TLP:CLEAR

PREMIER MINISTRE

Liberté
Égalité
Fraternité

Premier ministre

Agence nationale de la sécurité des systèmes d'information

Prestataires d'audit de la sécurité des systèmes d'information

Référentiel d'exigences

Version 2.2 du 1er août 2024

TABLE DES MATIERES

I. Introduction

I.1. Présentation générale

I.1.1. Contexte

Les systèmes d'information se transforment, s'ouvrent de plus en plus vers l'extérieur et font face à de nouvelles menaces. Pour s'en protéger, les organisations doivent, dans le cadre d'une démarche de gestion des risques, sécuriser leurs systèmes d'information de façon adaptée et proportionnée.

Les prestataires d'audit de la sécurité des systèmes d'information (PASSI) permettent de :

- évaluer le niveau de conformité d'un système d'information par rapport à des exigences de sécurité (règles, bonnes pratiques, de guides, référentiels, normes, etc.) ;
- évaluer le niveau de sécurité d'un système d'information ;
- proposer des mesures de sécurité pour corriger les non-conformités et/ou vulnérabilités identifiées lors de l'audit.

Le rapport d'audit élaboré par le prestataire d'audit de la sécurité des systèmes d'information peut notamment être utilisé dans le cadre de l'homologation de sécurité d'un système d'information.

I.1.2. Objet du document

Ce document constitue le référentiel d'exigences applicables à un prestataire d'audit de la sécurité des systèmes d'information (PASSI), 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'audit de disposer de garanties sur la compétence 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 peut également être utilisé à titre de bonnes pratiques en dehors de toutes exigences légales, réglementaires ou contractuelles.

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 (1) et classifiées (2) 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 au prestataire.

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.

I.2. Identification du document

Le présent référentiel est dénommé « Prestataires d'audit de la sécurité des systèmes d'information – référentiel d'exigences ». Il peut être identifié par son nom, numéro de version et sa date de mise à jour.

I.3. Acronymes et définitions

I.3.1. Acronymes

Les acronymes utilisés dans le présent référentiel sont :

ANSSI	Agence nationale de la sécurité des systèmes d'information
PACS	Prestataire d'accompagnement et de conseil en sécurité
PASSI	Prestataire d'audit de la sécurité des systèmes d'information

I.3.2. Définitions

Les définitions utilisées dans le présent référentiel sont les suivantes, elles s'appuient en partie sur la norme (3) :

Audit – processus systématique, indépendant et documenté en vue d'obtenir des preuves d'audit et de les évaluer de manière objective pour déterminer dans quelle mesure les critères d'audit sont satisfaits.

Audit de contrôle – un audit de contrôle a pour objectif d'établir un statut de la correction des non-conformités et/ou vulnérabilités identifiées lors d'un audit.

Attestation individuelle de compétence – document délivré par un centre d'évaluation à l'issue d'examens écrits et oraux et attestant qu'un auditeur ou un responsable d'équipe d'audit dispose des connaissances et compétences attendues au titre du présent référentiel.

Auditeur – personne physique réalisant une activité d'audit de la sécurité des systèmes d'information pour le compte d'un prestataire.

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.

Conformité – satisfaction d'un critère d'audit.

Constat d'audit – résultat de l'évaluation des preuves d'audit recueillies par rapport aux critères d'audit.

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

Critères d'audit – ensemble des politiques, référentiels, guides, procédures, exigences, recommandations, bonnes pratiques, etc. utilisés comme références vis-à-vis desquelles les preuves d'audit sont comparées.

Equipe d'audit – ensemble constitué du responsable de l'équipe d'audit, des auditeurs et, le cas échéant, d'experts.

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 auditeurs, sont nécessaires pour la bonne exécution de la prestation. L'expert peut être un personnel interne ou externe au prestataire.

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 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.

Note de cadrage – document élaboré et tenu à jour par le prestataire en concertation avec le commanditaire et précisant les modalités de la prestation. La note de cadrage est généralement élaborée après la signature de la convention de service.

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

Potentiel d'attaque – mesure de l'effort à fournir pour attaquer un système d'information exprimée en termes d'expertise, de ressources et de motivation d'un attaquant.

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

Preuves d'audit – enregistrements, énoncés de faits ou autres informations qui se rapportent aux critères d'audit et sont vérifiables.

Rapport d'audit – document élaboré par l'équipe d'audit présentant les résultats de la prestation et remis au commanditaire à l'issue de la prestation.

Référentiel – le présent document.

Responsable d'équipe – personne physique au sein du prestataire responsable de la prestation d'audit. Le responsable d'équipe est notamment en charge de constituer l'équipe d'audit en veillant à l'adéquation des compétences des auditeurs et, le cas échéant des experts, avec les objectifs, critères, périmètre et activités de la prestation. Le responsable d'équipe peut être un auditeur.

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 d'un contrat conclu entre le prestataire et le commanditaire.

Système d'information – ensemble organisé de ressources (matériels, logiciels, personnel, données, procédures, etc.) permettant de collecter, stocker, traiter et distribuer l'information.

Système d'information audité – système d'information objet de la prestation.

Système industriel – ensemble de moyens humains et matériels ayant pour finalité de contrôler ou commander des installations techniques (composées d'un ensemble de capteurs et d'actionneurs).

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

Vulnérabilité – faiblesse d'un système d'information ou d'une mesure de sécurité pouvant être exploitée par une menace.

II. Activités couvertes par le référentiel

Les activités couvertes par le présent référentiel sont les suivantes :

- audit d'architecture (ARCHI) ;
- audit de configuration (CONF) ;
- audit de code source (CODE) ;
- test d'intrusion (INTRUSION) ;
- audit organisationnel et physique (ORGAPHY).

Lorsqu'une exigence n'est applicable qu'à une seule et unique activité alors elle est précédée d'une mention entre crochets identifiant ladite activité. À titre d'exemple, une exigence précédée de la mention « [ARCHI] » est applicable exclusivement à l'activité d'audit d'architecture.

Lorsqu'une exigence est applicable à plusieurs activités sans toutefois être applicable à l'ensemble des activités alors elle est précédée d'une mention entre crochets identifiant lesdites activités. À titre d'exemple, une exigence précédée de la mention « [ARCHI, CONF] » est applicable exclusivement aux activités d'audit d'architecture et d'audit de configuration.

Lorsqu'une exigence n'est précédée d'aucune mention entre crochets identifiant une activité alors elle est applicable à l'ensemble des activités.

La réalisation entièrement automatisée d'une activité d'audit ne représente pas une activité au sens du référentiel.

II.1. Audit d'architecture

L'audit d'architecture consiste à évaluer le niveau de conformité et/ou de sécurité d'un système d'information notamment par l'analyse des choix de positionnement et de mise en œuvre des dispositifs matériels et logiciels déployés en son sein. L'audit d'architecture peut être étendu aux interconnexions du système d'information audité avec des réseaux tiers, et notamment Internet.

