Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Première ministre

Agence nationale de la sécurité des systèmes d'information

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

Référentiel d'exigences

Version 2.1-a du 01/09/2023

HISTORIQUE DES VERSIONS			
DATE	**VERSION**	**EVOLUTION DU DOCUMENT**	**REDACTEUR**
31/10/2011	1.0	*Version publiée pour commentaires.*	ANSSI
24/04/2012	1.1	*Version publiée pour commentaires.*	ANSSI
14/02/2013	2.0	*Première version applicable.* Modifications principales : • Ajout d'une recommandation concernant l'utilisation du Guide d'hygiène informatique de l'ANSSI pour la protection du système d'information du prestataire d'audit au chapitre IV.3. • Ajout de précisions concernant les modalités de qualification au chapitre III.1.	ANSSI
6/10/2015	2.1	Mise à jour. Modifications principales : • Ajout de la référence au décret 2015-350 relatif à la qualification pour les besoins de la sécurité nationale. • Ajout de l'activité d'audit de systèmes industriels.	ANSSI
01/09/2023	2.1-a	*Version pour appel à commentaires.* Modifications principales : • Répartition des exigences dans 2 niveaux d'assurance [ELEVE] et [SUBSTANTIEL]. • Autorisation de qualification sur les seules activités organisationnelles et physique, et tests d'intrusion. • Suppression de la portée système industriel. • Ajout de la notion audit de contrôle. • Allègement des exigences générales. • Allègement des attendus relatifs à la convention de service. • Ajout de la notion de « Note de cadrage ». • Mise à jour des exigences métiers et restructuration en chapitres dédiés (VI.4.7, VI.4.8) des exigences communes à toutes les activités. • Ajout de précisions sur les connaissances règlementaires décrites dans l'Annexe 2.	ANSSI

Les commentaires sur le présent document sont à adresser à :

Agence nationale de la sécurité des systèmes d'information

SGDSN/ANSSI

51 boulevard de La Tour-Maubourg
75700 Paris 07 SP

commentaires-passipdispris@ssi.gouv.fr

SOMMAIRE

I. Introduction

I.1. Présentation générale

I.1.1. Contexte

L'interconnexion croissante des réseaux et les besoins de dématérialisation des processus ou des documents augmentent l'exposition des systèmes d'information aux risques de vol, de modification ou de destruction de données. Ainsi, les points d'interconnexion avec l'extérieur, en particulier les accès Internet associés à la messagerie ou à des téléservices, sont autant d'accès qu'un attaquant peut tenter d'utiliser pour s'introduire et se maintenir au sein même du système d'information, pour dérober, dénaturer ou encore détruire son patrimoine informationnel.

Pour s'en protéger, les organismes doivent, à l'issue d'une démarche de gestion des risques, sécuriser leur système d'information de façon adaptée et proportionnée. Les mesures de sécurité mises en place dans ce but peuvent être de différentes natures : organisationnelles, physiques et techniques. Sur ce dernier volet, la mise en œuvre de produits de sécurité est certes fondamentale, mais elle ne suffit pas : l'absence d'application des mises à jour et des correctifs de sécurité, le maintien de mots de passe faibles ou constructeur, la mauvaise configuration de logiciels ou le non-respect de règles élémentaires de sécurité lors du développement d'un logiciel ou d'une application sont autant de vulnérabilités exploitables par un attaquant.

L'audit est l'un des moyens à disposition de tout organisme pour éprouver et s'assurer du niveau de sécurité de son système d'information. Il permet, en pratique, de mettre en évidence les forces mais surtout les faiblesses et vulnérabilités du système d'information. Ses conclusions permettent d'identifier des axes d'amélioration, de proposer des recommandations et de contribuer ainsi à l'élévation de son niveau de sécurité, en vue, notamment, de son homologation de sécurité.

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) délivrant des prestations d'audit d'architecture, d'audit de configuration, d'audit de code source, de tests d'intrusion, d'audit organisationnel et physique et d'audit des systèmes industriels, ci-après dénommé « le prestataire ».

Il a vocation à permettre la qualification de cette famille de prestataires conformément à la règlementation en vigueur [D_2015_350], selon les modalités décrites au chapitre III.1, et d'identifier un niveau d'assurance de qualification en fonction des risques et des profils d'attaquants. Les niveaux d'assurance couverts par le présent référentiel sont décrits dans le chapitre III.2.

Il permet au commanditaire d'une prestation de disposer de garanties sur la compétence du prestataire et de son personnel, sur la capacité organisationnelle et technique du prestataire à proposer une démarche d'audit conforme aux exigences du présent référentiel, et sur la protection des informations sensibles dont le prestataire aura connaissance au cours de la prestation.

Ce référentiel permet notamment de qualifier les prestataires susceptibles d'intervenir, pour l'audit de système d'information au profit des secteurs d'importance vitale concernés par l'application des règles de sécurité prévue au titre de la loi de programmation militaire [LOI_LPM]. Il peut également être utilisé, à titre de bonnes pratiques, en dehors de tout contexte réglementaire.

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

I.1.3. Structure du présent document

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

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

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

Le chapitre IV présente les exigences relatives aux prestataires.

Le chapitre V présente les exigences relatives aux auditeurs.

Le chapitre VI présente les exigences relatives au déroulement d'une prestation d'audit.

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

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

L'Annexe 3 présente des recommandations à l'intention des commanditaires de prestations d'audit.

L'Annexe 4 présente les prérequis au démarrage de la prestation

L'Annexe 5 propose une échelle de classification des vulnérabilités.

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. Définitions et acronymes

I.3.1. Acronymes

Les acronymes utilisés dans le présent référentiel sont les :

ANSSI	Agence nationale de la sécurité des systèmes d'information
CERT-FR	Centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques[1]
OIV	Opérateur d'importance vitale
PACS	Prestataire d'accompagnement et de conseil en sécurité
PASSI	Prestataire d'audit de la sécurité des systèmes d'information
PDIS	Prestataire de détection d'incidents de sécurité
PRIS	Prestataire de réponse aux incidents de sécurité

[1] http://www.cert.ssi.gouv.fr

I.3.2. Définitions

Les définitions ci-dessous s'appuient sur la norme [ISO19011] et la stratégie nationale pour la sécurité du numérique [STRAT_NUM].

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. Pour les besoins du référentiel, un audit est constitué d'un sous-ensemble des activités d'audit de la sécurité d'un système d'information décrites au chapitre II et des recommandations assorties.

Auditeur - personne réalisant un audit pour le compte d'un prestataire d'audit.

Autorité administrative - sont considérées comme autorités administratives les administrations de l'État, les collectivités territoriales, les établissements publics à caractère administratif, les organismes gérant des régimes de protection sociale relevant du code de la sécurité sociale et du code rural ou mentionnés aux articles L. 223-16 et L. 351-21 du code du travail et les autres organismes chargés de la gestion d'un service public administratif.

Bénéficiaire – entité bénéficiant du service d'audit. Le bénéficiaire de la prestation peut être ou non le commanditaire de la prestation.

Commanditaire - entité faisant appel au service d'audit de la sécurité des systèmes d'information. Le commanditaire de la prestation peut être ou non le bénéficiaire de la prestation.

Constats d'audit - résultats de l'évaluation des preuves d'audit recueillies par rapport aux critères d'audit.

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

Critères d'audit - ensemble des politiques, référentiels, guides, procédures ou exigences déterminées applicables à la sécurité du système d'information audité.

État de l'art - ensemble publiquement accessible de connaissances accumulées, de bonnes pratiques, de technologies et de documents de référence relatifs à la sécurité des systèmes d'information à un instant donné, et d'informations qui en découlent de manière évidente.

Expert - personne physique à laquelle le prestataire peut faire appel. L'expert est reconnu par le responsable de prestation comme ayant une ou plusieurs compétences spécifiques, nécessaires à l'appréhension du périmètre de la prestation et à l'exécution de certaines tâches nécessitant des compétences pointues ou la maitrise d'un domaine d'expertise, hors du périmètre des activités du référentiel, c'est-à-dire non nécessairement détenues par les analystes ou pilotes.

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

Niveau d'assurance – méthode permettant de garantir qu'un prestataire de service satisfait aux exigences de sécurité d'un schéma de qualification spécifique pour lequel il a été évalué. Les critères de différenciation entre les différents niveaux sont définis dans le présent référentiel.

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

Potentiel d'attaque – mesure de l'effort à fournir pour attaquer un service ou un produit, exprimée en termes d'expertise, de ressources et de motivation d'un attaquant. L'annexe B.4 du document [CC_CEM] fournit des indications relatives au calcul d'un potentiel d'attaque.

Prestataire - entité proposant une offre de service d'audit de la sécurité des systèmes d'information conforme au 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 de synthèse élaboré par l'équipe d'audit et remis au commanditaire à l'issue de l'audit. Il présente les résultats de l'audit et en particulier les vulnérabilités découvertes ainsi que les mesures correctives proposées.

Référentiel - le présent document.

Responsable d'équipe - personne responsable de l'audit et de la constitution de l'équipe d'audit, en particulier de la complémentarité de leurs compétences.

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

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

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 ou organisme reconnu comme indépendant du prestataire, du commanditaire et du bénéficiaire.

Vulnérabilité – faiblesse d'un bien ou d'une mesure pouvant être exploitée par une menace ou un groupe de menaces.

II. Activités visées par le référentiel

Ce chapitre présente les différentes activités d'audit traitées dans le présent document et dont les exigences spécifiques associées sont décrites au chapitre VI.

Les activités couvertes par ce référentiel sont les suivantes :

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

Les exigences spécifiques par activité sont identifiées par une mention entre crochets, respectivement [ARCHI], [CONF], [CODE], [PENTEST], [ORGAPHY]. Lorsqu'une exigence vaut pour plusieurs activités sans toutefois être valable pour toutes les activités, celles-ci seront inscrites dans un même crochet, par exemple [ARCHI, CONF].

Une prestation d'audit peut avoir pour objectif d'évaluer un niveau :

- de conformité vis-à-vis d'un ensemble de règles, de bonnes pratiques, de guides, de référentiels, ou de normes ;
- de sécurité afin d'identifier des vulnérabilités.

Une prestation d'audit peut avoir pour objectif d'évaluer un niveau de conformité, de sécurité ou de conformité et de sécurité.

Par ailleurs, chaque activité d'audit est, par principe, associée à la fourniture d'un rapport d'audit regroupant des recommandations et dont la forme et le contenu est décrit au chapitre VI.6.

II.1. Audit d'architecture

L'audit d'architecture consiste en l'évaluation du niveau de conformité et/ou de sécurité des choix, du positionnement et de la mise en œuvre des dispositifs matériels et logiciels déployés dans un système d'information du bénéficiaire afin de satisfaire les besoins en sécurité du périmètre audité. L'audit peut être étendu aux interconnexions avec des réseaux tiers, et notamment Internet.

