RÉPUBLIQUE
FRANÇAISE
Liberté
Égalité
Fraternité

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 1.1 du 3 juin 2025

HISTORIQUE DES VERSIONS			
DATE	**VERSION**	**EVOLUTION DU DOCUMENT**	**REDACTEUR**
05/11/2020	03.0	*Version publiée pour appel à commentaires*	ANSSI
13/12/2021	03.1	*Prise en compte des remarques suite à l'appel à commentaires*	ANSSI
17/10/2022	03.2	*Version publiée pour appel à commentaires intégrant l'activité de préparation à la gestion de crise d'origine cyber*	ANSSI
19/07/2023	1.0	*Prise en compte des remarques suite aux groupes de travail organisés avec les parties prenantes et les prestataires*	ANSSI
03/06/2025	1.1	*Prise en compte du nouveau guide de l'ANSSI « L'homologation de sécurité des systèmes d'information »*	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.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.2.1. 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 », etc..), interagir avec de plus en plus d'acteurs (fournisseurs de produits et services, partenaires, sous-traitants, etc.) 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 ([LOI_LPM], [NIS], [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 organisations doivent mettre en place des dispositifs adaptés et proportionnés pour protéger leurs systèmes d'information 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 risques et de définition de plans de traitement de ces risques. Enfin, les organisations doivent également se préparer aux crises affectant ces systèmes d'information ou services numériques et aux impacts sur les activités métiers qu'ils supportent, en adaptant leur dispositif de crise, de continuité d'activité et de résilience à la composante cyber.

Face à cette évolution permanente des risques et des réglementations, les entreprises et organisations doivent être soutenues dans leurs démarches de gestion des risques, de protection de leurs systèmes d'information, et dans les démarches de gestion des crises associées. Elles peuvent alors souhaiter être accompagnées par des prestataires afin de bénéficier de main d'œuvre et d'expertise souvent difficiles à réunir au sein même de leur organisation.

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.2.2. 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 conformément à la règlementation en vigueur [D_2015_350], 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 en vigueur, notamment en matière de protection des informations sensibles [II_901] et de protection du secret de la défense nationale [IGI_1300], 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.2.3. 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 du présent référentiel.

Le chapitre IV présente les exigences relatives aux prestataires.

Le chapitre V présente les exigences relatives aux consultants du 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 à fournir par les commanditaires dans le cadre d'une prestation d'accompagnement et de conseil en sécurité des systèmes d'information.

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
BIA	Bilan d'impact d'activité
CaaS	*Containers as a service*
GDC	Gestion de crise
IaaS	*Infrastructure as a service*
LID	Lutte informatique défensive

MCO	Maintien en condition opérationnelle
MCS	Maintien en condition de sécurité
MVC	Modèle-Vue-Contrôleur
OIV	Opérateur d'importance vitale
PACS	Prestataire d'accompagnement et de conseil en sécurité des systèmes d'information
PaaS	*Platform as a service*
PASSI	Prestataire d'audit de la sécurité des systèmes d'information
PCA	Plan de continuité d'activité
PCI	Plan de continuité informatique
PRA	Plan de reprise d'activité
PDIS	Prestataire de détection d'incidents de sécurité
PRIS	Prestataire de réponse aux incidents de sécurité
PSSI	Politique de sécurité des systèmes d'information
RETEX	Retour d'expérience
SaaS	*Software as a service*

I.3.2. Définitions

Les définitions ci-dessous s'appuient sur les normes et références documentaires de l'Annexe 1 ainsi que sur la stratégie nationale pour la sécurité du numérique.

Accompagnement et conseil en sécurité des systèmes d'information - prestation intellectuelle relative 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.

Bénéficiaire – entité bénéficiant de la prestation d'accompagnement et de conseil en sécurité des systèmes d'information. Le bénéficiaire de la prestation peut être ou non le commanditaire de la prestation.

Capacités opérationnelles - ensemble des processus, ressources et outils disponibles pour permettre d'atteindre un objectif précis.

Commanditaire - entité faisant appel à un prestataire d'accompagnement et de conseil en sécurité des systèmes d'information. Le commanditaire de la prestation peut être ou non le bénéficiaire de la prestation.

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 tout ou partie des activités identifiées au chapitre II du référentiel. Ses missions et compétences sont détaillées dans l'Annexe 2.

Convention de service - accord écrit entre un commanditaire et un prestataire pour la réalisation d'une prestation d'accompagnement et de conseil en sécurité des systèmes d'information.

Crise d'origine cyber - déstabilisation immédiate et majeure du fonctionnement courant d'une organisation (arrêt des activités, impossibilité de délivrer des services, pertes financières lourdes, perte d'intégrité majeure, etc.) en raison d'une ou de plusieurs actions malveillantes sur ses services et ses outils numériques ou systèmes (cyberattaques de type rançongiciel, déni de service, etc.).

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 à laquelle le prestataire peut faire appel au sein de son organisation. L'expert est reconnu par le responsable de 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. Il peut être qualifié ou non et ne peut être externe au prestataire.

Gestion de crise - Processus de gestion qui identifie les impacts potentiels qui menacent une organisation et fournit un cadre pour renforcer la résilience, avec la capacité d'une réponse efficace qui préserve les intérêts des principales parties prenantes de l'organisation, sa réputation, sa marque et ses activités créatrices de valeur, et qui rétablit efficacement les capacités opérationnelles[1].

Mesure de sécurité – Mise en œuvre de moyens physiques, techniques et organisationnels permettant à l'entité responsable d'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 aux exigences du présent référentiel.

Référentiel - le présent document.

Responsable de prestation - 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 et compétences sont détaillées dans l'Annexe 2.

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

Sécurité d'un système d'information - ensemble des mesures de sécurité permettant à un système d'information de résister à des évènements susceptibles de compromettre la disponibilité,

[1] Définition inspirée de la norme ISO 28002.

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 (le sous-traitant) tout ou partie de l'exécution de la convention de service. Le sous-traitant ainsi identifié est donc par essence extérieur à l'organisation du prestataire.

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

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

Tiers - personne ou organisation indépendante du prestataire, du commanditaire et du bénéficiaire.

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 ;
- le conseil en préparation à la gestion de crise d'origine cyber.

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 en condition de sécurité.

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'établir 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 risques, conseil en architecture, etc.) n'entrent pas dans la définition de cette activité et peuvent être menées conformément à d'autres parties du présent référentiel ou d'autres référentiels proposés par l'ANSSI.

Cet accompagnement peut intervenir dans le cadre de l'homologation initiale de sécurité d'un système d'information, du suivi de cette homologation, ou de son renouvellement.

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 dans le cadre de la conception d'un système d'information, de l'évolution d'un système d'information existant ou de la 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 d'un système d'information. Elle doit l'aider à définir des modèles de référence déclinant les principes du modèle de sécurité globale. La prestation de conseil doit être menée en s'assurant

de répondre à des exigences de sécurité adaptées au système d'information cible et au contexte d'activité du commanditaire. Ces choix doivent 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 peut intervenir dans le cadre de la conception d'un système d'information, de l'évolution d'un système d'information existant, ou de la revue d'un système d'information existant.

II.4. Conseil en préparation à la gestion de crise d'origine cyber

L'activité de conseil en préparation à la gestion de crise d'origine cyber consiste à accompagner le commanditaire dans la structuration de son dispositif de crise pour intégrer les dimensions spécifiques des crises d'origine cyber, ainsi que pour préparer les équipes à acquérir des réflexes de réponse à la crise. Elle permet au commanditaire de définir sa gouvernance de gestion de crise. Elle doit l'aider à définir des politiques et leurs déclinaisons, des modèles et des outils pour rendre plus concrète la réponse stratégique et opérationnelle durant la crise. Cette réponse à la crise comprend également la communication de crise, une prise en compte des aspects juridiques et potentiellement assurantiels.

Le conseil en préparation à la gestion de crise d'origine cyber doit s'assurer que les dispositifs de continuité d'activité adressent les risques d'origine cyber et s'adaptent aux spécificités de ce type de crise. Il convient notamment d'intégrer le risque d'origine cyber dans les plans de continuité d'activité (PCA), plans de reprise d'activité (PRA) et plans de continuité informatique (PCI). L'activité doit être menée en s'assurant de répondre aux exigences de continuité d'activité du commanditaire ainsi qu'à sa maturité.

