entre eux et les impacts pour le commanditaire.

VI.7. Étape 7 : clôture de la prestation

a) Une réunion de clôture de la prestation doit être organisée avec le commanditaire à la suite de la livraison du rapport global de prestation. Cette réunion permet de présenter la synthèse du rapport global de prestation, de la suite à donner à la prestation et d'organiser un jeu de questions / réponses. Il est recommandé que cette réunion implique au minimum[10] :

- le responsable d'équipe de la prestation chez le prestataire ;
- un consultant qualifié pour chaque activité demandée chez le prestataire ;
- un responsable projet du périmètre objet de la prestation ;
- un représentant métier du périmètre de la prestation ;
- au moins un architecte fonctionnel ou technique ayant une compréhension du système d'information cible ;
- un responsable technique du système ;
- un acteur en charge du MCO ;
- un acteur en charge du MCS ;
- un interlocuteur des équipes responsables de la sécurité des systèmes d'information ;
- le cas échéant, un représentant de chaque partie prenante (partenaire, éditeurs ou sous-traitants du commanditaire).

Le cas échéant, le rapport global de prestation devra être amendé à la suite de la réunion de clôture de la prestation pour prendre en compte les éventuelles informations complémentaires obtenues pendant la réunion.

b) Afin de garantir la confidentialité des échanges, la réunion de clôture doit se dérouler en présentiel, sauf accord explicite du commanditaire. Dans le cas où cette réunion se déroule à distance, les modalités de sécurisation des informations échangées pendant cette réunion doivent être convenues en amont entre le commanditaire et le prestataire.

c) Le responsable d'équipe de prestation de conseil doit, selon ce qui a été prévu dans la convention établie entre le prestataire et le commanditaire, s'assurer de la destruction ou de la restitution de l'ensemble des informations collectées ou documents relatifs au système d'information cible.

d) Le responsable d'équipe de prestation de conseil doit transmettre au commanditaire un procès-verbal de destruction ou de restitution, selon ce qui a été prévu dans la convention établie entre le prestataire et le commanditaire. Le procès-verbal de destruction ou de restitution doit identifier les informations détruites ou restituées ainsi que le mode de destruction ou de restitution utilisé.

e) Le prestataire doit recommander au commanditaire d'effectuer une revue régulière des constats issus de la prestation et de mettre en place des contrôles afin de s'assurer que les recommandations issues de la prestation sont effectivement mises en œuvre. Les fréquences des revues et des contrôles sont à adapter en fonction des évolutions, de la sensibilité et des besoins réglementaires associés au système d'information cible.

f) La prestation est considérée comme terminée lorsque toutes les activités prévues ont été réalisées et que le commanditaire a reçu et attesté, formellement et par écrit, que le rapport global de prestation est conforme aux objectifs visés dans la convention.

g) Le prestataire doit recommander au commanditaire d'effectuer une revue régulière des constats issus de la prestation et de mettre en place des contrôles afin de s'assurer que les recommandations issues de la prestation sont effectivement mises en œuvre. Les fréquences des revues et des contrôles sont à adapter en fonction des évolutions, de la sensibilité et des besoins réglementaires associés au système d'information cible.

[10] Ces rôles peuvent être cumulés par une même personne.

Annexe 1 Références documentaires

I. Codes, textes législatifs et réglementaires

Renvoi	Document
[CP_ART_314-1]	Article 334-1 du Code pénal relatif à l'abus de confiance. Disponible sur https://www.legifrance.gouv.fr
[CP_ART_226-1]	Article 226-1 du Code pénal relatif à l'atteinte à la vie privée. Disponible sur https://www.legifrance.gouv.fr
[CP_ART_226-13]	Article 226-13 du Code pénal relatif au secret professionnel. Disponible sur https://www.legifrance.gouv.fr
[CP_ART_226-15]	Article 226-15 du Code pénal relatif au secret des correspondances. Disponible sur https://www.legifrance.gouv.fr
[CSP_ART_L1110-4]	Article L1110-4 du Code de la santé publique relatif au secret médical. Disponible sur https://www.legifrance.gouv.fr
[CP_ART_323-1]	Article 323-1 du Code pénal relatif à l'accès ou au maintien frauduleux dans un système de traitement automatisé de données. Disponible sur https://www.legifrance.gouv.fr
[D_2015_350]	Décret n° 2015-350 du 27 mars 2015 relatif à la qualification des produits de sécurité et des prestataires de service de confiance pour les besoins de la sécurité des systèmes d'information. Disponible sur https://www.legifrance.gouv.fr
[EIDAS]	Règlement (UE) no 910/2014 du parlement européen et du conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE. Disponible sur https://eur-lex.europa.eu
[IGI_1300]	Instruction générale interministérielle n°1300 sur la protection du secret de la défense nationale, n°1300 /SGDSN/PSE/PSD, 30 novembre 2011. Disponible sur https://www.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 https://circulaires.legifrance.gouv.fr
[II_901]	Instruction interministérielle relative à la protection des systèmes d'information sensibles, n°901/SGDSN/ANSSI, 28 janvier 2015. Disponible sur https://circulaires.legifrance.gouv.fr
[LOI_IL]	Loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. Disponible sur https://www.legifrance.gouv.fr
[LPM]	Articles L. 1332-6-1 à L. 1332-6-6 du code de la défense, créés par la loi n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale (LPM 2014-19) Disponible sur https://www.legifrance.gouv.fr
[NIS]	Directive (UE) n° 2016/1148 du parlement européen et du conseil du 6 juillet 2016 concernant les mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union Disponible sur https://eur-lex.europa.eu 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 Disponible sur https://www.legifrance.gouv.fr

