Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Premier ministre

Agence nationale de la sécurité des systèmes d'information

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

référentiel d'exigences

Version 2.1 du 6 octobre 2015

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.4. • 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

Les commentaires sur le présent document sont à adresser à :

Agence nationale de la sécurité des systèmes d'information

SGDSN/ANSSI

51 boulevard de La Tour-Maubourg
75700 Paris 07 SP

qualification@ssi.gouv.fr

SOMMAIRE

I. Introduction

I.1. Présentation générale

I.1.1. Contexte

L'interconnexion croissante des réseaux et les besoins de dématérialisation des processus ou des documents exposent les systèmes d'information à des 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 selon les modalités décrites au chapitre III.

Il permet au commanditaire de disposer de garanties sur la compétence du prestataire et de son personnel, sur la qualité de sa prestation et sur la confiance que le commanditaire peut leur accorder, notamment en matière de confidentialité.

Il peut être utilisé, à titre de bonnes pratiques, en dehors de tout contexte réglementaire.

Il n'exclut ni l'application de la législation et de la réglementation nationale, ni l'application des règles générales imposées aux prestataires en leur qualité de professionnels et 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 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
CA	Correspondant Audit
COFRAC	Comité français d'accréditation
PASSI	Prestataire d'audit de la sécurité des systèmes d'information

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.

Audité - organisme(s) responsable(s) de tout ou partie du système d'information audité[1]. Le commanditaire peut être l'audité.

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.

Commanditaire - entité faisant appel au service d'audit de la sécurité des systèmes d'information.

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

[1] Exemples : prestataires d'hébergement, d'infogérance, d'exploitation et d'administration du système d'information, de tierce maintenance applicative, etc.

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

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

État de l'art - ensemble des bonnes pratiques, des technologies et des documents de référence relatifs à la sécurité des systèmes d'information publiquement accessibles à un instant donné, et des informations qui en découlent de manière évidente. Ces documents peuvent être mis en ligne sur Internet par la communauté de la sécurité des systèmes d'information, diffusés par des organismes de référence ou encore d'origine réglementaire.

Périmètre d'audit - environnement physique, logique et organisationnel dans lequel se trouve le système d'information ou la portion du système d'information, sur lequel l'audit est effectué.

Prestataire - organisme proposant une offre de service d'audit de la sécurité des systèmes d'information.

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

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

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).

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.

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.

L'Annexe 3 fournit des recommandations de l'ANSSI sur les types d'audit à réaliser en fonction du périmètre de l'audit.

II.1. Audit d'architecture

L'audit d'architecture consiste en la vérification de la conformité des pratiques de sécurité relatives au choix, au positionnement et à la mise en œuvre des dispositifs matériels et logiciels déployés dans un système d'information à l'état de l'art et aux exigences et règles internes de l'audité. L'audit peut être étendu aux interconnexions avec des réseaux tiers, et notamment Internet.

II.2. Audit de configuration

L'audit de configuration a pour vocation de vérifier la mise en œuvre de pratiques de sécurité conformes à l'état de l'art et aux exigences et règles internes de l'audité 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'analyse de tout ou partie du code source ou des conditions de compilation d'une application dans le but d'y découvrir des vulnérabilités, liées à de mauvaises pratiques de programmation ou des erreurs de logique, qui pourraient avoir un impact en matière de sécurité.

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.

Un test d'intrusion seul n'a pas vocation à être exhaustif. Il s'agit d'une activité qui doit être effectuée en complément d'autres activités d'audit afin d'en améliorer l'efficacité ou de démontrer la faisabilité de l'exploitation des failles et vulnérabilités découvertes à des fins de sensibilisation.

Les tests de vulnérabilité, notamment automatisés, ne représentent pas à eux seuls une activité d'audit au sens du référentiel.

II.5. Audit organisationnel et physique

L'audit de l'organisation de la sécurité logique et physique vise à s'assurer que :

- les politiques et procédures de sécurité définies par l'audité pour assurer le maintien en conditions opérationnelles et de sécurité d'une application ou de tout ou partie du système d'information sont conformes au besoin de sécurité de l'organisme audité, à l'état de l'art ou aux normes en vigueur ;
- elles complètent correctement les mesures techniques mises en place ;

- elles sont efficacement mises en pratique ;
- les aspects physiques de la sécurité de l'application ou du système d'information sont correctement couverts.

II.6. Audit de systèmes industriels

L'audit de systèmes industriels consiste en l'évaluation du niveau de sécurité d'un système industriel et des dispositifs de contrôle associés. Il se compose d'un audit d'architecture, d'un audit de la configuration des éléments composant l'architecture ainsi que d'un audit organisationnel et physique.