Les travaux peuvent porter sur des aspects organisationnels tels que la structuration d'équipes et de politiques, ou techniques tels que la définition de fiches réflexes, la mise en place d'outillage de crise, ou de dispositifs opérationnels permettant de répondre aux enjeux de continuité. Ils peuvent également porter sur l'entrainement et la formation des équipes mobilisées lors des crises.

Cet accompagnement peut intervenir dans le cadre de la conception d'un dispositif de gestion de crise, de l'évolution d'un dispositif de gestion de crise existant ou de la revue d'un dispositif de gestion de crise existant.

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

III.1. Modalités de la qualification

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

Une organisation 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 une organisation offrant des prestations d'accompagnement et de conseil en sécurité des systèmes d'information pour son propre compte ou pour le compte d'autres organisations.

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

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

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

Le référentiel donne également aux commanditaires des recommandations et la liste 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 dans le cadre du processus de qualification du prestataire.

III.2. Portée de la qualification

Le prestataire peut demander la qualification pour tout ou partie des activités décrites au chapitre II du présent référentiel. Toutefois, la qualification ne portant que sur l'activité de conseil en homologation de sécurité de systèmes d'information n'est pas autorisée ; l'activité de conseil en homologation de sécurité de systèmes d'information doit systématiquement être accompagnée de l'activité de conseil en gestion des risques de sécurité des systèmes d'information.

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 V 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.

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 sur la portée cible, peut potentiellement exposer le commanditaire ou le bénéficiaire 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.

IV. Exigences relatives au prestataire

IV.1. Exigences générales

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

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

c) Le prestataire doit, en sa qualité de professionnel, avoir un devoir de conseil vis-à-vis du commanditaire.

d) Le prestataire doit s'assurer du consentement du commanditaire avant toute communication d'informations obtenues ou produites dans le cadre de la prestation.

e) 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.

f) 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.

g) Le prestataire doit prévoir l'enregistrement et le traitement des plaintes portant sur sa prestation déposées par les commanditaires, les bénéficiaires et les tiers.

h) Des mesures de sécurité doivent être mises en place pour protéger les informations relatives à la prestation à toutes les étapes. En particulier, le prestataire doit protéger en confidentialité ces informations et notamment lors de la phase de qualification préalable d'aptitude à la réalisation de la prestation (voir chapitre VI.1). Ces mesures doivent tenir compte du niveau de sensibilité ou de classification de ces informations.

IV.2. 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 de l'équipe de réalisation doit disposer d'une attestation individuelle de compétence 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. Pour cela, le prestataire doit disposer d'un processus de formation continue et permettre à ses consultants d'assurer une veille.

c) Le prestataire doit, avant toute intégration d'un nouveau consultant dans ses équipes, procéder à une vérification des formations, compétences et références professionnelles et de la véracité de son 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.

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.4 , couvrant les domaines détaillés en Annexe 2.

f) Le prestataire doit mettre en place un processus de sensibilisation des consultants à la législation et réglementation en vigueur au sein de l'Union Européenne et applicables à leurs missions.

g) Le prestataire doit s'assurer que les consultants ne font pas l'objet d'une inscription au casier judiciaire incompatible avec l'exercice de leurs fonctions.

IV.3. Protection de l'information

Le prestataire peut traiter tout ou partie des informations relatives à la prestation sur son système d'information, celui du commanditaire ou du bénéficiaire. Lorsque le prestataire traite les informations sur son système d'information, il les traite exclusivement sur son système d'information homologué Diffusion Restreinte quel que soit leur marquage.

a) Le prestataire a un devoir de conseil vis-à-vis du commanditaire et doit lui proposer un marquage adapté des informations et supports relatifs à la prestation selon leur niveau de sensibilité, ainsi que les moyens de protection associés[2].

b) Le prestataire doit préserver la confidentialité des informations et supports relatifs à la prestation selon leur niveau de sensibilité. Il doit appliquer le principe du moindre privilège et limiter l'accès aux informations et supports aux strictes personnes ayant le droit et besoin d'en connaître.

c) Le prestataire doit élaborer une analyse des risques relative à son système d'information.

d) Il est recommandé que le prestataire mette en œuvre la méthode [EBIOS_RM] pour élaborer l'analyse des risques relative à son système d'information.

e) Le prestataire doit homologuer son système d'information au niveau Diffusion Restreinte [II_901].

f) Il est recommandé que le prestataire mette en œuvre la démarche décrite dans le guide [G_HOMOLOGATION] pour homologuer son système d'information Diffusion Restreinte.

g) Le prestataire doit, pour son système d'information homologué Diffusion Restreinte, respecter les règles relatives à la protection des systèmes d'information traitant des informations portant la mention Diffusion Restreinte définies dans [II_901].

h) Le prestataire doit, pour son système d'information homologué Diffusion Restreinte, mettre en œuvre les règles du niveau renforcé du guide d'hygiène informatique [G_HYGIENE].

i) Il est recommandé que le prestataire, pour son système d'information homologué Diffusion Restreinte, mette en œuvre les recommandations du guide [G_ARCHI_DR] pour la conception de l'architecture de son système d'information homologué Diffusion Restreinte.

[2] Le choix du marquage des informations et supports relatifs à la prestation ainsi que des moyens de protection associés revient *in fine* au commanditaire et est consigné dans la note de cadrage définie au chapitre VI.2.5.

V. Exigences relatives aux personnes

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 de prestation doit posséder les qualités personnelles identifiées au chapitre 7.2.3.4 de la norme [ISO19011].

c) Le responsable de prestation et le consultant doivent être sensibilisés aux lois et réglementations en vigueur au sein de l'Union européenne applicables à leurs missions.

d) Le responsable de prestation et le consultant doivent disposer des qualités rédactionnelles, de rigueur et de synthèse.

e) Le responsable de prestation et le consultant doivent disposer des qualités d'écoute et de communication leur permettant d'engager un dialogue constructif avec les différents niveaux d'interlocuteurs du commanditaire.

f) 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. Aptitudes spécifiques aux activités

a) Le responsable de prestation et le consultant doivent réaliser la prestation conformément aux exigences du chapitre VI.

b) Le responsable de prestation et le consultant doivent, selon leur profil, assurer les missions décrites dans l'Annexe 2.

c) Le responsable de prestation et le consultant doivent, selon leur profil, disposer des compétences décrites dans l'Annexe 2.

d) Le responsable de prestation et le consultant doivent, selon leur profil, disposer des connaissances décrites dans l'Annexe 2.

V.3. Expérience

a) Il est recommandé que le responsable de prestation 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 de sécurité des systèmes d'information justifie d'au moins :
   i. deux années d'expérience dans le domaine de la sécurité des systèmes d'information ;
   ii. trois années d'expérience dans le domaine de la gestion du risque.

c) Il est recommandé que le consultant en sécurité des architectures des systèmes d'information justifie d'au moins :
   i. deux années d'expérience dans le domaine de la sécurité des systèmes d'information ;
   ii. trois années d'expérience dans le domaine des technologies des systèmes d'information ;

iii. une année d'expérience dans le domaine de la sécurité des architectures des systèmes d'information.

d) Il est recommandé que le consultant préparation à la gestion de crise d'origine cyber justifie d'au moins :
   i. deux années d'expérience dans le domaine de la sécurité des systèmes d'information ;
   ii. trois années d'expérience dans le domaine de la préparation à la gestion de crise ;
   iii. une expérience dans la gestion de crises d'origine cyber.

V.4. Engagements

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

b) Le responsable de prestation doit avoir une relation contractuelle avec le prestataire.

VI. Exigences relatives au déroulement d'une 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. En particulier, le prestataire doit s'assurer que les composantes du périmètre sont identifiées avec un niveau de précision suffisant, sans ambiguïté et sont à la fois pertinentes et complètes relativement à l'objectif de la prestation.

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

c) Le prestataire doit informer le commanditaire des recommandations contenues dans l'Annexe 3.

d) Le prestataire doit obtenir un engagement du commanditaire sur la fourniture des prérequis nécessaires à la réalisation d'une prestation qualifiée, dont la liste est fournie à l'Annexe 4 du présent document.

e) Le prestataire doit demander au commanditaire, avant le début de la prestation :
   i. 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) ;
   ii. la liste des intervenants au sein 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 le prestataire et le commanditaire. Elle doit être signée par des représentants légaux ou toute personne pouvant engager le prestataire et le commanditaire. Dans le cas où le commanditaire n'est pas le bénéficiaire de la prestation, celui-ci atteste de l'accord du bénéficiaire pour démarrer la prestation. Toute modification de la convention de service doit être soumise à l'acceptation du commanditaire.