II.2. Audit de configuration

L'audit de configuration consiste à évaluer le niveau de conformité et/ou de sécurité de la configuration des dispositifs matériels et logiciels déployés au sein d'un système d'information. Ces dispositifs peuvent notamment être des équipements réseau, des systèmes d'exploitation, des applications ou des produits de sécurité.

II.3. Audit de code source

L'audit de code source consiste à évaluer le niveau de conformité et/ou de sécurité de tout ou partie du code source d'un logiciel, ou de ses conditions de compilation et d'exécution. Les non-conformités ou vulnérabilités identifiées peuvent notamment être relatives à de mauvaises pratiques de programmation ou à des erreurs de développement.

II.4. Test d'intrusion

Le test d'intrusion consiste à évaluer le niveau de sécurité d'un système d'information en identifiant, et le cas échéant en exploitant, des vulnérabilités. Le test d'intrusion peut être réalisé selon trois modes (boite noire, grise ou blanche) en fonction du niveau d'information et d'accès fournis à l'auditeur.

Le test d'intrusion permet de simuler des attaquants disposant ou non d'accès légitimes au système d'information et peut être mené soit depuis l'extérieur du système d'information audité (réseaux tiers, Internet, etc.) soit depuis l'intérieur du système audité.

Le test d'intrusion peut permettre de confirmer, par leur exploitation, des vulnérabilités identifiées lors d'autres activités d'audit.

II.5. Audit organisationnel et physique

L'audit organisationnel et physique consiste à évaluer le niveau de conformité et/ou de sécurité de la gouvernance, des politiques et procédures de sécurité mises en œuvre pour assurer le maintien en conditions de sécurité du système d'information audité.

L'audit organisationnel et physique peut couvrir l'évaluation de la protection des ressources physiques du système d'information audité comme par exemple les systèmes de contrôle d'accès physique, de détection d'intrusions physiques, de vidéoprotection, de prévention des risques naturels (incendie, inondations, etc.).

III. Qualification des prestataires

III.1. Modalités de la qualification

La qualification d'un prestataire est réalisée conformément au processus de qualification d'un service (4) 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 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'audit de la 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'audit de la 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 un ou plusieurs auditeurs respectant les exigences du chapitre V et travaillant pour un prestataire qualifié respectant les exigences du chapitre IV.

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 « [ELEVE] » 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.

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.

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

Les prestataires réalisant des prestations d'audit de la 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 (5).

L'audit de la sécurité des systèmes d'information pour les besoins de la sécurité nationale comprend notamment les contrôles des systèmes d'information d'importance vitale (SIIV) des opérateurs d'importance vitale (OIV) prévus à l'article L1332-6-3 du code de la Défense (6), les audits d'homologation des systèmes d'information d'importance vitale des opérateurs d'importance vitale (OIV) prévus dans l'annexe 4 des arrêtés (7) et les audits des systèmes d'information traitant des informations et supports classifiés FR, UE et OTAN respectivement au titre des instructions (2) (8) (9).

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 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 incorporation d'un auditeur ou d'un responsable d'équipe 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, disposent des connaissances et compétences associées à leurs activités conformément à l'Annexe 2.

c) [ELEVE] Le prestataire ne doit recourir qu'à des auditeurs et responsables d'équipe disposant d'une attestation individuelle de compétence pour réaliser la prestation.

   Le prestataire peut, avec l'accord du commanditaire, incorporer dans l'équipe d'audit 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 auditeurs et responsables d'équipe 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.

e) Le prestataire doit permettre aux auditeurs et responsables d'équipe 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'audit ainsi que de leur bonne utilisation durant la prestation.

g) Le prestataire doit sensibiliser les auditeurs et responsables d'équipe 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'audit ne fait l'objet d'une inscription au casier judiciaire incompatible avec l'exercice de ses missions.

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 (1).

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'audit.

b) Il est recommandé que le prestataire mette en œuvre la méthode (10) pour réaliser l'appréciation et le traitement des risques relatifs à son activité d'audit.

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.

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 audité. 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 audité 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 (11) pour homologuer son 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 (12) 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 (1) sur son système d'information homologué Diffusion Restreinte.

l) [ELEVE] Il est recommandé que le prestataire mette en œuvre les recommandations du guide (13) 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 (12) 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.

V. Exigences applicables aux personnels du prestataire

V.1. Connaissances et compétences générales

a) Les auditeurs et responsables d'équipe doivent maîtriser les bonnes pratiques et la méthodologie d'audit décrites dans la norme (3).

b) Les auditeurs doivent posséder les qualités personnelles décrites au chapitre « 7.2.2 Comportements personnels » de la norme (3).

c) Les responsables d'équipe doivent posséder les qualités personnelles décrites au chapitre « 7.2.3.4 Compétences générale du responsable d'une équipe d'audit » de la norme (3).

d) Les auditeurs et responsables d'équipe 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.).

V.2. Connaissances et compétences spécifiques

a) Les auditeurs et responsables d'équipe doivent, selon leur rôle, réaliser la prestation conformément aux exigences du chapitre VI.

b) Les auditeurs et responsables d'équipe doivent, selon leur rôle, assurer les missions décrites dans l'Annexe 2.

c) Les auditeurs et responsables d'équipe doivent, selon leur rôle, disposer des connaissances et compétences en matière de sécurité des systèmes d'information à jour, particulièrement celles décrites dans l'Annexe 2.

V.3. Expérience

a) Il est recommandé que les auditeurs et responsables d'équipe aient reçu une formation en sécurité des systèmes d'information.

b) Il est recommandé que les auditeurs et responsables d'équipe justifient d'au moins d'une année d'expérience dans le domaine de l'audit de la sécurité des systèmes d'information.

V.4. Engagement

a) Les auditeurs et responsable d'équipe doivent avoir un contrat de travail avec le prestataire.

b) Le prestataire doit avoir un cadre contractuel avec les experts.

VI. Exigences applicables à la prestation

VI.1. Etape 1 – Qualification préalable d'aptitude à la réalisation de la prestation

a) Le prestataire doit, en se fondant sur les informations communiquées par le commanditaire et notamment les objectifs, les critères, le périmètre, les activités d'audit et les éventuelles modalités particulières de la prestation[1], 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.

b) 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.

c) 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 – Elaboration 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 :

a) préciser que la prestation est qualifiée ;

b) identifier le niveau de qualification de la prestation ;

c) identifier les activités d'audit ;

d) inclure l'attestation de qualification du prestataire ;

e) [ELEVE] préciser que chaque auditeur et responsable d'équipe dispose d'une attestation individuelle de compétence ;

f) préciser que le commanditaire peut, conformément au processus de qualification d'un service (4), 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.

[1] Le choix des objectifs, critères, périmètre, activités d'audit 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.

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'audit, ainsi que les modalités de la prestation : prérequis, jalons, livrables, dates et lieux d'exécution de la prestation. Ces informations pourront être précisées et mises à jour si besoin dans la note de cadrage ou dans le plan d'audit ;

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 d'audit ;

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 audité et à la confidentialité de ses données.

