

TLP:CLEAR



**PREMIER
MINISTRE**

*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**

Référentiel d'exigences

Version 2.0 du 14 février 2026

SOMMAIRE

I.	Introduction	6
I.1.	Présentation générale	6
I.2.	Identification du document	7
I.3.	Acronymes et définitions	8
II.	Activités couvertes par le référentiel.....	11
II.1.	Conseil en homologation de sécurité des systèmes d’information	11
II.2.	Conseil en gestion des risques de sécurité des systèmes d’information	11
II.3.	Conseil en sécurité des architectures des systèmes d’information	11
II.4.	Conseil en préparation à la gestion de crise d’origine cyber.....	12
III.	Qualification des prestataires d'accompagnement et de conseil en sécurité des systèmes d’information	13
III.1.	Modalités de la qualification	13
III.2.	Niveaux de qualification	13
III.3.	Portée de la qualification	14
III.4.	Qualification pour les besoins de la sécurité nationale	14
IV.	Exigences applicables au prestataire	15
IV.1.	Exigences générales.....	15
IV.2.	Gestion des personnels	15
IV.3.	Protection de l’information.....	16
V.	Exigences applicables aux personnels du prestataire.....	18
V.1.	Connaissances et compétences générales.....	18
V.2.	Connaissances et compétences spécifiques.....	18
V.3.	Expérience.....	18
V.4.	Engagement	19
VI.	Exigences applicables à la prestation	20
VI.1.	Étape 1 - Qualification préalable d’aptitude à la réalisation de la prestation	20
VI.2.	Étape 2 - Élaboration de la convention de service.....	20
VI.3.	Étape 3 - Préparation de la prestation.....	23
VI.4.	Étape 4 - Exécution de la prestation	25

Prestataires d’accompagnement et de conseil en sécurité des systèmes d’information – Référentiel d’exigences			
Version	Date	Critère de diffusion	Page
2.0	14/02/2026	PUBLIC	2/62

VI.5. Étape 5 - Suivi régulier de la prestation.....	27
VI.6. Étape 6 - Élaboration du rapport.....	28
VI.7. Étape 7 - Clôture de la prestation	34
Annexe 1 Bibliographie	36
Annexe 2 Missions et compétences attendues des consultants et des responsables de prestation.....	40
I. Socle commun de connaissances en sécurité des systèmes d’information	40
I.1. Connaissances transverses de la réglementation	40
I.2. Connaissances transverses en sécurité des systèmes d’information	41
I.3. Connaissances en méthode de gestion des risques et d’homologation	41
I.4. Connaissances en architecture sécurisée des systèmes d’information	42
I.5. Connaissances en préparation à la gestion de crise d’origine cyber	42
II. Responsable de prestation	43
II.1. Missions.....	43
II.2. Compétences	43
II.2.1. Socle commun de connaissances en sécurité des systèmes d’information	43
II.2.2. Aptitudes interpersonnelles.....	44
III. Consultant en gestion des risques.....	44
III.1. Missions.....	44
III.2. Compétences	44
III.2.1. Socle commun de connaissances en sécurité des systèmes d’information	44
III.2.2. Connaissances en méthode de gestion des risques.....	44
III.2.3. Pratique d’une méthode de gestion des risques de sécurité des systèmes d’information	44
III.2.4. Aptitudes interpersonnelles	45
IV. Consultant en sécurité des architectures des systèmes d’information	45
IV.1. Missions.....	45
IV.2. Compétences	45
IV.2.1. Socle commun de connaissances en sécurité des systèmes d’information	45
IV.2.2. Connaissance en architecture sécurisée des systèmes d’information	46
IV.2.3. Maîtrise des concepts et protocoles réseaux	46
IV.2.3.1. Maîtrise des concepts système et des principaux systèmes d’exploitation.....	46
IV.2.3.2. Maîtrise des concepts d’administration sécurisée.....	47

Prestataires d’accompagnement et de conseil en sécurité des systèmes d’information – Référentiel d’exigences			
Version	Date	Critère de diffusion	Page
2.0	14/02/2026	PUBLIC	3/62

IV.2.3.3.	Maîtrise des concepts d’architectures applicatives	47
IV.2.3.4.	Maîtrise des concepts de gestion des accès et de la protection des données....	47
IV.2.3.5.	Maîtrise des principaux modèles de sécurité et des principes de défense en profondeur	48
IV.2.3.6.	Pratique de la conception d’une architecture sécurisée de systèmes d’information	49
IV.2.3.7.	Connaissances spécifiques des systèmes d’information selon leur nature	50
IV.2.3.8.	Aptitudes interpersonnelles.....	50
V.	Consultant en préparation à la gestion de crises d’origine cyber	51
V.1.	Missions.....	51
V.2.	Compétences	51
V.2.1.	Socle commun de connaissances en sécurité des systèmes d’information.....	51
V.2.2.	Connaissance en préparation à la gestion de crise d’origine cyber	51
V.2.2.1.	Maîtrise des concepts de gouvernance de gestion de crise d’origine cyber	51
V.2.2.2.	Maîtrise des concepts de continuité d’activité et de reprise d’activité.....	52
V.2.2.3.	Maitrise de l’anticipation durant les crises.....	52
V.2.2.4.	Maitrise de l’entraînement à la gestion de crise	53
V.2.2.5.	Maitrise de la communication de crise	53
V.2.2.6.	Maitrise des aspects juridiques dans des crises cyber	54
V.2.2.7.	Maitrise des composantes techniques.....	54
V.2.3.	Aptitudes interpersonnelles	55
Annexe 3	Recommandations à l’attention des commanditaires	56
I.	Avant la prestation	56
II.	Pendant la prestation.....	58
III.	Après la prestation	58
Annexe 4	Prérequis à fournir par les commanditaires.....	59
I.	Prérequis à fournir pour les activités de conseil en homologation de sécurité des systèmes d’information	59
II.	Prérequis à fournir pour les activités de conseil en gestion des risques de sécurité des systèmes d’information	60
III.	Prérequis à fournir pour les activités de conseil en sécurité des architectures des systèmes d’information	60
IV.	Prérequis à fournir pour les activités de conseil en préparation à la gestion de crises d’origine cyber	61

Prestataires d’accompagnement et de conseil en sécurité des systèmes d’information – Référentiel d’exigences			
Version	Date	Critère de diffusion	Page
2.0	14/02/2026	PUBLIC	4/62

Prestataires d'accompagnement et de conseil en sécurité des systèmes d'information – Référentiel d'exigences			
Version	Date	Critère de diffusion	Page
2.0	14/02/2026	PUBLIC	5/62

I. Introduction

I.1. Présentation générale

I.1.1. Contexte

Les systèmes d'information des entreprises et organisations se transforment en profondeur, s'ouvrent vers l'extérieur et accueillent en continu des services innovants. Les entreprises et organisations doivent intégrer des technologies de plus en plus nombreuses (« Big Data », « Internet des Objets », « Intelligence Artificielle », « Industrie 4.0 », 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 (la loi de programmation militaire et particulièrement les dispositions applicables aux systèmes d'information d'importance vitale (SIIV) des opérateurs d'importance vitale (OIV) (1) , les directives européennes relatives à la sécurité des réseaux et de l'information (2) (3), le référentiel général de sécurité (4), le règlement (UE) n° 910/2014 (5), la politique de sécurité des systèmes d'information de l'Etat (6) , etc.) qui obligent les entreprises et organisations à mieux maîtriser 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 d'information, la détection et la réponse aux incidents de sécurité des systèmes d'information, respectivement objet des référentiels PASSI (7), PDIS (8) et PRIS (9) également proposés par l'ANSSI.

Prestataires d'accompagnement et de conseil en sécurité des systèmes d'information – Référentiel d'exigences			
Version	Date	Critère de diffusion	Page
2.0	14/02/2026	PUBLIC	6/62

I.1.2. Objet du document

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

Il a vocation à permettre la qualification d'un prestataire conformément aux modalités décrites au chapitre III.

Il permet au commanditaire d'une prestation d'accompagnement et de conseil en sécurité des systèmes d'information de disposer de garanties sur les compétences du prestataire et de ses personnels, sur la capacité du prestataire à réaliser une prestation conforme aux exigences du présent référentiel et à protéger les informations et supports sensibles auxquels il a accès au cours de la prestation.

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 (10) et classifiées (11) ni aux obligations des prestataires en leur qualité de professionnels, notamment leur devoir de conseil vis-à-vis de leurs commanditaires.

I.1.3. Structure du document

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

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

Le chapitre III décrit les modalités de la qualification d'un prestataire.

Le chapitre IV décrit les exigences applicables aux prestataires.

Le chapitre V décrit les exigences applicables aux personnels du prestataire.

Le chapitre VI décrit les exigences applicables à la prestation.

L'Annexe 1 présente la bibliographie.

L'Annexe 2 décrit les connaissances, compétences et missions des personnels du prestataire.

L'Annexe 3 fournit des recommandations à l'attention des commanditaires avant, pendant et après la prestation.

L'Annexe 4 décrit les prérequis recommandés à fournir par les commanditaires.

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.

Prestataires d'accompagnement et de conseil en sécurité des systèmes d'information – Référentiel d'exigences			
Version	Date	Critère de diffusion	Page
2.0	14/02/2026	PUBLIC	7/62

I.3. Acronymes et définitions

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	<i>Containers as a service</i>
GDC	Gestion de crise
IaaS	<i>Infrastructure as a service</i>
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	<i>Platform as a service</i>
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	<i>Software as a service</i>

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.