VI.2.1. Modalités de la prestation

La convention de service doit :

a) indiquer que la prestation réalisée est une prestation qualifiée et inclure l'attestation de qualification du prestataire ;

b) identifier et appliquer le droit d'un État membre de l'Union Européenne ;

c) identifier le périmètre, les objectifs et les activités de la prestation ;

d) indiquer que les consultants et les responsables de prestation disposent d'une attestation individuelle de compétence pour les activités de la prestation et inclure ces attestations ;

e) préciser que le prestataire peut faire intervenir un expert pour la réalisation de certaines activités de la prestation au motif que certaines compétences spécifiques nécessaires ne sont couvertes par les consultants et les responsables de prestation, sous réserve que :
   i. il existe un cadre contractuel entre le prestataire et l'expert ;
   ii. le recours à un expert est accepté par écrit par le commanditaire ;
   iii. l'expert est dûment encadré par le responsable de la prestation.

   L'expert ne se substitue pas à un consultant ou à un responsable de prestation.

f) 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 ou le rapport de la prestation ;

g) spécifier que le prestataire ne recourt pas à des consultants ou des responsables de prestation n'ayant pas de relation contractuelle avec lui, n'ayant pas obtenu une attestation individuelle de compétence ou faisant l'objet d'une inscription au casier judiciaire incompatible avec l'exercice de leurs fonctions.

VI.2.2. Responsabilités

La convention de service doit :

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

b) spécifier que le commanditaire dispose de l'ensemble des droits de propriété et d'accès sur le périmètre de la prestation (systèmes d'information, supports matériels, etc.) ou, le cas échéant, qu'il a recueilli l'accord des tiers dont les systèmes d'information entrent dans le périmètre de la prestation.

VI.2.3. Confidentialité

La convention de service doit :

a) indiquer que le prestataire ne divulgue ou ne partage aucune information relative à la prestation à des tiers, sauf autorisation écrite du commanditaire ;

b) 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 ;

c) indiquer que le prestataire détruit l'ensemble des informations relatives à la prestation 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. Le cas échéant les modalités de conservation (par exemple anonymisation, décontextualisation, durée) doivent être approuvées par le commanditaire.

VI.2.4. Sous-traitance et expertise

La convention de service doit :

a) préciser que le prestataire peut sous-traiter une partie des activités à un autre prestataire qualifié conformément aux exigences du référentiel qui lui sont applicables sous réserve que :

i. il existe cadre contractuel entre le prestataire et son sous-traitant ;
ii. le recours à la sous-traitance est accepté par écrit par le commanditaire ;
iii. le sous-traitant respecte les exigences du référentiel sur l'activité cible.

VI.2.5. Note de cadrage

a) La convention de service doit prévoir que le prestataire élabore et tienne à jour une note de cadrage.

b) La note de cadrage doit être validée par le correspondant de la prestation chez le commanditaire et le responsable de prestation, au début de la prestation et à chaque modification durant la prestation.

c) La note de cadrage doit :
   i. préciser les prérequis à fournir par le commanditaire tels qu'identifiés dans l'Annexe 4 ;
   ii. identifier le marquage des informations et supports relatifs à la prestation selon leur niveau de sensibilité, ainsi que les moyens de protection associés ;
   iii. préciser les modalités relatives aux livrables de la prestation (contenu, forme, langue, etc.) ;
   iv. identifier le nom du correspondant de la prestation chez le commanditaire ;
   v. identifier les noms, rôles, responsabilités ainsi que les droits et besoin d'en connaître des personnes désignées par le prestataire et le commanditaire ;
   vi. le cas échant, prévoir et prendre en compte les modalités de collaboration avec les tiers (sous-traitants, etc.) ;
   vii. spécifier les instances de gouvernance de la prestation mises en place et leur fréquence de réunion (réunions de suivi, comités de pilotage, etc.) ;
   viii. identifier les éventuelles exigences légales et réglementaires spécifiques auxquelles est soumis le système d'information cible ;
   ix. identifier les éventuelles exigences légales et réglementaires spécifiques auxquelles est soumis le commanditaire.

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

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

b) Le responsable de prestation doit constituer une équipe de consultants ayant les compétences adaptées à la nature de la prestation[3].

c) Le responsable de prestation doit, dès le début de la préparation de la prestation, établir un contact avec le correspondant de la prestation chez le commanditaire. 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 de prestation doit également obtenir du correspondant de la prestation chez le commanditaire la liste des points de contact nécessaires à la réalisation de la prestation.

3 Le responsable de 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 de 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.

e) Le responsable de prestation élabore un plan de cadrage 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.

f) En fonction de l'objet de la prestation, l'équipe du prestataire doit obtenir du commanditaire toute la documentation existante (exemples : politique de sécurité, analyse de risques, 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. Elle doit ainsi, le cas échéant, demander au commanditaire des compléments d'informations par rapport aux documents déjà transmis lors de l'élaboration de la proposition de service répondant à la demande du commanditaire.

g) 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.

h) Il est recommandé que la réunion d'ouverture implique au minimum :
Prestataire :
- un responsable de prestation ;
- au moins un consultant pour chacune des activités d'accompagnement et de conseil en sécurité des systèmes d'information réalisées ;

Commanditaire :
- un responsable projet de la prestation ;
- un propriétaire du système d'information objet de la prestation ;
- un responsable de la sécurité du système d'information objet de la prestation ;
- un représentant métier du système d'information objet de la prestation ;
- un représentant informatique du système d'information objet de la prestation ;
- un architecte fonctionnel ou technique ayant une compréhension du système d'information objet de la prestation ;
- un acteur en charge du maintien en condition opérationnelle du système d'information objet de la prestation ;
- un acteur en charge du maintien en condition de sécurité du système d'information objet de la prestation ;
- le cas échéant, un représentant des équipes de communication ;
- le cas échéant, un représentant des équipes juridiques ;
- le cas échéant, un représentant des tiers (fournisseurs de produits et services, sous-traitants, etc.) impliqués dans le système d'information objet de la prestation.

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

VI.4. Étape 4 : exécution de la prestation

VI.4.1. Exigences générales

a) Le prestataire doit réaliser sa prestation dans le respect des personnels et des infrastructures du commanditaire.

VI.4.2. Exigences spécifiques à une activité

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

a) Le prestataire doit accompagner le commanditaire dans son projet d'homologation selon les principes de la démarche d'homologation des systèmes d'information décrits dans [G_HOMOLOGATION] ou conformément à la méthodologie d'homologation propre au commanditaire, si celle-ci préexiste au sein de son organisation.

b) Le prestataire doit identifier les interlocuteurs clés afin de comprendre le contexte de l'organisation et son système d'information. Il doit ensuite obtenir l'engagement des équipes de direction, puis organiser et conduire les entretiens avec les personnes identifiées.

c) Le prestataire doit procéder à la revue des documents identifiés dans la note de cadrage.

d) Le prestataire doit s'assurer que le dossier d'homologation est complet et conforme au [G_HOMOLOGATION] ou à la méthodologie propre du commanditaire, si celle-ci préexiste au sein de son organisation. Le prestataire doit fournir un avis motivé sur la pertinence des éléments collectés au regard des objectifs de la prestation.

e) Le cas échéant, le prestataire doit accompagner le commanditaire dans la collecte des éléments du dossier et doit informer le commanditaire de la nécessité d'initier la rédaction ou la mise à jour des éléments manquants ou à améliorer pour chacune des pièces du dossier.

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 risques 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 risques d'un système d'information.

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

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

e) Le prestataire doit identifier les interlocuteurs pertinents à rencontrer puis organiser et mener les entretiens avec ces derniers.

f) Le prestataire doit procéder à la revue des documents identifiés dans la note de cadrage.

g) Le prestataire doit procéder à la revue des documents et organiser la rencontre des interlocuteurs identifiés dans la convention de service conformément aux informations fournies par le commanditaire.

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

h) Le prestataire doit identifier les interlocuteurs pertinents à rencontrer puis organiser et mener les entretiens avec ces derniers. Les interlocuteurs pertinents sont notamment ceux impliqués dans la définition, la mise en place, le maintien en condition opérationnelle (MCO) et de sécurité (MCS) de toutes les briques du système d'information cible.