VI.2.4. Confidentialité

La convention de service doit :

a) préciser que le prestataire ne collecte et n'audite 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 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'audit un ou plusieurs experts pour participer à la réalisation de certaines activités d'audit lorsque ces dernières requièrent des connaissances ou des compétences spécifiques dont les auditeurs ne disposent pas sous réserve que :
   i. il existe une 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 d'équipe.

VI.2.6. Sous-traitance

La convention de service doit :

a) préciser que le prestataire peut sous-traiter tout ou partie des activités d'audit à un prestataire sous-traitant sous réserve que :
   i. le prestataire sous-traitant est qualifié pour les activités d'audit 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 ;

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 d'équipe.

b) [ELEVE] Le responsable d'équipe doit disposer d'une attestation individuelle de compétence en vigueur.

c) Le responsable d'équipe doit constituer une équipe composée d'auditeurs et, le cas échéant, d'experts disposant de toutes les connaissances et compétences requises pour mener la prestation. Le responsable d'équipe peut, s'il dispose des connaissances et compétences suffisantes, réaliser la prestation seul.

d) Le responsable d'équipe d'audit doit réévaluer régulièrement le profil et le nombre d'auditeurs et, le cas échéant, d'experts afin de s'assurer que l'engagement du prestataire reste adapté à la bonne exécution de la prestation.

e) [ELEVE] Les auditeurs doivent chacun disposer d'une attestation individuelle de compétence en vigueur pour les activités qui leur sont confiées.

VI.3.2. Elaboration de la note de cadrage

a) Le responsable d'équipe doit élaborer la note de cadrage en concertation avec l'équipe d'audit 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'audit, ainsi que les modalités de la prestation : prérequis, jalons, livrables, dates et lieux d'exécution de la prestation, etc. ;

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'audit 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'audit et préciser pour chacun d'eux leur rôle (responsable d'équipe, auditeur ou expert) et les activités d'audit qui leur sont confiées ;

h) [ELEVE] annexer les attestations individuelles de compétence du responsable d'équipe et des auditeurs ;

i) identifier les noms, rôles, et responsabilités des personnes désignées par le commanditaire et intervenant dans le cadre de la prestation ;

j) décrire, le cas échant, 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 sensibilité[2] ;

m) identifier les moyens de protection des informations et supports relatifs à la prestation selon leur niveau de sensibilité et leur marquage[3] ;

[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 d'audit.

[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.

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 audité ;

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 audité ou le commanditaire ;

r) [INTRUSION] identifier le mode des tests d'intrusion : boite noire, boite grise ou boite blanche ;

s) [INTRUSION] identifier les profils d'attaquants à simuler ;

t) être validée par le correspondant de la prestation au sein du commanditaire et par le responsable d'équipe et à chaque mise à jour durant la prestation.

VI.3.3. Mesures de précaution particulières

a) Le responsable d'équipe doit sensibiliser le commanditaire sur les thèmes identifiés en Annexe 3 et notamment :

   i. la mise en place de mesures de sauvegarde du système d'information audité ;

   ii. [INTRUSION] la gestion des risques associés aux tests d'intrusion sur les environnements de production ou mutualisés ;

   iii. [INTRUSION] la mise en place d'une fiche d'autorisation de tests d'intrusion ;

   iv. la mise en place de mesures de sécurité lorsque la prestation nécessite l'installation d'outils ou l'exécution de commandes sur le système audité.

b) Le responsable d'équipe doit obtenir l'accord du commanditaire pour la réalisation de toute action pouvant entraîner un dysfonctionnement voire un déni de service du système d'information audité.

VI.3.4. Elaboration du plan d'audit

a) Le responsable d'équipe doit élaborer le plan d'audit en concertation avec l'équipe d'audit et le correspondant de la prestation au sein du commanditaire.

Le plan d'audit doit décrire :

b) les objectifs, les critères, le périmètre de l'audit et les activités d'audit ;

c) le calendrier de la prestation faisant apparaître les principaux jalons ;

d) le nom du responsable de l'équipe d'audit ;

e) pour chaque des activités d'audit :

i. les noms des auditeurs, et le cas échéant des experts, en charge de la réalisation de l'activité,

ii. les dates et lieux de réalisation de l'activité,

iii. les éventuels prérequis pour la réalisation de l'activité : documents, personnels, etc.,

iv. la méthode d'audit. La méthode d'audit doit être adaptée aux objectifs, critères et périmètre d'audit ainsi qu'aux éventuelles demandes spécifiques formulées par le commanditaire. Elle doit préciser si l'activité d'audit est réalisée de manière exhaustive ou par échantillonnage, et dans ce cas justifier les motifs du choix d'un échantillonnage et préciser la méthode d'échantillonnage : méthode de sélection des échantillons, taille de l'échantillon, etc.

VI.3.5. Réunion d'ouverture

a) Il est recommandé que le responsable d'équipe organise une réunion d'ouverture à laquelle participent a minima le responsable d'équipe, les auditeurs, les experts le cas échéant, le correspondant de la prestation au sein du commanditaire ainsi que les responsables sécurité et métier du système d'information audité afin de confirmer, préalablement à l'exécution de la prestation, leur accord sur l'ensemble des modalités de la prestation, en particulier la note de cadrage et le plan d'audit.

VI.4. Étape 4 – Exécution de la prestation

VI.4.1. Exigences générales

a) Les auditeurs doivent, en adéquation avec les objectifs, critères, périmètre et activités d'audit, évaluer le niveau de conformité et/ou de sécurité du système d'information audité.

b) Les auditeurs doivent, en adoptant une approche par les risques, identifier les composants du système d'information et les documents pertinents à auditer ainsi que les personnes pertinentes à rencontrer.

c) Les auditeurs doivent rendre compte au responsable d'équipe des constats d'audit durant toute la prestation.

VI.4.2. Audit d'architecture

a) [ARCHI] Le prestataire doit être capable, en adéquation avec les objectifs, critères, et périmètre de l'audit, d'évaluer la conformité et/ou la sécurité de l'architecture du système d'information audité en analysant, lorsqu'ils existent, les documents suivants :

i. les documents d'architecture techniques (DAT) ;

ii. les schémas d'architecture de niveau 2 et 3 du modèle OSI ;

iii. les matrices de flux ;

iv. les inventaires des interconnexions avec des réseaux tiers ou Internet.

b) [ARCHI] Le prestataire doit être capable, en adéquation avec les objectifs, critères, et périmètre de l'audit, d'évaluer la configuration des composants du système d'information audité afin d'évaluer la conformité et/ou la sécurité de l'architecture du système d'information audité.

VI.4.3. Audit de configuration

a) [CONF] Le prestataire doit être capable, en adéquation avec les objectifs, critères, et périmètre de l'audit, d'évaluer la conformité et/ou la sécurité des configurations des éléments suivants :

   i. annuaires d'utilisateurs ;
   ii. composants de sécurité physique (UTL, lecteurs de badges, caméras, etc.) ;
   iii. composants réseaux (routeurs, commutateurs, etc.) ;
   iv. composants de sécurité réseaux (pare-feu, chiffreurs, antivirus, etc.) ;
   v. composants de sécurité locaux (antivirus, *Endpoint Detection and Response* (EDR), etc.) ;
   vi. systèmes d'exploitation (serveurs, postes de travail, équipements spécifiques) ;
   vii. applications (métier, base de données, serveurs Web, etc.) ;
   viii. environnements d'informatique en nuage, de conteneurisation et de virtualisation.