II.2. Audit de configuration

L'audit de configuration consiste en l'évaluation du niveau de conformité et/ou de sécurité en matière de configuration des dispositifs matériels et logiciels déployés dans un système d'information. Ces dispositifs peuvent notamment être des équipements réseau, des systèmes d'exploitation (serveur ou poste de travail), des applications ou des produits de sécurité.

II.3. Audit de code source

L'audit de code source consiste en l'évaluation du niveau de conformité et/ou de sécurité de tout ou partie du code source ou des conditions de compilation d'une application dans le but d'y découvrir des vulnérabilités ou non-conformités qui pourraient avoir un impact en matière de sécurité. Celles-ci peuvent être :

- liées à de mauvaises pratiques de programmation, par un mauvais usage ou une limitation intrinsèque de la technologie d'implémentation (par exemple dans un programme écrit en C, un dépassement de tampon dû à l'utilisation de fonctions de copie de chaîne de

caractères, une clé secrète laissée en mémoire car sa mise à zéro a été supprimée par le compilateur en raison d'options d'optimisation à la compilation).
- liées à des erreurs et vulnérabilités logiques qui ne peuvent qu'être vérifiées qu'au niveau du code source, propres à une application (par exemple la présence d'information résiduelle de type mot de passe en clair) ou un produit (par exemple sur une carte à puce, le manque de protection contre les injections de fautes).

II.4. Tests d'intrusion

Le principe du test d'intrusion est de découvrir des vulnérabilités sur le système d'information audité et de vérifier leur exploitabilité et leur impact, dans les conditions réelles d'une attaque sur le système d'information, à la place d'un attaquant potentiel. Les vulnérabilités testées peuvent également avoir été identifiées au cours d'autres activités d'audit définies dans ce chapitre.

Cette activité d'audit peut être réalisée soit depuis l'extérieur du système d'information audité (notamment depuis Internet ou le réseau interconnecté d'un tiers), soit depuis l'intérieur.

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

Il est recommandé d'effectuer un audit de type test d'intrusion en complément d'autres activités d'audit (notamment celles présentées au chapitre II de ce présent référentiel) afin d'améliorer l'exhaustivité du contrôle et de démontrer la faisabilité de l'exploitation des failles et vulnérabilités découvertes.

II.5. Audit organisationnel et physique

L'audit organisationnel et physique consiste en l'évaluation du niveau de conformité et/ou de sécurité de la gouvernance, des politiques et procédure de sécurité mises en œuvre pour assurer le maintien en conditions opérationnelles et de sécurité d'une application ou de tout ou partie du système d'information audité.

Cet audit permet d'évaluer conformément aux critères d'audit :

- si celles-ci complètent les mesures techniques mises en place ;
- si celles-ci sont efficacement mises en pratique ;
- si les aspects physiques de la sécurité de l'application ou du système d'information sont correctement couverts.

III. Qualification des prestataires d'audit

III.1. Modalités de la qualification

Le référentiel contient des exigences et des recommandations à destination des prestataires d'audit de la sécurité des systèmes d'information.

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

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 en audit de la sécurité des systèmes d'information. Dans ce cas, le processus de qualification ainsi que les exigences applicables pour obtenir la qualification sont strictement identiques à ceux définis dans le présent référentiel. Le terme « prestataire » désigne donc indifféremment un organisme offrant des prestations d'audit de la sécurité des systèmes d'information pour son propre compte ou pour le compte d'autres organismes.

Les exigences doivent être respectées par les prestataires pour obtenir la qualification souhaitée, conformément au chapitre III. 2.

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.

III.2. Portée de la qualification

Les prestataires d'audit peuvent se faire qualifier selon deux niveaux d'assurance : substantiel et élevé.

Les différences entre les deux niveaux d'assurance sont définies par rapport à :

- la sécurité et à la capacité du prestataire à protéger les informations relatives à ses prestations au travers de ses moyens informatiques et de sa gouvernance ;
- l'efficacité métier du prestataire, c'est-à-dire le niveau de profondeur de l'activité et les méthodes employées durant la prestation ;
- la méthode d'évaluation pour l'obtention de la qualification.

Les deux niveaux d'assurance visés par le référentiel sont les suivants :

- le niveau d'assurance élevé. Le service délivré par le prestataire vise à résister et répondre à des attaques de potentiel élevé, modéré et élémentaire amélioré (respectivement « *high* », « *moderate* », « *enhanced basic*», voir [CC_CEM]) ;
- le niveau d'assurance substantiel. Le service délivré par le prestataire vise à résister et répondre à des attaques de potentiel élémentaire (« *basic* »).

Pour être qualifié, un prestataire doit répondre à toutes les exigences du présent référentiel sur la portée choisie, aux exceptions suivantes :

- les exigences et recommandations identifiées par le préfixe [SUBSTANTIEL] ne sont applicables que pour le niveau d'assurance substantiel ;
- les exigences et recommandations identifiées par le préfixe [ELEVE] ne sont applicables que pour le niveau d'assurance élevé.

Les exigences de niveau d'assurance [ELEVE] sont par défaut des recommandations pour le niveau d'assurance [SUBSTANTIEL].

La qualification de niveau élevé permet d'attester de l'aptitude du prestataire à effectuer des prestations de niveau d'assurance [ELEVE] et [SUBSTANTIEL].

Si un prestataire demande la qualification pour un niveau d'assurance donné, l'ensemble des activités d'audit devront répondre au même niveau d'assurance : il n'est pas possible de se faire qualifier sur un niveau d'assurance sur une activité et sur un autre niveau d'assurance pour une autre activité.

Le tableau ci-dessous illustre les cibles pour chacun des deux niveaux d'assurance. Ce tableau est fourni à titre indicatif, le choix du prestataire qualifié, ainsi que du ou des types de prestations est de responsabilité du commanditaire.

Typologie de menaces	**Potentiel d'attaque permettant de mesurer l'effort à fournir pour attaquer une entité**	**Niveau de prestataire et prestation cible[2]**
Menace de niveau stratégique : cyberattaques ciblées, menées ou financées par une entité aux ressources importantes (ex : Etats) possédant des aptitudes solides. **Exemples de motivations** : espionnage, déstabilisation, sabotage. **Exemples de types de cyberattaques** : pré-positionnement, attaques par chaîne d'approvisionnement.	Potentiel d'attaque élevé (« *high* »), modéré (« *moderate* ») (voir [CC_CEM])	Prestataire et prestation de niveau d'assurance élevé
Menace cybercriminelle et de masse : cyberattaques opportunistes menées par une entité aux ressources limitées et aux aptitudes solides. **Exemples de motivations** : divulgation et revente de données. **Exemples de types d'attaque** : rançongiciel.	Potentiel d'attaque élémentaire amélioré (« *enhanced basic* ») (voir [CC_CEM])	Prestataire et prestation de niveau d'assurance élevé
Menace isolée : attaques menées par un individu isolé, un hacktiviste, ou une entité aux ressources limitées, ayant ou non des aptitudes solides. **Exemples de motivations** : vengeance, déstabilisation, recherche non régulée.	Potentiel d'attaque élémentaire (« *basic* ») (voir [CC_CEM])	Prestataire et prestation de niveau d'assurance substantiel

[2] Si le bénéficiaire est soumis à plusieurs typologies de menaces différentes, il est recommandé à ce qu'il recourt à des prestations qualifiées de niveau d'assurance [ELEVE].

Exemples de types d'attaques : déni de service, attaques avec outils automatisés.		

Tout bénéficiaire soumis à des obligations afférentes à la loi de programmation militaire [LOI_LPM] doit faire appel dans ce cadre, à un prestataire de niveau d'assurance [ELEVE] et possédant la mention LPM. Pour obtenir cette mention, le prestataire de niveau élevé doit en plus des exigences du présent référentiel, répondre aux exigences supplémentaires définies dans [PASSI_LPM].

Dans le cas où le bénéficiaire de la prestation n'est soumis à aucune obligation règlementaire, le choix du niveau ainsi que du prestataire est de la responsabilité du commanditaire. Ce choix doit notamment découler d'une analyse de risques permettant d'identifier le niveau de menace auquel il est soumis.

Le prestataire peut demander la qualification pour tout ou partie des activités d'audit décrites au chapitre II. Toutefois, la qualification d'un prestataire d'audit portant sur les seules activités de tests d'intrusion ou d'audit organisationnel et physique n'est pas recommandée, de telles activités pouvant ne pas être exhaustives si elles sont menées seules.

Est considérée comme une prestation qualifiée au sens du référentiel, une prestation respectant la démarche décrite au chapitre VI, dont les activités sont réalisées par un ou plusieurs auditeurs respectant les attendus du chapitre V et de l'Annexe 2 et travaillant pour un prestataire qualifié respectant les exigences du chapitre IV. Pour le niveau d'assurance [ELEVE], les auditeurs ont été évalués individuellement et disposent d'attestation de compétence pour la ou les activités effectuées durant la prestation.

Est considérée comme une prestation qualifiée au sens de la loi de programmation militaire [LPM], une prestation qualifiée au sens du référentiel et respectant les exigences supplémentaires définies dans [PASSI_LPM].

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

Les prestataires peuvent également demander la qualification pour l'audit des systèmes industriels. Dans ce cas, ils doivent être qualifiés sur les activités d'audit d'architecture, d'audit de configuration, d'audit organisationnel et physique et disposer de compétences d'audit de systèmes industriels (voir Annexe 2).

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

III.3. Avertissement

Une prestation d'audit de la sécurité des systèmes d'information non qualifiée, c'est-à-dire ne respectant pas intégralement les exigences du présent référentiel sur la portée de qualification faisant l'objet de la prestation, peut potentiellement exposer le commanditaire ou le bénéficiaire à certains risques et notamment la fuite d'informations confidentielles, la compromission, la perte ou l'indisponibilité de son système d'information. La qualification d'un prestataire et la mise en œuvre d'une prestation qualifiée permettent de réduire ces risques sur le périmètre de la prestation.

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

IV. Exigences relatives au prestataire d'audit

IV.1. Exigences générales

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

   Une autorité administrative qui réalise des activités d'audit peut être considérée comme un prestataire d'audit quand elle réalise tout ou partie de ces activités pour le compte d'autres entités juridiques.

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

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

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

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

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

   Lorsque le prestataire est amené à effectuer une prestation d'audit qualifiée (au travers de la qualification PASSI) après une prestation d'accompagnement et de conseil qualifiée (au travers de la qualification PACS), dans une temporalité d'un an, les personnes physiques mobilisées doivent être différentes entre les deux prestations. Les exigences de ce référentiel portant sur le personnel restent applicables.

g) Le prestataire doit informer le commanditaire lorsque ce dernier est tenu de déclarer un incident de sécurité à une instance gouvernementales (par exemple dans le cadre de la loi de programmation militaire ou de la directive NIS[3]) et doit l'accompagner dans cette démarche si ce dernier en fait la demande.