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.

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

Pour être qualifié, un prestataire doit répondre à toutes les exigences du présent référentiel sur les activités d'audit choisies.

Pour être qualifié dans le cadre de la loi de programmation militaire, un prestataire doit, en plus des exigences du présent référentiel, répondre aux exigences supplémentaires définies dans [PASSI_LPM].

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 ne portant que sur l'activité de tests d'intrusion ou l'activité d'audit organisationnel et physique n'est pas autorisée, une telle activité étant jugée insuffisante si elle est menée seule.

Le prestataire respectera en conséquence les exigences du chapitre VI.2 en cohérence avec la portée demandée.

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 évalués individuellement et reconnus compétents pour ces activités, conformément au chapitre V et travaillant pour un prestataire respectant les exigences du chapitre IV.

Est considérée comme une prestation qualifiée au sens de la loi de programmation militaire, 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 (PRIS, PDIS).

III.3. Avertissement

Une prestation d'audit non qualifiée peut potentiellement exposer le commanditaire à certains risques et notamment la fuite d'informations confidentielles, la compromission, la perte ou l'indisponibilité de son système d'information. Ainsi, dans le cas d'une prestation non qualifiée, il est recommandé au commanditaire d'exiger de la part de son 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 respecter la législation et la réglementation en vigueur sur le territoire national.

c) Le prestataire doit décrire l'organisation de son activité d'audit auprès du commanditaire.

d) Le prestataire a, en sa qualité de professionnel, un devoir de conseil vis-à-vis du commanditaire.

e) Le prestataire doit assumer la responsabilité des activités qu'il réalise pour le compte du commanditaire dans le cadre de la prestation et en particulier les éventuels dommages causés au commanditaire.

f) Le prestataire doit souscrire une assurance professionnelle couvrant les éventuels dommages causés au commanditaire et notamment à son système d'information dans le cadre de la prestation.

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

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

i) Le prestataire doit apporter une preuve suffisante que les modalités de son fonctionnement, notamment financières, ne sont pas susceptibles de compromettre son impartialité et la qualité de ses prestations à l'égard du commanditaire ou de provoquer des conflits d'intérêts.

j) 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.

k) Le prestataire doit disposer des licences valides des outils (logiciels ou matériels) utilisés pour la réalisation de la prestation.

l) Le prestataire doit demander au commanditaire de lui communiquer les éventuelles exigences légales et réglementaires spécifiques auxquelles il est soumis et notamment celles liées à son secteur d'activité.

m) Le prestataire doit informer le commanditaire lorsque ce dernier est tenu de déclarer un incident de sécurité à une instance gouvernementale et doit l'accompagner dans cette démarche si ce dernier en fait la demande.

n) Le prestataire doit réaliser sa prestation dans le cadre d'une convention approuvée formellement et par écrit par le commanditaire, et conforme aux exigences du chapitre VI.1.

IV.2. Charte d'éthique

a) Le prestataire doit disposer d'une charte d'éthique prévoyant notamment que :

   - les prestations sont réalisées avec loyauté, discrétion et impartialité ;
   - les auditeurs ne recourent qu'aux méthodes, outils et techniques validés par le prestataire ;
   - les auditeurs s'engagent à ne pas divulguer d'informations à un tiers, même anonymisés et décontextualisées, obtenues ou générées dans le cadre de leurs activités, sauf autorisation du commanditaire ;

- les auditeurs signalent au commanditaire tout contenu manifestement illicite découvert durant la prestation ;
- les auditeurs s'engagent à respecter la législation et la réglementation nationale en vigueur ainsi que les bonnes pratiques liées à leurs activités d'audit.

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

IV.3. Gestion des ressources et des compétences

a) Le prestataire doit employer un nombre suffisant d'auditeurs, de responsables d'équipe d'audit et éventuellement recourir à des sous-traitants pour assurer totalement et dans tous leurs aspects les activités d'audit pour lesquels il a établi des conventions avec des commanditaires. Le prestataire doit s'assurer, pour chaque prestation, que les auditeurs désignés ont les qualités et les compétences requises. Chaque auditeur doit disposer d'une attestation individuelle de compétence[2] pour les types d'audits qu'il réalise.