Prestataires d'accompagnement et de conseil en sécurité des systèmes d'information – Référentiel d'exigences			
Version	Date	Critère de diffusion	Page
2.0	14/02/2026	PUBLIC	8/62

Bénéficiaire - personne morale dont le système d'information est l'objet de la prestation. Le bénéficiaire peut être ou non le commanditaire de la prestation.

Commanditaire - personne morale faisant appel à un prestataire pour la réalisation d'une prestation qualifiée. Le commanditaire peut être ou non le bénéficiaire de la prestation.

Consultant - personne physique réalisant une activité d'accompagnement et de conseil.

Convention de service - accord écrit entre le commanditaire et le prestataire pour la réalisation de la prestation.

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 d'origine cyber, 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 pour réaliser une partie de la prestation lorsque des connaissances et compétences spécifiques, hors du périmètre des activités du référentiel et non détenues par les consultants, sont nécessaires pour la bonne exécution de la prestation. L'expert peut être un personnel interne ou externe au prestataire.

Gestion de crise (d'origine cyber) – processus d'actions visant à limiter les impacts d'une crise en apportant une capacité de réponse efficace et de soutien adéquate afin de préserver les intérêts principaux du bénéficiaire ou du commanditaire (réputation, continuité des activités, rétablissement des capacités opérationnelles, etc.).

Menace hacktiviste ou isolée – cette menace s'illustre par la conduite d'attaques informatiques menées par un individu isolé ou un groupe hacktiviste. Les moyens mis en œuvre incluent notamment des attaques par déni de service ou des fuites de données. La menace isolée comprend également des individus utilisant des outils peu sophistiqués ou bénéficiant d'accès privilégiés au sein d'une entité, mais disposant de peu de moyens.

Menace stratégique – cette menace s'illustre par la conduite d'attaques informatiques persistantes et ciblées, menées ou financées par un État. Elle est caractérisée par des moyens techniques et organisationnels importants, ainsi qu'un effort de discrétion. Ces attaques peuvent être conduites notamment à des fins d'espionnage, de pré-positionnement ou de déstabilisation.

Menace systémique – cette menace s'illustre par sa capacité à affecter une large proportion d'entités. Elle inclut la menace cybercriminelle, caractérisée par la conduite d'attaques informatiques majoritairement opportunistes. Ces attaques sont généralement conduites à des fins lucratives et peuvent se matérialiser par des rançongiciels ou des fraudes. Ces menaces sont également représentées par la prolifération d'outils et de services offensifs disponibles sur étagère ou commercialisés par des entreprises privées. Ces services peuvent être utilisés

Prestataires d'accompagnement et de conseil en sécurité des systèmes d'information – Référentiel d'exigences			
Version	Date	Critère de diffusion	Page
2.0	14/02/2026	PUBLIC	9/62

dans des actions d'intelligence économique ou d'espionnage industriel ou permettre à certains États aux ressources limitées d'accéder à des capacités offensives.

Mesure de sécurité – mesure permettant de satisfaire une exigence de sécurité, d'empêcher ou réduire la survenance d'un risque d'atteinte à la sécurité de l'information ou d'en diminuer la gravité.

Niveau de qualification élevé – niveau de qualification permettant d'avoir, par rapport au niveau de qualification substantiel, une garantie renforcée notamment sur la compétence du prestataire, la confiance que l'on peut lui accorder et sa capacité à protéger les informations et supports relatifs à la prestation. Une prestation de niveau élevé est recommandée lorsque les risques qui pèsent sur le système d'information objet de la prestation sont élevés et/ou lorsque les scénarios de risque de nature intentionnelle impliquent une menace stratégique.

Niveau de qualification substantiel – niveau de qualification permettant d'avoir un premier niveau de garantie notamment sur la compétence du prestataire, la confiance que l'on peut lui accorder et sa capacité à protéger les informations et supports relatifs à la prestation. Une prestation de niveau substantiel est recommandée lorsque les scénarios de risque de nature intentionnelle qui pèsent sur le système d'information objet de la prestation impliquent une menace systémique, hacktiviste ou isolée.

Périmètre de la prestation – environnement physique, logique et organisationnel du système d'information objet de la prestation.

Prestataire - personne morale réalisant une prestation qualifiée c'est-à-dire conforme aux exigences du présent référentiel.

Référentiel - le présent document.

Responsable de prestation - personne physique au sein du prestataire responsable de la prestation d'accompagnement et de conseil en sécurité des systèmes d'information. Le responsable de prestation est notamment en charge de constituer l'équipe d'accompagnement et de conseil en veillant à l'adéquation des compétences des consultants, le cas échéant des experts, avec les objectifs, critères périmètre et activités de la prestation.

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

Sécurité d'un système d'information - préservation des besoins de sécurité, notamment la confidentialité, l'intégrité et la disponibilité, des informations collectées, stockées, traitées et distribuées au sein d'un système d'information.

Sous-traitance - opération par laquelle le prestataire confie, sous sa responsabilité, à une personne morale (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 collecter, stocker, traiter et distribuer l'information.

Système d'information cible - système d'information objet de la prestation.

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

Prestataires d'accompagnement et de conseil en sécurité des systèmes d'information – Référentiel d'exigences			
Version	Date	Critère de diffusion	Page
2.0	14/02/2026	PUBLIC	10/62

II. Activités couvertes par 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

Le 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.

Cette activité 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.

Cette activité 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.

Prestataires d'accompagnement et de conseil en sécurité des systèmes d'information – Référentiel d'exigences			
Version	Date	Critère de diffusion	Page
2.0	14/02/2026	PUBLIC	11/62

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.).

Cette activité 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'entraînement et la formation des équipes mobilisées lors des crises.

Cette activité 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.

Prestataires d'accompagnement et de conseil en sécurité des systèmes d'information – Référentiel d'exigences			
Version	Date	Critère de diffusion	Page
2.0	14/02/2026	PUBLIC	12/62

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 (12) et permet d'attester de la conformité du prestataire aux exigences du présent référentiel.

Le référentiel contient des exigences et des recommandations applicables aux prestataires, à leurs personnels et à la prestation.

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

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

Est considérée comme une prestation qualifiée, une prestation respectant la démarche décrite au chapitre VI dont les activités décrites au chapitre II sont réalisées par le personnel respectant les exigences du chapitre V et travaillant pour un prestataire qualifié respectant les exigences du chapitre IV. Pour chaque type de prestation, le personnel doit respecter les profils de compétences attendus, conformément à Annexe 2.

III.2. Niveaux de qualification

Les prestataires peuvent se faire qualifier selon deux niveaux de qualification : substantiel ou élevé.

Lorsqu'une exigence n'est applicable qu'à un seul et unique niveau de qualification, alors elle est précédée d'une mention entre crochets identifiant ledit niveau. Ainsi, une exigence précédée de la mention « [SUBSTANTIEL] » est applicable exclusivement au niveau de qualification substantiel et une exigence précédée de la mention « [ELEVÉ] » est applicable exclusivement au niveau de qualification élevé.

Lorsqu'une exigence n'est précédée d'aucune mention entre crochets identifiant un niveau de qualification, alors elle est applicable à l'ensemble des niveaux de qualification.

Les exigences applicables au niveau de qualification élevé sont par défaut des recommandations pour le niveau de qualification substantiel.

Un prestataire ne peut pas obtenir la qualification pour plusieurs activités à des niveaux de qualification différents.

Prestataires d'accompagnement et de conseil en sécurité des systèmes d'information – Référentiel d'exigences			
Version	Date	Critère de diffusion	Page
2.0	14/02/2026	PUBLIC	13/62

La qualification d'un prestataire au niveau élevé atteste de son aptitude à réaliser l'ensemble des activités qui constituent sa portée de qualification au niveau substantiel et élevé.

La qualification d'un prestataire au niveau substantiel atteste de son aptitude à réaliser l'ensemble des activités qui constituent sa portée de qualification au niveau substantiel uniquement.

L'Annexe 3 fournit des recommandations aux commanditaires quant au choix du niveau de qualification de la prestation.

III.3. Portée de la qualification

La portée de qualification est constituée d'une ou plusieurs activités décrites au chapitre II et d'un niveau de qualification décrit au chapitre III.2.

Le prestataire peut demander la qualification pour une ou plusieurs activités et pour un niveau de qualification.

Pour être qualifié selon une portée de qualification, le prestataire doit satisfaire l'ensemble des exigences du référentiel applicables aux activités et au niveau de qualification qui constituent la portée de qualification.

Le prestataire peut demander la qualification pour un niveau de qualification et pour une ou plusieurs activités de conseils décrites au chapitre II. 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.

III.4. Qualification pour les besoins de la sécurité nationale

Les prestataires réalisant des prestations d'accompagnement et de conseil en sécurité des systèmes d'information pour les besoins de la sécurité nationale doivent satisfaire, en sus des exigences du présent référentiel pour le niveau élevé, les exigences du référentiel (13).

L'accompagnement et le conseil pour les besoins de la sécurité nationale comprend notamment l'accompagnement et le conseil affectant les systèmes d'information d'importance vitale (SIIV) des opérateurs d'importance vitale (OIV) et les systèmes d'information traitant des informations et supports classifiés FR (11) UE (14) et OTAN (15).