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

b) 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.4.2.4. Exécution des activités de conseil en préparation à la gestion de crise d'origine cyber

a) Le prestataire doit accompagner le commanditaire dans sa préparation à la gestion de crise d'origine cyber selon les principes décrits dans [G_GESTION_CRISE].

b) Le prestataire doit être capable d'organiser et mener des entretiens avec le personnel concerné par la définition, la mise en place ou l'amélioration du dispositif de crise du commanditaire et des dispositifs opérationnels associés.

c) Le prestataire doit procéder à la revue des documents et organiser la rencontre des interlocuteurs identifiés (voir Annexe 4, section VI) dans la convention de service.

d) Le prestataire doit être capable de formaliser ou d'accompagner le commanditaire dans la formalisation de fiches réflexes, de procédures ou de tout autre livrable jugé pertinent (logigramme, fiche de rôle, etc.) pour faciliter l'intervention des cellules stratégiques et des équipes opérationnelles dans le cadre d'incidents majeurs et de crises.

e) Dans le cadre d'organisation d'entrainements à la gestion de crise d'origine cyber, le prestataire doit s'appuyer sur la méthodologie proposée dans le guide [G_GESTION_CRISE]. Le prestataire doit être en mesure d'organiser ou de coordonner des exercices pour des cellules stratégiques et/ou opérationnelles et/ou pour des équipes techniques.

f) Dans le cadre d'un accompagnement sur l'anticipation d'une communication de crise d'origine cyber, le prestataire doit mettre en place la méthodologie proposée dans le guide [G_COM_CRISE].

g) Dans le cadre d'un accompagnement sur l'outillage de crise, le prestataire doit pouvoir accompagner le commanditaire dans la mise en place d'outils identifiés, lors de la phase de diagnostic.

h) Le prestataire doit baser ses recommandations sur des standards éprouvés, maintenus, pérennes, respectant les principes des textes et guides publiés par l'ANSSI ou reconnus

comme conformes aux normes existantes en matière de gestion de crise d'origine cyber. 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 : suivi régulier de la prestation

a) Le prestataire doit organiser des points de suivi selon les modalités définies dans la note de cadrage. 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 ;
   - tout changement dans les consultants réalisant la prestation au sein de l'équipe du prestataire ;
   - tout changement des modalités de la prestation.

b) Dès la fin de l'étape VI.4, et sans attendre que le rapport de prestation soit achevé, le responsable de prestation doit informer le commanditaire des constats et des premières conclusions de la prestation.

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

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

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

b) Le rapport 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 réalisées.

c) 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 globale,
   - le périmètre et les objectifs de la prestation ;
   - la cartographie du système d'information cible ;
   - les différentes étapes de la prestation, les entretiens réalisés et les documents analysés dans le cadre de la prestation ;
   - la synthèse des résultats de chacune des activités d'accompagnement et conseil en sécurité des systèmes d'information réalisées dans le cadre de la prestation.
   - la synthèse globale de la prestation.

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

e) Le rapport de prestation doit mentionner les noms, coordonnées et fonctions des responsables de prestation, consultant et, le cas échéants experts, qui ont réalisé la prestation.

f) Le rapport de prestation doit mentionner les noms, coordonnées et fonctions des interlocuteurs que le prestataire a rencontré lors d'entretiens et préciser la date de l'entretien.

g) Le rapport de prestation doit identifier l'ensemble des documents sur lesquels s'appuie 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 de prestation, les éléments suivants :
   - un document d'accompagnement présentant le système d'information dans son contexte et justifiant la démarche adoptée ;
   - 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 constitutif du dossier d'homologation ;
      iii. le socle de sécurité[4] 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 risques, la politique de sécurité spécifique appliquée au système d'information cible, la synthèse des audits et travaux de certification menés si existants et la synthèse des risques résiduels ;
      v. le plan de traitement des risques 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 de traitement des risques.

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 de prestation, les éléments spécifiques suivants :
   - la méthodologie d'analyse des risques utilisée ;
   - 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 ;

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

- la cartographie des risques résiduels après traitement par les mesures de sécurité préconisées ;

b) 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.

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

d) 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.

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 de prestation, les éléments spécifiques suivants :
   - 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[5] :
      i. politique de sécurité des systèmes d'information (PSSI) ;
      ii. cartographie / documentation ;
      iii. maintien en condition opérationnelle (MCO) ;
      iv. maintien en condition de sécurité (MCS) ;
      v. journalisation ;
      vi. détection des incidents de sécurité ;
      vii. traitement des incidents de sécurité ;
      viii. identification (utilisateurs/processus) ;
      ix. authentification (utilisateurs/processus) ;
      x. gestion des droits d'accès ;
      xi. gestion des comptes à privilèges ;
      xii. administration sécurisée ;
      xiii. cloisonnement réseau et chiffrement des données en transit ;
      xiv. cloisonnement système et chiffrement des données au repos ;
      xv. filtrage des flux ;
      xvi. accès à distance (nomadisme, partenaires) ;
      xvii. sécurité physique, contrôle d'accès physique, et vidéoprotection ;
      xviii. sauvegardes, plan de reprise d'activité (PRA), plan de continuité d'activité (PCA) ;
      xix. stockage et hébergement.
   - 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

[5] Ces thématiques sont à adapter en fonction du périmètre et des objectifs de la prestation.

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 priorisées 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.6.4. Rapport de prestation de conseil en préparation à la gestion de crise d'origine cyber

a) Le rapport de prestation concernant les activités de conseil en préparation à la gestion de crises d'origine cyber doit comprendre, en complément des éléments requis dans le cadre du rapport de prestation, les éléments spécifiques suivants :
   - un rappel des objectifs de la prestation ainsi que du périmètre technique et métier du dispositif de gestion de crise cible ;
   - un ensemble documentaire composé, selon les prestations :
      i. Prestation d'évaluation ou de revue d'un dispositif de gestion de crise d'origine cyber :
         - un rapport d'audit évaluant le niveau de maturité du dispositif de crise vis-à-vis de l'état de l'art, en s'appuyant sur [G_GESTION_CRISE] et le retour d'expérience d'incidents et/ou de crises passés, si existants ;
         - un document définissant les capacités opérationnelles existantes et à mettre en place pour garantir un niveau adapté de gestion de crise d'origine cyber ;
      ii. Prestation d'évaluation ou de revue d'un dispositif de continuité d'activité :
         - un rapport d'audit évaluant le niveau de maturité du dispositif de continuité d'activité face à la menace d'origine cyber vis-à-vis de l'état de l'art, en s'appuyant sur [G_GESTION_CRISE] et le retour d'expérience d'incidents et/ou de crises passés, si existants ;
         - un document définissant les capacités opérationnelles existantes et à mettre en place pour garantir un niveau adapté de continuité d'activité face à la menace d'origine cyber ;
      iii. Mise en place d'un dispositif de gestion de crise d'origine cyber :
         - un document décrivant la gouvernance cible de crise d'origine cyber de l'organisation commanditaire, en incluant son évaluation régulière et les dispositifs d'amélioration continue ;
         - un ensemble de fiche réflexes, de fiches rôles et de procédures pour outiller la gestion de crise, conformément aux attentes de [G_GESTION_CRISE] et [EBIOS_RM] ;
         - l'identification du personnel en charge d'armer le dispositif de crise ;
         - un document décrivant la stratégie de vérification, d'audit et de retour sur expérience (après crise réelle) des capacités opérationnelles garantissant un niveau adapté de gestion de crise d'origine cyber ;

- un document formalisant une stratégie d'entrainement et de formation du dispositif de crise au niveau stratégique et opérationnel et incluant les supports de formation / sensibilisation si conduites lors de la prestation ;
- un document formalisant la méthodologie et les modèles à utiliser dans l'anticipation de crise d'origine cyber ;
- un document formalisant
  - les scénarios de crise, la stratégie de communication de réponse à la crise d'origine cyber, le schéma d'organisation de la communication en cas de crise, les outils de pilotage de la communication (un fichier presse, les codes de connexion aux comptes réseaux sociaux, applications mobiles, site web et Intranet), l'annuaire des acteurs de la gestion de crise, et des éléments de langage sur des sujets sensibles ou de crise ;
  - la procédure type de notification aux autorités pertinentes ;
- une liste de modèles et d'outils (mis en place durant la prestation ou déjà présents) et de lieux disponibles pour la gestion de crise.
  - pour les outils mis en place durant la prestation, un guide d'utilisation.