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[3].

c) Le prestataire doit, en matière de recrutement, procéder à une vérification des formations, compétences et références professionnelles des auditeurs candidats et de la véracité de leur *curriculum vitae*. Le prestataire est responsable des méthodes, outils (logiciels ou matériels) et techniques utilisés par ses auditeurs et de leur bonne utilisation (précautions d'usage, maîtrise de la configuration, etc.) 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).

d) Le prestataire doit disposer des licences valides des outils (logiciels ou matériels) utilisés pour la réalisation de la prestation.

e) Le prestataire justifie, au travers des auditeurs évalués au titre de la qualification du prestataire, qu'il dispose des compétences techniques, théoriques et pratiques, afférentes aux activités d'audit citées aux chapitres II.1 à II.4, couvrant les domaines détaillés en Annexe 2.

f) Le prestataire justifie, au travers des auditeurs évalués au titre de la qualification du prestataire, qu'il dispose des compétences organisationnelles, théoriques et pratiques, afférentes aux activités d'audit citées au chapitre II.5, couvrant les domaines détaillés en Annexe 2.

g) Le prestataire justifie, au travers des auditeurs évalués au titre de la qualification du prestataire, qu'il maîtrise la loi de programmation militaire, le Référentiel générale de sécurité et ses annexes ainsi que les référentiels et guides relatifs à la sécurité des systèmes d'information de l'ANSSI (voir Annexe 1).

h) Le prestataire doit mettre en place un processus de sensibilisation des auditeurs à la législation en vigueur sur le territoire français applicable à leurs missions.

i) Le prestataire doit s'assurer que les auditeurs ne font pas l'objet d'une inscription au bulletin n°3 du casier judiciaire.

j) Un processus disciplinaire doit être élaboré par le prestataire à l'intention des auditeurs ayant enfreint les règles de sécurité ou la charte d'éthique.

[2] Voir [PROCESS_QUALIF].

[3] Le prestataire d'audit 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, 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 ses auditeurs.

IV.4. Protection de l'information

a) Le prestataire doit protéger au minimum au niveau *Diffusion Restreinte* [IGI_1300] [II_901] les informations sensibles relatives à la prestation, et notamment les preuves, les constats et les rapports.

b) Le prestataire doit respecter les règles établies par l'ANSSI et relatives aux mesures de protection des systèmes d'information traitant d'informations sensibles non classifiées de défense de niveau *Diffusion Restreinte*.

c) Le prestataire doit homologuer son système d'information au niveau *Diffusion Restreinte*.

d) Il est recommandé que le prestataire utilise la démarche décrite dans le guide [HOMOLOGATION] pour homologuer son système d'information.

e) Le prestataire doit appliquer le guide d'hygiène informatique de l'ANSSI [HYGIENE] sur le système d'information utilisé par le prestataire dans le cadre du traitement des informations sensibles relatives à la prestation.

V. Exigences relatives aux auditeurs

V.1. Aptitudes générales

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

b) L'auditeur doit disposer des qualités personnelles décrites au chapitre 7.2.2 de la norme ISO 19011.

c) Le responsable d'équipe d'audit doit maîtriser la législation en vigueur sur le territoire français et applicable à ses missions ainsi qu'à celles des auditeurs.

d) L'auditeur doit être sensibilisé à la législation en vigueur sur le territoire français et applicable à leurs missions.

e) L'auditeur doit disposer de qualités rédactionnelles et de synthèse et savoir s'exprimer à l'oral de façon claire et compréhensible, en langue française.

f) L'auditeur doit régulièrement mettre à jour ses compétences conformément aux processus de formation et de veille du prestataire (voir chapitre IV.3, paragraphe b), par une veille active sur la méthodologie, les techniques et les outils utilisés dans le cadre de ses missions.

g) Il est recommandé que l'auditeur participe 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) L'auditeur doit avoir reçu une formation en technologies des systèmes d'information.

b) Il est recommandé que l'auditeur justifie :

- 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 ;
- d'au moins deux années d'expérience dans le domaine des systèmes industriels, pour réaliser l'activité d'audit de la sécurité des systèmes industriels.

Ces recommandations ne sont pas cumulatives.

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

a) L'auditeur doit maîtriser les bonnes pratiques et la méthodologie d'audit décrite dans la norme [ISO19011].

b) L'auditeur doit réaliser la prestation conformément aux exigences du chapitre VI.

c) L'auditeur doit assurer les missions selon son profil, telles que définies dans l'Annexe 2.

d) L'auditeur doit disposer des compétences requises par son profil, telles que définies dans l'Annexe 2.

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

V.4. Engagements

a) L'auditeur doit avoir un contrat avec le prestataire.

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

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

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

VI.1. Étape 1 – 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 doit être signée par un représentant légal du commanditaire et du prestataire.