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

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

[3] Directive *Network Information Security*, résultant de la coopération entre les Etats membres de l'Union Européenne et portant sur les aspects politiques et opérationnels de la cybersécurité.

IV.2. Gestion des ressources et des compétences

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

b) Le prestataire doit s'assurer du maintien à jour des compétences des auditeurs dans les types d'audits pour lesquelles ils ont obtenu une attestation individuelle de compétence[7]. Pour cela, le prestataire doit disposer d'un processus de formation continue et permettre à ses auditeurs d'assurer une veille technologique[5].

c) Le prestataire doit, au moment du recrutement, procéder à une vérification, sauf impossibilité tracée, des formations, compétences et références professionnelles des auditeurs, et de la véracité de leur *curriculum vitae*.

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

e) Le prestataire doit justifier, au travers de son recrutement, qu'il dispose des compétences techniques, théoriques et pratiques, afférentes aux activités d'audit citées en Annexe 2.

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

g) Le prestataire doit s'assurer que les auditeurs ne font pas l'objet d'une inscription, qui n'est pas compatible avec l'exercice de leurs fonctions, au bulletin n°3 du casier judiciaire français ou extrait de casier judiciaire étranger pour les candidats résidant hors du territoire français.

IV.3. Protection de l'information

Le prestataire peut traiter tout ou partie des informations relatives à la prestation sur ses systèmes d'information, ceux du commanditaire ou du bénéficiaire.

Note : Pour le niveau d'assurance [ELEVE], le prestataire doit, dans tous les cas, disposer d'un système d'information homologué Diffusion Restreinte. Lorsque le prestataire doit traiter sur ses systèmes d'information des informations non classifiées de défense et ne portant pas la mention Diffusion Restreinte, il peut choisir de (1) les traiter sur son système d'information homologué Diffusion Restreinte ou (2) les traiter sur un système d'information non homologué Diffusion Restreinte. Dans ce derniers cas, le prestataire dispose alors de deux systèmes d'information, l'un homologué Diffusion Restreinte et l'autre non.

Les exigences énoncées dans ce chapitre s'appliquent aux systèmes d'information du prestataire, et sauf mention contraire, homologués Diffusion Restreinte ou non.

[4] Voir [PROCESS_QUALIF].

[5] Le prestataire peut par exemple mettre en place une formation continue, des modules d'auto-formation, des séminaires internes, s'abonner à des revues spécialisées, contracter avec un ou plusieurs CERT (*Computer Emergency Response Team*) / CSIRT (*Computer Security Incident Response Team*), disposer d'un accès à une ou plusieurs bases de vulnérabilités offrant un certain niveau de garantie en matière de couverture et de réactivité ou toute autre méthode lui permettant d'assurer l'évolutivité de ses compétences ainsi que celles de son personnel.

a) Le prestataire a un devoir de conseil vis-à-vis du commanditaire et doit lui proposer un marquage adapté des informations et supports relatifs à la prestation selon leur niveau de sensibilité, ainsi que les moyens de protection associés[6].

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

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

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

e) Le prestataire doit homologuer la sécurité de son système d'information.

f) [ELEVE] Le prestataire doit disposer d'un système d'information homologué pour la protection des informations portant la mention Diffusion Restreinte [II_901], [IGI_1300].

g) Il est recommandé que le prestataire mette en œuvre la démarche décrite dans le guide pour homologuer son système d'information.

h) Le prestataire doit, s'il dispose d'un système d'information homologué Diffusion Restreinte, respecter les règles relatives à la protection des systèmes d'information traitant des informations portant la mention Diffusion Restreinte définies dans [II_901], [IGI_1300].

i) Le prestataire doit, s'il dispose d'un système d'information homologué Diffusion Restreinte, mettre en œuvre sur celui-ci les règles du niveau renforcé du guide d'hygiène informatique [G_HYGIENE], et le cas échéant, mettre en œuvre les règles du niveau standard pour son système d'information non homologué Diffusion Restreinte.

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

k) Le prestataire doit disposer de moyens maîtrisés et déconnectés, c'est-à-dire, qui ne soient connectés à quelconque réseau :

   i. pour l'archivage des rapports d'audit ;

   ii. pour la consultation de l'archivage.

   Le niveau d'homologation et de protection de ces moyens doit correspondre au niveau de sensibilité [II_901] ou de classification [IGI_1300] des éléments archivés. Des mesures de sécurité doivent être mises en place pour couvrir le risque de vol, de perte et de piégeage de ces équipements.

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

V. Exigences relatives aux auditeurs

V.1. Aptitudes générales

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

b) Les auditeurs doivent disposer des qualités personnelles décrites au chapitre 7.2.2 de la norme ISO 19011.

c) Les auditeurs doivent disposer de qualités rédactionnelles et de synthèse et savoir s'exprimer à l'oral de façon claire et compréhensible.

d) Les auditeurs doivent régulièrement mettre à jour leurs compétences conformément aux processus de formation et de veille du prestataire (voir chapitre IV.2), par une veille active sur la méthodologie, les techniques et les outils utilisés dans le cadre de ses missions.

   [ELEVE] Il est recommandé que les auditeurs contribuent à l'évolution de l'état de l'art par une participation à des évènements professionnels de son domaine de compétence, à des travaux de recherche ou la publication d'articles.

V.2. Expérience

a) Il est recommandé que les auditeurs aient reçu une formation en technologies des systèmes d'information.

b) Il est recommandé que les auditeurs justifient :

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

Ces recommandations ne sont pas cumulatives.

V.3. Aptitudes et connaissances spécifiques aux activités d'audit

a) Les auditeurs doivent maîtriser les bonnes pratiques et la méthodologie d'audit décrite dans la norme [ISO19011].

b) Les auditeurs doivent réaliser la prestation conformément aux exigences du chapitre VI.

c) Les auditeurs doivent assurer les missions selon son profil, telles que définies dans l'Annexe 2.

d) Les auditeurs doivent disposer des compétences requises par le profil cible, telles que définies dans l'Annexe 2.

e) Il est recommandé que les auditeurs soient sensibilisés à l'ensemble des autres activités d'audit pour lesquelles le prestataire demande la qualification.

V.4. Engagements

a) Les auditeurs doivent avoir un contrat avec le prestataire.

VI. Exigences relatives au déroulement d'une prestation d'audit

La définition du périmètre de la prestation et la description de la prestation attendue, formulées généralement dans un appel d'offres, sont du ressort du commanditaire. L'Annexe 3 du référentiel fournit des recommandations de l'ANSSI à cet effet.

Bien que le prestataire ne puisse qu'adapter et moduler sa proposition de service à la demande, il doit informer, dans la mesure du possible, et à titre de conseil, le commanditaire des recommandations issues de l'Annexe 3.

Le prestataire s'assure que le commanditaire lui fournit un environnement de travail adapté à ses missions.

Le prestataire vérifie que le commanditaire a identifié correctement le système audité ainsi que ses dépendances externes.

Le prestataire s'assure que la prestation est adaptée au contexte et aux objectifs souhaités par le commanditaire.

A défaut, le prestataire en informe le commanditaire préalablement à la prestation.

Dans la suite de ce chapitre, les exigences auxquelles doivent se conformer les prestataires sont regroupées dans les différentes étapes du déroulement d'un audit, à savoir :

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

D'une manière générale, le déroulement de l'audit doit respecter les dispositions de la norme ISO 19011.

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

a) [ELEVE] Le prestataire doit vérifier que le commanditaire a identifié correctement le périmètre de la prestation. En particulier, le prestataire doit s'assurer que les composantes du périmètre sont identifiées avec un niveau de précision suffisant, sans ambiguïté et sont à la fois pertinentes et complètes relativement à l'objectif de la prestation.

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

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

d) Il est recommandé que le prestataire demande au commanditaire de lui fournir les informations de contexte sur la prestation à mener, notamment celle identifiées dans l'Annexe 4.

e) Le prestataire doit informer le commanditaire des résultats de la qualification préalable d'aptitude à la réalisation de la prestation. Il doit notamment indiquer sa capacité à répondre totalement, partiellement ou non à la prestation. Le cas échéant, le prestataire a un devoir de conseil sur la redirection du commanditaire vers les entités adaptées pour répondre à ses besoins (par exemple autres types de prestataires qualifiés, prise d'un prestataire de niveau d'assurance [ELEVE], etc.).

VI.2. Étape 2 – Etablissement de la convention

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

b) La convention de service doit être signée par le prestataire et le commanditaire. Elle doit être signée par des représentants légaux ou toute personne pouvant engager le prestataire et le commanditaire. Dans le cas où le commanditaire n'est pas le bénéficiaire de la prestation, celui-ci atteste de l'accord du bénéficiaire pour démarrer la prestation. Toute modification de la convention de service doit être soumise à l'acceptation du commanditaire.

VI.2.1. Modalités de la prestation

La convention de service doit :

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

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

c) décrire le périmètre de la prestation, la démarche générale d'audit de la sécurité des système d'information, les activité et les modalités de la prestations (objectifs, jalons, livrables attendus en entrée, prérequis, etc) le lieu d'exécution de la prestation (pays) ;

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

e) préciser que le prestataire peut faire intervenir un expert pour la réalisation de certaines activités de la prestation au motif que certaines compétences spécifiques nécessaires ne sont couvertes par les auditeurs, sous réserves que :

   i. il existe une convention ou un cadre contractuel documenté entre le prestataire et l'expert ;

   ii. le recours est connu et formellement accepté par écrit par le commanditaire ;

   iii. l'expert est dûment encadré par le responsable d'équipe de la prestation.

   L'expert ne se substitue pas à un auditeur, ce dernier disposant ou non d'une attestation de compétence.

f) préciser les prérequis attendus en entrée du commanditaire. Il est recommandé d'utiliser l'Annexe 4 ;

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

h) spécifier que le prestataire ne recourt pas à des auditeurs n'ayant pas de relation contractuelle avec lui, n'ayant pas obtenu une attestation individuelle de compétence ou ayant fait l'objet

d'une inscription au bulletin n°3 du casier judiciaire français ou extrait de casier judiciaire étranger pour les candidats résidant hors du territoire français.

VI.2.2. Responsabilités

La convention de service doit :

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

b) spécifier que le commanditaire dispose de l'ensemble des droits de propriété et d'accès sur le périmètre de la prestation (systèmes d'information, supports matériels, etc.) ou qu'il a recueilli l'accord des éventuels parties impliquées, et notamment de ses prestataires ou partenaires, dont les systèmes d'information entrent dans le périmètre de la prestation.