Renvoi	Document
[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, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (Texte présentant de l'intérêt pour l'EEE) Disponible sur https://eur-lex.europa.eu
[R_OTAN]	Instruction interministérielle n° 2100/SGDSN/SSD du 1er décembre 1975 pour l'application en France du système de sécurité de l'Organisation du Traité de l'Atlantique nord Disponible sur https://circulaires.legifrance.gouv.fr
[R_UE]	Instruction interministérielle n° 2102/SGDSN/PSD du 12 juillet 2013 sur la protection en France des informations classifiées de l'Union Européenne Disponible sur https://circulaires.legifrance.gouv.fr

II. Normes et documents techniques

Renvoi	Document
[EBIOS_RM]	Méthode de gestion de risques EBIOS Risk Manager. Disponible sur https://www.ssi.gouv.fr/ebios
[G_802.1]	Guide de recommandations de déploiement du protocole 802.1x pour le contrôle d'accès à des réseaux locaux. Dernière version en vigueur. Disponible sur https://www.ssi.gouv.fr
[G_ADMIN]	Guide de recommandations relatives à l'administration sécurisée des systèmes d'information. Dernière version en vigueur. Disponible sur https://www.ssi.gouv.fr
[G_APPLI_WEB]	Guide de recommandations pour la sécurisation des sites web. Dernière version en vigueur. Disponible sur https://www.ssi.gouv.fr
[G_CARTOGRAPHIE]	Guide de recommandations pour la cartographie du système d'information Dernière version en vigueur. Disponible sur https://www.ssi.gouv.fr
[G_CLOISONNEMENT]	Guide de recommandations pour la mise en place de cloisonnement système. Dernière version en vigueur. Disponible sur https://www.ssi.gouv.fr
[G_CONTROLE_ACCES]	Guide de 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
[G_CRYPTO]	Web Doc Crypto de l'ANSSI et annexes B1, B2 et B3 du [RGS]. Dernière version en vigueur. Disponible sur https://www.ssi.gouv.fr
[G_DEF_PROF]	La défense en profondeur appliquée aux systèmes d'information. Dernière version en vigueur. Disponible sur https://www.ssi.gouv.fr
[G_FICHES_SIIV_LPM]	Fiches techniques relatives à la loi de programmation militaire (2014-2019) traitant des systèmes d'information d'importance vitale (SIIV). Document de niveau Diffusion Restreinte, il peut être obtenu auprès de l'ANSSI.
[G_HOMOLOGATION]	L'homologation de sécurité en neuf étapes simples, ANSSI. Dernière version en vigueur. Disponible sur https://www.ssi.gouv.fr
[G_HYGIENE]	Guide d'hygiène informatique. Dernière version en vigueur. Disponible sur https://www.ssi.gouv.fr
[G_INTERCO]	Guide de recommandations relatives à l'interconnexion d'un système d'information 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. Dernière version en vigueur. Disponible sur https://www.ssi.gouv.fr

Renvoi	Document
[G_NOMADISME]	Guide de recommandations sur le nomadisme numérique. Dernière version en vigueur. Disponible sur https://www.ssi.gouv.fr
[G_PAREFEUX]	Guide de recommandations pour choisir des pare-feux maîtrisés dans les zones exposées à internet. Dernière version en vigueur. Disponible sur https://www.ssi.gouv.fr
[G_SEC_LINUX]	Guide de recommandations de configuration d'un système GNU/LINUX. Dernière version en vigueur. Disponible sur https://www.ssi.gouv.fr
[G_SEC_VIRTUAL]	Problématiques de sécurité associées à la virtualisation des systèmes d'information. Dernière version en vigueur. Disponible sur https://www.ssi.gouv.fr
[G_SWITCH]	Guide de recommandations pour la sécurisation d'un commutateur de desserte. Dernière version en vigueur. Disponible sur https://www.ssi.gouv.fr
[G_SYS_INDUS]	Guide de recommandations relatives à la cybersécurité des systèmes industriels. Dernière version en vigueur. Disponible sur https://www.ssi.gouv.fr
[G_TLS]	Guide de recommandations de sécurité relatives à TLS. Dernière version en vigueur. Disponible sur https://www.ssi.gouv.fr
[G_TOIP]	Guide de recommandations relatives à la sécurisation d'une architecture de téléphonie sur IP. Dernière version en vigueur. Disponible sur https://www.ssi.gouv.fr
[G_WIFI]	Recommandations de sécurité relatives aux réseaux Wi-Fi Dernière version en vigueur. Disponible sur https://www.ssi.gouv.fr
[ISO19011]	Norme internationale ISO/IEC 19011:2018: Lignes directrices pour l'audit des systèmes de management. Disponible sur https://www.iso.org
[ISO27000]	Norme internationale ISO/IEC 27000:2014 : Technologies de l'information – Techniques de sécurité – Systèmes de gestion de la sécurité de l'information – vue d'ensemble et vocabulaire. Disponible sur https://www.iso.org
[ISO27001]	Norme internationale ISO/IEC 27001:2013 : Techniques de sécurité – Systèmes de gestion de la sécurité de l'information – Exigences. Disponible sur https://www.iso.org
[ISO27002]	Norme internationale ISO/IEC 27002:2013 : Techniques de sécurité – Code de bonne pratique pour la gestion de la sécurité de l'information. Disponible sur https://www.iso.org
[ISO27005]	Norme internationale ISO/IEC 27005:2018 – Technologies de l'information – Techniques de sécurité – Gestion des risques liés à la sécurité de l'information. Disponible sur https://www.iso.org
[NT_SEC_AD]	Recommandations de sécurité relatives à Active Directory. Dernière version en vigueur. Disponible sur https://www.ssi.gouv.fr