Prestataires d'accompagnement et de conseil en sécurité des systèmes d'information – Référentiel d'exigences			
Version	Date	Critère de diffusion	Page
2.0	14/02/2026	PUBLIC	14/62

IV. Exigences applicables au prestataire

IV.1. Exigences générales

- a) Le prestataire doit être une personne morale.
- b) Le prestataire doit être soumis au droit d'un État membre de l'Union Européenne.
- 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 à des tiers d'informations et supports relatifs à la prestation.
- e) Le prestataire doit apporter la preuve que son organisation, les moyens qu'il met en œuvre pour réaliser la prestation et les modalités de son fonctionnement, notamment financières, ne sont pas susceptibles de compromettre son impartialité à l'égard du commanditaire.
- f) Le prestataire doit réaliser la prestation de manière impartiale, en toute bonne foi et dans le respect du commanditaire, de ses personnels et de ses infrastructures.
- g) Le prestataire doit enregistrer et traiter les plaintes relatives aux prestations qualifiées déposées par les commanditaires, les bénéficiaires et, de manière générale, l'ensemble des tiers.
- h) Le prestataire doit informer sans délai l'ANSSI de tout dépôt d'une plainte relative à une prestation qualifiée et du traitement de celle-ci.

IV.2. Gestion des personnels

- a) Le prestataire doit, avant toute intégration d'un nouveau consultant ou d'un responsable de prestation dans ses équipes, procéder à la vérification des formations, connaissances, compétences et références professionnelles, et de la véracité de leur curriculum vitae.
- b) Le prestataire doit s'assurer, avant le début de chaque prestation, que les membres de l'équipe d'accompagnement et de conseil disposent des connaissances et compétences associées à leurs activités conformément à l'Annexe 2.
- c) [ELEVE] Le prestataire ne doit recourir qu'à des consultants et des responsables de prestation disposant d'une attestation individuelle de compétence pour réaliser la prestation.

Le prestataire peut, avec l'accord du commanditaire, incorporer dans l'équipe d'accompagnement et de conseil, des personnes ne disposant pas d'attestation individuelle de compétence au titre de leur formation ou de leur montée en compétence. Ces personnes sont présentes en tant qu'observateurs et ne participent pas à la réalisation de la prestation.

- d) Le prestataire doit assurer la formation continue des consultants et des responsables de prestation afin de maintenir à jour leurs connaissances et compétences en matière de sécurité des systèmes d'information, et en particulier celles requises pour la réalisation de leurs missions.

Prestataires d'accompagnement et de conseil en sécurité des systèmes d'information – Référentiel d'exigences			
Version	Date	Critère de diffusion	Page
2.0	14/02/2026	PUBLIC	15/62

- e) Le prestataire doit permettre aux consultants et responsables de prestation d’assurer une veille afin de maintenir à jour leurs connaissances et compétences en matière de sécurité des systèmes d’information, et en particulier celles requises pour la réalisation de leurs missions.
- f) Le prestataire est responsable des méthodes et outils utilisés par l’équipe d’accompagnement et de conseil ainsi que de leur bonne utilisation durant la prestation.
- g) Le prestataire doit sensibiliser les consultants et les responsables de prestation à la réglementation en vigueur au sein de l'Union Européenne en matière de sécurité des systèmes d’information, et en particulier celle applicable à leurs missions.
- h) [ELEVE] Le prestataire doit s’assurer qu’aucun membre de l’équipe d’accompagnement et de conseil ne fait l’objet d’une inscription au casier judiciaire incompatible avec l’exercice de ses fonctions.

IV.3. Protection de l’information

Le prestataire peut, selon la demande du commanditaire, traiter tout ou partie des informations et supports relatifs à la prestation sur son système d’information, celui du commanditaire ou du bénéficiaire.

Pour obtenir la qualification au niveau élevé, le prestataire doit, dans tous les cas, disposer d’un système d’information homologué pour la protection d’informations et supports portant la mention Diffusion Restreinte (10).

Dans le cadre de la réalisation d’une prestation qualifiée de niveau élevé, le prestataire doit utiliser son système d’information homologué Diffusion Restreinte et ce quel que soit le marquage des informations et supports relatifs à la prestation.

Dans le cadre de la réalisation d’une prestation qualifiée de niveau substantiel, le prestataire qualifié au niveau élevé peut choisir de disposer, en plus de son système d’information homologué Diffusion Restreinte, d’un second système d’information respectant les exigences du présent chapitre pour le niveau substantiel. Ainsi le prestataire qualifié au niveau élevé peut, dans le cadre de la réalisation d’une prestation qualifiée de niveau substantiel, selon la demande du commanditaire, traiter les informations et supports relatifs à la prestation ne portant pas la mention Diffusion Restreinte soit sur son système d’information homologué Diffusion Restreinte soit sur son second système d’information.

- a) Le prestataire doit élaborer et tenir à jour une appréciation des risques relatifs à son activité d’accompagnement et de conseil.
- b) Il est recommandé que le prestataire mette en œuvre la méthode (16) pour réaliser l’appréciation des risques relatifs à son activité d’accompagnement et de conseil.
- c) Le prestataire doit protéger en intégrité et en confidentialité les informations et supports relatifs à la prestation selon leur marquage et leur niveau de sensibilité.
- d) Le prestataire doit appliquer le principe du moindre privilège et limiter l’accès aux informations et supports relatifs à la prestation aux strictes personnes ayant le droit et le besoin d’en connaître.

Prestataires d’accompagnement et de conseil en sécurité des systèmes d’information – Référentiel d’exigences			
Version	Date	Critère de diffusion	Page
2.0	14/02/2026	PUBLIC	16/62

- e) Le prestataire peut être amené à connecter un même équipement (clé USB, ordinateur, etc.) à son système d'information homologué et au système d'information cible potentiellement compromis. Le prestataire doit mettre en œuvre des mesures de sécurité adaptées pour ces équipements afin de répondre aux besoins opérationnels de la prestation et aux besoins de sécurité de son système d'information homologué. [ELEVE] Il n'est pas exigé du prestataire qu'il homologue ces équipements Diffusion Restreinte si le système d'information cible n'est pas homologué Diffusion Restreinte.
- f) Le prestataire doit homologuer son système d'information.
- g) [ELEVE] Le prestataire doit homologuer son système d'information pour la protection d'informations et supports portant la mention Diffusion Restreinte.
- h) Il est recommandé que le prestataire mette œuvre la démarche décrite dans le guide (17) pour homologuer son système d'information.
- i) Le prestataire doit être capable d'utiliser son système d'information pour réaliser la totalité d'une prestation.
- j) [ELEVE] Le prestataire doit mettre en œuvre l'ensemble des règles du guide d'hygiène informatique (18) pour le niveau renforcé sur son système d'information homologué Diffusion Restreinte.
- k) [ELEVE] Le prestataire doit mettre en œuvre l'ensemble des règles relatives à la protection des systèmes d'information traitant des informations et supports portant la mention Diffusion Restreinte définies dans (10) sur son système d'information homologué Diffusion Restreinte.
- l) [ELEVE] Il est recommandé que le prestataire mette en œuvre les recommandations du guide (18) sur son système d'information homologué Diffusion Restreinte.
- m) [SUBSTANTIEL] Le prestataire doit mettre en œuvre l'ensemble des règles du guide d'hygiène informatique (18) pour le niveau standard sur son système d'information.
- n) Le prestataire doit réaliser une revue périodique des droits d'accès sur son système d'information.
- o) [ELEVE] Le prestataire doit réaliser une revue des droits d'accès sur son système d'information tous les six mois.
- p) Le prestataire doit disposer d'un système d'information hors-ligne afin de conserver l'ensemble des informations et supports relatifs à la prestation pour lesquels il a reçu une autorisation de conservation du commanditaire.

Prestataires d'accompagnement et de conseil en sécurité des systèmes d'information – Référentiel d'exigences			
Version	Date	Critère de diffusion	Page
2.0	14/02/2026	PUBLIC	17/62

V. Exigences applicables aux personnels du prestataire

V.1. Connaissances et compétences générales

- a) Les consultants doivent posséder les qualités personnelles identifiées au chapitre 7.2.2 de la norme (19).
- b) Les responsables de prestation doivent posséder les qualités personnelles identifiées au chapitre 7.2.3.4 de la norme (19).
- 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) Les responsables de prestation et les consultants doivent disposer de qualités rédactionnelles et de synthèse, et savoir restituer les informations pertinentes et adaptées aux profils de leurs interlocuteurs (direction, services techniques, responsables métier et sécurité, etc.).
- e) Les responsables de prestation et les consultants 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 événements professionnels de leurs domaines de compétence, à des travaux de recherche ou la publication d'articles.

V.2. Connaissances et compétences spécifiques

- a) Les responsables de prestation et les consultants doivent, selon leur rôle, réaliser la prestation conformément aux exigences du chapitre VI.
- b) Les responsables de prestation et les consultants doivent, selon leur rôle, assurer les missions décrites dans l'Annexe 2.
- c) Les responsables de prestation et les consultants doivent, selon leur rôle, disposer des compétences décrites dans l'Annexe 2.
- d) Les responsables de prestation et les consultants doivent, selon leur rôle, disposer des connaissances décrites dans l'Annexe 2.

V.3. Expérience

- a) Il est recommandé que les responsables de prestation justifient d'au moins trois années d'expérience dans le domaine de la sécurité des systèmes d'information.
- b) Il est recommandé que les consultants en gestion des risques de sécurité des systèmes d'information justifient 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 de risque.