iv. Mise en place d'un dispositif de continuité d'activité face à la menace d'origine cyber :
- un bilan d'impact d'activité (BIA) précisant le besoin de continuité cyber, la stratégie de continuité ;
- un plan de continuité d'activité (PCA) cyber ainsi que d'un plan de reprise d'activité (PRA) cyber, notamment en incluant un plan de continuité informatique (PCI) ;
- un ensemble de fiche réflexes, de fiches rôles et de procédures pour outiller la continuité d'activité, en prenant en compte les besoins établis par le BIA ainsi que les scénarios cyber redoutés, conformément aux attentes de [G_GESTION_CRISE] et [EBIOS_RM] ;
- un document décrivant la stratégie de vérification, d'audit et de retour sur expérience (après crise réelle) des capacités opérationnelles garantissant un niveau adapté de continuité d'activité face à la menace d'origine cyber ;
- un document formalisant une stratégie d'entrainement et de formation sur la continuité d'activité, et incluant les supports des formations et des sensibilisations si elles ont été conduites lors de la prestation ;
- une liste de modèles et d'outils (mis en place durant la prestation ou déjà présents) et de lieux disponibles pour continuité d'activité face à la menace d'origine cyber.
  - Pour les outils mis en place durant la prestation, un guide d'utilisation doit également être fourni.

v. Organisation d'exercice de gestion de crise :
- le cadrage des exercices (objectifs, périmètres métiers et techniques, typologie des joueurs, dimensionnement) ;
- des scénarios, chronogrammes, dossier de mise en situation pour les joueurs et l'animation, les stimuli (socio-économiques, cyber (technique et non technique), métier et médiatiques), ainsi que les règles de sécurité et les conventions d'exercice pour les joueurs ;

        - un rapport de type « Retour d'expérience (RETEX) » décrivant le déroulement de l'exercice, la perception des participants, l'atteinte des objectifs et les enseignements pour le dispositif de crise du commanditaire, précisant les recommandations et le plan d'action associé ;
    - une liste de recommandations priorisées, permettant d'atteindre le niveau cible de gestion de crise et de continuité d'activité du commanditaire, avec des indicateurs de priorité et d'effort de mise en œuvre pour chacune d'entre elles.

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 de prestation. Cette réunion permet de présenter la synthèse du rapport de prestation, de la suite à donner à la prestation et de répondre aux éventuelles questions du commanditaire.

b) Il est recommandé que la réunion de clôture implique au minimum[6] :
Prestataire :
    - un responsable de prestation ;
    - au moins un consultant pour chacune des activités d'accompagnement et de conseil en sécurité des systèmes d'information réalisées ;

Commanditaire :
    - un responsable projet de la prestation ;
    - un propriétaire du système d'information objet de la prestation ;
    - un responsable de la sécurité du système d'information objet de la prestation ;
    - un représentant métier du système d'information objet de la prestation ;
    - un représentant informatique du système d'information objet de la prestation ;
    - un architecte fonctionnel ou technique ayant une compréhension du système d'information objet de la prestation ;
    - un acteur en charge du maintien en condition opérationnelle du système d'information objet de la prestation ;
    - un acteur en charge du maintien en condition de sécurité du système d'information objet de la prestation ;
    - le cas échéant, un représentant des équipes de communication ;
    - le cas échéant, un représentant des équipes juridiques ;
      le cas échéant, un représentant des tiers (fournisseurs de produits et services, sous-traitants, etc.) impliqués dans le système d'information objet de la prestation.

c) Le prestataire doit, le cas échéant, amender le rapport de prestation à la suite de la réunion de clôture de la prestation pour prendre en compte les éventuelles informations complémentaires obtenues pendant la réunion.

d) 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.

6 Ces rôles peuvent être cumulés par une même personne.

e) Le responsable de prestation 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.

f) Le responsable de prestation 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.

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.

h) 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 de prestation est conforme aux objectifs visés dans la convention.

Annexe 1 Références documentaires

I. Codes, textes législatifs et réglementaires

Renvoi	Document
[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, règlement modifié par le règlement (UE) n°2024/1183. Disponible sur https://eur-lex.europa.eu
[IGI_1300]	Instruction générale interministérielle n° 1300/SGDSN/PSE/PSD du 9 août 2021 sur la protection du secret de la défense nationale. Disponible sur https://www.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
[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
[LOI_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
[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

Renvoi	Document
[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
[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

II. Normes et documents techniques

Renvoi	Document
[EBIOS_RM]	Méthode de gestion de risques EBIOS Risk Manager. Disponible sur https://www.cyber.gouv.fr
[G_802.1]	Recommandations de déploiement du protocole 802.1x pour le contrôle d'accès à des réseaux locaux, ANSSI, version en vigueur. Disponible sur https://www.cyber.gouv.fr
[G_ADMIN]	Recommandations relatives à l'administration sécurisée des systèmes d'information, ANSSI, version en vigueur. Disponible sur https://www.cyber.gouv.fr
[G_APPLI_WEB]	Recommandations pour la sécurisation des sites web, ANSSI, version en vigueur. Disponible sur https://www.cyber.gouv.fr
[G_ARCHI_DR]	Recommandations pour les architectures des systèmes d'information sensibles ou diffusion restreinte, ANSSI, version en vigueur. Disponible sur https://www.cyber.gouv.fr
[G_AUTH_MULTI_MDP]	Recommandations relatives à l'authentification multifacteurs et aux mot de passe, ANSSI, version en vigueur. Disponible sur https://www.cyber.gouv.fr
[G_CARTOGRAPHIE]	Cartographie du système d'information, Guide d'élaboration en 5 étapes, ANSSI, version en vigueur. Disponible sur https://www.cyber.gouv.fr
[G_CLOISONNEMENT]	Recommandations pour la mise en place de cloisonnement système, ANSSI, version en vigueur. Disponible sur https://www.cyber.gouv.fr
[G_COM_CRISE]	Anticiper et gérer sa communication de crise cyber, ANSSI, version en vigueur. Disponible sur https://www.cyber.gouv.fr

Renvoi	Document
[G_CONTROLE_ACCES]	Recommandations sur la sécurisation des systèmes de contrôle d'accès physique et de vidéoprotection, ANSSI, version en vigueur. Disponible sur https://www.cyber.gouv.fr
[G_CRYPTO_1]	Guide de sélection d'algorithmes cryptographiques, ANSSI, version en vigueur. Disponible sur https://www.cyber.gouv.fr
[G_CRYPTO_2]	Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, ANSSI, version en vigueur. Disponible sur https://www.cyber.gouv.fr
[G_DEF_PROF]	La défense en profondeur appliquée aux systèmes d'information, ANSSI, version en vigueur. Disponible sur https://www.cyber.gouv.fr
[G_EXERCICE_CRISE]	Organiser un exercice de gestion de crise cyber, ANSSI, version en vigueur. Disponible sur https://www.cyber.gouv.fr
[G_GESTION_CRISE]	Crise d'origine cyber, les clés d'une gestion opérationnelle et stratégique, ANSSI, version en vigueur. Disponible sur https://www.cyber.gouv.fr
[G_HOMOLOGATION]	L'homologation de sécurité des systèmes d'information, ANSSI, version en vigueur. Disponible sur https://www.cyber.gouv.fr
[G_HYGIENE]	Guide d'hygiène informatique, ANSSI, version en vigueur. Disponible sur https://www.cyber.gouv.fr
[G_INTERCO]	Recommandations relatives à l'interconnexion d'un système d'information à Internet, ANSSI, version en vigueur. Disponible sur https://www.cyber.gouv.fr
[G_IPSEC]	Recommandations de sécurité relatives à IPsec pour la protection des flux réseau, ANSSI, version en vigueur. Disponible sur https://www.cyber.gouv.fr
[G_NOMADISME]	Recommandations sur le nomadisme numérique, ANSSI, version en vigueur. Disponible sur https://www.cyber.gouv.fr
[G_PAREFEUX]	Recommandations pour choisir des pare-feux maîtrisés dans les zones exposées à internet, ANSSI, version en vigueur. Disponible sur https://www.cyber.gouv.fr
[G_RANCONGICIEL]	Attaques par rançongiciels, tous concernés - Comment les anticiper et réagir en cas d'incident ?, ANSSI, version en vigueur. Disponible sur https://www.cyber.gouv.fr
[G_SEC_AD]	Recommandations de sécurité relatives à Active Directory, ANSSI, version en vigueur. Disponible sur https://www.cyber.gouv.fr
[G_SEC_DNS]	Bonnes pratiques pour l'acquisition et l'exploitation de noms de domaine, ANSSI, version en vigueur. Disponible sur https://www.cyber.gouv.fr