Renvoi	Document
[NT_SEC_DNS]	Bonnes pratiques pour l'acquisition et l'exploitation de noms de domaine. Dernière version en vigueur. Disponible sur https://www.ssi.gouv.fr
[NT_SEC_WIND]	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
[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
[PDIS]	Référentiel d'exigences applicables à un prestataire de détection des incidents de sécurité, ANSSI. Dernière version en vigueur. Disponible sur https://www.ssi.gouv.fr
[PRIS]	Référentiel d'exigences applicables à un prestataire de réponse aux incidents de sécurité, ANSSI. Dernière version en vigueur. Disponible sur https://www.ssi.gouv.fr
[PSSIE]	Politique de sécurité des systèmes d'information de l'Etat. Dernière version en vigueur. Disponible sur https://ssi.gouv.fr
[RGS]	Référentiel général de sécurité - ANSSI et SGMAP. Dernière version en vigueur. Disponible sur https://ssi.gouv.fr

III. Autres références documentaires

Renvoi	Document
[GUIDE_ACHAT]	Guide d'achat de produits de sécurité et de services de confiance qualifiés, version en vigueur. Disponible sur http://www.ssi.gouv.fr
[PROCESS_QUALIF]	Processus de qualification d'un service, version en vigueur. Disponible sur http://www.ssi.gouv.fr
[STRAT_NUM]	Stratégie nationale pour la sécurité du numérique, octobre 2015. Disponible sur http://www.ssi.gouv.fr

Annexe 2 Missions et compétences attendues du personnel du prestataire

Cette annexe présente, pour chaque profil de consultant, les missions à assurer et les compétences requises.

I. Socle commun de connaissances en sécurité des systèmes d'information

Les consultants et responsables d'équipes intervenant dans le cadre d'une prestation d'accompagnement et de conseil en sécurité des systèmes d'information doivent connaitre l'ensemble des éléments du socle commun de connaissances en sécurité des systèmes d'information, décrit ci-après. Ces éléments sont complétés par les compétences spécifiques requises pour chaque profil, décrites dans la suite de cette annexe.

Il est entendu par « connaître » la compréhension des principaux concepts, des processus dans lesquels ils s'inscrivent et la capacité à savoir fournir une explication macroscopique des éléments cités.

I.1. Connaissances transverses en sécurité des systèmes d'information

Le socle commun est composé de la connaissance des documents suivants :

- [G_HYGIENE] ;
- [ISO27001] ;
- [ISO27002].

Le socle commun est composé des domaines relatifs à l'organisation de la sécurité des systèmes d'information :

- analyse de la menace numérique ;
- analyse de risque ;
- politique de sécurité des systèmes d'information ;
- chaines de responsabilités en sécurité des systèmes d'information ;
- sécurité liée aux ressources humaines ;
- gestion de l'exploitation et de l'administration des systèmes d'information ;
- contrôle d'accès logique aux systèmes d'information ;
- développement et maintenance des applications ;
- gestion des incidents liés à la sécurité de l'information ;
- gestion du plan de continuité de l'activité ;
- sécurité physique ;
- protection des données.

I.2. Connaissances en méthode de gestion des risques

Le socle commun est composé de connaissances en méthode de gestion des risques, comprenant :

- la connaissance de :
    - [G_HOMOLOGATION] ;
    - une ou plusieurs méthodologies d'analyse du risque numérique.
- la connaissance et la compréhension de :
    - la définition du risque en général ;
    - la définition du risque numérique en particulier et de ses composantes ;
    - la terminologie de la méthode appliquée ;
    - la définition de la gestion des risques.

Il est notamment attendu de connaître les concepts suivants :

- identification des valeurs métiers et des besoins de sécurité associés ;
- identification des événements redoutés ;
- analyse de l'écosystème et cartographie de la menace ;
- élaboration de scénarios stratégiques et opérationnels.