Prestataires d'accompagnement et de conseil en sécurité des systèmes d'information – Référentiel d'exigences			
Version	Date	Critère de diffusion	Page
2.0	14/02/2026	PUBLIC	18/62

- c) Il est recommandé que les consultants en sécurité des architectures des systèmes d'information justifient 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 les consultants préparation à la gestion de crise d'origine cyber justifient 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 d'origine cyber ;
 - iii. une expérience dans la gestion de crise d'origine cyber.

V.4. Engagement

- a) Les consultants et le responsable de prestation doivent avoir un contrat de travail avec le prestataire.
- b) Le prestataire doit avoir un cadre contractuel avec les experts (Voir chapitre VI.2.5).

Prestataires d'accompagnement et de conseil en sécurité des systèmes d'information – Référentiel d'exigences			
Version	Date	Critère de diffusion	Page
2.0	14/02/2026	PUBLIC	19/62

VI. Exigences applicables à la prestation

VI.1. Étape 1 - Qualification préalable d'aptitude à la réalisation de la prestation

- a) 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 ce 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.
- b) Le prestataire doit informer le commanditaire des recommandations contenues dans l'Annexe 3.
- c) 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.
- d) Le prestataire doit, en se fondant sur les informations communiquées par le commanditaire et notamment les objectifs, les critères, le périmètre, les activités de conseil et d'accompagnement et les éventuelles modalités particulières de la prestation¹, réaliser une qualification préalable d'aptitude afin d'évaluer de manière impartiale s'il est en mesure de réaliser pleinement, partiellement ou non la prestation.
- e) Le prestataire doit informer le commanditaire des conclusions de la qualification préalable d'aptitude à la réalisation de la prestation et notamment s'il estime être en mesure de réaliser pleinement, partiellement ou non la prestation.
- f) Le prestataire ne doit accepter de réaliser la prestation que si les conclusions de la qualification préalable d'aptitude confirment qu'il est en mesure de réaliser pleinement la prestation.

VI.2. Étape 2 - Élaboration de la convention de service

- a) Le prestataire doit établir une convention de service avec le commanditaire.
- b) La convention de service doit être signée par un représentant légal du prestataire et un représentant légal du commanditaire, ou toute personne pouvant engager le prestataire et le commanditaire.

VI.2.1. Qualification

La convention de service doit :

¹ Le choix des objectifs, critères, périmètre, activités de conseil et d'accompagnement et éventuelles modalités particulières de la prestation revient in fine au commanditaire. Cependant le prestataire a, en sa qualité de professionnel en matière de sécurité des systèmes d'information, un devoir de conseil sur leur pertinence et leur cohérence.

Prestataires d'accompagnement et de conseil en sécurité des systèmes d'information – Référentiel d'exigences			
Version	Date	Critère de diffusion	Page
2.0	14/02/2026	PUBLIC	20/62

- a) préciser que la prestation est qualifiée ;
- b) identifier le niveau de la qualification de la prestation ;
- c) identifier les activités d’accompagnement et de conseil ;
- d) inclure l’attestation de qualification du prestataire ;
- e) [ELEVE] préciser que chaque consultant et responsable de prestation disposent d’une attestation individuelle de compétence ;
- f) [ELEVE] doit préciser que le commanditaire peut, conformément au processus de qualification d’un service (12), déposer auprès de l’ANSSI une réclamation lorsqu’il estime que le prestataire n’a pas respecté une ou plusieurs exigences du référentiel dans le cadre d’une prestation qualifiée, et rappeler qu’en cas de manquement du prestataire, la qualification du prestataire peut être retirée, la portée de qualification réduite, ou le niveau de recommandation du prestataire dégradé.

VI.2.2. Modalités de la prestation

La convention de service doit :

- a) décrire de manière générale la démarche, les objectifs, les critères, le périmètre et les activités d’accompagnement et de conseil, ainsi que les modalités de la prestation notamment les prérequis, les jalons, les livrables, les dates et lieux d’exécution de la prestation. Ces informations pourront être précisées et mises à jour si besoin dans la note de cadrage ;
- b) préciser que le droit applicable à la convention de service est celui d’un État membre de l’Union européenne et préciser lequel ;
- c) préciser 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 et les livrables de la prestation, en particulier le rapport de prestation ;
- d) préciser que toute modification de la convention de service doit être soumise à l’acceptation d’un représentant légal du prestataire et d’un représentant légal du commanditaire, ou toute personne pouvant engager le prestataire et le commanditaire.

VI.2.3. Responsabilités

La convention de service doit :

- a) préciser que le commanditaire dispose de l’ensemble des droits de propriété et d’accès sur le périmètre de la prestation ou qu’il a recueilli l’accord des éventuelles parties dont les systèmes d’information entrent dans le périmètre de la prestation ;
- b) préciser que le prestataire informe le commanditaire par écrit et sans délai en cas de manquement à la convention de service ;
- c) décrire les principaux risques relatifs à la prestation, en particulier ceux concernant les atteintes à la disponibilité du système d’information cible et à la confidentialité de ses données.

Prestataires d’accompagnement et de conseil en sécurité des systèmes d’information – Référentiel d’exigences			
Version	Date	Critère de diffusion	Page
2.0	14/02/2026	PUBLIC	21/62

VI.2.4. Confidentialité

La convention de service doit :

- a) préciser que le prestataire ne collecte et n'utilise que les informations et supports strictement nécessaires à la bonne exécution de la prestation en adéquation avec les objectifs, critères, périmètre et activités de la prestation ;
- b) préciser que le prestataire ne divulgue ou ne partage aucune information ou support relatif à la prestation à des tiers, sauf autorisation écrite du commanditaire ;
- c) préciser que le prestataire, à l'issue de la prestation, restitue, supprime ou détruit l'ensemble des informations et supports relatifs à la prestation à l'exception de ceux pour lesquels il a reçu une autorisation de conservation du commanditaire ;
- d) préciser que le prestataire, à l'issue de la prestation, conserve sur un système d'information hors-ligne l'ensemble des informations et supports relatifs à la prestation pour lesquels il a reçu une autorisation de conservation du commanditaire.

VI.2.5. Experts

La convention de service doit :

- a) préciser que le prestataire peut incorporer dans l'équipe d'accompagnement et de conseil un ou plusieurs experts pour participer à la réalisation de certaines activités d'accompagnement et de conseil lorsqu'elles requièrent des connaissances ou des compétences spécifiques dont les consultants ne disposent pas sous réserve que :
 - i. il existe un cadre contractuel entre le prestataire et les experts ;
 - ii. le recours aux experts est accepté par le commanditaire ;
 - iii. les experts sont dûment encadrés par le responsable de la prestation.

VI.2.6. Sous-traitance

La convention de service doit :

- a) préciser que le prestataire peut sous-traiter une partie des activités d'accompagnement et de conseil en sécurité des systèmes d'information à un autre prestataire sous-traitant sous réserve que :
 - i. le prestataire sous-traitant est qualifié pour les activités d'accompagnement et de conseil en sécurité des systèmes d'information sous-traitées ;
 - ii. la prestation sous-traitée est qualifiée au même niveau de qualification ;
 - iii. il existe un cadre contractuel entre le prestataire et le prestataire sous-traitant ;
 - iv. le recours à la sous-traitance est accepté par le commanditaire dans la note de cadrage.

VI.2.7. Note de cadrage

La convention de service doit :

- a) prévoir l'élaboration d'une note de cadrage et sa mise à jour durant la prestation.

Prestataires d'accompagnement et de conseil en sécurité des systèmes d'information – Référentiel d'exigences			
Version	Date	Critère de diffusion	Page
2.0	14/02/2026	PUBLIC	22/62

b) indiquer que la note de cadrage respecte les exigences énoncées au chapitre VI.3.2.

VI.3. Étape 3 - Préparation de la prestation

VI.3.1. Constitution de l'équipe

- a) Le prestataire doit désigner un responsable de prestation.
- b) [ELEVE] Les consultants et les responsables de prestation doivent chacun disposer d'une attestation individuelle de compétence en vigueur pour les activités qui leur sont confiées.
- c) Le responsable de prestation doit constituer une équipe composée de consultants et, le cas échéant, d'experts disposant de toutes les connaissances et compétences requises pour mener la prestation. Le responsable de prestation peut, s'il dispose des connaissances et compétences suffisantes, réaliser la prestation seul.
- d) Le responsable de prestation doit réévaluer régulièrement le profil et le nombre de consultants et, le cas échéant, d'experts afin de s'assurer que l'engagement du prestataire reste adapté à la bonne exécution de la prestation.

VI.3.2. Elaboration de la note de cadrage

- a) Le responsable de la prestation doit élaborer la note de cadrage en concertation avec l'équipe d'accompagnement et de conseil et le correspondant de la prestation au sein du commanditaire.