VI.2.3. Confidentialité

La convention de service doit :

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

b) indiquer que le prestataire met en place une liste des informations transmises aux tiers autorisés ; cette dernière précise pour chaque information le tiers auquel elle a été transmise. Cette liste est maintenue à jour et mise à disposition du commanditaire lorsque ce dernier en fait la demande.

c) reprendre les modalités suivantes de partage à un tiers d'informations relatives à la prestation :

   - les informations partagées à un tiers doivent être protégées en confidentialité, conformément à leur niveau de sensibilité, de classification, et à leurs modalités de diffusion et d'utilisation. Elles peuvent si besoin être anonymisées et décontextualisées ;
   - le prestataire propose au bénéficiaire de partager ces informations au CERT-FR

d) indiquer que le prestataire détruit l'ensemble des informations relatives à la prestation à l'issue de celle-ci ou à la date d'échéance de la durée de conservation, au premier terme échu, à l'exception de celles pour lesquelles il a reçu une autorisation de conservation de la part du commanditaire. Le cas échéant les modalités de conservations (par exemple anonymisation, décontextualisation, durée) doivent être approuvées par le commanditaire.

   Le rapport d'audit fait figure d'exception et doit être conservé par défaut par le prestataire sur les moyens d'archivages dédiés (voir exigence IV.3.k) sauf refus formel du commanditaire ou du bénéficiaire de la prestation. Le cas échéant, le responsable d'équipe produit un procès-verbal de destruction de ces données qu'il remet au commanditaire et précisant les données détruites et leur mode de destruction.

VI.2.4. Sous-traitance

La convention de service doit :

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

   i. il existe un cadre contractuel documenté entre le prestataire et son sous-traitant ;

ii. le recours à la sous-traitance est connu et formellement accepté par écrit par le commanditaire ;

iii. le sous-traitant respecte les exigences du référentiel sur l'activité cible.

VI.2.5. Note de cadrage

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

b) La note de cadrage doit être validée par le correspondant[7] de la prestation chez le commanditaire et le responsable d'équipe chez le prestataire au début de la prestation et à chaque modification durant la prestation.

c) La note de cadrage doit :

i. préciser le nom du correspondant de la prestation chez le bénéficiaire ;

ii. identifier le marquage des informations et supports relatifs à la prestation selon leur niveau de sensibilité, ainsi que les moyens de protection associés ;

iii. préciser les modalités relatives aux livrables de la prestation (contenu, forme, langue, etc.) ;

iv. identifier le nom du correspondant de la prestation chez le commanditaire ;

v. identifier les noms, rôles, responsabilités ainsi que les droits et besoin d'en connaître des personnes désignées par le prestataire et le commanditaire ;

vi. le cas échant, prévoir et prendre en compte les modalités de collaboration avec les tiers (sous-traitants, etc.) ;

vii. spécifier les instances de gouvernance de la prestation mises en place et leur fréquence de réunion (réunions de suivi, réunions d'ouverture[8] ou de clôture[9], etc.) ;

viii. identifier les éventuelles exigences légales et réglementaires spécifiques auxquelles est soumis le système d'information cible ;

ix. identifier les éventuelles exigences légales et réglementaires spécifiques auxquelles est soumis le commanditaire.

VI.3. Étape 3 – Préparation et déclenchement de la prestation

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

b) Le responsable d'équipe doit constituer une équipe d'auditeurs ayant les compétences adaptées à la nature de l'audit. Le responsable d'équipe peut, s'il dispose des compétences suffisantes, réaliser l'audit lui-même et seul.

c) Le responsable d'équipe doit, dès le début de la préparation de l'audit, établir un contact avec le bénéficiaire. Ce contact, formel ou informel, a notamment pour objectif de mettre en place

[7] Le correspondant de la prestation chez le commanditaire est la personne chargée de la gestion des relations avec le prestataire et des modalités de réalisation des activités.

[8] Les réunions d'ouverture peuvent permettre notamment aux parties engagées de confirmer leurs accords sur l'ensemble des modalités de la prestation.

[9] Les réunions de clôtures peuvent permettre de présenter la synthèse du rapport d'audit et la suite à donner à la prestation, par exemple la tenue d'un audit de contrôle (voir chapitre VI.7).

les circuits de communication et de décision et de préciser les modalités d'exécution de la prestation. Le responsable d'équipe doit également obtenir la liste des points de contact nécessaires à la réalisation de la prestation.

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

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

f) Les objectifs, le champ, les critères et le planning de l'audit doivent être définis entre le prestataire et le commanditaire, le niveau à atteindre en matière de sécurité et/ou de conformité, en considération des contraintes d'exploitation du système d'information du bénéficiaire. Ces éléments doivent figurer dans la convention d'audit ou dans le plan d'audit.

g) En fonction de l'activité d'audit, l'équipe d'auditeurs doit obtenir, au préalable, toute la documentation existante du bénéficiaire (exemples : politique de sécurité, analyse des risques, procédures d'exploitation de la sécurité, etc.), relative à la cible auditée dans l'objectif d'en faire une revue.

h) L'audit ne doit débuter qu'après une réunion formelle au cours de laquelle les représentants habilités du prestataire et ceux de l'audité confirment leur accord sur l'ensemble des modalités de la prestation. Cette réunion peut être téléphonique mais doit, dans ce cas, faire l'objet d'une confirmation écrite.

i) Le prestataire doit sensibiliser avant l'audit son client sur l'intérêt de sauvegarder et préserver les données, applications et systèmes présents sur les machines auditées.

j) [PENTEST] En préalable, et dans le cas spécifique des tests d'intrusion, une fiche d'autorisation doit être signée par le commanditaire, l'audité et d'éventuelles tierces parties. Elle précise en particulier :

   - la liste des cibles auditées (adresses IP, noms de domaine, etc.) ;
   - la liste des adresses IP de provenance des tests ;
   - la date et les heures exclusives des tests ;
   - la durée de l'autorisation.

VI.4. Étape 4 – Exécution de la prestation

VI.4.1. Méthodologie et précautions

a) Le prestataire doit évaluer le niveau de conformité et/ou de sécurité attendu dans le cadre de l'audit selon les critères d'audit et les risques encourus par le périmètre audité.

b) Le prestataire doit réaliser l'audit dans le respect des personnels et des infrastructures physiques et logiques du bénéficiaire.

c) Le prestataire doit émettre des constatations et observations factuelles, et basées sur la preuve.

d) Le prestataire doit proposer une méthode à employer durant l'audit selon les critères d'audit et les risques encourus, comprenant les approches suivantes :

   i. échantillonnage (le cas échéant, le périmètre de l'échantillonnage doit être justifié) ou exhaustif ;

   ii. revue documentaire et/ou revue technique ;

   iii. moyens de réalisation (méthodes d'extractions, utilisation d'outils automatisés, audit en boîte noire/blanche/grise pour le test d'intrusion).

   Le prestataire doit justifier de la méthode proposée initialement dans le rapport et les risques et limites éventuelles du non-respect de cette proposition. Ces éléments doivent apparaitre dans le rapport d'audit. Le choix définitif de la méthode appartient au commanditaire.

e) Dès lors que l'audit implique une action sur le système audité (extraction de données, revue technique, etc.), le prestataire doit recommander au commanditaire l'utilisation de ses propres moyens (ou ceux du bénéficiaire). Si cette situation n'est pas réalisable, le prestataire doit mettre en œuvre des mesures de protection et de prévention des mauvaises manipulations afin de limiter les impacts de l'audit.

f) [ELEVE] Durant toute la durée de l'audit, le prestataire doit tracer toutes modifications effectuées sur le périmètre du bénéficiaire.

g) Les constats d'audit doivent être documentés, tracés, et conservés par le prestataire durant toute la durée de l'audit.

h) [ELEVE] Le prestataire doit tracer les actions et résultats des auditeurs sur le périmètre audité, ainsi que leurs dates de réalisation. Ces traces peuvent par exemple servir à identifier les causes d'un incident technique survenu lors de l'audit.

i) En fin d'audit, le système d'information concerné doit retrouver un état dont la sécurité n'est pas dégradée par rapport à l'état initial.

VI.4.2. Audit d'architecture

a) [ARCHI] Le prestataire doit évaluer au minimum des documents suivants, lorsqu'ils existent :

   i. schémas d'architectures de niveau 2 et 3 du modèle OSI ;

   ii. matrices de flux ;

   iii. règles de filtrage ;

   iv. configuration des équipements réseau (routeurs et commutateurs) ;

   v. inventaires des interconnexions avec des réseaux tiers ou Internet ;

   vi. documents d'architecture technique liés à la cible.

[ELEVE] Lorsque ces documents n'existent pas, les recommandations émises par le prestataire doivent prendre en compte l'inexistence de ces documents et identifier les risques associés.

b) [ELEVE] [ARCHI] Par défaut, sauf indication contraire du commanditaire, l'audit doit au minimum être effectuée :

   i. sur les équipement (s) assurant la sécurité périmétrique ;

ii. sur les équipement(s) assurant les mécanismes d'authentification ;

iii. sur les équipement(s) assurant les fonctions principales d'administration du système d'information audité.

VI.4.3. Audit de configuration

Les éléments de configuration des cibles peuvent être récupérés manuellement ou automatiquement, à partir d'un accès sur les cibles auditées, sous la forme de fichiers de configuration ou de captures d'écran. Il est recommandé à ce que ce soit le bénéficiaire de la prestation qui effectue cette tâche, au travers de moyens dédiés.

a) [CONF] Le prestataire doit être capable d'évaluer les configurations :

   i. des équipements de sécurité type chiffreurs, pare-feu ou relais inverse (filtrant ou non) et leurs règles de filtrage, etc. ;

   ii. des systèmes d'exploitation (serveurs, postes de travail, équipement spécifiques) ;

   iii. des équipements réseau de type commutateurs ou routeurs ;

   iv. [ELEVE] des environnements de virtualisation.

   [ELEVE] Il est recommandé en complément que le prestataire soit capable d'évaluer les configurations d'équipements de téléphonie, de services d'infrastructures, de systèmes de gestion de bases de données, des applications métiers.

b) [ELEVE] Le prestataire doit organiser des entretiens avec le personnel concerné par la mise en place et l'administration de la cible auditée, notamment en ce qui concerne les standards de configuration.

VI.4.4. Audit de code source

Le code source, la documentation relative à la mise en œuvre, les méthodes et rapports de tests et l'architecture du composant ou logiciel audité doivent être fournis au prestataire ainsi que la configuration des éléments de compilation et d'exécution, dans les limites des droits dont disposent le commanditaire et le bénéficiaire.

L'audit de code source doit notamment permettre d'éviter les fuites d'information et les altérations du fonctionnement du système d'information.