VI.1.1. Modalités de la prestation

La convention de service doit :

a) décrire le périmètre de la prestation, la démarche générale d'audit de sécurité des systèmes d'information, les activités et les modalités de la prestation (objectifs, champs et critères de l'audit, jalons, livrables attendus en entrée, prérequis, etc.) ;

b) préciser si la prestation est qualifiée ou non ;

c) préciser les livrables attendus en sortie, les réunions d'ouverture et de clôture, les publics destinataires, leur niveau de sensibilité ou de classification et les modalités associées ;

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

e) décrire les méthodes de communication qui seront employées lors de la prestation entre le prestataire, le commanditaire et l'audité ;

f) prévoir les moyens logistiques devant être mis à disposition du prestataire par le commanditaire et l'audité (moyens matériels, humains, techniques, etc.) ;

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 indicateurs de compromission ou le rapport d'audit.

h) préciser les actions qui ne peuvent être menées sur le système d'information ou sur les informations collectées sans autorisation expresse du commanditaire et éventuellement accord ou présence du commanditaire, ainsi que les modalités associées (mise en œuvre, personnes présentes, durée, plage horaire, exécutant, description des données sensibles et des actions autorisées, etc.) ;

i) définir les moyens assurant la traçabilité entre l'audité et le prestataire des informations et supports matériels remis pour analyse.

VI.1.2. Organisation

La convention de service doit :

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

b) préciser les noms, rôles, responsabilités ainsi que les droits et besoins d'en connaître des personnes désignées par le prestataire, le commanditaire et l'audité. Cette exigence est d'autant plus importante si l'existence d'un incident de sécurité ne doit pas être divulguée ;

c) stipuler que le prestataire doit, le cas échéant, collaborer avec des prestataires tiers qui travaillent pour le compte de l'audité et qui auront été spécifiquement désignés par le commanditaire et distinguer clairement les responsabilités du prestataire tiers. Cette exigence doit notamment permettre au prestataire de collaborer avec un prestataire de détection d'incidents de sécurité ;

d) stipuler que le prestataire ne fait pas intervenir d'auditeurs n'ayant pas de relation contractuelle avec lui, n'ayant pas signé sa charte d'éthique, n'ayant pas obtenu une attestation individuelle de compétence[4] ou ayant fait l'objet d'une inscription au bulletin n°3 du casier judiciaire.

VI.1.3. Responsabilités

La convention de service doit :

a) stipuler que le prestataire ne réalisera la prestation qu'après une autorisation formelle et écrite du commanditaire ;

b) stipuler que le prestataire informe le commanditaire en cas de manquement à la convention ;

c) stipuler que le prestataire s'engage à ce que les actions réalisées dans le cadre de la prestation restent strictement en adéquation avec les objectifs de la prestation ;

d) stipuler que le commanditaire garantit disposer de l'ensemble des droits de propriété et d'accès sur le périmètre de la prestation (systèmes d'information, supports matériels, etc.) ou d'avoir recueilli l'accord des éventuels tiers, et notamment de ses prestataires ou de ses partenaires, dont les systèmes d'information entreraient dans le périmètre ;

e) stipuler que le commanditaire et le prestataire remplit toutes les obligations légales et réglementaires nécessaires aux activités d'audit ;

f) stipuler que le commanditaire autorise provisoirement le prestataire, aux seules fins de réaliser la prestation, d'accéder et de se maintenir dans tout ou partie du périmètre et d'effectuer des traitements sur les données hébergées, quelle que soit la nature de ces données ;

[4] Voir [PROCESS_QUALIF].

g) stipuler que le commanditaire autorise provisoirement le prestataire à reproduire, collecter et analyser, aux seules fins de réaliser la prestation, des données appartenant au périmètre du système d'information cible ;

h) définir les responsabilités et les précautions d'usage à respecter par l'ensemble des parties concernant les risques potentiels liés à la prestation, en matière de confidentialité des informations collectées et analysées ainsi qu'en matière de disponibilité (déni de service lors du scan de vulnérabilités d'une machine ou d'un serveur par exemple) et d'intégrité du système d'information ciblé ;

i) stipuler si le prestataire dispose d'une assurance professionnelle couvrant les éventuels dommages causés lors de la réalisation des activités d'audit et, le cas échéant, préciser la couverture de celle-ci et inclure l'attestation d'assurance.

VI.1.4. Confidentialité

La convention de service doit :

a) prévoir la non divulgation à un tiers, par le prestataire et par les auditeurs, de toute information relative à l'audit et à l'audité, sauf autorisation écrite ;

b) stipuler que le prestataire puisse, sauf refus formel et écrit du commanditaire, conserver certains types d'informations liées à la prestation une fois celle-ci terminée. Le prestataire devra identifier ces types d'informations dans la convention (ex : livrables, informations, documents, etc.) ;

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

d) stipuler que le prestataire détruit l'ensemble des informations relatives au commanditaire à l'issue de la prestation à l'exception de celles pour lesquelles il a reçu une autorisation de conservation de la part du commanditaire ;

e) préciser les modalités (contenu, forme, portée, etc.) de rédaction des recommandations.

f) Il est recommandé que la convention prévoie une procédure de recueil du consentement des audités et des éventuels partenaires pour la réalisation de l'audit.