La note de cadrage doit :

- b) préciser les objectifs, les critères, le périmètre et les activités d'accompagnement et de conseil, ainsi que les modalités de la prestation : prérequis, jalons, livrables, dates et lieux d'exécution de la prestation, etc. L'Annexe 4 identifie pour, pour chaque activité d'accompagnement et de conseil, les documents prérequis devant a minima être mis à disposition par le commanditaire ;
- c) identifier les instances de gouvernance de la prestation et préciser leurs rôles et fréquences de réunion ;
- d) identifier le nom du correspondant de la prestation au sein du commanditaire dont le rôle est de gérer la relation avec le prestataire, de veiller à la bonne exécution de la prestation et de s'assurer que la convention de service et la note de cadrage sont respectées ;
- e) identifier si le commanditaire autorise le prestataire à sous-traiter tout ou partie de la prestation et, le cas échéant, identifier le prestataire sous-traitant et les activités d'accompagnement et de conseil en sécurité des systèmes d'information sous-traitées ;
- f) identifier si le commanditaire autorise le prestataire à recourir à des experts ;
- g) identifier les noms et les coordonnées des membres de l'équipe d'accompagnement et de conseil et préciser pour chacun d'eux leur rôle (responsable de prestation, consultant ou expert) et les activités qui leur sont confiées ;
- h) [ELEVE] annexer les attestations individuelles de compétence du responsable de prestation et des consultants ;

Prestataires d'accompagnement et de conseil en sécurité des systèmes d'information – Référentiel d'exigences			
Version	Date	Critère de diffusion	Page
2.0	14/02/2026	PUBLIC	23/62

- i) identifier les noms, rôles, et responsabilités des personnes désignées par le commanditaire et intervenant dans le cadre de la prestation. L'Annexe 4 identifie pour, pour chaque activité d'accompagnement et de conseil, les profils des personnes devant a minima être désignées par le commanditaire ;
- j) décrire, le cas échéant, les modalités de collaboration avec les tiers (sous-traitants, etc.) ;
- k) identifier les droits et besoins d'en connaître des informations et supports relatifs à la prestation ;
- l) identifier le marquage des informations et supports relatifs à la prestation selon leur niveau de sensibilité² ;
- m) identifier les moyens de protection des informations et supports relatifs à la prestation selon leur niveau de sensibilité et leur marquage³ ;
- n) préciser les livrables de la prestation et décrire les modalités applicables : contenu, forme, langue, etc. ;
- o) identifier pour chaque information et support relatif à la prestation lesquels seront conservés, effacés ou détruits par le prestataire ou restitués au commanditaire, et préciser les modalités de conservation, effacement, destruction et restitution ;
- p) identifier, le cas échéant, les exigences légales et réglementaires spécifiques auxquelles est soumis le commanditaire, en particulier celles applicables au système d'information cible ;
- q) identifier, le cas échéant, les demandes spécifiques du commanditaire notamment les sujets pour lesquels il souhaite que le prestataire ait une attention particulière. Il peut s'agir par exemple de contraintes particulières auxquelles pourraient être soumis le système d'information cible ou le commanditaire ;
- r) être validée par le correspondant de la prestation au sein du commanditaire et par le responsable de la prestation et à chaque mise à jour durant la prestation.

VI.3.3. Réunion d'ouverture

- a) Le responsable de prestation doit s'assurer auprès du commanditaire que les représentants légaux des entités impactées par la prestation ont été préalablement avertis et qu'ils ont donné leur accord.
- b) 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'acquiescer une compréhension suffisante du système d'information cible. Elle doit ainsi, le cas échéant, demander au commanditaire des compléments d'informations par rapport

² Le choix du marquage des informations et supports relatifs à la prestation revient in fine au commanditaire cependant le prestataire a, en sa qualité de professionnel en matière de sécurité des systèmes d'information, un devoir de conseil et doit proposer un marquage adapté. L'Annexe 3 fournit des recommandations aux commanditaires sur le marquage des livrables de la prestation notamment le rapport de prestation.

³ Le choix des moyens de protection des informations et supports relatifs à la prestation revient in fine au commanditaire cependant le prestataire a, en sa qualité de professionnel en matière de sécurité des systèmes d'information, un devoir de conseil et doit proposer des moyens de protection adaptés.

Prestataires d'accompagnement et de conseil en sécurité des systèmes d'information – Référentiel d'exigences			
Version	Date	Critère de diffusion	Page
2.0	14/02/2026	PUBLIC	24/62

aux documents déjà transmis lors de l'élaboration de la proposition de service répondant à la demande du commanditaire.

c) 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.

d) 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. 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 le guide (17) 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

Prestataires d'accompagnement et de conseil en sécurité des systèmes d'information – Référentiel d'exigences			
Version	Date	Critère de diffusion	Page
2.0	14/02/2026	PUBLIC	25/62

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 guide (17) 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. 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 (20).
- b) [ELEVE] Le prestataire doit préconiser auprès du commanditaire l'utilisation de la méthode EBIOS RM (16) 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) [ELEVE] 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.

VI.4.3. Exécution des activités de conseil en sécurité des architectures des systèmes d'information

- a) 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.
- b) Le prestataire doit procéder à la revue des documents et organiser la rencontre des interlocuteurs identifiés dans la note de cadrage.
- c) Le prestataire doit baser ses recommandations sur des standards éprouvés, maintenus, pérennes, respectant les principes des textes et guides de sécurisation techniques publiés par l'ANSSI ou reconnus comme conformes aux normes existantes en matière d'architecture des systèmes d'information sécurisés. Le prestataire doit justifier ses recommandations et mettre en avant les écarts avec l'état de l'art pour toute recommandation alternative.

Prestataires d'accompagnement et de conseil en sécurité des systèmes d'information – Référentiel d'exigences			
Version	Date	Critère de diffusion	Page
2.0	14/02/2026	PUBLIC	26/62

VI.4.4. 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 le guide (21).
- 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 dans la note de cadrage.
- 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) 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) [ELEVE] Dans le cadre d'organisation d'entraînements à la gestion de crise d'origine cyber, le prestataire doit s'appuyer sur la méthodologie proposée dans le guide (21).
- g) 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 (22).
- h) 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.
- i) 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) [ELEVE] 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.

Prestataires d'accompagnement et de conseil en sécurité des systèmes d'information – Référentiel d'exigences			
Version	Date	Critère de diffusion	Page
2.0	14/02/2026	PUBLIC	27/62

- 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

- a) Le prestataire doit élaborer un rapport⁴.

VI.6.1. Qualification

Le rapport de prestation doit :

- a) préciser que la prestation est qualifiée ;
- b) identifier le niveau de qualification de la prestation ;
- c) identifier les activités d'accompagnement et de conseil ;
- d) identifier les noms et coordonnées des membres de l'équipe d'accompagnement et de conseil et préciser pour chacun d'eux leur rôle (responsable de prestation, consultant, expert) et les activités d'accompagnement et de conseil réalisées.

VI.6.2. Cadre

Le rapport de prestation doit :

- a) identifier les noms, coordonnées et fonctions des interlocuteurs que le prestataire a rencontré lors d'entretiens et préciser la date de l'entretien ;
- b) identifier l'ensemble des documents sur lesquels s'appuie la prestation.

VI.6.3. Synthèse managériale

- a) Le rapport doit présenter une synthèse managériale.

La synthèse managériale doit :

- b) être compréhensible par des personnes non expertes en sécurité des systèmes d'information ;
- c) préciser le contexte, dont une analyse de la menace globale ;
- d) préciser la cartographie du système d'information cible ;
- e) préciser les différentes étapes de la prestation, les entretiens réalisés et les documents analysés dans le cadre de la prestation ;
- f) préciser la synthèse des résultats de chacune des activités d'accompagnement et de conseil réalisées dans le cadre de la prestation ;
- g) préciser la synthèse globale de la prestation ;

⁴ Lorsque plusieurs activités sont menées durant la prestation, le choix d'avoir un ou plusieurs rapports revient au commanditaire.

Prestataires d'accompagnement et de conseil en sécurité des systèmes d'information – Référentiel d'exigences			
Version	Date	Critère de diffusion	Page
2.0	14/02/2026	PUBLIC	28/62

- h) [ELEVE] 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.

VI.6.4. Résultats

VI.6.4.1. 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 sécurité⁵ 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.

⁵ Le socle de sécurité sous-entend la liste des référentiels applicables, l'état d'application et l'identification et justification des écarts.

Prestataires d'accompagnement et de conseil en sécurité des systèmes d'information – Référentiel d'exigences			
Version	Date	Critère de diffusion	Page
2.0	14/02/2026	PUBLIC	29/62

VI.6.4.2. 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 ;
 - 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) [ELEVE] Le rapport de prestation doit, dans la mesure du possible, 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.6.4.3. 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 suivantes⁶ :
 - 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 ;

⁶ Ces thématiques sont à adapter en fonction du périmètre et des objectifs de la prestation.

Prestataires d'accompagnement et de conseil en sécurité des systèmes d'information – Référentiel d'exigences			
Version	Date	Critère de diffusion	Page
2.0	14/02/2026	PUBLIC	30/62

- 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 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 pour chaque scénario, permettant d'atteindre les objectifs de sécurité du commanditaire ;
 - [ELEVE] un indicateur de priorité et d'efforts de mise en œuvre pour chacune des recommandations de la liste ;
 - 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 ;
 - [ELEVE] 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.6.4.4. 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 :

Prestataires d'accompagnement et de conseil en sécurité des systèmes d'information – Référentiel d'exigences			
Version	Date	Critère de diffusion	Page
2.0	14/02/2026	PUBLIC	31/62

- [ELEVE] un rapport d'évaluation du niveau de maturité du dispositif de crise vis-à-vis de l'état de l'art, en s'appuyant sur le guide (21) 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 :
- [ELEVE] un rapport d'évaluation du 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 le guide (21) 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 des guides gestion de crise d'origine cyber (21) et EBIOS RM (16) ;
 - 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'entraînement 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 :

Prestataires d'accompagnement et de conseil en sécurité des systèmes d'information – Référentiel d'exigences			
Version	Date	Critère de diffusion	Page
2.0	14/02/2026	PUBLIC	32/62

- 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) ;
 - [ELEVE] 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 des guides (21) et EBIOS_RM (16) ;
 - 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'entraînement 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, permettant d'atteindre le niveau cible de gestion de crise et de continuité d'activité du commanditaire,
 - [ELEVE] une liste de recommandations accompagnée d'indicateurs de priorité et d'effort de mise en œuvre pour chacune d'entre elles.