Les audits de code source peuvent être réalisés manuellement ou automatiquement par des outils spécialisés.

a) [CODE] Le prestataire doit être capable d'évaluer le niveau de conformité et/ou de sécurité des parties de code relatives :

   i. aux mécanismes d'authentification

   ii. aux mécanismes cryptographiques ;

   iii. à la gestion des utilisateurs ;

   iv. [ELEVE] aux contrôles d'accès aux ressources ;

   v. [ELEVE] aux interactions avec d'autres applications ;

   vi. [ELEVE] aux relations avec les systèmes de gestion de bases de données.

b) [ELEVE] [CODE] Le prestataire doit être capable de rechercher les vulnérabilités les plus répandues dans les domaines suivants : *cross-site scripting*, injections SQL, *cross-site request*

forgery, erreurs de logique applicative, erreur de gestion mémoire, exécution de commandes arbitraires, inclusion de fichiers (locaux ou distants).

c) [ELEVE] [CODE] Le prestataire doit orienter le bénéficiaire sur les parties de code, code source, documentations, méthodes, rapports de tests et éléments d'architecture pertinentes pour répondre aux objectifs et critères d'audit conformément à la méthode employée (voir exigence VI.4.1.d).

d) [ELEVE] [CODE] Le prestataire doit effectuer préalablement à l'audit de code, une analyse de la sécurité de l'application auditée afin d'ajuster le périmètre de l'audit, notamment en identifiant les parties critiques de son code.

e) [ELEVE] [CODE] Par défaut, sauf indication contraire du commanditaire, le prestataire doit évaluer au minimum les parties de codes relatives :

   i. aux mécanismes d'authentification ;

   ii. aux mécanismes cryptographiques ;

   iii. à la gestion des utilisateurs ;

   iv. aux exigences de sécurité relative à l'environnement dans laquelle est déployée l'application.-

VI.4.5. Tests d'intrusion

L'équipe d'audit en charge de la réalisation d'un test d'intrusion sur une cible donnée peut effectuer une ou plusieurs des phases suivantes :

- phase boîte noire : les auditeurs ne disposent d'aucune autre information que les adresses IP et URL associées à la cible auditée. Cette phase est généralement précédée de la découverte d'informations et l'identification de la cible par interrogation des services DNS, par le balayage des ports ouverts, par la découverte de la présence d'équipements de filtrage, etc. ;
- phase boîte grise : les auditeurs disposent des connaissances d'un utilisateur standard du système d'information (authentification légitime, poste de travail « standard », etc.). Les identifiants peuvent appartenir à des profils d'utilisateurs différents afin de tester des niveaux de privilèges distincts ;
- phase boîte blanche : les auditeurs disposent du maximum d'informations techniques (architecture, code source, contacts téléphoniques, identifiants, etc.) avant de démarrer l'analyse. Ils ont également accès à des contacts techniques liés à la cible.

Si plusieurs de ces prestations sont effectuées, il est recommandé de préserver l'ordre d'exécution décrit ci-dessus.

a) [PENTEST] Le prestataire doit être capable d'effectuer les trois phases : boîte noire, boîte grise, boîte blanche.

b) [PENTEST] Le prestataire doit orienter le commanditaire sur le choix d'une ou de plusieurs phases pour répondre aux objectifs et critères d'audit conformément à la méthode employée (voir exigence VI.4.1.d).

c) [ELEVE] [PENTEST] Le prestataire doit être capable de simuler un potentiel d'attaque élevé, modéré et élémentaire amélioré (voir chapitre III.2).

d) [SUBSTANTIEL] [PENTEST] Le prestataire doit être capable de simuler un potentiel d'attaque élémentaire.

e) [PENTEST] Le prestataire et le commanditaire doivent, préalablement à tout test d'intrusion, définir un profil d'attaquant simulé. [ELEVE] Par défaut, la prestation proposée par le prestataire doit adresser un profil d'attaquant possédant un potentiel d'attaque élevé.

f) [PENTEST] Lorsqu'elles sont connues pour rendre la cible auditée instable voire provoquer un déni de service, les vulnérabilités découvertes ne doivent pas être exploitées sauf accord du commanditaire et du bénéficiaire. L'absence de tentative d'exploitation de telles vulnérabilités doit être indiquée et justifiée dans le rapport d'audit par le prestataire.

VI.4.6. Audit organisationnel et physique

a) [ORGAPHY] Le prestataire doit évaluer l'organisation de la sécurité des systèmes d'information du bénéficiaire sur la base des référentiels techniques et réglementaires en accord avec les réglementations, politiques et méthodes applicables dans le domaine d'activité du bénéficiaire en accord avec les critères d'audit.

b) [ELEVE] [ORGAPHY] Par défaut, sauf indication contraire du commanditaire, le prestataire doit intégrer l'analyse des systèmes d'information liés à la sécurité des aspects physiques et notamment la protection des locaux hébergeant les systèmes d'information et les données du bénéficiaire ou le contrôle d'accès aux ressources.

VI.4.7. Entretiens avec le personnel

a) [ELEVE] Le prestataire doit organiser des entretiens avec le personnel concerné par la mise en place, l'administration et l'exploitation de la cible auditée selon le périmètre d'audit. Au travers de ces entretiens, le prestataire doit identifier :

   i. la connaissance et la maîtrise du personnel de la cible audité adaptées à leurs fonctions individuelles (exemples : priorités d'action, consignes claires de la hiérarchie ou de l'environnement humain, connaissance techniques de la cible audité, applicabilité) ;

   ii. les éventuelles différences de perceptions entre l'auditeur et l'audité (exemples : maîtrise, gouvernance, techniques) du système audité ;

   iii. tout sujet pouvant amener à un risque ou une vulnérabilité vis-à-vis des critères d'audit et du périmètre d'audit.

Ces entretiens sont demandés pour l'ensemble des activités de ce référentiel, le personnel dépendant de l'activité visée (administrateur, développeur, officier de sureté, chaîne de commandement hiérarchique, etc.).

VI.4.8. Notifications et communications spécifiques durant l'audit

a) Le responsable d'équipe doit tenir informé le commanditaire des vulnérabilités critiques découvertes au cours de l'audit. Il doit rendre compte immédiatement à l'audité de tout élément constaté présentant un risque immédiat et significatif, et dans la mesure du possible, lui proposer des mesures permettant de lever ce risque.

b) Le prestataire doit notifier l'ANSSI[10] de la découverte des vulnérabilités non publiques affectant les produits commerciaux, open-source ou largement répandus.

[10] Les modalités de contact sont disponibles sur https://www.ssi.gouv.fr.

c) Les auditeurs doivent rendre compte des constats d'audit au responsable d'équipe d'audit, lequel peut en avertir sans délai sa hiérarchie ainsi que le bénéficiaire, dans le respect des clauses de confidentialité fixées dans la convention d'audit

d) Le prestataire doit avoir un contact permanent avec le bénéficiaire et l'auditeur doit prévenir le commanditaire et le bénéficiaire avant toute action qui pourrait entraîner un dysfonctionnement, voire un déni de service de la cible auditée.

VI.5. Étape 5 – Restitution

a) Dès la fin de l'audit, et sans attendre que le rapport d'audit soit achevé, le responsable d'équipe doit informer le bénéficiaire et le commanditaire des constats et des premières conclusions de l'audit. Le cas échéant, il présente les vulnérabilités majeures et critiques qui nécessiteraient une action rapide et décrit les recommandations associées.

VI.6. Étape 6 – Elaboration du rapport d'audit

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

b) Le prestataire doit mentionner explicitement dans le rapport d'audit :

- si la prestation réalisée est une prestation qualifiée ainsi que le niveau d'assurance associé [ELEVE] ou [SUBSTANTIEL] ;
- les activités (voir chapitre II.) réalisées dans le cadre de l'audit.

c) Le rapport d'audit doit contenir en particulier :

- une synthèse, compréhensible par des non experts, qui précise :
  - le contexte et le périmètre de la prestation[11] ;
  - les vulnérabilités ou non-conformités critiques, d'origine technique ou organisationnelle, et les mesures correctives proposées ;
  - l'appréciation du niveau de sécurité du système d'information audité par rapport à l'état de l'art et en considération du périmètre d'audit.
- un tableau synthétique des résultats de l'audit, qui précise :
  - la synthèse des vulnérabilités et non-conformités relevées, classées selon une échelle de valeur ;
  - la synthèse des mesures correctives proposées (recommandations), classées par criticité et par complexité ou coût estimé de correction ;
- lorsque réalisés, une description du déroulement linéaire des tests d'intrusion et de la méthodologie employée pour détecter les vulnérabilités et, le cas échéant, les exploiter ;
- une analyse de la sécurité du système d'information audité, qui présente les résultats des différentes activités d'audit réalisées.

d) Le rapport d'audit doit être adapté en fonction de l'activité d'audit réalisée par le prestataire.

[11] Compte tenu du fait que le commanditaire de l'audit dispose généralement déjà d'une description du périmètre audité, dans la convention d'audit ou dans le plan d'audit, la synthèse du contexte du périmètre de l'audit peut être très succincte.

e) Les non-conformités identifiées lors de l'évaluation d'un audit de conformité doivent être spécifiées dans le rapport d'audit. Pour chaque non-conformité, le prestataire évaluera de la gravité de celles-ci en fonction des risques encourus.

f) Les vulnérabilités, qu'elles soient d'origine technique ou organisationnelle, doivent être classées en fonction de leur impact sur la sécurité du système d'information et leur difficulté d'exploitation.

   Il est recommandé d'utiliser l'échelle proposée par l'ANSSI en Annexe 4. A défaut, le prestataire doit être en mesure de proposer une échelle pertinente.

g) Chaque vulnérabilité et non-conformité doit être associée à une ou plusieurs recommandations. Les recommandations décrivent les solutions permettant de résoudre une vulnérabilité ou une non-conformité et d'améliorer le niveau de sécurité.

   Ces recommandations doivent :

   i. être proportionnées, adaptées à la cible de l'audit, réalistes, non ambiguës ;
   ii. pouvoir être priorisées.
   Les critères suivants doivent notamment être pris en compte ou estimés par le prestataire : mesures de corrections immédiates, recommandation de mesures d'amélioration en continue ou de minimisation de reconduction de la vulnérabilité, complexités de mise en œuvre.

h) [ELEVE] Le prestataire doit disposer d'une échelle de priorités pour la mise en œuvre des recommandations.

i) Il est recommandé que le rapport d'audit présente également des recommandations générales non associées à des vulnérabilités et destinées à conseiller l'audité pour les actions liées à la sécurité de son système d'information qu'il entreprend.

j) Le rapport d'audit doit mentionner les réserves relatives à l'exhaustivité des résultats de l'audit (liées aux délais alloués, à la disponibilité des informations demandées, à la collaboration de l'audité, à l'échantillonnage et périmètre audité, etc.) ou à la pertinence de la cible auditée.

k) Le prestataire doit identifier dans les livrables, et en particulier dans le rapport d'audit, les phases automatisées réalisées dans le cadre de l'audit lorsque des outils automatisés sont utilisés.

l) Le rapport d'audit doit mentionner les noms et coordonnées des auditeurs, responsables d'équipe d'audit et commanditaires de l'audit.