Renvoi	Document
[G_SEC_LINUX]	Recommandations de configuration d'un système GNU/Linux, ANSSI, version en vigueur. Disponible sur https://www.cyber.gouv.fr
[G_SEC_VIRTUAL]	Problématiques de sécurité associées à la virtualisation des systèmes d'information, ANSSI, version en vigueur. Disponible sur https://www.cyber.gouv.fr
[G_SEC_WIND]	Recommandations pour la mise en œuvre d'une politique de restrictions logicielles sous Windows, ANSSI, version en vigueur. Disponible sur https://www.cyber.gouv.fr
[G_SWITCH]	Recommandations pour la sécurisation d'un commutateur de desserte, ANSSI, version en vigueur. Disponible sur https://www.cyber.gouv.fr
[G_SYS_INDUS]	Recommandations relatives à la cybersécurité des systèmes industriels, ANSSI, version en vigueur. Disponible sur https://www.cyber.gouv.fr
[G_TLS]	Recommandations de sécurité relatives à TLS, ANSSI, version en vigueur. Disponible sur https://www.cyber.gouv.fr
[G_TOIP]	Guide de recommandations relatives à la sécurisation d'une architecture de téléphonie sur IP, ANSSI, version en vigueur. Disponible sur https://www.cyber.gouv.fr
[G_WIFI]	Recommandations de sécurité relatives aux réseaux Wi-Fi, ANSSI, version en vigueur. Disponible sur https://www.cyber.gouv.fr
[ISO19011]	Norme internationale ISO/IEC 19011 : Lignes directrices pour l'audit des systèmes de management, version en vigueur. Disponible sur https://www.iso.org
[ISO22301]	Norme internationale ISO/IEC 22301 : Sécurité et résilience — Systèmes de management de la continuité d'activité — Exigences, version en vigueur. Disponible sur https://www.iso.org
[ISO22313]	Norme internationale ISO/IEC 22313 : Sécurité et résilience — Systèmes de management de la continuité d'activité — Lignes directrices sur l'utilisation de l'ISO 22301, version en vigueur. Disponible sur https://www.iso.org
[ISO22317]	Norme internationale ISO/IEC 22317 : Sécurité et résilience — Systèmes de management de la continuité d'activité — Lignes directrices pour le bilan d'impact sur l'activité, version en vigueur. Disponible sur https://www.iso.org
[ISO22361]	Norme internationale ISO/IEC 22361 : Sécurité et résilience — Gestion de crise — Lignes directrices, version en vigueur. Disponible sur https://www.iso.org
[ISO22398]	Norme internationale ISO/IEC 22398 : Sécurité sociétale — Lignes directrices pour exercice, version en vigueur. Disponible sur https://www.iso.org

Renvoi	Document
[ISO27000]	Norme internationale ISO/IEC 27000 : Technologies de l'information – Techniques de sécurité – Systèmes de gestion de la sécurité de l'information – vue d'ensemble et vocabulaire, version en vigueur. Disponible sur https://www.iso.org
[ISO27001]	Norme internationale ISO/IEC 27001 : Techniques de sécurité – Systèmes de gestion de la sécurité de l'information – Exigences, version en vigueur. Disponible sur https://www.iso.org
[ISO27002]	Norme internationale ISO/IEC 27002 : Techniques de sécurité – Code de bonne pratique pour la gestion de la sécurité de l'information, version en vigueur. Disponible sur https://www.iso.org
[ISO27005]	Norme internationale ISO/IEC 27005 : Technologies de l'information – Techniques de sécurité – Gestion des risques liés à la sécurité de l'information, version en vigueur. Disponible sur https://www.iso.org
[ISO27031]	Norme internationale ISO/IEC 27031 : Techniques de sécurité — Lignes directrices pour la préparation des technologies de la communication et de l'information pour la continuité d'activité, version en vigueur. Disponible sur https://www.iso.org
[PASSI]	Référentiel d'exigences applicables à un prestataire d'audit de la sécurité des systèmes d'information, ANSSI, version en vigueur. Disponible sur https://www.cyber.gouv.fr
[PDIS]	Référentiel d'exigences applicables à un prestataire de détection des incidents de sécurité, ANSSI, version en vigueur. Disponible sur https://www.cyber.gouv.fr
[PRIS]	Référentiel d'exigences applicables à un prestataire de réponse aux incidents de sécurité, ANSSI, version en vigueur. Disponible sur https://www.cyber.gouv.fr
[PSSIE]	Politique de sécurité des systèmes d'information de l'État, version en vigueur. Disponible sur https://www.cyber.gouv.fr
[RGS]	Référentiel général de sécurité, ANSSI et SGMAP, version en vigueur. Disponible sur https://www.cyber.gouv.fr
[SECNUMCLOUD]	Référentiel d'exigences applicables à un prestataire de services d'informatique en nuage (SecNumCloud), ANSSI, version en vigueur. Disponible sur https://www.cyber.gouv.fr

III. Autres références documentaires

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

Annexe 2 Missions et compétences attendues des consultants et des responsables de prestation

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

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

Les consultants et responsables de prestation intervenant dans le cadre d'une prestation d'accompagnement et de conseil en sécurité des systèmes d'information doivent connaître 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 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] ;
- [LOI_LPM] ;
- [NIS] ;
- [EIDAS] ;
- [PSSIE] ;
- [RGS] et notamment ses annexes A, B et C ;
- [RGPD] ;
- [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.2. Connaissances transverses en sécurité des systèmes d'information

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 risques ;
- 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 de crise d'origine cyber ;
- gestion des incidents liés à la sécurité de l'information ;
- gestion du plan de continuité de l'activité ;
- sécurité physique ;
- protection des données.

En particulier, le socle commun est composé de la connaissance des documents suivants :
- [G_HYGIENE] ;
- [ISO27001] ;
- [ISO27002].

I.3. Connaissances en méthode de gestion des risques et d'homologation

Le socle commun est composé de connaissances en méthode de gestion des risques, comprenant :
- la connaissance de :
  i. [G_HOMOLOGATION] ;
  ii. une ou plusieurs méthodologies d'analyse du risque numérique.
- la connaissance et la compréhension de :
  i. la définition du risque en général ;
  ii. la définition du risque numérique en particulier et de ses composantes ;
  iii. la terminologie de la méthode appliquée ;
  iv. 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.4. Connaissances en architecture sécurisée des systèmes d'information

Le socle commun est composé de connaissances des principaux éléments qui composent l'architecture d'un système d'information et de leurs rôles, ainsi que des 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, les 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, CaaS, PaaS, SaaS, privés et publics).

I.5. Connaissances en préparation à la gestion de crise d'origine cyber

Le socle commun est composé de connaissances en méthode de gestion de crise d'origine cyber, comprenant :

- la connaissance de :
  i. [G_GESTION_CRISE] ;
  ii. [G_EXERCICE_CRISE] ;
  iii. [G_COM_CRISE].
- la connaissance et la compréhension de :
  i. la définition de la gestion de crise ;
  ii. les spécificités associées aux crises d'origine cyber ;
  iii. la terminologie de la gestion de crise ;
  iv. la réglementation et les acteurs pertinents dans la gestion de crise d'origine cyber ;
  v. les notions de continuité et de reprise d'activité.

Il est notamment attendu de connaître les concepts suivants :

- identification des chaines de valeurs métiers et des besoins de sécurité associés ;
- identification des menaces d'origine cyber, leur évolution et de leurs principales conséquences ;
- fonctionnement de cellules de crise ;
- développement de politiques et de procédures de gestion de crise et de continuité d'activité ;
- organisation d'exercices de crise.

II. Responsable de prestation

II.1. Missions

Le responsable de prestation 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.) ;
- déterminer et contrôler le niveau d'habilitation requis ;
- 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 de prestation doit connaître l'ensemble des éléments transverses 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 de prestation 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

III.1. Missions

Les missions du consultant en gestion des risques de sécurité des systèmes d'information consistent à prendre en charge les activités telles qu'identifiées aux chapitres II.1 et II.2 du référentiel.

III.2. Compétences

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

Le consultant en gestion des risques de sécurité des systèmes d'information 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 de sécurité des systèmes d'information doit maîtriser les éléments relatifs aux connaissances en méthode de gestion des risques, identifiés au chapitre I.3 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 de sécurité des systèmes d'information 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 de sécurité des systèmes d'information 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 du référentiel.

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 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.cyber.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] ;
- [G_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] ;
- [G_SEC_WIND].