VI.6.5. Annexes

Le rapport doit annexer :

- a) La note de cadrage.

Prestataires d'accompagnement et de conseil en sécurité des systèmes d'information – Référentiel d'exigences			
Version	Date	Critère de diffusion	Page
2.0	14/02/2026	PUBLIC	33/62

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 minimum⁷ :

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) [ELEVE] 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.

⁷ Ces rôles peuvent être cumulés par une même personne.

Prestataires d'accompagnement et de conseil en sécurité des systèmes d'information – Référentiel d'exigences			
Version	Date	Critère de diffusion	Page
2.0	14/02/2026	PUBLIC	34/62

- e) Le prestataire doit procéder à la restitution, à l'effacement ou à la destruction des informations ou supports relatifs à la prestation pour lesquels il n'a pas obtenu l'accord de conservation du commanditaire dans la note de cadrage.
- f) Le prestataire doit conserver hors ligne les informations et supports relatifs à la prestation pour lesquels il a obtenu l'accord de conservation du commanditaire dans la note de cadrage.
- g) [ELEVE] Il est recommandé que le prestataire produise un procès-verbal de destruction, d'effacement ou de restitution des informations ou supports relatifs à la prestation pour lesquels il n'a pas obtenu l'accord de conservation du commanditaire dans la note de cadrage. Ce procès-verbal, remis au commanditaire, devrait identifier de manière précise les informations ou supports détruits, effacés ou restitués, la date et le mode de destruction, d'effacement ou de restitution.
- h) 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.

Prestataires d'accompagnement et de conseil en sécurité des systèmes d'information – Référentiel d'exigences			
Version	Date	Critère de diffusion	Page
2.0	14/02/2026	PUBLIC	35/62

Annexe 1 Bibliographie

1. Loi relative à la programmation militaire, version en vigueur. *Disponible sur <https://cyber.gouv.fr>.*
2. Directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union. *Disponible sur <https://eur-lex.europa.eu>.*
3. 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 et la loi n°2018-133 du 26 février 2018. *Disponible sur <https://eur-lex.europa.eu>. - <https://www.legifrance.gouv.fr>.*
4. Référentiel général de sécurité, version en vigueur. *Disponible sur <https://legifrance.gouv.fr>.*
5. 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. *Disponible sur <https://eur-lex.europa.eu>.*
6. Politique de sécurité des systèmes d'information de l'État, version en vigueur. *Disponible sur <https://www.cyber.gouv.fr>.*
7. QUAL - 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>.*
8. QUAL - Référentiel d'exigences applicables à un prestataire de détection des incidents de sécurité, ANSSI, version en vigueur. *Disponible sur <https://www.cyber.gouv.fr>.*
9. QUAL - Référentiel d'exigences applicables à un prestataire de réponse aux incidents de sécurité, ANSSI, version en vigueur. *Disponible sur <https://www.cyber.gouv.fr>.*
10. Instruction interministérielle relative à la protection des systèmes d'information sensibles, n°901/SGDSN/ANSSI, version en vigueur. *Disponible sur <https://circulaires.legifrance.gouv.fr>.*
11. Instruction générale interministérielle n° 1300/SGDSN/PSE/PSD sur la protection du secret de la défense nationale, version en vigueur. *Disponible sur <https://www.legifrance.gouv.fr/>.*
12. Processus de qualification d'un service, ANSSI, version en vigueur. *Disponible sur <https://www.cyber.gouv.fr>.*
13. Référentiel d'exigences applicables aux prestataires d'accompagnement et de conseil en sécurité des systèmes d'information (PACS) pour les besoins de la sécurité nationale. *Document Diffusion Restreinte, il peut être obtenu auprès de l'ANSSI.*
14. Instruction interministérielle n° 2102/SGDSN/PSD sur la protection en France des informations classifiées de l'Union Européenne, version en vigueur. *Disponible sur <https://circulaires.legifrance.gouv.fr>.*
15. Instruction interministérielle n° 2100/SGDSN/SSD pour l'application en France du système de sécurité de l'Organisation du Traité de l'Atlantique Nord, version en vigueur. *Disponible sur <https://circulaires.legifrance.gouv.fr>.*
16. Méthode de gestion de risques EBIOS Risk Manager. *Disponible sur <https://www.cyber.gouv.fr>.*

Prestataires d'accompagnement et de conseil en sécurité des systèmes d'information – Référentiel d'exigences			
Version	Date	Critère de diffusion	Page
2.0	14/02/2026	PUBLIC	36/62

17. Guide - L'homologation de sécurité des systèmes d'information, ANSSI, version en vigueur. *Disponible sur <https://www.cyber.gouv.fr>.*
18. Guide - Guide d'hygiène informatique, ANSSI, version en vigueur. *Disponible sur <https://www.cyber.gouv.fr>.*
19. ISO/IEC - Norme internationale ISO/IEC 19011 : Lignes directrices pour l'audit des systèmes de management, version en vigueur. *Disponible sur <https://www.iso.org>.*
20. ISO/IEC - 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>.*
21. Guide - Crise d'origine cyber, les clés d'une gestion opérationnelle et stratégique, ANSSI, version en vigueur. *Disponible sur <https://www.cyber.gouv.fr>.*
22. Guide - Anticiper et gérer sa communication de crise cyber, ANSSI, version en vigueur. *Disponible sur <https://www.cyber.gouv.fr>.*
23. Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données. *Disponible sur <https://eur-lex>.*
24. ISO/IEC - 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>.*
25. ISO/IEC - 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>.*
26. Guide - Organiser un exercice de gestion de crise cyber, ANSSI, version en vigueur. *Disponible sur <https://www.cyber.gouv.fr>.*
27. Guide - Recommandations relatives à l'interconnexion d'un système d'information à Internet, ANSSI, version en vigueur. *Disponible sur <https://www.cyber.gouv.fr>.*
28. Guide - 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>.*
29. Guide - Recommandations de sécurité relatives à TLS, ANSSI, version en vigueur. *Disponible sur <https://www.cyber.gouv.fr>.*
30. Guide - Recommandations pour la sécurisation d'un commutateur de desserte, ANSSI, version en vigueur. *Disponible sur <https://www.cyber.gouv.fr>.*
31. Guide - Recommandations de sécurité relatives aux réseaux Wi-Fi, ANSSI, version en vigueur. *Disponible sur <https://www.cyber.gouv.fr>.*
32. Guide - Recommandations de sécurité relatives à IPsec pour la protection des flux réseau, ANSSI, version en vigueur. *Disponible sur <https://www.cyber.gouv.fr>.*
33. Guide - Recommandations pour choisir des pare-feux maîtrisés dans les zones exposées à internet, ANSSI, version en vigueur. *Disponible sur <https://www.cyber.gouv.fr>.*

Prestataires d'accompagnement et de conseil en sécurité des systèmes d'information – Référentiel d'exigences			
Version	Date	Critère de diffusion	Page
2.0	14/02/2026	PUBLIC	37/62

34. Guide - Bonnes pratiques pour l'acquisition et l'exploitation de noms de domaine, ANSSI, version en vigueur. *Disponible sur <https://www.cyber.gouv.fr>.*
35. Guide - Recommandations pour la mise en place de cloisonnement système, ANSSI, version en vigueur. *Disponible sur <https://www.cyber.gouv.fr>.*
36. Recommandations sur le nomadisme numérique, ANSSI, version en vigueur. *Guide - Recommandations sur le nomadisme numérique, ANSSI, version en vigueur. Disponible sur <https://www.cyber.gouv.fr>.*
37. Guide - Recommandations de configuration d'un système GNU/Linux, ANSSI, version en vigueur. *Disponible sur <https://www.cyber.gouv.fr>.*
38. Guide - Recommandations pour la mise en oeuvre d'une politique de restrictions logicielles sous Windows, ANSSI, version en vigueur. *Disponible sur <https://www.cyber.gouv.fr>.*
39. Guide - Recommandations relatives à l'administration sécurisée des systèmes d'information, ANSSI, version en vigueur. *Disponible sur <https://www.cyber.gouv.fr>.*
40. Guide - Recommandations pour la sécurisation des sites web, ANSSI, version en vigueur. *Disponible sur <https://www.cyber.gouv.fr>.*
41. Guide - Recommandations de sécurité relatives à Active Directory, ANSSI, version en vigueur. *Disponible sur <https://www.cyber.gouv.fr>.*
42. Guide - Recommandations relatives à l'authentification multifacteurs et aux mots de passe, ANSSI, version en vigueur. *Disponible sur <https://www.cyber.gouv.fr>.*
43. Guide - Guide de sélection d'algorithmes cryptographiques, ANSSI, version en vigueur. *Disponible sur <https://www.cyber.gouv.fr>.*
44. Guide - Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, ANSSI, version en vigueur. *Disponible sur <https://www.cyber.gouv.fr>.*
45. Guide - La défense en profondeur appliquée aux systèmes d'information, ANSSI, version en vigueur. *Disponible sur <https://www.cyber.gouv.fr>.*
46. Guide - Cartographie du système d'information, Guide d'élaboration en 5 étapes, ANSSI, version en vigueur. *Disponible sur <https://www.cyber.gouv.fr>.*
47. Guide - Recommandations relatives à la cybersécurité des systèmes industriels, ANSSI, version en vigueur. *Disponible sur <https://www.cyber.gouv.fr>.*
48. Guide - Problématiques de sécurité associées à la virtualisation des systèmes d'information, ANSSI, version en vigueur. *Disponible sur <https://www.cyber.gouv.fr>.*
49. Guide - 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>.*
50. Guide - 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>.*
51. QUAL - 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>.*