VI.7. Étape 7 – Clôture de la prestation

a) [ELEVE] Le prestataire doit organiser une réunion de clôture de l'audit avec le commanditaire et/ou le bénéficiaire suite à la livraison du rapport d'audit. Cette réunion permet de présenter la synthèse du rapport d'audit, des scénarios d'exploitation de certaines failles, des recommandations, et de la suite à donner à la prestation (audit de contrôle). Elle est également l'occasion d'expliquer les recommandations complexes et, éventuellement, de proposer d'autres solutions plus aisées à mettre en œuvre. Elles peuvent permettre de répondre aux questions résiduelles du bénéficiaire ou du commanditaire.

b) Le prestataire doit recommander au commanditaire d'effectuer ultérieurement un audit de contrôle afin de vérifier si les mesures correctives proposées lors de l'audit ont été correctement mises en œuvre.

Un audit de contrôle est un audit complémentaire à l'audit initial et permettant d'évaluer si la sécurité du système d'information s'est améliorée suite à celui-ci. Cet audit permet également d'établir un statut de la correction des non-conformités ou vulnérabilités identifiées lors de l'audit initial. L'audit de contrôle ne se substitue pas à des audits supplémentaires et n'est pas suffisante à elle seule : l'audit de contrôle n'a pour objectif que de les compléter.

c) Le responsable d'équipe doit demander au bénéficiaire de signer un document attestant que le système d'information qui a été audité est, à l'issue de l'audit, dans un état dont la sécurité n'est pas dégradée par rapport à l'état initial, dégageant ainsi, dans le principe, la responsabilité des auditeurs et du prestataire de tout problème postérieur à l'audit.

d) Toutes les traces, relevés de configuration, informations ou documents relatifs au système d'information audité obtenus par le prestataire doivent être restitués au bénéficiaire ou, sur sa demande, détruits conformément à la convention d'audit. Seul le rapport d'audit doit être conservé par défaut par le prestataire sur les moyens d'archivages dédiés (voir exigence IV.3.k) sauf refus formel du commanditaire ou du bénéficiaire de la prestation. Le cas échéant, le responsable d'audit produit un procès-verbal de destruction de ces données qu'il remet au commanditaire et précisant les données détruites et leur mode de destruction.

e) Afin qu'il puisse s'assurer de la pertinence des mesures correctives mises en œuvre pour corriger les vulnérabilités découvertes lors de l'audit, le commanditaire peut demander au prestataire la fourniture des développements spécifiques autonomes réalisés lors de l'audit pour valider les scénarios d'exploitation des vulnérabilités. Ces développements peuvent être fournis sous la forme de scripts ou de programmes compilés, accompagnés de leur code source, ainsi que d'une brève documentation de mise en œuvre et d'utilisation. Les modalités relatives à cette mise à disposition sont précisées dans la convention.

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

Annexe 1 Références documentaires

I. Codes, textes législatifs et réglementaires

Renvoi	Document
[D_2015_350]	Décret n° 2015-350 du 27 mars 2015 relatif à la qualification des produits de sécurité et des prestataires de service de confiance pour les besoins de la sécurité des systèmes d'information. Disponible sur https://www.legifrance.gouv.fr
[IGI_1300]	Instruction générale interministérielle n°1300 sur la protection du secret de la défense nationale, n°1300 /SGDSN/PSE/PSD, 30 novembre 2011. Disponible sur http://www.legifrance.gouv.fr
[II_901]	Instruction interministérielle relative à la protection des systèmes d'information sensibles, n°901/SGDSN/ANSSI, 28 janvier 2015. Disponible sur http://www.legifrance.gouv.fr
[II_910]	Instruction interministérielle relative aux articles contrôlés de la sécurité des systèmes d'information (ACSSI), n°910/SGDSN/ANSSI, 22 octobre 2013. Disponible sur http://www.legifrance.gouv.fr
[LOI_LPM]	Articles L. 1332-6-1 à L. 1332-6-6 du code de la défense, créés par la loi n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale (LPM 2014-19). Disponible sur https://www.legifrance.gouv.fr
[NIS]	Directive (UE) n° 2016/1148 du parlement européen et du conseil du 6 juillet 2016 concernant les mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union. Disponible sur https://eur-lex.europa.eu Loi n° 2018-133 du 26 février 2018 portant diverses dispositions d'adaptation au droit de l'Union européenne dans le domaine de la sécurité. Disponible sur https://www.legifrance.gouv.fr
[R_OTAN]	Instruction interministérielle n° 2100/SGDSN/SSD du 1er décembre 1975 pour l'application en France du système de sécurité de l'Organisation du Traité de l'Atlantique nord. Disponible sur https://circulaires.legifrance.gouv.fr
[R_UE]	Instruction interministérielle n°2102/SGDSN/PSD du 12 juillet 2013 sur la protection en France des informations classifiées de l'Union Européenne. Disponible sur https://circulaires.legifrance.gouv.fr
[RGPD]	Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (Texte présentant de l'intérêt pour l'EEE) Disponible sur https://eur-lex.europa.eu

II. Normes et documents techniques

Renvoi	Document
[PASSI_LPM]	Exigences supplémentaires applicables aux prestataires d'audit de la sécurité des systèmes d'information dans le cadre de la loi n°2013-1168 du 18 décembre 2013. Document de niveau *Diffusion Restreinte*, il peut être obtenu auprès de l'ANSSI.
[EBIOS_RM]	Méthode de gestion de risques EBIOS Risk Manager. Disponible sur https://www.ssi.gouv.fr
[G_ARCHI_DR]	Recommandations pour les architectures des systèmes d'information sensibles ou diffusion restreinte, ANSSI, version en vigueur. Disponible sur https://www.ssi.gouv.fr
[G_AUTH_MULTI_MDP]	Recommandations relatives à l'authentification multifacteurs et aux mots de passe, ANSSI, version en vigueur. Disponible sur https://www.ssi.gouv.fr
[G_CRYPTO_1]	Guide de sélection d'algorithmes cryptographiques, ANSSI, version en vigueur. Disponible sur https://www.ssi.gouv.fr
[G_CRYPTO_2]	Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, ANSSI, version en vigueur. Disponible sur https://www.ssi.gouv.fr
[G_HOMOLOGATION]	L'homologation de sécurité en neuf étapes simples, ANSSI, version en vigueur. Disponible sur https://www.ssi.gouv.fr
[G_HYGIENE]	Guide d'hygiène informatique, ANSSI, version en vigueur. Disponible sur https://www.ssi.gouv.fr
[G_INTERCO]	Recommandations relatives à l'interconnexion d'un système d'information à Internet, ANSSI, version en vigueur. Disponible sur https://www.ssi.gouv.fr
[ISO19011]	Norme internationale ISO/IEC 19011 : Lignes directrices pour l'audit des systèmes de management, version en vigueur. Disponible sur http://www.iso.org
[ISO27000]	Norme internationale ISO/IEC 27000 : Technologies de l'information – Techniques de sécurité – Systèmes de gestion de la sécurité de l'information – vue d'ensemble et vocabulaire, version en vigueur. Disponible sur http://www.iso.org
[ISO27001]	Norme internationale ISO/IEC 27001 : Techniques de sécurité – Systèmes de gestion de la sécurité de l'information – Exigences, version en vigueur. Disponible sur http://www.iso.org
[ISO27002]	Norme internationale ISO/IEC 27002 : Techniques de sécurité – Code de bonne pratique pour la gestion de la sécurité de l'information, version en vigueur. Disponible sur http://www.iso.org
[PSSI]	Guide d'élaboration de politiques de sécurité des systèmes d'information Disponible sur http://www.ssi.gouv.fr/pssi/

III. Autres références documentaires

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

Annexe 2 Missions et compétences attendues du personnel du prestataire

Cette annexe identifie les missions et compétences attendues du personnel du prestataire dans le cadre de la délivrance d'une prestation d'audit. Les connaissances de la réglementation citées en chapitre I sont complétés par les compétences spécifiques requises pour chaque profil d'auditeur et du responsable d'équipe d'audit, décrites dans la suite de l'annexe.

I. Connaissances de la réglementation

Le personnel du prestataire (auditeurs et responsables d'équipe d'audit) doit avoir des connaissances et une compréhension des principaux concepts relatifs aux différents textes règlementaires cités ci-dessous :

- [IGI_1300] ;
- [II_901] ;
- [LOI_LPM] ;
- [NIS] ;
- [RGS] et notamment ses annexes A, B et C ;
- [RGPD] ;
- [R_OTAN] ;
- [R_UE].

Le personnel doit avoir la capacité à savoir fournir une explication macroscopique des éléments cités ainsi que la faculté à faire le lien entre les exigences du présent référentiel et le contexte de la demande du commanditaire.

II. Responsable d'équipe

1. Missions

Le responsable d'équipe doit assurer les missions suivantes :

- mettre en œuvre une organisation adaptée aux objectifs de la prestation (voir chapitre VI.3) ;
- structurer l'équipe d'auditeurs (compétences, effectif) ;
- assurer la définition, le pilotage et le contrôle des activités des auditeurs (voir chapitre VI.4) ;
- mettre en œuvre les moyens adaptés aux objectifs de la prestation (voir chapitre VI.3) ;
- définir et gérer les priorités ;
- maintenir à jour un état de la progression de l'audit et présenter l'information utile au commanditaire ;
- soutenir l'audité dans l'évaluation des impacts métier associés menaces pouvant potentiellement exploiter les vulnérabilités découvertes au cours de la prestation, notamment en matière de confidentialité, d'intégrité et de disponibilité ;
- proposer les recommandations adaptées pour remédier aux risques découlant des vulnérabilités découvertes ;
- contrôler la qualité des productions ;

- valider les livrables.

2. Compétences

Le responsable d'équipe doit avoir des compétences approfondies dans la plupart des domaines requis pour les auditeurs qu'il encadre.

Il doit par ailleurs avoir les qualités suivantes :

- savoir piloter des équipes d'auditeurs ;
- savoir définir et gérer les priorités ;
- savoir synthétiser et restituer l'information utile pour du personnel technique et non technique ;
- savoir rédiger des documentations adaptées à différents niveaux d'interlocuteurs (services techniques, organe de direction, etc.).

3. Compétences recommandées lorsque l'audit porte sur des systèmes industriels

Il est recommandé que le responsable d'équipe de systèmes industriels disposent de compétences approfondies dans les domaines techniques suivants :

- architectures fonctionnelles à base d'automate programmable industriel (*programmable logic controller*, PLC) ;
- réseaux et protocoles industriels :
    - topologie des réseaux industriels ;
    - cloisonnement 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 couche 802.15.4) ;
- rôle fonctionnel des différents équipements.