VI.4.4. Audit de code source

a) [CODE] Le prestataire doit être capable, en adéquation avec les objectifs, critères, et périmètre de l'audit, d'évaluer la conformité et/ou la sécurité du code source du logiciel audité en analysant, lorsqu'ils existent, les documents relatifs :

   i. aux spécifications du logiciel ;
   ii. à l'architecture du logiciel ;
   iii. à l'implémentation du logiciel ;
   iv. à l'administration du logiciel ;
   v. à l'utilisation du logiciel ;
   vi. aux méthodes et résultats de tests du logiciel.

b) [CODE] Le prestataire doit être capable, en adéquation avec les objectifs, critères, et périmètre de l'audit, d'évaluer la conformité et/ou la sécurité des parties de code source du logiciel audité relatives :

   i. aux mécanismes d'authentification ;
   ii. aux mécanismes cryptographiques ;
   iii. à la gestion des utilisateurs ;
   iv. aux contrôles d'accès aux ressources ;
   v. aux interactions avec d'autres applications ;
   vi. à la validation des données.

VI.4.5. Test d'intrusion

Le test d'intrusion peut être réalisé selon l'un des trois modes :

- boite noire : les auditeurs ne disposent, avant de démarrer le test d'intrusion, d'aucune information sur le système d'information audité à l'exception d'adresses IP, d'URL ou de noms de domaines ;
- boite grise : les auditeurs disposent, avant de démarrer le test d'intrusion, de quelques informations sur le système d'information audité (architecture, etc.) et de privilèges associés aux profils d'utilisateurs légitimes du système d'information retenus comme des attaquants potentiels ;
- boite blanche : les auditeurs disposent, avant de démarrer le test d'intrusion, du maximum d'informations sur le système d'information audité (architecture, code source, configuration, etc.) et de privilèges associés aux profils d'utilisateurs légitimes du système d'information retenus comme des attaquants potentiels.

a) [INTRUSION] Le prestataire doit être capable de réaliser un test d'intrusion selon les trois modes : boite noire, boite grise, boite blanche.

b) [ELEVE] [INTRUSION] Le prestataire doit être capable de simuler des profils d'attaquants disposant de potentiels d'attaque associés à une menace stratégique.

c) [INTRUSION] Le prestataire doit être capable de simuler des profils d'attaquants disposant de potentiels d'attaque associés à une menace systémique, hacktiviste ou isolée.

d) [INTRUSION] Le prestataire ne doit exploiter les vulnérabilités susceptibles de rendre le système d'information audité instable voire provoquer un déni de service qu'avec l'accord écrit du commanditaire ;

e) [INTRUSION] Le prestataire doit, si le test d'intrusion n'est pas, à la demande du commanditaire, réalisé sur l'environnement de production mais sur un autre environnement (test, préproduction, etc.), vérifier que cet environnement est comparable à l'environnement de production, et vérifier que les résultats du test d'intrusion sont applicables à l'environnement de production.

VI.4.6. Audit organisationnel et physique

a) [ORGAPHY] Le prestataire doit, en adéquation avec les objectifs, critères, et périmètre de l'audit, évaluer l'organisation de la sécurité des systèmes d'information.

b) [ORGAPHY] Le prestataire doit être capable d'évaluer l'organisation de la sécurité en analysant, lorsqu'ils existent, les documents suivants :

   i. l'appréciation des risques ;
   ii. la politique de sécurité des systèmes d'information (PSSI) ;
   iii. le dossier d'homologation ;
   iv. le plan de reprise d'activité (PRA) ;
   v. le plan de continuité d'activité (PCA) ;
   vi. le plan d'assurance sécurité (PAS) ;
   vii. le processus de gestion des incidents.

c) [ELEVE] [ORGAPHY] Le prestataire doit être capable d'évaluer la sécurité physique du système d'information audité et notamment les systèmes de :

i. contrôle d'accès physique ;

ii. détection d'intrusions physiques ;

iii. vidéoprotection ;

iv. prévention des risques naturels : incendie, inondations, etc.

VI.5. Étape 5 – Restitution

a) [ELEVE] Le responsable d'équipe doit organiser une restitution dite « à chaud » à la fin de chaque journée afin de présenter au correspondant de la prestation au sein du commanditaire :

i. un état d'avancement de la prestation ;

ii. une synthèse des résultats des activités d'audit de la journée ;

iii. les éventuelles non-conformités et/ou vulnérabilités identifiées au cours de la journée dont l'exploitation pourrait engendrer des risques critiques, les scénarios de menace associés ainsi que les mesures de sécurité recommandées pour traiter ces risques ;

iv. les éventuelles difficultés rencontrées durant la journée : collaboration difficile ou indisponibilité du personnel du commanditaire ou du bénéficiaire, difficulté d'accès aux locaux, au système d'information ou à la documentation, etc.

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

c) [ELEVE] Le responsable d'équipe doit, dès la fin des activités d'audit et sans attendre que le rapport d'audit soit achevé, fournir au commanditaire un support écrit présentant pour chaque non-conformité majeure et/ou vulnérabilité dont l'exploitation pourrait engendrer des risques critiques, les scénarios de menace associés ainsi que les mesures de sécurité recommandées pour traiter ces risques.

VI.6. Étape 6 – Elaboration du rapport

a) Le prestataire doit élaborer un rapport d'audit[4].

VI.6.1. Qualification

Le rapport d'audit doit :

a) préciser que la prestation est qualifiée ;

b) identifier le niveau de qualification de la prestation ;

c) identifier les activités d'audit ;

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

d) identifier les noms et les coordonnées des membres de l'équipe d'audit et préciser pour chacun d'eux leur rôle (responsable d'équipe, auditeur ou expert) et les activités d'audit réalisées.

VI.6.2. Cadre

Le rapport d'audit doit :

a) décrire les objectifs, les critères, le périmètre d'audit ainsi que les éventuelles modalités particulières de la prestation ;

b) identifier les dates et lieux de la prestation ;

c) identifier de manière précise (référence, numéro de version, date, etc.) les documents sur lesquels le prestataire s'est fondé pour réaliser la prestation.

VI.6.3. Synthèse managériale

a) Le rapport d'audit doit présenter une synthèse managériale.