Prestataires d'accompagnement et de conseil en sécurité des systèmes d'information – Référentiel d'exigences			
Version	Date	Critère de diffusion	Page
2.0	14/02/2026	PUBLIC	38/62

52. ISO/IEC - Norme internationale ISO/IEC 22361 : Sécurité et résilience — Gestion de crise — Lignes directrices, version en vigueur. *Disponible sur <https://www.iso.org>.*
53. ISO/IEC - 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>.*
54. ISO/IEC - 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>.*
55. ISO/IEC - 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>.*
56. ISO/IEC - 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>.*
57. ISO/IEC - Norme internationale ISO/IEC 22398 : Sécurité sociétale — Lignes directrices pour exercice, version en vigueur. *Disponible sur <https://www.iso.org>.*
58. Guide - 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>.*
59. Guide - Guide d'achat de produits de sécurité et de services de confiance qualifiés, ANSSI, version en vigueur. *Disponible sur <https://www.cyber.gouv.fr>.*
60. Instruction interministérielle relative aux articles contrôlés de la sécurité des systèmes d'information (ACSSI), n°910/SGDSN/ANSSI, version en vigueur. *Disponible sur <https://circulaires.legifrance.gouv.fr>.*
61. 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>.*
62. Guide - Recommandations pour les architectures des systèmes d'information sensibles ou diffusion restreinte, ANSSI, version en vigueur. *Disponible sur <https://www.cyber.gouv.fr>.*
63. ISO/IEC - 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>.*
64. Stratégie nationale pour la sécurité du numérique, octobre 2015. *Disponible sur <https://www.cyber.gouv.fr>.*
65. <https://google.fr>. *page d'accueil de google.* [En ligne] <https://google.fr>.

Prestataires d'accompagnement et de conseil en sécurité des systèmes d'information – Référentiel d'exigences			
Version	Date	Critère de diffusion	Page
2.0	14/02/2026	PUBLIC	39/62

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 :

- La protection du secret de la défense national (11);
- La protection des systèmes d'information sensibles (10)
- La loi de programmation militaire et particulièrement les dispositions applicables aux systèmes d'information d'importance vitale (SIIV) des opérateurs d'importance vitale (OIV) (1) ;
- Les directives européennes relatives à la sécurité des réseaux et des systèmes d'information dans l'Union (2) (3) ;
- La réglementation européenne sur l'identification électronique et les services de confiance pour les transactions électroniques (5) ;
- La Politique de sécurité des systèmes d'information de l'Etat (6) ;
- Le référentiel général de sécurité (4) et notamment ses annexes A, B et C ;
- Le règlement général sur la protection des données (23) ;
- La protection des informations classifiées de l'Organisation du traité de l'Atlantique nord (OTAN) (15) ;
- La protection des informations classifiées de l'Union européenne (UE) (14).

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

Prestataires d'accompagnement et de conseil en sécurité des systèmes d'information – Référentiel d'exigences			
Version	Date	Critère de diffusion	Page
2.0	14/02/2026	PUBLIC	40/62

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 ;
- chaînes 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 :

- le guide d'hygiène informatique (18) ;
- la norme internationale ISO/IEC 27001 (24) ;
- la norme internationale ISO/IEC 27002 (25).

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 :
 - i. du guide d'homologation (17) ;
 - ii. d'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 ;

Prestataires d'accompagnement et de conseil en sécurité des systèmes d'information – Référentiel d'exigences			
Version	Date	Critère de diffusion	Page
2.0	14/02/2026	PUBLIC	41/62

- 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 des guides :
 - i. crise d'origine cyber (21) ;
 - i. organiser un exercice de gestion de crise cyber (26) ;
 - ii. anticiper et gérer sa communication de crise cyber (22).
- la connaissance et la compréhension de :
 - i. la définition de la gestion de crise ;
 - ii. les spécificités associées aux crises d'origine cyber ;

Prestataires d'accompagnement et de conseil en sécurité des systèmes d'information – Référentiel d'exigences			
Version	Date	Critère de diffusion	Page
2.0	14/02/2026	PUBLIC	42/62

- 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 chaînes 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, d'outils 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.

Prestataires d'accompagnement et de conseil en sécurité des systèmes d'information – Référentiel d'exigences			
Version	Date	Critère de diffusion	Page
2.0	14/02/2026	PUBLIC	43/62

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 connaît 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 ;

Prestataires d'accompagnement et de conseil en sécurité des systèmes d'information – Référentiel d'exigences			
Version	Date	Critère de diffusion	Page
2.0	14/02/2026	PUBLIC	44/62

- 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.

Prestataires d'accompagnement et de conseil en sécurité des systèmes d'information – Référentiel d'exigences			
Version	Date	Critère de diffusion	Page
2.0	14/02/2026	PUBLIC	45/62

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.2.3. 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 :

- Recommandations relatives à l'interconnexion d'un système d'information à Internet (27) ;
- Recommandations de déploiement du protocole 802.1x pour le contrôle d'accès à des réseaux locaux (28) ;
- Recommandations de sécurité relatives à TLS (29) ;
- Recommandations pour la sécurisation d'un commutateur de desserte (30) ;
- Recommandations de sécurité relatives aux réseaux Wi-Fi (31) ;
- Recommandations de sécurité relatives à IP sec pour la protection des flux réseau (32) ;
- Recommandations pour choisir des pare-feux maîtrisés dans les zones exposées à internet (33) ;
- Bonnes pratiques pour l'acquisition et l'exploitation de noms de domaine (34).

IV.2.3.1. 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.

Prestataires d'accompagnement et de conseil en sécurité des systèmes d'information – Référentiel d'exigences			
Version	Date	Critère de diffusion	Page
2.0	14/02/2026	PUBLIC	46/62

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 :

- Recommandations pour la mise en place de cloisonnement système (35) ;
- Recommandations sur le nomadisme numérique (36) ;
- Recommandations de configuration d'un système GNU/Linux (37) ;
- Recommandations pour la mise en œuvre d'une politique de restrictions logicielles sous Windows (38).

IV.2.3.2. 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 : recommandations relatives à l'administration sécurisée des systèmes d'information (39).

IV.2.3.3. 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 : recommandations pour la sécurisation des sites web (40).

IV.2.3.4. 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 ;

Prestataires d'accompagnement et de conseil en sécurité des systèmes d'information – Référentiel d'exigences			
Version	Date	Critère de diffusion	Page
2.0	14/02/2026	PUBLIC	47/62

- 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 :

- Recommandations de sécurité relatives à Active Directory (41);
- Recommandations relatives à l'authentification multifacteurs et aux mots de passe (42) ;
- Guide de sélection d'algorithmes cryptographiques (43) ;
- Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques (44).

IV.2.3.5. 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 : la défense en profondeur appliquée aux systèmes d'information (45).

Prestataires d'accompagnement et de conseil en sécurité des systèmes d'information – Référentiel d'exigences			
Version	Date	Critère de diffusion	Page
2.0	14/02/2026	PUBLIC	48/62

IV.2.3.6. 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.

Prestataires d'accompagnement et de conseil en sécurité des systèmes d'information – Référentiel d'exigences			
Version	Date	Critère de diffusion	Page
2.0	14/02/2026	PUBLIC	49/62

Il doit connaître les guides de recommandations liés à ces différents éléments, parmi lesquels de façon non exhaustive : cartographie du système d'information (46).

IV.2.3.7. 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 : recommandations relatives à la cybersécurité des systèmes industriels (47).

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 :

- Problématiques de sécurité associées à la virtualisation des systèmes d'information (48) ;
- Guide de recommandations relatives à la sécurisation d'une architecture de téléphonie sur IP (49) ;
- Recommandations sur la sécurisation des systèmes de contrôle d'accès physique et de vidéoprotection (50) ;
- Référentiel d'exigences applicables à un prestataire de services d'informatique en nuage (SecNumCloud) (51).

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.2.3.8. 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.) ;

Prestataires d'accompagnement et de conseil en sécurité des systèmes d'information – Référentiel d'exigences			
Version	Date	Critère de diffusion	Page
2.0	14/02/2026	PUBLIC	50/62

- 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 ;

Prestataires d'accompagnement et de conseil en sécurité des systèmes d'information – Référentiel d'exigences			
Version	Date	Critère de diffusion	Page
2.0	14/02/2026	PUBLIC	51/62

- 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 le guide crise d'origine cyber (21) et la norme internationale ISO/IEC 22361 (52).