III. Auditeur d'architecture

1. Missions

L'auditeur d'architecture doit assurer les missions suivantes :

- adopter une vision globale du système d'information afin d'identifier :
    - les vulnérabilités et les éventuels chemins d'attaque associés,
    - les éléments pertinents à auditer ;
- collecter les éléments de configuration des équipements réseau à auditer ;
- auditer la configuration des équipements réseau préalablement choisis ;
- développer des outils adaptés à la cible auditée, le cas échéant ;
- mener les entretiens avec les administrateurs réseau pour le niveau d'assurance [ELEVE] ;
- identifier les vulnérabilités présentes dans l'architecture et dans la configuration des équipements audités ;

- proposer les recommandations adaptées pour remédier aux risques découlant des vulnérabilités découvertes ;
- capitaliser les connaissances acquises, assurer une restitution et produire un rapport d'audit.

2. Compétences

L'auditeur d'architecture 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 ;
    - services externalisés largement répandu (ex. technologies relatives à l'informatique en nuage) ;
    - technologie sans fil ;
    - téléphonie.
- équipements et logiciels de sécurité :
    - pare-feu ;
    - système de sauvegarde ;
    - système de stockage mutualisé ;
    - dispositifs de chiffrement des communications ;
    - serveurs d'authentification ;
    - serveurs mandataires inverses ;
    - solutions de gestion de la journalisation ;
    - équipements de détection et prévention d'intrusion ;

Il doit par ailleurs avoir les qualités 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).

3. Compétences recommandées lorsque l'audit porte sur des systèmes industriels

Il est recommandé que l'auditeur d'architecture de systèmes industriels dispose de compétences approfondies dans les domaines techniques suivants :

- architectures fonctionnelles à base de PLC ;
- réseaux et protocoles industriels :

- topologie des réseaux industriels ;
- cloisonnement 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 couche 802.15.4) ;

- rôle fonctionnel des différents équipements.

IV. Auditeur de configuration

1. Missions

L'auditeur de configuration doit assurer les missions suivantes :

- adopter une vision globale du système d'information afin :
  - de comprendre le rôle de l'infrastructure à auditer,
  - d'identifier les éléments pertinents à auditer ;
- collecter les éléments de configuration des éléments à auditer ;
- auditer la configuration des éléments préalablement choisis ;
- développer des outils adaptés à la cible auditée, le cas échéant ;
- mener les entretiens avec les administrateurs système et/ou applicatifs pour le niveau d'assurance [ELEVE] ;
- identifier les vulnérabilités présentes dans la configuration des éléments audités ;
- proposer les recommandations adaptées pour remédier aux risques découlant des vulnérabilités découvertes ;
- capitaliser les connaissances acquises, assurer une restitution et produire un rapport d'audit.

2. Compétences

L'auditeur de configuration 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 ;
  - services externalisés largement répandu (ex. technologies relatives à l'informatique en nuage) ;
  - technologie sans fil ;
  - téléphonie.

- équipements et logiciels de sécurité :
    - pare-feu ;
    - système de sauvegarde ;
    - système de stockage mutualisé ;
    - dispositif de chiffrement des communications ;
    - 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.
- systèmes d'exploitation (environnement et durcissement) :
    - systèmes Microsoft ;
    - systèmes UNIX/Linux ;
    - systèmes centralisés (basés par exemple sur OS400 ou zOS) ;
    - solution de virtualisation.
- couche applicative :
    - applications de type client/serveur ;
    - langages de programmation utilisés pour la configuration (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.

Il doit par ailleurs avoir les qualités 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).

3. Compétences recommandées lorsque l'audit porte sur des systèmes industriels

Il est recommandé que l'auditeur de configuration de systèmes industriels dispose de 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 couche 802.15.4) ;
- équipements :
    - configuration et sécurisation des principaux automates et équipements industriels du marché.

V. Auditeur de code source

1. Missions

L'auditeur de code source doit assurer les missions suivantes :

- adopter une vision globale du système d'information afin de comprendre le rôle de l'application à auditer ;
- identifier au sein de l'application les éléments pertinents à auditer au sein du code source ;
- auditer le code source ;
- développer des outils adaptés à la cible auditée, le cas échéant ;
- employer des techniques d'ingénierie inverse, le cas échéant ;
- mener les entretiens avec les développeurs pour le niveau d'assurance [ELEVE], le cas échéant ;
- identifier les vulnérabilités présentes dans le code source ;
- proposer les recommandations adaptées pour remédier aux risques découlant des vulnérabilités découvertes ;
- capitaliser les connaissances acquises, assurer une restitution et produire un rapport d'audit.

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.

Il doit par ailleurs avoir les qualités 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).

3. Compétences recommandées lorsque l'audit porte sur des systèmes industriels

Il est recommandé que l'auditeur de code source d'applications présentes dans des systèmes industriels dispose de 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 utilisateur 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

1. Missions

L'auditeur en tests d'intrusion doit assurer les missions suivantes :

- adopter une vision globale du système d'information afin d'identifier :
    - les cibles pertinentes à attaquer (ex : documents métier, données sensibles, serveurs sensibles, etc.),
    - les scénarios d'attaque adaptés ;
- identifier au sein de l'infrastructure les éléments à attaquer permettant d'exécuter les scénarios d'attaque choisis ;
- réaliser des attaques pertinentes sur l'infrastructure cible ;
- développer des outils adaptés à la cible attaquée, le cas échéant ;

- employer des techniques d'ingénierie inverse, le cas échéant ;
- identifier les vulnérabilités présentes dans tout élément de l'infrastructure permettant de mener à bien les attaques ;
- proposer les recommandations adaptées pour remédier aux risques découlant des vulnérabilités découvertes ;
- capitaliser les connaissances acquises, assurer une restitution et produire un rapport d'audit.

2. Compétences

L'auditeur en tests d'intrusion 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 ;
    - système de sauvegarde ;
    - système de stockage mutualisé ;
    - dispositif de chiffrement des communications ;
    - 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.
- systèmes d'exploitation :
    - systèmes Microsoft ;
    - systèmes UNIX/Linux ;
    - systèmes centralisés (basés par exemple sur OS400 ou zOS) ;
    - 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.

Il doit par ailleurs avoir les qualités 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).

3. Compétences recommandées lorsque l'audit porte sur des systèmes industriels

Il est recommandé que l'auditeur en tests d'intrusion de systèmes industriels dispose de compétences approfondies dans les domaines techniques suivants :

- architectures fonctionnelles à base de PLC ;
- réseaux et protocoles industriels :
  - topologie des réseaux industriels ;
  - cloisonnement 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 couche 802.15.4) ;
- équipements :
  - configuration et sécurisation des principaux automates et équipements industriels du marché.

VII. Auditeur en sécurité organisationnelle et physique

1. Missions

L'auditeur en sécurité organisationnelle et physique doit assurer les missions suivantes :

- adopter une vision globale de l'organisation afin d'identifier :
    - les politiques et processus pertinents à auditer,
    - les lieux pertinents à auditer,
    - les vulnérabilités et les éventuels chemins d'attaque physiques associés ;
- collecter les documents associés aux processus à auditer ;
- auditer les processus et lieux préalablement choisis ;
- mener les entretiens avec les responsables de processus et responsables de la sureté pour le niveau d'assurance [ELEVE] ;
- identifier les vulnérabilités présentes dans les processus et l'architecture physique des lieux audités ;
- proposer les recommandations adaptées pour remédier aux risques découlant des vulnérabilités découvertes ;
- capitaliser les connaissances acquises, assurer une restitution et produire un rapport d'audit.

2. Compétences

L'auditeur en sécurité organisationnelle et physique doit disposer de compétences approfondies dans les domaines suivants :

- maîtrise des référentiels techniques :
- maîtrise du cadre normatif :
    - les normes [ISO27001] et [ISO27002] ;
    - les textes réglementaires relatifs à la sécurité des systèmes d'information, aux audits et aux sujets connexes[12].
- maîtrise des domaines relatifs à l'organisation de la sécurité des systèmes d'information :
    - analyse 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.

[12] 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.

- maîtrise des pratiques liées à l'audit :
    - conduite d'entretien ;
    - visite sur site ;
    - analyse documentaire.

Il doit par ailleurs avoir les qualités 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).

3. Compétences recommandées lorsque l'audit porte sur des systèmes industriels

Il est recommandé que l'auditeur en sécurité organisationnelle et physique dispose de connaissances sur les sujets suivants :

- normes de sécurité fonctionnelle telle que l'IEC 61508 ;
- architectures fonctionnelles à base de PLC ;
- rôles et utilisation des protocoles industriels ;
- connaissance du rôle fonctionnel des différents équipements.

Annexe 3 Recommandations aux commanditaires

Cette annexe liste les recommandations de l'ANSSI à l'intention des commanditaires de prestations d'audits de sécurité des systèmes d'information.

I. Qualification

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

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

c) Le niveau d'assurance du prestataire ainsi que sa portée de qualification choisit par le commanditaire doit répondre aux obligations légales du commanditaire si celui-ci est soumis à une ou plusieurs réglementations spécifiques (voir chapitre III.2 Portée de la qualification).

d) Pour bénéficier d'une prestation qualifiée, c'est-à-dire conforme à l'ensemble des exigences du présent référentiel, le commanditaire doit :

- choisir le prestataire dans le catalogue des prestataires qualifiés publié sur le site de l'ANSSI et ;
- exiger du prestataire de stipuler dans la convention de service que la prestation réalisée est une prestation qualifiée.

En effet, un prestataire qualifié garde la faculté de réaliser des prestations non qualifiées. Le recours à un prestataire issu du catalogue des prestataires qualifiés est donc une condition nécessaire mais non suffisante. Pour bénéficier d'une prestation qualifiée, le commanditaire doit donc également exiger une prestation qualifiée au niveau d'assurance et sur la portée adaptée à son besoin.

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

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

g) Il est recommandé que le commanditaire demande au prestataire de lui transmettre les attestations individuelles de compétence de chaque auditeur intervenant dans le cadre de la prestation.

h) Le commanditaire peut, conformément au processus de qualification des prestataires de service de confiance [PROCESS_QUALIF], déposer auprès de l'ANSSI une réclamation contre un prestataire qualifié pour lequel il estime que ce dernier n'a pas respecté une ou plusieurs exigences du présent référentiel dans le cadre d'une prestation qualifiée.

S'il s'avère après instruction de la réclamation que le prestataire n'a pas respecté une ou plusieurs exigences du présent référentiel dans le cadre d'une prestation qualifiée, et selon la gravité, la qualification du prestataire peut être suspendue retirée ou sa portée de qualification réduite.

i) La qualification d'un prestataire n'atteste pas de sa capacité à accéder ou à détenir des informations classifiées de défense [IGI_1300] et par conséquent ne se substitue pas à une habilitation de défense.

Lorsque la prestation requiert que le prestataire accède à des informations classifiées de défense [IGI_1300], il est de la responsabilité du commanditaire de vérifier que le prestataire et son personnel respectent les principes régissant l'accès des personnes morales et physiques au secret de la défense nationale.

j) La qualification d'un prestataire n'atteste pas de sa capacité à accéder ou à détenir des articles contrôlés de la sécurité des systèmes d'information (ACSSI) [II_901].