VI.1.5. Lois et réglementations

La convention de service doit :

a) être rédigée en français. Le prestataire doit fournir une traduction de courtoisie de la convention de service si le commanditaire en fait la demande ;

b) stipuler que seule la version française fait foi, notamment dans le cadre d'un litige ;

c) stipuler que la législation applicable à la convention de service est la législation française ;

d) préciser les moyens techniques et organisationnels mis en œuvre par le prestataire pour le respect de la législation française applicable notamment ceux concernant :

- les données à caractère personnel [LOI_IL] ;
- l'abus de confiance [CP_ART_314-1],
- le secret des correspondances privées [CP_ART_226-15],
- le secret médical [CSP_ART_L1110-4],
- l'atteinte à la vie privée [CP_ART_226-1],
- l'accès ou le maintien frauduleux à un système d'information [CP_ART_323-1],
- le secret professionnel [CP_ART_226-13], le cas échéant sans préjudice de l'application de l'article 40 alinéa 2 du Code de procédure pénale relatif au signalement à une autorité judiciaire ;

e) préciser les éventuelles exigences légales et réglementaires spécifiques auxquelles est soumis le commanditaire et notamment celles liées à son secteur d'activité ;

f) prévoir les exigences à respecter par le prestataire dans le cadre d'une affaire judiciaire, civile ou arbitrale ;

g) définir la durée de conservation des informations liées à la prestation et notamment les évènements collectés et les incidents de sécurité détectés. Si besoin, une distinction de la durée de conservation peut être faite en fonction des types d'information. La durée minimale de conservation est de six mois sous réserve de la législation et de la réglementation française en vigueur.

VI.1.6. Sous-traitance

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

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

b) La convention doit préciser que le prestataire peut faire intervenir un expert sur une partie des activités, pour des besoins ponctuels, sous réserve que :

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

VI.1.7. Livrables

a) La convention doit préciser que tous les livrables produits par le prestataire au titre de la prestation sont fournis en langue française sauf si le commanditaire en fait la demande formelle et écrite.

VI.1.8. Qualification

La convention de service doit :

a) indiquer que la prestation réalisée est

- une prestation qualifiée et inclure l'attestation de qualification du prestataire[5] et des éventuels sous-traitants ;
- une prestation non qualifiée. Dans ce cas, le prestataire doit sensibiliser le commanditaire aux risques de ne pas exiger une prestation qualifiée.

b) indiquer que les auditeurs disposent d'une attestation individuelle de compétence[10] pour les activités d'audit et inclure ces attestations.

VI.2. Étape 2 – Préparation et déclenchement de la prestation

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

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

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

[5] Voir [PROCESS_QUALIF].

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

d) Le responsable d'équipe d'audit 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 d'audit 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 de démarrage 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, en considération des contraintes d'exploitation du système d'information de l'audité. 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 de l'audité (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) 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.3. Étape 3 – Exécution de la prestation

a) Le responsable d'équipe d'audit 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) L'audit doit être réalisé dans le respect des personnels et des infrastructures physiques et logiques de l'audité.

c) Les constatations et observations effectuées par les auditeurs doivent être factuelles et basées sur la preuve.

d) 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 l'audité, dans le respect des clauses de confidentialité fixées dans la convention d'audit.

e) Toute modification effectuée sur le système d'information audité, durant l'audit, doit être tracée, et 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.

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

g) Le prestataire et les auditeurs doivent prendre toutes les précautions utiles pour préserver la confidentialité des documents et informations relatives à l'audité.

h) Les actions et résultats des auditeurs du prestataire sur le système d'information audité, ainsi que leurs dates de réalisation, devraient être tracés. Ces traces peuvent par exemple servir à identifier les causes d'un incident technique survenu lors de l'audit.

VI.4. Exigences relatives au prestataire

Lorsqu'elles sont demandées par le commanditaire, les activités d'audit réalisées par le prestataire doivent être conformes aux exigences précisées dans les chapitres VI.4.1 à VI.4.5.

Le cas échéant, conformément au RGS, il est recommandé d'utiliser des produits qualifiés.