La synthèse managériale doit :

b) être compréhensible par des personnes non expertes en sécurité des systèmes d'information ;

c) fournir une appréciation générale de la conformité et/ou de la sécurité du système d'information audité corrélant les résultats de l'ensemble des activités d'audit ;

d) décrire les risques critiques et les scénarios de menace associés exploitant les non-conformités et/ou vulnérabilités identifiées durant l'audit ainsi que les mesures de sécurité recommandées pour traiter ces risques ;

e) décrire les éventuelles réserves relatives aux résultats de la prestation : inadéquation entre les objectifs, les critères, le périmètre, les activités et la charge, difficultés rencontrées durant la prestation, limite de l'échantillonnage, collaboration difficile ou indisponibilité du personnel du commanditaire ou du bénéficiaire, difficulté d'accès aux locaux, au système d'information ou à la documentation, etc. ;

f) recommander un audit de contrôle afin de vérifier que les mesures de sécurité permettant de traiter les risques critiques ont été correctement mises en œuvre.

VI.6.4. Résultats

Le rapport d'audit doit :

a) identifier de manière unique chaque non-conformité et/ou vulnérabilité identifiée durant l'audit ;

b) fournir, pour chaque non-conformité et/ou vulnérabilité, les preuves d'audit sur lesquelles le constat d'audit est fondé ;

c) décrire chaque non-conformité et identifier la ou les exigences non satisfaites ;

d) décrire chaque vulnérabilité et préciser pour chacune d'elle : les profils d'attaquants, les scénarios d'attaque, les conditions d'exploitation, si une tentative d'exploitation a été réalisée et le résultat de cette tentative.

e) définir, en adéquation avec les objectifs et les critères de l'audit, une échelle de classement de la gravité des non-conformités et/ou vulnérabilités en fonction des risques encourus ;

f) proposer, pour chaque non-conformité et/ou vulnérabilité, un niveau de gravité selon l'échelle de classement définie ;

g) recommander, pour chaque non-conformité et/ou vulnérabilité, une ou plusieurs mesures de sécurité. Ces mesures doivent être proportionnées et adaptées ;

h) définir, en adéquation avec les objectifs et les critères de l'audit, une échelle de classement de la priorité des mesures de sécurité recommandées. Cette échelle doit au minimum prendre en compte les critères suivants : complexité, coût et délai de mise en œuvre de la mesure de sécurité ;

i) proposer, pour chaque mesure de sécurité, un niveau de priorité selon l'échelle de classement définie ;

j) identifier, le cas échéant, les activités d'audit ayant été réalisées en partie de manière automatique ;

k) identifier les noms et fonctions des personnes au sein du commanditaire, du bénéficiaire et des éventuels tiers (sous-traitants, etc.) avec qui le prestataire a interagi pour réaliser la prestation ;

l) Il est recommandé que le rapport d'audit catégorise chaque vulnérabilité selon une nomenclature reconnue.

m) Il est recommandé que le prestataire utilise l'échelle de classement de la gravité des non-conformités et/ou vulnérabilités du commanditaire si ce dernier en dispose d'une.

n) Il est recommandé que le prestataire utilise l'échelle de classement de la priorité des mesures de sécurité du commanditaire si ce dernier en dispose d'une.

VI.6.5. Annexes

Le rapport d'audit doit annexer :

a) le plan d'audit ;

b) la note de cadrage.

VI.7. Étape 7 – Clôture de la prestation

a) Il est recommandé que, suite à la remise du rapport d'audit, le responsable d'équipe organise une réunion de clôture à laquelle participent a minima le responsable d'équipe, les auditeurs, les experts le cas échéant, le correspondant de la prestation au sein du commanditaire, la direction du commanditaire ainsi que les responsables sécurité et métier du système d'information audité. Cette réunion permet de présenter la synthèse du rapport d'audit et de répondre aux éventuelles questions du commanditaire.

b) 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.

c) 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.

d) [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.

Annexe 1 Bibliographie

1. Instruction interministérielle n° 901 relative à la protection des systèmes d'information sensibles, n° 901/SGDSN/ANSSI, version en vigueur. *Disponible sur https://www.legifrance.gouv.fr*.

2. Instruction générale interministérielle n° 1300 sur la protection du secret de la défense nationale, n° 1300/SGDSN/PSE/PSD, version en vigueur. *Disponible sur https://www.legifrance.gouv.fr*.

3. Norme internationale ISO/IEC 19011 : Lignes directrices pour l'audit des systèmes de management, version en vigueur. *Disponible sur https://www.iso.org*.

4. Processus de qualification d'un service, version en vigueur. *Disponible sur https://www.cyber.gouv.fr*.

5. Référentiel d'exigences applicables aux prestataires d'audit de la sécurité des systèmes d'information pour les besoins de la sécurité nationale, version en vigueur. *Document Diffusion Restreinte, il peut être obtenu auprès de l'ANSSI.*

6. Code de la défense. *Disponible sur https://www.legifrance.gouv.fr*.

7. Arrêtés fixant les règles de sécurité et les modalités de déclaration des systèmes d'importance vitale et des incidents de sécurité relatives aux secteurs d'activités d'importance vitale et pris en application des articles R. 1332-41-1, R. 1332-41-10. *du code de la Défense.*

8. Instruction interministérielle n° 2102 sur la protection en France des informations classifiées de l'Union Européenne, n° 2102/SGDSN/PSD, version en vigueur. *Disponible sur https://www.legifrance.gouv.fr*.

9. Instruction interministérielle n° 2100 pour l'application en France du système de sécurité de l'Organisation du traité de l'Atlantique nord, version en vigueur. *Disponible sur https://legifrance.gouv.fr*.

10. Guide - Méthode de gestion de risques EBIOS Risk Manager. *Disponible sur https://www.cyber.gouv.fr*.

11. Guide - L'homologation de sécurité en neuf étapes simples, ANSSI, version en vigueur. *Disponible sur https://cyber.gouv.fr*.

12. *Guide - Guide d'hygiène informatique, ANSSI, version en vigueur.* Disponible sur https://cyber.gouv.fr.

13. Guide - Recommandations pour les architectures des systèmes d'information sensibles ou Diffusion Restreinte – version en vigueur. *Disponible sur https://www.cyber.gouv.fr*.

14. Loi relative à la programmation militaire, version en vigueur. *https://www.legifrance.gouv.fr*.

15. Directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant les mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union. *Disponible sur https://eur-lex.europa.eu*.

16. 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*.

17. Référentiel général de sécurité, version en vigueur. *Disponible sur https://legifrance.gouv.fr.*

18. 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.*

19. 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.*

20. 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.*

21. Guide - Guide d'achat de produits de sécurité et de services de confiance qualifiés, version en vigueur. *Disponible sur https://www.cyber.gouv.fr.*

22. Instruction interministérielle n° 910 relative aux articles contrôlés de la sécurité des systèmes d'information (ACSSI), n°910/SGDSN/ANSSI, version en vigueur. *Disponible sur https://www.legifrance.gouv.fr.*

23. Loi relative à la programmation militaire, version en vigueur. *Disponible sur https://www.legifrance.gouv.fr.*

Annexe 2 Connaissances, compétences et missions des personnels du prestataire

Cette annexe décrit les connaissances, compétences et missions des personnels du prestataire.

Les connaissances de la règlementation citées en chapitre I sont complétées par les missions et compétences spécifiques requises pour chaque profil de personnel décrites aux chapitres suivants de la présente annexe.