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

k) Il est recommandé que le commanditaire demande au prestataire de lui fournir des références : références clients, participation à des programmes de recherche, etc.

II. Recommandations générales

a) Les audits devraient être le plus exhaustif possible, tout en tenant compte des contraintes temporelles et budgétaires allouées à l'audit.

b) La durée de l'audit demandé par les commanditaires d'audits devrait être adaptée en fonction :

- du périmètre d'audit et de sa complexité ;
- des exigences de sécurité attendues du système d'information audité.

c) Afin de réduire le volume global d'éléments à auditer et donc le coût de l'audit, et tout en conservant un périmètre d'audit pertinent, il devrait être réalisé un échantillonnage respectant les principes suivants :

- pour les audits de configuration, seuls les serveurs les plus sensibles sont audités : contrôleurs de domaine Active Directory, serveurs de fichiers, serveurs d'infrastructure (DNS, SMTP, etc.), serveurs applicatifs, etc.
- pour un audit de code source, seules les parties sensibles du code source sont auditées : gestion des authentifications, gestion des contrôles d'accès des utilisateurs, accès aux bases de données, contrôle des saisies utilisateur, etc.

d) Il est préférable de réaliser les tests d'intrusion sur un environnement de test (ou de « pré-production ») afin d'éviter les conséquences liées aux éventuels dysfonctionnements sur un environnement de production. Ceci dit, afin de garantir la pertinence de l'audit, il convient de s'assurer que cet environnement soit similaire à celui de production.

L'applicabilité des résultats des audits techniques dans l'environnement de production doit être vérifiée. Les audits d'architecture, de configuration, de code source et organisationnels doivent être réalisés dans l'environnement de production.

e) La définition du périmètre d'un audit doit être basée sur une analyse préalable des risques « métier » de l'audité. Il est recommandé au commanditaire d'indiquer les éléments les plus sensibles de la cible auditée au prestataire. Cette recommandation est fondamentale dans le cas de l'audit de systèmes industriels.

f) Dans le cas où le commanditaire souhaiterait mandater sur un même périmètre, un prestataire d'audit de sécurité (PASSI) et un prestataire d'accompagnement et de conseil en sécurité des systèmes d'information (PACS), il est recommandé que ces deux entités mandatées soient juridiquement indépendantes l'une de l'autre.

III. Pendant la prestation

a) Il est recommandé que le commanditaire désigne, en son sein, un référent chargé de la gestion des relations avec le prestataire et des modalités de réalisation des activités d'audit (horaires des interventions, autorisations, etc.).

b) Il est recommandé que le commanditaire et l'audité prennent les mesures de sauvegarde nécessaires à la protection de leurs systèmes d'information et de leurs données préalablement et au cours de la prestation. Cette démarche doit être réalisée en collaboration avec le prestataire afin de ne pas gêner les activités d'audit, notamment les équipes informatiques du commanditaire ne doivent pas porter atteinte à l'intégrité des traces collectées.

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 dont il n'est pas le titulaire mais tout de même utilisés à des fins professionnelles (BYOD[13]) en l'absence du titulaire du matériel ou sans son accord explicite.

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

e) Il est recommandé que le commanditaire mette en œuvre des moyens de communication sécurisés et dédiés pour tous les échanges en rapport avec l'audit, en interne et avec le prestataire.

f) Il est recommandé que le commanditaire ait la capacité à révoquer un auditeur.

IV. Après la prestation

a) Il est fortement recommandé que la prestation réalisée soit complétée par un audit de contrôle (voir chapitre VI.7.).

V. Types d'audit recommandés par l'ANSSI

a) L'ANSSI recommande aux commanditaires d'audits et aux prestataires d'audit de recourir et demander des audits composés des activités d'audit suivantes :

- *audit applicatif :*
    - audit de code source ;
    - audit de configuration (serveur d'application, serveur HTTP, base de données, etc.).
- *audit d'un centre serveur :*
    - audit d'architecture (liaison entre les différentes zones et entités, filtrage, etc.) ;
    - audit de configuration (équipements réseau et de sécurité, serveurs d'infrastructure) ;

[13] *Bring Your Own Device* (Apporter Votre Equipement personnel de Communication).

- audit organisationnel et physique.

- *audit d'un réseau bureautique :*
  - audit d'architecture ;
  - audit de configuration (postes bureautique, équipements réseau, serveurs bureautique, serveurs AD, etc.) ;
  - audit organisationnel et physique.
- *audit d'une plate-forme de téléphonie :*
  - audit d'architecture ;
  - audit de configuration (équipements réseau et de sécurité, IPBX, téléphones, etc.).
- *audit d'une plate-forme de virtualisation :*
  - audit d'architecture ;
  - audit de configuration (équipements réseau et de sécurité, systèmes de virtualisation, etc.).
- *audit de système industriel, dont la salle de contrôle :*
  - audit d'architecture ;
  - audit de configuration (automates programmables industriels, capteurs/actionneurs, serveurs d'applications, stations opérateur, stations d'ingénierie, consoles de programmation, équipements réseau et de sécurité, serveurs d'authentification, etc.) ;
  - audit organisationnel et physique ;
  - audit de code source (automates programmables industriels, pupitres, systèmes embarqués, applications métier, etc.)

Cette liste est non exhaustive et peut être complétée par les commanditaires d'audits et les prestataires d'audit.

b) Chacun des types d'audit décrits ci-dessus peut inclure l'activité de tests d'intrusion.

c) En revanche, l'activité de tests d'intrusion ne devrait jamais être réalisée seule et sans aucune autre activité d'audit. En effet, un test d'intrusion peut servir de complément pour un audit de configuration ou de code auquel il est adossé afin d'améliorer la portée, en terme d'impacts, de ce dernier. Ceci permet par exemple de vérifier qu'une faille découverte lors d'un audit de code source est bien exploitable dans les conditions d'exploitation de la plate-forme, ainsi que les conséquences de cette exploitation (exécution de code, fuite d'informations, rebond, etc.).

d) Les tests d'intrusion ne devraient pas être réalisés sur des plates-formes d'hébergement mutualisées sauf accord express de l'hébergeur et après que les risques aient été évalués et maîtrisés, et que les responsabilités aient été clairement établies.

Annexe 4 Prérequis au démarrage de la prestation

Préalablement à la réalisation de la prestation, il est recommandé que le commanditaire mette à disposition du prestataire les informations concernant :

- l'organigramme de l'organisation ;
- l'organisation générale du système d'information ;
- (selon l'activité d'audit) l'architecture du système d'information :
    - plages d'adresses IP, équipements réseau et sécurité, etc. ;
    - passerelles de sortie avec Internet (relais Web, DNS, chaîne de messagerie, etc.) ;
    - passerelles d'entrées (VPN, nomades, accès distant à la messagerie, téléphonie) ;
    - serveurs exposés à Internet ou à un tiers (serveur web, serveur applicatif, etc.) ;
    - architecture des zones réseau et filtrage ;
    - dépendances et interconnexions du système d'information ;
- les spécificités et les contraintes du système d'information (réglementation applicable, SIIV, contraintes métier et/ou techniques, sous-traitance, etc.) ainsi que la localisation géographique ;
- le système d'information :
    - systèmes d'exploitation (postes d'administration, postes utilisateurs, postes nomades, serveurs d'infrastructure et métier, etc.) ;
    - technologies employées pour les applications métier ;
    - technologies employées pour les services d'infrastructure ;
    - préciser si les horloges des équipements du système d'information sont synchronisés (NTP) et les différentes zones utilisées (GMT, Paris) ;
    - particularités de systèmes (impossibilité de les arrêter ou d'en modifier la configuration) ;
- (selon l'activité d'audit) l'architecture des domaines d'administration et des liens entre les domaines ;
- (selon l'activité d'audit) la politique de journalisation, les moyens de supervision et de détection ;
- (selon l'activité d'audit) les périodes de gel technique et les projets en cours ou prévus pour le système d'information ;
- les éventuelles démarches déjà entreprises par le commanditaire :
    - audits préalablement effectuées et résultats associés;

Le prestataire doit protéger ces informations conformément à leur niveau de sensibilité ou de classifications éventuelles.

Annexe 5 Echelle de classification des vulnérabilités

L'ANSSI propose l'échelle de classification des vulnérabilités suivante.

Les vulnérabilités, qu'elles soient d'origine technique ou organisationnelle, sont classées en fonction du risque qu'elles font peser sur le système d'information, c'est-à-dire en fonction de l'impact de la vulnérabilité sur le système d'information et de sa difficulté d'exploitation.

Le niveau du risque lié à chaque vulnérabilité est apprécié selon l'échelle de valeur suivante :

- *Mineur* : faible risque sur le système d'information et pouvant nécessiter une correction ;
- *Important* : risque modéré sur le système d'information et nécessitant une correction à moyen terme ;
- *Majeur* : risque majeur sur le système d'information nécessitant une correction à court terme ;
- *Critique* : risque critique sur le système d'information et nécessitant une correction immédiate ou imposant un arrêt immédiat du service.

La facilité d'exploitation correspond au niveau d'expertise et aux moyens nécessaires à la réalisation de l'attaque. Elle est appréciée selon l'échelle suivante :

- *Facile* : exploitation triviale, sans outil particulier ;
- *Modérée* : exploitation nécessitant des techniques simples et des outils disponibles publiquement ;
- *Elevée* : exploitation de vulnérabilités publiques nécessitant des compétences en sécurité des systèmes d'information et le développement d'outils simples ;
- *Difficile* : exploitation de vulnérabilités non publiées nécessitant une expertise en sécurité des systèmes d'information et le développement d'outils spécifiques et ciblés.

L'impact correspond aux conséquences que l'exploitation de la vulnérabilité peut entrainer sur le système d'information de l'audité. Il est apprécié selon l'échelle suivante :

- *Mineur* : pas de conséquence directe sur la sécurité du système d'information audité ;
- *Important* : conséquences isolées sur des points précis du système d'information audité ;
- *Majeur* : conséquences restreintes sur une partie du système d'information audité ;
- *Critique* : conséquences généralisées sur l'ensemble du système d'information audité.

Le tableau suivant indique le niveau de risque inhérent à chaque vulnérabilité découverte, en fonction de leur difficulté d'exploitation et de leur impact présumé :

Facilité d'exploitation / **Impact**	**Difficile**	**Elevée**	**Modérée**	**Facile**
Mineur	*Mineur*	*Mineur*	*Important*	*Majeur*
Important	*Mineur/Important*[14]	*Important*	*Important*	*Majeur*
Majeur	*Important*	*Majeur*	*Majeur*	*Critique*
Critique	*Important*	*Majeur*	*Critique*	*Critique*

[14] Dans le cas des systèmes industriels des opérateurs d'importance vitale, au sens de la loi de programmation militaire, pour un impact *Important*, le niveau de risque est estimé à *Important*, même pour une facilité d'exploitation estimée à *Difficile*.