IV.2.2.3. Maîtrise des concepts d'administration sécurisée

Le consultant doit être en mesure de :

- définir les bonnes pratiques de cloisonnement entre le système d'information d'administration et les systèmes d'information administrés ;
- proposer des mesures de sécurisation d'un poste d'administration ;
- 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 bonnes pratiques d'architecture dans les environnements *DevOps* / *DevSecOps*, notamment la sécurisation des chaînes CI/CD ;
- 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'authentification multi-facteurs ;
- l'annuaire centralisé ;
- la cryptographie ;
- l'infrastructure de gestion de clés (IGC).

Le consultant doit maîtriser les principales technologies de stockage, les besoins et les 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_AUTH_MULTI_MDP] ;
- [G_CRYPTO_1] ;
- [G_CRYPTO_2].

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 zones 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 (*Traffic Access Point*), sonde de prévention d'intrusion, diode, serveur mandataire, SIEM (*Security Information and Event Management*), WAF (*Web Application Firewall*), concentrateur VPN (*Virtual Private Network*).

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.2.2.7. 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 :
  i. de prendre en compte toutes les dimensions du contexte du commanditaire impactant la sécurité des systèmes d'information (technique, organisationnelle, humaine, réglementaire, etc.) ;
  ii. de comprendre, interpréter et exploiter les résultats d'un audit.
- être en mesure de proposer un plan de traitement des risques de l'architecture pertinent et raisonnable vis-à-vis de l'état des lieux réalisé, et notamment :
  i. permettant de couvrir les principaux risques et justifiant chaque mesure en regard d'un scénario d'attaque à adresser ;
  ii. prenant en compte le maintien en condition de sécurité dans la cible proposée (corrections, migrations, obsolescences, etc.) ;
  iii. 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 :
  i. d'avoir la capacité à sensibiliser les décideurs sur les enjeux de sécurité selon leur domaine de compétence et de connaissance de la problématique ;
  ii. 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 du(des) 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.2.2.8. 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 et les référentiels liés à ces différents éléments, parmi lesquels de façon non exhaustive :

- [G_SEC_VIRTUAL] ;
- [G_TOIP] ;
- [G_CONTROLE_ACCES] ;
- [SECNUMCLOUD].

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.2.2.9. 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.

V. Consultant en préparation à la gestion de crises d'origine cyber

V.1. Missions

Les missions du consultant en préparation à la gestion de crise d'origine cyber consistent à prendre en charge les activités telles qu'identifiées au chapitre II.4 du référentiel.

V.2. Compétences

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

Le consultant en préparation à la gestion de crise d'origine cyber 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.

V.2.2. Connaissance en préparation à la gestion de crise d'origine cyber

Le consultant en préparation à la gestion de crise d'origine cyber doit maîtriser les éléments relatifs à la gestion de crise d'origine cyber, identifiés au chapitre I.5 de cette annexe, et complétés par les éléments associés ci-dessous. Il est entendu par « maîtriser » la connaissance des concepts, la compréhension des méthodologies associées, et la capacité à les décliner dans un contexte spécifique présenté.

Il doit également connaître la documentation pertinente présente sur le site Web de l'ANSSI (www.cyber.gouv.fr) vis-à-vis des missions décrites dans les parties suivantes.

V.2.2.1. Maîtrise des concepts de gouvernance de gestion de crise d'origine cyber

Le consultant en préparation à la gestion de crise d'origine cyber doit :

- savoir adapter une gouvernance de gestion de crise pour adresser le volet cyber en prenant en compte le contexte du commanditaire ;
- savoir identifier les forces et faiblesses d'une gouvernance de gestion de crise vis-à-vis du risque de crise d'origine cyber, en cohérence avec l'état de l'art ;
- savoir élaborer et documenter une gouvernance de gestion de crise d'origine cyber, en prenant en compte les aspects liés aux ressources humaines (astreintes, temps de repos, etc.) ;
- savoir établir des fiches réflexes et accélérateurs pour outiller la gouvernance de gestion de crise d'origine cyber ;
- savoir identifier les collaborateurs pertinents pour armer le dispositif de crise en fonction de leurs compétences ;
- savoir identifier, mettre en place (ou conduire la mise en place de) l'outillage de gestion de crise d'origine cyber (main courante, outil de point de situation, outil de visualisation, etc.) ;
- savoir former les collaborateurs de l'organisation commanditaire vis-à-vis à la gestion de crise d'origine cyber, en prenant en compte la gouvernance cible de gestion de crise d'origine cyber et les facteurs humains.

Il doit connaître les recommandations liées à ces différents éléments, notamment [G_GESTION_CRISE] et [ISO22361].

V.2.2.2. Maîtrise des concepts de continuité d'activité et de reprise d'activité

Le consultant en préparation à la gestion de crise d'origine cyber doit :

- savoir identifier les chaines de valeurs d'une organisation ;
- savoir identifier les biens supports des chaines de valeur, en utilisant la méthodologie de [EBIOS_RM] ;
- savoir identifier les principaux risques sur les biens supports des chaines de valeur et réaliser un bilan d'impact sur l'activité ;

- savoir déterminer des mesures de sécurité pour réduire les risques et atteindre les objectifs de continuité de l'organisation.

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

- [EBIOS_RM] ;
- [ISO22301]
- [ISO22313] ;
- [ISO22317] ;
- [ISO27031].

V.2.2.3. Maitrise de l'anticipation durant les crises

Le consultant en préparation à la gestion de crise d'origine cyber doit :

- savoir formaliser une méthodologie d'anticipation de crise compatible avec les spécificités de l'organisation commanditaire ;
- savoir formaliser des documents / modèles permettant d'accélérer l'anticipation pendant la crise d'origine cyber (liste de questions pour la compréhension de la situation, scénarios d'évolution standards, modèle de restitution, etc.) ;
- savoir conduire des ateliers avec l'organisation commanditaire pour aider à l'appropriation à la méthodologie et aux outils d'anticipation de crise d'origine cyber.

V.2.2.4. Maitrise de l'entrainement à la gestion de crise

Le consultant en préparation à la gestion de crise d'origine cyber doit :

- savoir formaliser un plan d'entrainement pour une organisation selon les besoins de formation des collaborateurs et du niveau de maturité de l'organisation ;
- savoir identifier les objectifs et hypothèses à tester d'un exercice et les mécanismes adéquats pour atteindre ces objectifs et tester ces hypothèses ;
- savoir organiser ou coordonner des exercices de gestion de crise de différents formats (exercice basé sur la discussion, simulation, exercice majeur[7]) et pour tout type de population, en prenant en compte le niveau de maturité de l'organisation commanditaire ;
- savoir impliquer les équipes pertinentes en préparation et durant l'exécution d'un exercice ;
- savoir mettre en place ou coordonner la mise en place d'outils de simulation de crise (outil de simulation de pression médiatique ; outil de *cyberrange* ou outil de *Capture the Flag*) et des outils de modélisation et d'automatisation de l'animation de l'exercice ;
- savoir maitriser l'observation d'exercice ;
- savoir formaliser le rapport de RETEX après la conduite d'un exercice, pour identifier les forces et faiblesses d'un dispositif et établir un plan d'action en conséquence.

7 L'exercice basé sur la discussion consiste en la conduite d'une discussion sur la base d'un scénario déroulé pendant une réunion ou un atelier. La simulation consiste en une stimulation fortement contextualisée (généralement à travers des outils de simulation d'environnement) afin de tester des capacités ou des procédures contre un scénario établi. L'exercice majeur est un exercice nécessitant une coopération forte entre de multiples niveaux (parmi les niveaux stratégique, opérationnel et tactique) et/ou avec un large périmètre organisationnel (intra-organisation ou inter-organisation), avec un fort niveau de complexité et de durée de préparation.

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

- [G_EXERCICE_CRISE] ;
- [ISO22398].

V.2.2.5. Maitrise de la communication de crise

Le consultant en préparation à la gestion de crise d'origine cyber doit :

- savoir initier un dialogue entre les équipes cyber et les équipes communication hors période de crise, dans l'objectif de préparer la stratégie de communication de crise cyber ;
- savoir anticiper les scénarios de crise les plus pertinents pour l'organisation commanditaire ;
- savoir concevoir une stratégie de communication de crise en réponse à la crise d'origine cyber ;
- savoir intégrer la fonction communication dans l'organisation d'une gestion de crise d'origine cyber ;
- savoir organiser la communication de crise ;
- savoir formaliser une boite à outils de communication de crise d'origine cyber, comprenant les outils de pilotage de la communication (un fichier presse, les codes de connexion aux comptes réseaux sociaux, applications mobiles, site web et Intranet, l'annuaire des acteurs de la gestion de crise) et des éléments de langage sur des sujets sensibles ou de crise ;
- savoir former les équipes aux bonnes pratiques de communication de crise.