Pour être qualifié, le prestataire doit disposer par activité d'audit des profils suivants :

Activité	Profil(s)
ARCHI	Auditeur d'architecture
CONF	Auditeur de configuration
CODE	Auditeur de code source
INTRUSION	Auditeur en tests d'intrusion
ORGAPHY	Auditeur organisationnel et physique

I. Connaissance de la réglementation

Les auditeurs et les responsables d'équipe doivent connaître les réglementations suivantes :

- la protection du secret de la défense nationale (2) ;
- la protection des systèmes d'informations sensibles (1) ;
- la loi de programmation militaire (14) et particulièrement les dispositions applicables aux systèmes d'information d'importance vitale (SIIV) des opérateurs d'importance vitale (OIV) ;
- les directives européennes relatives à la sécurité des réseaux et de l'information (15) et (16) ;
- le référentiel général de sécurité (17) et particulièrement les dispositions applicables aux autorités administratives ;
- le règlement général sur la protection des données (18) ;
- la protection des informations classifiées de l'Organisation du traité de l'Atlantique nord (OTAN) (9) ;
- la protection des informations classifiées de l'Union européenne (UE) (8).

II. Responsable d'équipe

Ce chapitre décrit les missions et compétences du responsable d'équipe.

II.1. Missions

Le responsable d'équipe doit assurer les missions suivantes :

- définir et mettre en œuvre une organisation adaptée aux objectifs, critères, périmètre, et activités d'audit ;
- constituer l'équipe d'audit composée d'auditeurs, et le cas échéant d'experts ;
- piloter et contrôler les activités de l'équipe d'audit ;
- définir et gérer les priorités de la prestation ;
- maintenir à jour un état de la progression de la prestation ;
- fournir une appréciation générale de la conformité et/ou de la sécurité du système d'information audité corrélant les résultats de l'ensemble des activités d'audit ;
- fournir une appréciation générale des risques critiques et des scénarios de menace associés corrélant les résultats de l'ensemble des activités d'audit ;
- fournir des recommandations adaptées pour remédier aux risques critiques identifiés durant la prestation ;
- contrôler la qualité et valider les livrables de la prestation, notamment la note de cadrage, le plan d'audit et le rapport d'audit.

II.2. Compétences

Le responsable d'équipe doit avoir des compétences approfondies dans la plupart des domaines requis pour la prestation.

III. Auditeur d'architecture

Ce chapitre décrit les missions et compétences de l'auditeur d'architecture.

III.1. Missions

L'auditeur doit assurer les missions suivantes :

- adopter une vision globale du système d'information audité, et par une approche par les risques, identifier :
  - les composants pertinents à auditer,
  - les documents pertinents à consulter,
  - les personnels pertinents à rencontrer,
- collecter et auditer les éléments pertinents du système d'information audité ;
- mener les entretiens avec les personnels pertinents ;
- identifier les non-conformités et/ou vulnérabilités dans l'architecture du système d'information audité ;
- identifier les risques et les scénarios de menace associés aux non-conformités et/ou vulnérabilités identifiées ;

- recommander des mesures de sécurité adaptées pour remédier aux non-conformités et/ou vulnérabilités identifiées.

III.2. Compétences

L'auditeur doit disposer de compétences approfondies dans les domaines techniques suivants :

- réseaux et protocoles :
  - protocoles réseau et infrastructures ;
  - protocoles applicatifs courants et services d'infrastructures ;
  - configuration et sécurisation des principaux équipements réseau du marché ;
  - réseaux de télécommunication ;
  - technologies sans fil ;
  - téléphonie.
- équipements et logiciels de sécurité :
  - pare-feu ;
  - chiffreurs ;
  - systèmes de sauvegarde ;
  - systèmes de stockage mutualisé ;
  - serveurs d'authentification ;
  - serveurs mandataires inverses ;
  - solutions de gestion de la journalisation ;
  - équipements de détection et prévention d'intrusion ;
- topologies particulières :
  - informatique en nuage, conteneurisation et virtualisation ;
  - cartographie, inventaires des flux et interconnexions, cloisonnements associés.

Lorsque le système d'information audité est un système industriel, l'auditeur doit en sus disposer des compétences approfondies dans les domaines techniques suivants :

- architectures fonctionnelles à base de PLC ;
- réseaux et protocoles industriels :
  - topologies des réseaux industriels ;
  - cloisonnements des réseaux industriels vis-à-vis des autres systèmes d'information ;
  - protocoles de transmission et de communication utilisés par les automates programmables et équipements industriels (Modbus, S7, EtherNetIP, Profibus, Profinet, OPC (classique et UA), IEC 61850) ;

  - technologies radio et sans fil issues du monde industriel (dont les protocoles s'appuyant sur la norme IEEE 802.15.4) ;
- rôle fonctionnel des différents équipements.

IV. Auditeur de configuration

Ce chapitre décrit les missions et compétences de l'auditeur de configuration.

IV.1. Missions

L'auditeur doit assurer les missions suivantes :

- adopter une vision globale du système d'information audité, et par une approche par les risques, identifier :
  - les composants d'information à auditer,
  - les documents pertinents à consulter,
  - les personnels pertinents à rencontrer ;
- collecter et auditer les éléments pertinents du système d'information audité ;
- mener les entretiens avec les personnels pertinents ;
- identifier les non-conformités et/ou vulnérabilités dans la configuration du système d'information audité ;
- identifier les risques et les scénarios de menace associés aux non-conformités et/ou vulnérabilités identifiées ;
- recommander des mesures de sécurité adaptées pour remédier aux non-conformités et/ou vulnérabilités identifiées.

IV.2. Compétences

L'auditeur doit disposer de compétences approfondies dans les domaines techniques suivants :

- réseaux et protocoles :
  - protocoles réseau et infrastructures ;
  - protocoles applicatifs courants et service d'infrastructure ;
  - configuration et sécurisation des principaux équipements réseau du marché ;
  - réseaux de télécommunication ;
  - technologie sans fil ;
  - téléphonie.
- équipements et logiciels de sécurité :
  - pare-feu ;
  - chiffreurs ;
  - systèmes de sauvegarde ;

  - systèmes de stockage mutualisé ;
  - serveurs d'authentification ;
  - serveurs mandataires inverses ;
  - solutions de gestion de la journalisation ;
  - équipements de détection et prévention d'intrusion ;
  - logiciels de sécurité côté poste client (p. ex. : antivirus, EDR, XDR, SOAR, etc.).
- systèmes d'exploitation (environnement et durcissement) :
  - systèmes Microsoft ;
  - systèmes UNIX/Linux ;
  - systèmes centralisés (basés par exemple sur OS400 ou zOS) ;
  - systèmes nomades et ordiphones (basés sur Android ou iOS) ;
  - solutions de virtualisation.
- couche applicative :
  - applications de type client/serveur ;
  - langages de programmation utilisés pour la configuration (p. ex. : scripts, filtres WMI, etc.) ;
  - mécanismes cryptographiques ;
  - socle applicatif :
    - serveurs web,
    - serveurs d'application,
    - systèmes de gestion de bases de données,
    - progiciels ;
- techniques d'intrusion ;
- topologies particulières :
  - informatique en nuage, conteneurisation et virtualisation ;
  - cloisonnement et défense en profondeur.