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 chaînes de valeurs d'une organisation ;
- savoir identifier les biens supports des chaînes de valeur, en utilisant la méthodologie EBIOS RM (16) ;
- savoir identifier les principaux risques sur les biens supports des chaînes 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 (16) ;
- ISO22301 (53) ;
- ISO22313 (54) ;
- ISO22317 (55) ;
- ISO27031 (56).

V.2.2.3. Maîtrise 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.

Prestataires d'accompagnement et de conseil en sécurité des systèmes d'information – Référentiel d'exigences			
Version	Date	Critère de diffusion	Page
2.0	14/02/2026	PUBLIC	52/62

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

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

- savoir formaliser un plan d'entraînement 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 majeur⁸) 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 adaptés aux différents niveaux (outil de simulation de pression médiatique pour les équipes communication ; outil de cyberrange ou outil de Capture the Flag pour les équipes techniques) et des outils de modélisation et d'automatisation de l'animation de l'exercice ;
- savoir maîtriser 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.

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

- Organiser un exercice de gestion de crise cyber (26) ;
- ISO22398 (57).

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 ;

⁸ 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.

Prestataires d'accompagnement et de conseil en sécurité des systèmes d'information – Référentiel d'exigences			
Version	Date	Critère de diffusion	Page
2.0	14/02/2026	PUBLIC	53/62

- 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 boîte 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 anticiper et gérer sa communication de crise cyber (22).

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 le guide crise d'origine cyber (21).

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.

Prestataires d'accompagnement et de conseil en sécurité des systèmes d'information – Référentiel d'exigences			
Version	Date	Critère de diffusion	Page
2.0	14/02/2026	PUBLIC	54/62

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

- le guide d'hygiène informatique (18) ;
- le guide attaques par rançongiciels, tous concernés (58).

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 travaux ou des exercices d'entraînement ;
- 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.

Prestataires d'accompagnement et de conseil en sécurité des systèmes d'information – Référentiel d'exigences			
Version	Date	Critère de diffusion	Page
2.0	14/02/2026	PUBLIC	55/62

Annexe 3 Recommandations à l'attention des 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. Avant la prestation

- 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 utilise le guide (59) pour rédiger le cahier des charges d'un appel d'offres ou d'un contrat en matière d'accompagnement et de conseil en sécurité des systèmes d'information.
- c) Le commanditaire peut consulter le catalogue des prestataires de services qualifiés sur le site de l'ANSSI. Ce catalogue présente pour chaque prestataire les activités pour lesquelles il est qualifié, la période de validité de la qualification, le niveau de qualification et le niveau de recommandation.
- d) Les prestataires qualifiés gardent la faculté de réaliser des prestations non qualifiées mais ne peuvent dans ce cas se prévaloir de la qualification sur ces prestations. Le commanditaire doit donc, s'il souhaite bénéficier d'une prestation qualifiée, c'est-à-dire conforme aux exigences du présent référentiel, s'assurer que la convention de service établie avec le prestataire indique explicitement que la prestation est qualifiée.
- e) Une prestation non qualifiée, c'est-à-dire ne respectant pas les exigences du présent référentiel, expose le commanditaire à certains risques, notamment la compromission d'informations confidentielles, la perte ou l'indisponibilité du système d'information objet de la prestation. Le recours à une prestation qualifiée permet de réduire ces risques. Si toutefois le commanditaire ne souhaite pas recourir à une prestation qualifiée, il est néanmoins recommandé qu'il demande au prestataire un document identifiant l'ensemble des exigences du présent référentiel non satisfaites dans le cadre de sa prestation afin de connaître les risques auxquels il s'expose.
- f) Si le commanditaire souhaite recourir sur un même périmètre à un prestataire d'audit de sécurité (PASSI) et à un prestataire d'accompagnement et de conseil en sécurité des systèmes d'information (PACS) alors il est recommandé que le PASSI et le PACS soient deux prestataires distincts afin de garantir un niveau d'impartialité et d'indépendance renforcé
- g) Le commanditaire peut, conformément au processus de qualification d'un service (12) déposer auprès de l'ANSSI une réclamation lorsqu'il estime que le prestataire n'a pas respecté une ou plusieurs exigences du présent référentiel dans le cadre d'une prestation qualifiée. La réclamation peut également être déposée directement auprès du prestataire qualifié qui a l'obligation d'en informer sans délai l'ANSSI.

S'il s'avère après instruction de la réclamation que le prestataire qualifié n'a pas respecté une ou plusieurs exigences du présent référentiel dans le cadre d'une prestation qualifiée, la qualification du prestataire peut être retirée, la portée de qualification réduite, ou le niveau de recommandation du prestataire dégradé conformément au processus de qualification d'un service (12).

Prestataires d'accompagnement et de conseil en sécurité des systèmes d'information – Référentiel d'exigences			
Version	Date	Critère de diffusion	Page
2.0	14/02/2026	PUBLIC	56/62

- h) Sauf si le commanditaire est soumis à une obligation légale, réglementaire ou contractuelle, le choix du niveau de qualification de la prestation relève exclusivement du commanditaire. Dans ce cas, il est recommandé que le niveau de qualification de la prestation qualifiée soit déterminé à l'aide d'une approche par les risques.

Il est recommandé qu'une prestation de niveau élevé soit réalisée lorsque les risques qui pèsent sur le système d'information objet de la prestation sont élevés et/ou lorsque les scénarios de risque de nature intentionnelle impliquent des menaces stratégiques. Dans les autres cas, une prestation de niveau substantiel devrait suffire.

De ce fait, dans le cadre d'une prestation qualifiée au niveau élevé, il est recommandé que le commanditaire exige du prestataire dans la note de cadrage que le rapport de la prestation porte la mention Diffusion Restreinte.

- i) Lorsque le système d'information objet de la prestation relève de la sécurité nationale, le commanditaire doit réaliser une prestation qualifiée pour les besoins de la sécurité nationale, c'est-à-dire conforme, en sus des exigences pour le niveau élevé du présent référentiel, aux exigences du référentiel (13).
- j) La qualification d'un prestataire n'atteste pas de sa capacité à accéder ou à détenir des informations classifiées et par conséquent ne se substitue pas à l'habilitation d'une personne morale ou physique au titre de l'instruction (11).

Lorsque la prestation requiert que le prestataire accède ou détienne des informations classifiées, le commanditaire doit vérifier que le prestataire et son personnel respectent les principes régissant l'accès des personnes morales et physiques au secret de la défense nationale.

- k) 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) (60).

Lorsque la prestation requiert que le prestataire accède ou détienne des articles contrôlés de la sécurité des systèmes d'information, le commanditaire doit vérifier que le prestataire dispose des décisions d'accès aux ACSSI (DACSSI) pour les ACSSI classifiés ou des attestations de formation à la manipulation des ACSSI pour les ACSSI non classifiés.

- l) Il est recommandé que le commanditaire détermine les objectifs, critères, périmètre et activités de la prestation en utilisant une approche par les risques.
- m) Il est recommandé que le commanditaire demande au prestataire de lui fournir des références de prestations réalisées dont les objectifs, critères, périmètre et activités sont proches de ceux souhaités par le commanditaire.
- n) 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.).

Prestataires d'accompagnement et de conseil en sécurité des systèmes d'information – Référentiel d'exigences			
Version	Date	Critère de diffusion	Page
2.0	14/02/2026	PUBLIC	57/62

- o) 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

- p) Le commanditaire doit désigner en son sein un correspondant de la prestation dont le rôle est d'établir et tenir à jour, en collaboration avec le prestataire, la note de cadrage de la prestation. Le correspondant de la prestation gère la relation avec le prestataire et veille à la bonne exécution de la prestation en s'assurant que la convention de service et la note de cadrage sont respectées.

Il est recommandé que le correspondant de la prestation au sein du commanditaire dispose des moyens lui permettant d'engager la responsabilité du commanditaire et de répondre rapidement aux demandes du prestataire.

- q) 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.

II. Pendant la prestation

- a) Dans le cadre d'une prestation qualifiée au niveau substantiel réalisée par un prestataire qualifié au niveau élevé, il est recommandé que le commanditaire, dans la note de cadrage, exige que le prestataire traite l'ensemble des informations et supports relatifs à la prestation sur son système d'information homologué Diffusion Restreinte et ce quel que soit le marquage de ces informations et supports.
- b) 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.
- c) 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.
- 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.

III. 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.

Prestataires d'accompagnement et de conseil en sécurité des systèmes d'information – Référentiel d'exigences			
Version	Date	Critère de diffusion	Page
2.0	14/02/2026	PUBLIC	58/62

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.

Prestataires d'accompagnement et de conseil en sécurité des systèmes d'information – Référentiel d'exigences			
Version	Date	Critère de diffusion	Page
2.0	14/02/2026	PUBLIC	59/62

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.
- b) 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.
- c) 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 ;

Prestataires d'accompagnement et de conseil en sécurité des systèmes d'information – Référentiel d'exigences			
Version	Date	Critère de diffusion	Page
2.0	14/02/2026	PUBLIC	60/62

- 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.

IV. 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)

Prestataires d'accompagnement et de conseil en sécurité des systèmes d'information – Référentiel d'exigences			
Version	Date	Critère de diffusion	Page
2.0	14/02/2026	PUBLIC	61/62

- 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.

Prestataires d'accompagnement et de conseil en sécurité des systèmes d'information – Référentiel d'exigences			
Version	Date	Critère de diffusion	Page
2.0	14/02/2026	PUBLIC	62/62