I.3. Connaissance de la réglementation

Le socle commun est composé de la connaissance des différents textes réglementaires, sur lesquels s'appuie généralement une prestation d'accompagnement et de conseil en sécurité des systèmes d'information :

- [IGI_1300] ;
- [II_901] ;
- [LPM] ;
- [NIS] ;
- [EIDAS] ;
- [PSSIE] ;
- [RGS] et notamment ses annexes A, B et C ;
- [R_OTAN] ;
- [R_UE].

Il est également attendu la faculté à faire le lien entre ces exigences et le contexte de la demande du commanditaire.

I.4. Connaissances en architecture sécurisée des systèmes d'information

Le socle commun est composé de connaissances des principaux éléments qui composent une architecture d'un système d'information et de leur rôle ainsi que les principes fondamentaux en architecture sécurisée des systèmes d'information, notamment sur les domaines suivants :

- le réseau, notamment les différents équipements réseaux, les grands principes de cloisonnement, les fonctions de sécurité associées, des principes de sécurisation des interconnexions des systèmes d'information ;
- les systèmes, notamment les principaux systèmes d'exploitation et les fonctions de sécurité associées, les grands principes de durcissement système ainsi que les moyens de réaliser le maintien en condition opérationnelle et de sécurité ;
- l'administration sécurisée, notamment les principes de moindre privilège, les objectifs du cloisonnement de la zone d'administration et des zones administrées ;
- les applications, notamment les architectures applicables type « n-tiers » (MVC) et les grands principes de sécurisation des applications ;
- les accès et les données, notamment les grands principes de gestion des identités et des accès, les systèmes de stockage de données et les principaux mécanismes et mesures de protection des données.

Le socle commun est également composé de la connaissance des principaux modèles de sécurité (forteresse, aéroport, *zero trust*, etc.) et des grands principes de défense en profondeur.

De plus, il est composé de connaissances des spécificités des systèmes d'information selon leur nature ainsi que les principes de sécurisation associés, tels que les systèmes de virtualisation et les environnements cloud (IaaS, PaaS, SaaS, privés et publics).

II. Responsable d'équipe de prestation de conseil

II.1. Missions

Le responsable d'équipe de prestation de conseil doit assurer les missions suivantes :

- mettre en œuvre une organisation adaptée aux objectifs de la prestation ;
- structurer l'équipe de consultants (compétences, connaissances, expérience, etc.) ;
- assurer la définition, le pilotage et le contrôle des activités des consultants ;
- mettre en œuvre les moyens adaptés aux objectifs de la prestation ;
- définir et gérer les priorités ;
- maintenir à jour un état de la progression de la prestation et présenter l'information utile au commanditaire ;
- contrôler la qualité des productions ;
- assurer sa présence aux réunions d'ouverture et de clôture de la prestation et se porter garant des messages (constats, analyses, préconisations, éléments-clés de démarche, etc.) de l'équipe de la prestation ;
- valider en interne les livrables de la prestation sur leur fond et leur forme.

II.2. Compétences

II.2.1. Socle commun de connaissances en sécurité des systèmes d'information

Le responsable d'équipe doit connaître l'ensemble des éléments du socle commun de connaissances en sécurité des systèmes d'information, décrit dans la partie I de cette Annexe.

II.2.2. Aptitudes interpersonnelles

Le responsable d'équipe de prestation de conseil doit présenter les aptitudes suivantes :

- piloter des équipes de consultants ;
- définir et gérer les priorités ;
- conduire des entretiens et des réunions pour obtenir des informations;
- impliquer et responsabiliser les parties prenantes ;
- préparer et obtenir des arbitrages et validations ;
- arbitrer entre les propositions de tous les consultants de l'équipe de prestation pour en tirer les meilleures conclusions ;
- argumenter les conclusions de manière claire et compréhensible ;
- présenter une communication au niveau décisionnel.

III. Consultant en gestion des risques et conformité

III.1. Missions

Les missions du consultant en gestion des risques et conformité consistent à prendre en charge les activités telles qu'identifiées aux chapitres II.1 et II.2.

III.2. Compétences

III.2.1. Socle commun de connaissances en sécurité des systèmes d'information

Le consultant en gestion des risques et conformité doit connaître l'ensemble des éléments du socle commun de connaissances en sécurité des systèmes d'information, décrit dans la partie I de cette annexe.

III.2.2. Connaissances en méthode de gestion des risques

Le consultant en gestion des risques et conformité doit maîtriser les éléments relatifs aux connaissances en méthode de gestion des risques, identifiés au chapitre I.2 de cette annexe.

Il est entendu par « maîtriser » la compréhension fonctionnelle et technique des éléments cités ainsi qu'un savoir-faire sur ces éléments.

III.2.3. Pratique d'une méthode de gestion des risques de sécurité des systèmes d'information

Le consultant en gestion des risques et conformité doit :

- savoir choisir le niveau de détail d'une étude ;
- avoir suivi le déroulement d'études dans leur intégralité, par exemple en tant que maîtrise d'ouvrage ou assistance à maîtrise d'ouvrage ;
- avoir réalisé des études dans leur intégralité ;
- savoir identifier les informations nécessaires pour mener une étude ;
- connaître les types de fonctions à impliquer selon les activités de la méthode ;
- savoir analyser et utiliser les informations obtenues ;
- utiliser et ajuster les bases de connaissances opérationnelles ;
- savoir proposer des mesures de sécurité raisonnables selon la réalité de l'organisme (selon sa maturité) ;
- savoir expliquer les différents types de livrables principalement produits et leurs finalités.