Il doit connaître et appliquer les recommandations du guide [G_COM_CRISE].

V.2.2.6. Maitrise des aspects juridiques dans des crises cyber

Le consultant en préparation à la gestion de crise d'origine cyber doit :

- savoir aider à l'identification des obligations législatives et réglementaires auxquelles l'organisation commanditaire est soumise ainsi que les actions associées à ces obligations et à mettre en œuvre dans le cadre d'une gestion de crise ;
- savoir appuyer la mise en place de procédures juridiques applicables durant la crise ;
- connaître les principales mesures juridiques à prendre dans le cas de crises d'origine cyber, notamment vis-à-vis de la judiciarisation et conseiller le commanditaire pour respecter les textes applicables.

Il doit connaître les guides de recommandations liés à ces différents éléments, notamment [G_GESTION_CRISE].

V.2.2.7. Maitrise des composantes techniques

Le consultant doit comprendre les concepts et principes techniques suivants, sans nécessairement avoir les compétences pour les mettre en œuvre :

- les menaces cyber, l'analyse de la menace (CTI) et leurs matérialisations en termes de tactiques, techniques & procédures (TTP) ;
- la segmentation du réseau et l'interconnexion entre systèmes d'information ;
- la gestion des utilisateurs et des droits ;
- la gestion des vulnérabilités et des mises à jour ;
- la journalisation et la supervision ;

- les sauvegardes et la restauration de données ou de systèmes ;
- la réponse à incident, la remédiation et la reconstruction.

Dans le cadre de la prestation, le consultant en préparation à la gestion de crise d'origine cyber n'effectuera pas d'actions sur les systèmes liés aux éléments mentionnés ci-dessous.

Il doit connaître les guides de recommandations liés à ces différents éléments, parmi lesquels de façon non exhaustive :
- [G_HYGIENE] ;
- [G_RANCONGICIEL].

V.2.3. Aptitudes interpersonnelles

Le consultant en préparation à la gestion de crise d'origine cyber doit présenter les aptitudes suivantes :
- savoir analyser, synthétiser et restituer l'information utile pour le personnel opérationnel et le personnel stratégique (notamment les équipes dirigeantes) ;
- 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 mener une réunion ;
- savoir conduire des formations, des sensibilisations, des ateliers de travails ou des exercices d'entrainement ;
- savoir impliquer et responsabiliser les parties prenantes ;
- savoir préparer et obtenir des arbitrages et validations ;
- savoir assurer les aspects logistiques et informatiques dans le cadre d'exercice de gestion de crise.

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. Il est également nécessaire d'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 [G_ACHAT] qui a 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 d'un service [P_QUALIF_SERVICE] déposer auprès de l'ANSSI une réclamation contre un prestataire qualifié lorsqu'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 [IGI_1300] et par conséquent ne se substitue pas à une habilitation de sécurité.

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) [II_910].

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.).

b) Il est recommandé que le commanditaire désigne en son sein un correspondant de la prestation 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) 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 correspondant de la prestation chez le commanditaire 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 qu'il utilise cependant à des fins professionnelles en l'absence du titulaire du matériel ou sans son accord explicite.

c) Il est recommandé que, tout au long de la prestation, le commanditaire informe 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.

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.

Annexe 4 Prérequis à fournir par les commanditaires

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

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 pour 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 :
   - réglementations ou textes de référence encadrant l'homologation (cadre réglementaire, PSSI, etc.) ;
   - les spécifications fonctionnelles ;
   - les spécifications techniques ;
   - le cas échéant, le dossier d'architecture du système d'information cible, incluant un schéma d'architecture à jour, clair et exhaustif, les vues des applications, les vues des infrastructures logiques et les flux de données associés.

   Certains documents attendus pourront ne pas encore être disponibles dans le cas d'une prestation menée en phase de conception du système d'information cible.

b) Au lancement de 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 projet de la prestation ;
   - un responsable du projet l'homologation ;
   - un propriétaire du système d'information objet de la prestation ;
   - un responsable de la sécurité du système d'information objet de la prestation ;
   - un représentant métier du système d'information objet de la prestation ;
   - un représentant informatique du système d'information objet de la prestation ;
   - un architecte fonctionnel ou technique ayant une compréhension du système d'information objet de la prestation ;
   - un acteur en charge du maintien en condition opérationnelle du système d'information objet de la prestation ;
   - un acteur en charge du maintien en condition de sécurité du système d'information objet de la prestation.

   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 pour 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 des applications, les vues des infrastructures et les flux de données associés.

Certains documents attendus pourront ne pas encore être disponibles dans le cas d'une prestation menée en phase de conception du système d'information cible.

b) Au lancement de 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 projet de la prestation ;
   - un propriétaire du système d'information objet de la prestation ;
   - un responsable de la sécurité du système d'information objet de la prestation ;
   - un représentant métier du système d'information objet de la prestation ;
   - un représentant informatique du système d'information objet de la prestation ;
   - un architecte fonctionnel ou technique ayant une compréhension du système d'information objet de la prestation ;
   - un acteur en charge du maintien en condition opérationnelle du système d'information objet de la prestation ;
   - un acteur en charge du maintien en condition de sécurité du système d'information objet de la prestation.

   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 pour 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 des applications, les vues des infrastructures logiques et les flux de données associés ;
   - la liste existante de mesures applicables au système d'information cible (l'un des documents suivants : PSSI, rapports des précédentes analyses de risques, tests, audits et plans d'actions associés, dossier d'homologation).

     Certains documents attendus pourront ne pas encore être disponibles dans le cas d'une prestation menée en phase de conception du système d'information cible.

b) Au lancement de 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 de la prestation ;
   - un propriétaire du système d'information objet de la prestation ;
   - un responsable de la sécurité du système d'information objet de la prestation ;
   - un représentant métier du système d'information objet de la prestation ;
   - un représentant informatique du système d'information objet de la prestation ;

- un architecte fonctionnel ou technique ayant une compréhension du système d'information objet de la prestation ;
- un acteur en charge du maintien en condition opérationnelle du système d'information objet de la prestation ;
- un acteur en charge du maintien en condition de sécurité du système d'information objet de la prestation.

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

VI. Prérequis à fournir pour les activités de conseil en préparation à la gestion de crises d'origine cyber

a) Les documents suivants constituent les éléments de base à la réalisation des activités de conseil en préparation à la gestion de crises d'origine cyber et sont attendus du commanditaire par le prestataire au début de la prestation :
   - les statuts, la nationalité et qualification juridique de l'organisation du commanditaire ;
   - un descriptif de l'organisation fonctionnelle, son périmètre géographique et métier, son organigramme ;
   - une liste des tiers pertinents à intégrer à la démarche ;
   - un descriptif des activités métiers et informatiques de l'organisation commanditaire ;
   - le référentiel des exigences métiers applicables (cadre réglementaire, besoins opérationnels, analyses de risques, etc.) ;
   - le corpus sur le dispositif de gestion de crise global et d'origine cyber s'il existe ;
   - le corpus sur la continuité d'activité s'il existe (PCA, PRA, cartographie des applications et infrastructures, schéma d'architecture du SI)
   - une liste des équipes et collaborateurs intervenant dans le cadre du dispositif de gestion de crise d'origine cyber ;
   - le dernier RETEX issue d'un exercice de crise d'origine cyber ou d'une crise (s'il existe et selon le consentement du commanditaire au regards de la sensibilité de certaines informations).

   Certains documents attendus pourront ne pas encore être disponibles dans le cas d'une prestation menée en phase de conception d'un dispositif de gestion de crise d'origine cyber.

b) Au lancement de 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 projet de la prestation ;
   - un responsable du dispositif de gestion de crise et/ou de la continuité d'activité ;
   - un propriétaire du système d'information objet de la prestation ;
   - un responsable de la sécurité du système d'information objet de la prestation ;
   - un représentant métier du système d'information objet de la prestation ;
   - un représentant informatique du système d'information objet de la prestation ;
   - un architecte fonctionnel ou technique ayant une compréhension du système d'information objet de la prestation ;
   - un acteur en charge du maintien en condition opérationnelle du système d'information objet de la prestation ;

- un acteur en charge du maintien en condition de sécurité du système d'information objet de la prestation.
- un représentant des équipes communication ;
- un représentant des équipes juridiques.

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