Remarques :

- les activités techniques décrites dans les paragraphes VI.4.1 à VI.4.4 n'excluent pas l'évaluation de l'organisation de la sécurité logique et physique des éléments audités. Cette évaluation consiste en la vérification que les politiques de sécurité et procédures définies pour assurer le maintien en conditions de sécurité du système d'information audité sont conformes à l'état de l'art ;
- les énumérations listées dans les chapitres VI.4.1 à VI.4.5 sont données à titre indicatif et ne sont pas exhaustives. Par ailleurs, elles ne doivent être réalisées que lorsqu'elles sont applicables à la cible auditée.

VI.4.1. Audit d'architecture

a) Le prestataire doit procéder à la revue des documents suivants lorsqu'ils existent :
   - schémas d'architectures de niveau 2 et 3 du modèle OSI ;
   - matrices de flux ;
   - règles de filtrage ;
   - configuration des équipements réseau (routeurs et commutateurs) ;
   - interconnexions avec des réseaux tiers ou Internet ;
   - analyses de risques système ;
   - documents d'architecture technique liés à la cible.

b) Le prestataire doit pouvoir 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 procédures d'administration.

VI.4.2. Audit de configuration

a) Les éléments de configuration des cibles auditées doivent être fournis au prestataire. Ils peuvent être récupérés manuellement ou automatiquement, à partir d'un accès privilégié sur les cibles auditées, sous la forme de fichiers de configuration ou de captures d'écran.

   Cette action peut être entreprise directement par l'auditeur après accord de l'audité.

   Il est recommandé que le prestataire vérifie, conformément à l'état de l'art ou aux exigences et règles spécifiques de l'audité, la sécurité des configurations :
   - des équipements réseau filaire ou sans fil de type commutateurs ou routeurs ;
   - des équipements de sécurité (type pare-feu ou relais inverse (filtrant ou non) et leurs règles de filtrage, chiffreurs, etc.) ;
   - des systèmes d'exploitation ;
   - des systèmes de gestion de bases de données ;

- des services d'infrastructure ;
- des serveurs d'applications ;
- des postes de travail ;
- des équipements de téléphonie ;
- des environnements de virtualisation.

b) Le prestataire doit pouvoir 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.4.3. Audit de code source

a) Le code source, la documentation relative à la mise en œuvre, les méthodes et rapports de tests et l'architecture du système d'information 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 l'audité.

b) Il est recommandé de procéder à des entretiens avec un développeur ou le responsable de la mise en œuvre du code source audité afin de disposer d'informations relatives au contexte applicatif, aux besoins de sécurité et aux pratiques liées au développement.

c) Il est recommandé que l'audit de code fasse préalablement l'objet d'une analyse de la sécurité de l'application auditée afin de limiter l'audit aux parties critiques de son code.

d) Il est recommandé que le prestataire vérifie la sécurité des parties du code source relatives :
- aux mécanismes d'authentification ;
- aux mécanismes cryptographiques ;
- à la gestion des utilisateurs ;
- au contrôle d'accès aux ressources ;
- aux interactions avec d'autres applications ;
- aux relations avec les systèmes de gestion de bases de données ;
- à la conformité à des exigences de sécurité relative à l'environnement dans laquelle est déployée l'application.

e) Il est recommandé que le prestataire recherche les vulnérabilités les plus répandues dans les domaines suivants : cross-site scripting, injections SQL, cross-site request forgery, erreurs de logique applicative, débordement de tampon, exécution de commandes arbitraires, inclusion de fichiers (locaux ou distants).

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

f) Les audits de code source peuvent être réalisés manuellement ou automatiquement par des outils spécialisés. Les phases automatisées, ainsi que les outils utilisés, doivent être identifiés dans les livrables et en particulier dans le rapport d'audit.

VI.4.4. Tests d'intrusion

a) 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 : l'auditeur ne dispose 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.

b) Le prestataire et le commanditaire doivent, préalablement à tout test d'intrusion, définir un profil d'attaquant simulé.

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

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

e) Les vulnérabilités non publiques découvertes lors de l'audit doivent être communiquées à l'ANSSI.

VI.4.5. Audit organisationnel et physique

a) Le prestataire doit analyser l'organisation de la sécurité des systèmes d'information sur la base des référentiels techniques et réglementaires en accord avec les réglementations et méthodes applicables dans le domaine d'activité de l'audité.

b) L'audit organisationnel et physique doit permettre de mesurer la conformité du système d'information audité par rapport aux référentiels et identifier les écarts présentant les vulnérabilités majeures du système audité.

c) L'audit organisationnel et physique peut intégrer l'analyse des éléments liés à la sécurité des aspects physiques des systèmes d'information et notamment la protection des locaux hébergeant les systèmes d'information et les données de l'audité ou le contrôle d'accès de ces locaux.