III.2.4. Aptitudes interpersonnelles

Le consultant en gestion des risques et conformité doit présenter les aptitudes suivantes :

- savoir synthétiser et restituer l'information utile pour du personnel technique et non technique ;
- savoir rédiger des rapports et des documentations adaptées à différents niveaux d'interlocuteurs (services techniques, organe de direction, etc.) ;
- savoir travailler en équipe (partage de connaissances, collaboration technique et entraide) ;
- savoir conduire des entretiens pour obtenir des informations et une réunion ;
- savoir impliquer et responsabiliser les parties prenantes ;
- savoir produire des documents livrables adaptés à partir d'une étude ;
- savoir préparer et obtenir des arbitrages et validations.

IV. **Consultant en sécurité des architectures des systèmes d'information**

IV.1. **Missions**

Les missions du consultant en sécurité des architectures des systèmes d'information consistent à prendre en charge les activités telles qu'identifiées au chapitre II.3.

IV.2. **Compétences**

IV.2.1. Socle commun de connaissances en sécurité des systèmes d'information

Le consultant en sécurité des architectures des systèmes d'information doit connaître l'ensemble des éléments du socle commun de connaissances en sécurité des systèmes d'information, décrit dans la Partie I.4 de cette annexe.

IV.2.2. Connaissance en architecture sécurisée des systèmes d'information

Le consultant en sécurité des architectures des systèmes d'information doit maîtriser les éléments relatifs aux architectures sécurisées des systèmes d'information, identifiés au chapitre I.4 de cette annexe, et

complétés par les éléments associés ci-dessous. Il est entendu par « maîtriser » la connaissance des concepts, la compréhension de leur fonctionnement technique, et la capacité à les décliner dans un contexte spécifique présenté.

Il doit également connaître la doctrine de l'ANSSI à travers la connaissance et la bonne compréhension des différents guides de recommandations et techniques présents sur le site Web de l'ANSSI (www.ssi.gouv.fr), notamment ceux listés pour chacun des éléments décrits dans cette partie.

IV.2.2.1. Maîtrise des concepts et protocoles réseaux

Le consultant en sécurité des architectures des systèmes d'information doit :

- avoir une parfaite compréhension du modèle OSI, ainsi que des principaux protocoles fréquemment rencontrés sur chaque couche de ce modèle, et des moyens de les sécuriser ;
- maîtriser les concepts de cloisonnement et de filtrage ;
- être capable d'appréhender la sécurisation de flux entre zones de sensibilités différentes ;
- maîtriser les concepts d'interconnexion de réseaux et les principes de sécurisation associés.

Il doit connaître les guides de recommandations liés à ces différents éléments, parmi lesquels de façon non exhaustive :

- [G_INTERCO] ;
- [G_802.1] ;
- [G_TLS] ;
- [G_SWITCH] ;
- [G_WIFI] ;
- [G_IPSEC] ;
- [G_PAREFEUX] ;
- [NT_SEC_DNS].

IV.2.2.2. Maîtrise des concepts système et des principaux systèmes d'exploitation

Le consultant en sécurité des architectures des systèmes d'information doit maîtriser les principaux systèmes d'exploitation, les moyens de les sécuriser et de durcir leur configuration.

Il est recommandé que le consultant ait connaissance de la doctrine de l'ANSSI à travers les guides de sécurisation système, parmi lesquels de façon non exhaustive :

- [G_CLOISONNEMENT] ;
- [G_NOMADISME] ;
- [G_SEC_LINUX] ;
- [NT_SEC_WIND].

IV.2.2.3. Maîtrise des concepts d'administration sécurisée

Le candidat doit être en mesure de :

- de définir les bonnes pratiques de cloisonnement entre le système d'information d'administration et les systèmes d'information administrées ;
- de proposer des mesures de sécurisation d'un poste d'administration ;
- de définir des mesures adaptées en fonction des rôles d'administration et des privilèges associés (administration réseaux, administrateurs de domaine, exploitant, mainteneur, etc.).

Il lui est recommandé de connaître les guides de recommandations liés à ces différents éléments, parmi lesquels de façon non exhaustive : [G_ADMIN].

IV.2.2.4. Maîtrise des concepts d'architectures applicatives

Le consultant en sécurité des architectures des systèmes d'information doit connaître :

- les modèles d'architectures applicatives les plus courants ;
- les principaux concepts d'architectures applicatives sécurisées ;
- les vulnérabilités les plus répandues concernant les applications Web.

Il est recommandé que le consultant ait une bonne connaissance de la doctrine de l'ANSSI à travers les guides de sécurisation système, parmi lesquels de façon non exhaustive : [G_APPLI_WEB].