Lorsque le système d'information audité est un système industriel, l'auditeur doit en sus disposer des compétences approfondies dans les domaines techniques suivants :

- réseaux et protocoles industriels :
  - protocoles de transmission et de communication utilisés par les automates programmables et équipements industriels (Modbus, S7, EtherNetIP, Profibus, Profinet, OPC (classique et UA), IEC 61850) ;
  - technologies radio et sans fil issues du monde industriel (dont les protocoles s'appuyant sur la norme IEEE 802.15.4) ;
- équipements :

- configuration et sécurisation des principaux automates et équipements industriels du marché.

V. Auditeur de code source

Ce chapitre décrit les missions et compétences de l'auditeur de code source.

V.1. Missions

L'auditeur doit assurer les missions suivantes :

- adopter une vision globale du système d'information audité, et par une approche par les risques, identifier :
  - les composants pertinents du code à audite,
  - les documents pertinents à consulter,
  - les personnels pertinents à rencontrer ;
- collecter et auditer les éléments pertinents du système d'information audité ;
- mener les entretiens avec les personnels pertinents ;
- identifier les non-conformités et/ou vulnérabilités dans le code audité ;
- identifier les risques et les scénarios de menace associés aux non-conformités et/ou vulnérabilités identifiées ;
- recommander des mesures de sécurité adaptées pour remédier aux non-conformités et/ou vulnérabilités identifiées.

V.2. Compétences

L'auditeur de code source doit disposer de compétences approfondies dans les domaines techniques suivants :

- couche applicative :
  - guides et principes de développement sécurité ;
  - architectures applicatives (client/serveur, n-tiers, etc.) ;
  - langages de programmation ;
  - mécanismes cryptographiques ;
  - mécanismes de communication (internes au système et par le réseau) et protocoles associés ;
  - socle applicatif :
    - serveurs web ;
    - serveurs d'application ;
    - systèmes de gestion de bases de données ;
    - progiciels ;
- attaques :

  - principes et méthodes d'intrusion applicatives ;
  - contournement des mesures de sécurité logicielles ;
  - techniques d'exploitation de vulnérabilités et d'élévation de privilèges.
- recherche des vulnérabilités les plus répandues notamment :
  - *cross-site scripting (XSS) ;*
  - injections SQL *(Structured Query Langage) ;*
  - *cross-site request forgery (CSRF) ;*
  - erreurs de logique applicative ;
  - erreurs de gestion mémoire ;
  - exécution de commandes arbitraires ;
  - inclusion de fichiers (locaux ou distants).

Lorsque le système d'information audité est un système industriel, l'auditeur doit en sus disposer des compétences approfondies dans les domaines techniques suivants :

- architectures fonctionnelles à base de PLC ;
- architectures applicatives SCADA (basées ou non sur un progiciel) ;
- architectures applicatives des programmes utilisateurs présents dans les automates programmables industriels ;
- réseaux et protocoles industriels :
  - protocoles de transmission et de communication utilisés par les automates programmables et équipements industriels (Modbus, S7, EtherNetIP, Profibus, Profinet, OPC (classique et UA), IEC 61850).

VI. Auditeur en tests d'intrusion

Ce chapitre décrit les missions et compétences de l'auditeur en tests d'intrusion.

VI.1. Missions

L'auditeur doit assurer les missions suivantes :

- adopter une vision globale du système d'information audité, et par une approche par les risques, identifier :
  - les composants pertinents à attaquer,
  - les documents pertinents à consulter,
  - les personnels pertinents à rencontrer ;
- identifier les vulnérabilités du système d'information audité et, le cas échéant les exploiter ;
- identifier les risques et les scénarios de menace associés aux vulnérabilités identifiées ;
- recommander des mesures de sécurité adaptées pour remédier aux vulnérabilités identifiées.

VI.2. Compétences

L'auditeur doit disposer de compétences approfondies dans les domaines techniques suivants :

- réseaux et protocoles :
    - protocoles réseau et infrastructures ;
    - protocoles applicatifs courants et service d'infrastructure ;
    - configuration et sécurisation des principaux équipements réseau du marché ;
    - réseaux de télécommunication ;
    - technologies sans fil ;
    - téléphonie.
- équipements et logiciels de sécurité :
    - pare-feu ;
    - chiffreurs ;
    - système de sauvegarde ;
    - système de stockage mutualisé ;
    - serveur d'authentification ;
    - serveur mandataire inverse ;
    - solution de gestion de la journalisation ;
    - équipement de détection et prévention d'intrusion ;
    - logiciels de sécurité côté poste client (p. ex. : antivirus, EDR, XDR, SOAR, etc.).
- systèmes d'exploitation :
    - systèmes Microsoft ;
    - systèmes UNIX/Linux ;
    - systèmes centralisés (basés par exemple sur OS400 ou zOS) ;
    - systèmes nomades et ordiphones (basés sur Android et iOS) ;
    - solutions de virtualisation.
- couche applicative :
    - guides et principes de développement sécurité ;
    - applications de type client/serveur ;
    - langages de programmation dans le cadre d'audits de code ;
    - mécanismes cryptographiques ;
    - mécanismes de communication (internes au système et par le réseau) et protocoles associés ;
    - socle applicatif :

- serveurs web ;
- serveurs d'application ;
- systèmes de gestion de bases de données ;
- progiciels.

- attaques :
  - principes et méthodes d'intrusion applicatives ;
  - contournement des mesures de sécurité logicielles ;
  - techniques d'exploitation de vulnérabilités et d'élévation de privilèges.

Lorsque le système d'information audité est un système industriel, l'auditeur doit en sus disposer des compétences approfondies dans les domaines techniques suivants :

- architectures fonctionnelles à base de PLC ;
- réseaux et protocoles industriels :
  - topologies des réseaux industriels ;
  - cloisonnements des réseaux industriels vis-à-vis des autres systèmes d'information ;
  - protocoles de transmission et de communication utilisés par les automates programmables et équipements industriels (Modbus, S7, EtherNetIP, Profibus, Profinet, OPC (classique et UA), IEC 61850) ;
  - technologies radio et sans fil issues du monde industriel (dont les protocoles s'appuyant sur la norme IEEE 802.15.4) ;
- équipements :
  - configuration et sécurisation des principaux automates et équipements industriels du marché.

VII. Auditeur en sécurité organisationnelle et physique

Ce chapitre décrit les missions et compétences de l'auditeur en sécurité organisationnelle et physique.

VII.1. Missions

L'auditeur doit assurer les missions suivantes :

- adopter une vision globale du système d'information audité, et par une approche par les risques, identifier :
  - les composants pertinents du système d'information à auditer,
  - les documents pertinents à consulter,
  - les personnels pertinents à rencontrer,
  - les locaux pertinents à auditer ;
- collecter et auditer les éléments pertinents du système d'information audité ;

- mener les entretiens avec les personnels pertinents ;
- auditer la sécurité des locaux ;
- identifier les non-conformités et/ou vulnérabilité ;
- identifier les risques et les scénarios de menace associés aux non-conformités et/ou vulnérabilités identifiées ;
- recommander des mesures de sécurité adaptées pour remédier aux non-conformités et/ou vulnérabilités identifiées.