VI.4.6. Audit d'un système industriel

a) Le prestataire doit réaliser les activités suivantes sur le périmètre du système industriel et le cas échéant de son centre de contrôle :

- audit de l'architecture ;
- audit de configuration des composants ;
- audit organisationnel et physique ;

b) Le prestataire doit pouvoir organiser des entretiens avec le personnel concerné par la sécurité du système industriel, notamment le RSSI, le responsable opérationnel du système et le cas échéant, les correspondants techniques.

c) Il est recommandé au prestataire de sensibiliser le commanditaire aux risques de la réalisation de tests d'intrusion sur un environnement comportant des systèmes industriels.

VI.5. Étape 4 – Restitution

Dès la fin de l'audit, et sans attendre que le rapport d'audit soit achevé, le responsable d'équipe d'audit doit informer l'audité 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 5 – 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.

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[6] ;
  - les vulnérabilités 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 relevées, classées selon une échelle de valeur ;
  - la synthèse des mesures correctives proposées, 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.

e) 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.

f) Chaque vulnérabilité doit être associée à une ou plusieurs recommandations adaptées au système d'information de l'audité. Les recommandations décrivent les solutions permettant de résoudre temporairement ou définitivement la vulnérabilité et d'améliorer le niveau de sécurité.

g) Le rapport d'audit peut également présenter 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.

h) 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, etc.) ou à la pertinence de la cible auditée.

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

[6] 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.

j) Le rapport d'audit doit mentionner s'il s'agit d'une prestation d'audit qualifiée et préciser les activités d'audit associées.

VI.7. Étape 6 – Clôture de la prestation

a) Il est recommandé qu'une réunion de clôture de l'audit soit organisée avec le commanditaire et l'audité 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 d'organiser un jeu de questions / réponses. Elle est également l'occasion d'expliquer les recommandations complexes et, éventuellement, de proposer d'autres solutions plus aisées à mettre en œuvre.

b) Le responsable d'équipe d'audit doit demander à l'audité 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.

c) Toutes les traces, relevés de configuration, informations ou documents relatifs au système d'information audité obtenus par le prestataire doivent être restitués à l'audité ou, sur sa demande, détruits conformément à la convention d'audit. Le cas échéant, le responsable d'audit produit un procès verbal de destruction de ces données qu'il remet à l'audité et précisant les données détruites et leur mode de destruction.

d) 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.

e) 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.

f) Il est recommandé que le prestataire propose au commanditaire d'effectuer ultérieurement un audit de validation afin de vérifier si les mesures correctives proposées lors de l'audit ont été correctement mises en œuvre.

Annexe 1 Références documentaires

I. Codes, textes législatifs et réglementaires

Renvoi	Document
[LOI_IL]	Loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. Disponible sur http://www.legifrance.gouv.fr
[CP_ART_314-1]	Article 334-1 du Code pénal relatif à l'abus de confiance. Disponible sur http://www.legifrance.gouv.fr
[CP_ART_226-1]	Article 226-1 du Code pénal relatif à l'atteinte à la vie privée. Disponible sur http://www.legifrance.gouv.fr
[CP_ART_226-13]	Article 226-13 du Code pénal relatif au secret professionnel. Disponible sur http://www.legifrance.gouv.fr
[CP_ART_226-15]	Article 226-15 du Code pénal relatif au secret des correspondances. Disponible sur http://www.legifrance.gouv.fr
[CP_ART_323-1]	Article 323-1 du Code pénal relatif à l'accès ou au maintien frauduleux dans un système de traitement automatisé de données. Disponible sur http://www.legifrance.gouv.fr
[CSP_ART_L1110-4]	Article L1110-4 du Code de la santé publique relatif au secret médical. Disponible sur http://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_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
[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. 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.
[ETSI_ISG_ISI]	Standards ETSI ISI Indicators (ISI 001-1 and Guides 001-2), ISI Event Model (ISI-002), ISI Maturity (ISI-003), ISI Event Detection (ISI-004) – 5 standards sur la détection des incidents de sécurité. Disponible sur http://www.etsi.org
[ISO17020]	Norme internationale ISO/IEC 17020 :1998 : Critères généraux pour le fonctionnement de différents types d'organismes procédant à l'inspection. Disponible sur http://www.iso.org
[ISO19011]	Norme internationale ISO/IEC 19011 :2011: Lignes directrices pour l'audit des systèmes de management. Disponible sur http://www.iso.org
[ISO27000]	Norme internationale ISO/IEC 27000:2014 : Technologies de l'information – Techniques de sécurité – Systèmes de gestion de la sécurité de l'information – vue d'ensemble et vocabulaire. Disponible sur http://www.iso.org