IV.2.2.5. Maîtrise des concepts de gestion des accès et de la protection des données

Le consultant doit maîtriser les principaux concepts et principes techniques liés à :

- la gestion des identités et des accès ;
- l'annuaire centralisé ;
- la cryptographie ;
- l'infrastructure de gestion de clés (IGC).

Le consultant doit maîtriser les principales technologies de stockage, les besoins et des principes de sécurité associés, notamment en étant en mesure de :

- proposer des mesures de cloisonnement en fonction des technologies de stockage utilisées ;
- de proposer des mesures d'effacement sécurisé ;
- d'aider à la mise en place d'une politique de sauvegarde sécurisée.

Il lui est recommandé de connaître les guides de recommandations liés à ces différents éléments, parmi lesquels de façon non exhaustive :

- [G_SEC_AD] ;
- [G_CRYPTO].

IV.2.2.6. Maîtrise des principaux modèles de sécurité et des principes de défense en profondeur

Le consultant doit maîtriser les différents modèles de sécurité, être en mesure de comprendre et d'expliquer le concept de zone de sécurité, la manière de les identifier, de les contextualiser et de les justifier dans les propositions de sécurisation de l'architecture.

Le consultant doit comprendre et savoir appliquer les principes de la défense en profondeur, notamment en sachant :

- mettre en œuvre les principes de la défense en profondeur sur tout système d'information en fonction des besoins de sécurité et selon les cinq grands axes (prévenir, bloquer, limiter, détecter, réparer) ;
- expliquer ces principes et proposer pour leur mise en œuvre des solutions adaptées aux contraintes ;
- maîtriser les concepts liés à la gestion des événements de sécurité.

Le consultant doit maîtriser les principaux équipements et produits de sécurité, parmi lesquels de façon non exhaustive : pare-feu, sonde de détection d'intrusion, TAP, sonde de prévention d'intrusion, diode, serveur mandataire, SIEM (Security information management system), WAF (Web application firewall), concentrateur VPN.

Il lui est recommandé de connaître les guides de recommandations liés à ces différents éléments, parmi lesquels de façon non exhaustive : [G_DEF_PROF].

IV.2.3. Pratique de la conception d'une architecture sécurisée de systèmes d'information

Le consultant en sécurité des architectures des systèmes d'information doit :

- être en mesure de réaliser un état des lieux réaliste et pertinent du niveau de sécurité d'un système d'information, et notamment :
    - de prendre en compte toutes les dimensions du contexte du commanditaire impactant la sécurité des systèmes d'information (technique, organisationnelle, humaine, réglementaire, etc.) ;
    - de comprendre, interpréter et exploiter les résultats d'un audit.
- être en mesure de proposer un plan d'amélioration sécurité de l'architecture pertinent et raisonnable vis-à-vis de l'état des lieux réalisé, et notamment :
    - permettant de couvrir les principaux risques et justifiant chaque mesure en regard d'un scénario d'attaque à adresser ;
    - prenant en compte le maintien en condition de sécurité dans la cible proposée (corrections, migrations, obsolescences, etc.) ;
    - proposant une trajectoire vers la cible progressive adaptée au niveau de maturité, aux contraintes et aux enjeux constatés du commanditaire.
- savoir expliquer les recommandations produites et leurs finalités, et notamment :
    - d'avoir la capacité à sensibiliser les décideurs sur les enjeux de sécurité selon leur domaine de compétence et de connaissance de la problématique ;
    - d'adapter son discours au niveau de ses interlocuteurs.

Le consultant en sécurité des architectures des systèmes d'information doit également être capable de comprendre, d'étudier et d'analyser un dossier d'architecture complexe, en prenant en compte toutes les composantes pertinentes pour la sécurité, qui détaille de façon claire :

- les services d'infrastructure les plus pertinents dans le contexte de la prestation ;
- les différentes zones de sensibilité s'il y en a (non-protégé, diffusion restreinte, etc.) ;
- les flux réseau les plus pertinents dans le contexte de la prestation ;
- les interconnexions avec d'autres systèmes d'information (maîtrisés par l'entité ou non) ;
- les équipements de sécurité les plus pertinents dans le contexte de la prestation ;
- les zones d'administration et les zones de supervision de(s) système(s) d'information concerné(s).

Il doit ainsi être capable de réaliser un dossier de sécurité associé, de porter un regard critique sur un système ou sur un composant d'un système et de remettre en cause les choix d'architectures discutables ou peu pertinents et être en mesure de justifier et positionner les principaux équipements de sécurité dans une recommandation d'architecture.

Il doit connaître les guides de recommandations liés à ces différents éléments, parmi lesquels de façon non exhaustive [G_CARTOGRAPHIE].

IV.2.4. Connaissances spécifiques des systèmes d'information selon leur nature

Le consultant en sécurité des architectures des systèmes d'information doit avoir une connaissance macroscopique des spécificités des systèmes d'information industriels. Il doit connaître le guide de recommandations et les notes techniques liés à ces différents éléments, parmi lesquels de façon non exhaustive : [G_SYS_INDUS].