VII.2. Compétences

L'auditeur doit disposer de compétences approfondies dans les domaines suivants :

- maîtrise des référentiels techniques :
- maîtrise du cadre normatif :
    - les normes (19) et (20) ;
    - les textes réglementaires relatifs à la sécurité des systèmes d'information, aux audits et aux sujets connexes[16].
- maîtrise des domaines relatifs à l'organisation de la sécurité des systèmes d'information :
    - appréciation des risques ;
    - politique de sécurité des systèmes d'information (PSSI) ;
    - chaines de responsabilités en sécurité des systèmes d'information ;
    - sécurité liée aux ressources humaines ;
    - gestion de l'exploitation et de l'administration du système d'information ;
    - contrôle d'accès logique au système d'information ;
    - développement et maintenance des applications ;
    - gestion des incidents liés à la sécurité de l'information ;
    - gestion du plan de continuité de l'activité ;
    - sécurité physique.
- maîtrise des pratiques liées à l'audit :
    - conduite d'entretien ;
    - visite sur site ;
    - analyse documentaire.

[16] Notamment les règles relatives à la protection de la vie privée, du secret professionnel, des correspondances privées ou des données à caractère personnel, aux atteintes aux intérêts fondamentaux de la nation, au terrorisme, aux atteintes à la confiance publique, à la propriété intellectuelle, à l'usage des moyens de cryptologie, au patrimoine scientifique et technique national.

Lorsque le système d'information audité est un système industriel, l'auditeur doit en sus disposer des compétences approfondies dans les domaines techniques suivants :

- normes de sécurité fonctionnelle telle que l'IEC 61508
- normes spécifiques sur les systèmes d'automatisation et de commande industriel tel que l'IEC 62443 ;
- architectures fonctionnelles à base de PLC ;
- rôles et utilisation des protocoles industriels ;
- connaissance du rôle fonctionnel des différents équipements.

Annexe 3 Recommandations à l'attention des commanditaires

Cette annexe liste les recommandations de l'ANSSI à l'attention des commanditaires de prestations d'audit de la 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 d'un appel d'offres ou d'un contrat en matière d'audit de la sécurité des systèmes d'information.

b) Il est recommandé que le commanditaire utilise le guide (21) pour rédiger le cahier des charges d'un appel d'offres ou d'un contrat en matière d'audit de la 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 indépendance renforcé.

g) Le commanditaire peut, conformément au processus de qualification d'un service (4), 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 (4).

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 d'audit 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 (5).

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 (2).

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) (22).

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) Les audits devraient être les plus exhaustifs possible tout en tenant compte des contraintes temporelles et budgétaires du commanditaire.

Le prestataire doit proposer une charge adaptée aux objectifs, critères, périmètre et activités cependant la charge in fine retenue relève exclusivement du commanditaire. Le prestataire mentionnera dans le rapport d'audit les éventuelles réserves quant à la prestation pouvant avoir un impact sur les résultats de l'audit notamment en cas d'inadéquation entre la charge d'une part et les objectifs, critères, périmètre et activités d'autre part.

o) Afin de réduire la charge de la prestation et donc son coût tout en répondant aux objectifs de la prestation, le prestataire peut proposer au commanditaire de réaliser un échantillonnage en utilisant une approche par les risques.

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) [INTRUSION] Il est recommandé que l'activité de tests d'intrusion ne soit jamais réalisée seule mais toujours complétée des activités d'audit de configuration, d'audit d'architecture et, si besoin, d'audit de code source.

r) [INTRUSION] Il est recommandé, lorsque cela est possible, que les tests d'intrusion soient réalisés sur un environnement de test ou de préproduction plutôt que sur un environnement de production d'éviter les conséquences d'une éventuelle perturbation du système audité.

s) [INTRUSION] Il est recommandé que les tests d'intrusion ne soient pas réalisés sur des environnements mutualisés sauf accord de l'hébergeur et après que les risques aient été évalués et maîtrisés, et que les responsabilités aient été clairement établies.

t) [ARCHI, CONF, CODE] Il est recommandé que les audits d'architecture, de configuration, de code source et organisationnels et physique soient réalisés sur les environnements de production.

u) [INTRUSION] Il est recommandé que le commanditaire exige du prestataire dans la note de cadrage, préalablement à la réalisation d'un test d'intrusion, qu'il élabore une fiche d'autorisation signée par l'audité identifiant notamment : la liste des cibles auditées (adresses IP, noms de domaine, URL, etc.), la liste des adresses IP de provenance des tests d'intrusion, les dates et les heures des tests d'intrusion, et la durée de l'autorisation.

II. Pendant la prestation

a) Il est recommandé que le commanditaire autorise dans la note de cadrage le prestataire à conserver le rapport d'audit à l'issue de la prestation lorsqu'un audit de contrôle destiné à vérifier la correction des non-conformités et/ou vulnérabilités consignées dans le rapport d'audit est envisagé.

b) 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.

c) Il est recommandé que le commanditaire prenne les mesures de sauvegarde du système d'information audité préalablement et au cours de la prestation. Cette démarche doit être réalisée en collaboration avec le prestataire afin de ne pas perturber la prestation.

d) Il est recommandé que le commanditaire informe tout au long de la prestation le prestataire des actions qu'il réalise sur le système d'information audité (opérations d'administration, sauvegarde, restauration, etc.) et qui pourraient affecter la prestation.

e) Il est recommandé que le commanditaire, dès lors que la prestation nécessite l'installation d'un outil ou l'exécution d'une commande sur le système audité, réalise lui-même ces actions ou, à défaut, autorise le prestataire à réaliser ces actions avec des comptes dédiés bénéficiant du principe du moindre privilège et sous la supervision constante du commanditaire.

III. Après la prestation

a) Il est recommandé que le commanditaire fasse appel à une prestation de conseil et d'accompagnement qualifiée réalisée par un prestataire d'accompagnement et de conseil en sécurité des systèmes d'information (PACS) qualifié pour décliner les mesures de sécurité proposées par le prestataire d'audit de la sécurité des systèmes d'information (PASSI) et aider à leur mise en œuvre.

b) Il est recommandé que le commanditaire fasse réaliser un audit de contrôle afin de vérifier que les mesures de sécurité permettant de corriger les non-conformités et/ou vulnérabilités identifiées lors de l'audit ont correctement été appliquées et permettent d'atteindre effectivement le niveau de conformité et/ou de sécurité visé.

   Il est recommandé que l'audit de contrôle soit réalisé dans le cadre d'une prestation d'audit qualifiée réalisée par un prestataire d'audit qualifié et que le prestataire qui réalise l'audit de contrôle soit celui qui a réalisé l'audit initial.