Il est recommandé qu'il ait également une connaissance macroscopique des spécificités des systèmes d'information suivants :

- les systèmes de contrôle d'accès physique et vidéo surveillance ;
- les systèmes de téléphonie sur IP (ToIP) et plus généralement les systèmes temps-réel ;
- les systèmes virtualisés dans les environnements cloud.

Il est également recommandé de connaître les guides de recommandations liés à ces différents éléments, parmi lesquels de façon non exhaustive :

- [G_SEC_VIRTUAL] ;

- [G_TOIP] ;
- [G_CONTROLE_ACCES].

Ces connaissances macroscopiques doivent lui permettre d'identifier et justifier le recours nécessaire à des experts dans ces domaines. Les connaissances dans ces systèmes d'information spécifiques doivent permettre au consultant de pouvoir échanger techniquement avec les experts, d'être capable de monter en compétence sur ces systèmes, et d'être en mesure de définir avec pertinence les mesures de sécurisation de l'architecture en adéquation avec les spécificités de ces systèmes.

IV.2.5. Aptitudes interpersonnelles

Le consultant en sécurité des architectures des systèmes d'information doit présenter les aptitudes suivantes :

- savoir analyser, synthétiser et restituer l'information utile pour du personnel technique et non technique ;
- savoir rédiger des rapports et des documentations adaptées à différents niveaux d'interlocuteurs (services techniques, organe de direction, etc.) ;
- savoir travailler en équipe (partage de connaissances, collaboration technique et entraide) ;
- savoir conduire des entretiens pour obtenir des informations et une réunion ;
- savoir impliquer et responsabiliser les parties prenantes ;
- savoir produire des documents livrables adaptés à partir d'une étude ;
- savoir préparer et obtenir des arbitrages et validations.

Annexe 3 Recommandations aux commanditaires

Cette annexe liste les recommandations de l'ANSSI à l'intention des commanditaires de prestations d'accompagnement et de conseil en sécurité des systèmes d'information.

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 de l'ANSSI, la qualification d'un prestataire d'accompagnement et de conseil en sécurité des systèmes d'information attestant 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 de l'ANSSI ;
- exiger du prestataire de spécifier 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 utilise le guide d'achat des produits de sécurité et des services de confiance qui a pour vocation à accompagner la fonction achat des commanditaires lors des appels d'offres.

e) 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.

f) Le commanditaire peut, conformément au processus de qualification des prestataires de service de confiance 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.

g) La qualification d'un prestataire n'atteste pas de sa capacité à accéder ou à détenir des informations classifiées de défense et par conséquent ne se substitue pas à une habilitation de sécurité.

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.

h) 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) .

Il est possible pour un commanditaire de 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) La définition du périmètre de la prestation et la description de la prestation attendue, formulées généralement dans un appel d'offres, sont de la responsabilité du commanditaire. Il est recommandé que le commanditaire identifie de manière la plus précise possible le contexte, le périmètre et les objectifs à adresser par la prestation en amont de la demande de prestation. Dans la mesure du possible et suivant la nature de la prestation, il est également recommandé que le commanditaire précise la nature des SI impliqués (SI bureautique, SI industriel, etc.), les besoins de sécurité déjà identifiés et les parties prenantes du périmètre de la prestation (éditeurs, prestataires, fournisseurs, hébergeurs, etc.). Il est recommandé que le commanditaire fasse appel à un prestataire d'accompagnement et conseil en sécurité des systèmes d'information (PACS) qualifié préalablement à la prestation.

b) ⓘ Il est recommandé que le commanditaire désigne en son sein un CDC chargé de la gestion des relations avec le prestataire et des modalités de réalisation des activités.

c) ⓘ 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.

d) ⓘ Il est recommandé que le commanditaire demande que toutes les informations relatives à la prestation soient stockées par le prestataire dans un espace logique dédié au commanditaire, et accessible uniquement par les consultants dûment identifiés par le prestataire.

e) La durée et les charges de la prestation demandée par le commanditaire devront être adaptées en fonction :

- du périmètre de la prestation et de sa complexité ;
- des exigences de sécurité attendues du système d'information cible.

III. Pendant la prestation

a) Il est recommandé que le commanditaire fournisse au prestataire, dès le début de la prestation, les éléments identifiés dans la convention de service. En particulier, le CPC sera facilitateur dans les relations entre le prestataire et les parties prenantes du commanditaire.

b) Il est recommandé, afin d'éviter toute dénonciation de vol ou d'abus de confiance, que le commanditaire évite de remettre au prestataire des matériels (terminaux, médias amovibles, etc.) dont il n'est pas le titulaire mais tout de même utilisés à des fins professionnelles en l'absence du titulaire du matériel ou sans son accord explicite.

c) Il est recommandé que le commanditaire informe, tout au long de la prestation, le prestataire des évolutions portées ou prévues sur le système d'information cible et qui pourraient impacter les résultats de la prestation.

d) Il est recommandé que le commanditaire mette en œuvre des moyens de communication sécurisés et dédiés pour tous les échanges en rapport avec la prestation, en interne et avec le prestataire.

e) Il est recommandé que le commanditaire ait la capacité de révoquer un consultant.

f) Il est recommandé que le commanditaire exige du prestataire que la fréquence des comités de pilotage (voir VI.2.2) devant être définie dans la convention de service soit au minimum mensuelle.

IV. Après la prestation

a) Il est recommandé au commanditaire d'effectuer une revue régulière des conclusions issues de la prestation et de mettre en place des contrôles afin de s'assurer que les recommandations issues de la prestation sont effectivement mises en œuvre. Les fréquences des revues et des contrôles sont à

adapter en fonction des évolutions, de la sensibilité et des besoins réglementaires associés au système d'information cible.

b) Il est recommandé au commanditaire de mettre en place, au même titre que la prestation, une structure projet pour la mise en place du plan d'action de traitement des risques : identification des traitants, identification des personnes requises, estimation des charges, planification des actions, etc.

Annexe 4 Prérequis à fournir par les commanditaires

Cette annexe liste les prérequis à l'intention des commanditaires nécessaires à la réalisation des prestations d'accompagnement et de conseil en sécurité des systèmes d'information.

I. Prérequis à fournir pour les activités de conseil en homologation de sécurité des systèmes d'information

a) Les documents suivants constituent les éléments de base à la réalisation des activités de conseil en homologation de sécurité des systèmes d'information et sont attendus du commanditaire par le prestataire au début de la prestation :

- le référentiel d'homologation (cadre réglementaire, PSSI, etc.) ;
- les spécifications fonctionnelles ;
- les spécifications techniques[11] ;
- le dossier d'architecture du système d'information cible, incluant un schéma d'architecture à jour, clair et exhaustif du système d'information cible, les vues données applications et infrastructures logiques du système d'information cible et les flux de données associés[11].

b) Pendant la prestation, le commanditaire doit être capable de fournir les noms des interlocuteurs correspondant à chaque profil ci-dessous et de les mettre en contact avec le prestataire en cas de besoin pendant la prestation :

- un responsable du projet d'homologation ;
- un responsable projet du périmètre objet de la prestation ;
- un représentant métier du périmètre de la prestation ;
- au moins un architecte fonctionnel et technique ayant une compréhension du système d'information cible ;
- un responsable technique du système ;
- un acteur en charge du MCO ;
- un acteur en charge du MCS ;
- un interlocuteur des équipes responsables de la sécurité des systèmes d'information.

Un même interlocuteur peut cumuler plusieurs profils de la liste ci-dessus.

II. Prérequis à fournir pour les activités de conseil en gestion des risques de sécurité des systèmes d'information

a) Les documents suivants constituent les éléments de base à la réalisation des activités de conseil en gestion des risques de sécurité des systèmes d'information et sont attendus du commanditaire par le prestataire au début de la prestation :

- les spécifications fonctionnelles détaillées du système d'information cible ;
- le dossier d'architecture du système d'information cible, incluant un schéma d'architecture à jour, clair et exhaustif du système d'information cible, les vues données applications et infrastructures logiques du système d'information cible et les flux de données associés.

b) Pendant la prestation, le commanditaire doit être capable de fournir les noms des interlocuteurs correspondant à chaque profil ci-dessous et de les mettre en contact avec le prestataire en cas de besoin pendant la prestation :

[11] Par exemple, certains documents pourront ne pas exister lors d'une prestation intervenant dans le cadre de la conception d'un système d'information.

- un responsable projet du périmètre objet de la prestation ;
- un représentant métier du périmètre de la prestation ;
- au moins un architecte fonctionnel et technique ayant une compréhension du système d'information cible ;
- un responsable technique du système ;
- un acteur en charge du MCO ;
- un acteur en charge du MCS ;
- un interlocuteur des équipes responsables de la sécurité des systèmes d'information.

Un même interlocuteur peut cumuler plusieurs profils de la liste ci-dessus.

III. Prérequis à fournir pour les activités de conseil en sécurité des architectures des systèmes d'information

a) Les documents suivants constituent les éléments de base à la réalisation des activités de conseil en architecture de sécurité des systèmes d'information et sont attendus du commanditaire par le prestataire au début de la prestation :

- les spécifications fonctionnelles ;
- les spécifications techniques ;
- le dossier d'architecture du système d'information cible, incluant un schéma d'architecture à jour, clair et exhaustif du système d'information cible, les vues données applications et infrastructures logiques du système d'information cible et les flux de données associés ;
- la liste existante de mesures applicables au système d'information cible (au minimum l'un des documents suivants : PSSI, rapports des précédentes analyses de risques, tests, audits et plans d'actions associés, dossier d'homologation, etc.).

b) Pendant la prestation, le commanditaire doit être capable de fournir les noms des interlocuteurs pour chaque profil ci-dessous et de les mettre en contact avec le prestataire en cas de besoin dans le cadre de la prestation :

- un responsable projet du périmètre objet de la prestation ;
- un représentant métier du périmètre de la prestation ;
- au moins un architecte fonctionnel ou technique ayant une compréhension du système d'information cible ;
- un responsable technique du système ;
- un acteur en charge du MCO ;
- un acteur en charge du MCS ;
- un interlocuteur des équipes responsables de la sécurité des systèmes d'information.