Renvoi	Document
[ISO27001]	Norme internationale ISO/IEC 27001 : 2005 : Techniques de sécurité – Systèmes de gestion de la sécurité de l'information – Exigences. Disponible sur http://www.iso.org
[ISO27002]	Norme internationale ISO/IEC 27002 : 2005 : Techniques de sécurité – Code de bonne pratique pour la gestion de la sécurité de l'information. Disponible sur http://www.iso.org
[ISO27011]	Norme internationale ISO/IEC 27011 : 2008 : Lignes directrices de la gestion de la sécurité de l'information pour les télécoms. Disponible sur http://www.iso.org
[EBIOS]	Méthode de gestion de risques EBIOS 2010 Disponible sur http://www.ssi.gouv.fr/ebios/
[PSSI]	Guide d'élaboration de politiques de sécurité des systèmes d'information Disponible sur http://www.ssi.gouv.fr/pssi/
[TABLEAU_BORD]	Guide d'élaboration de tableaux de bord de sécurité des systèmes d'information Disponible sur http://www.ssi.gouv.fr/tdbssi/
[PROJETS]	Guide d'intégration de la sécurité des systèmes d'information dans les projets Disponible sur http://www.ssi.gouv.fr/gissip/
[MATURITE_SSI]	Guide relatif à la maturité SSI Disponible sur http://www.ssi.gouv.fr/maturite-ssi/
[EXTERNALISATION]	Externalisation et sécurité des systèmes d'information : un guide pour maîtriser les risques Disponible sur http://www.ssi.gouv.fr/externalisation/
[DEFENSE_PROF]	La défense en profondeur appliquée aux systèmes d'information Disponible sur http://www.ssi.gouv.fr/defense-profondeur/
[SYS_INDUS]	Maîtriser la SSI pour les systèmes industriels Cas pratique Méthodes de classification et mesures principales Mesures détaillées Disponibles sur http://www.ssi.gouv.fr/systemesindustriels/
[JAVA]	Sécurité et langage Java (Javasec) Disponible sur http://www.ssi.gouv.fr/javasec/
[NT_JOURNAL]	Recommandations de sécurité pour la mise en œuvre d'un système de journalisation, note technique n° DAT-NT-012/ANSSI/SDE/NP du 2 décembre 2013, ANSSI. Disponible sur http://www.ssi.gouv.fr/journalisation.
[NT_PASSE]	Recommandations de sécurité relatives aux mots de passe, note technique n° DAT-NT-001/ANSSI/SDE/NP du 5 juin 2012, ANSSI. Disponible sur http://www.ssi.gouv.fr/mots-de-passe.
[HOMOLOGATION]	L'homologation de sécurité en neuf étapes simples, ANSSI, version en vigueur. Disponible sur http://www.ssi.gouv.fr
[HYGIENE]	Guide d'hygiène informatique – version en vigueur. Disponible sur http://www.ssi.gouv.fr/hygiene-informatique.
[ENISA]	Guides de l'ENISA, notamment Technical Guideline on Minimum Security Measures Disponible sur http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/technical-guideline-on-minimum-security-measures
[JAVA]	Guides de développement sécurité Java Disponible sur http://www.oracle.com/technetwork/java/seccodeguide-139067.html
[MICROSOFT]	Guides de développement sécurisé Microsoft Disponible sur http://msdn.microsoft.com/fr-fr/library/ms954624.aspx

Renvoi	Document
[OWASP]	Guides et documentation de l'Open Web Application Security Project Disponible sur http://www.owasp.org

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

I. Responsable d'équipe d'audit

I.1. Missions

Le responsable d'équipe d'audit doit assurer les missions suivantes :

- mettre en œuvre une organisation adaptée aux objectifs de la prestation (voir chapitre VI.2) ;
- structurer l'équipe d'auditeurs (compétences, effectif) ;
- assurer la définition, le pilotage et le contrôle des activités des auditeurs (voir chapitre VI.3) ;
- mettre en œuvre les moyens adaptés aux objectifs de la prestation (voir chapitre VI.2) ;
- 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.

I.2. Compétences

Le responsable d'équipe d'audit 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.).

I.3. Compétences requises pour l'audit de systèmes industriels

Le responsable d'équipe d'audit de systèmes industriels doit de plus disposer 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.

II. Auditeur d'architecture

II.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 ;
- 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.

II.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 ;
  - 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).

II.3. Compétences requises pour l'audit de systèmes industriels

L'auditeur d'architecture de systèmes industriels doit de plus disposer 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.

III. Auditeur de configuration

III.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 ;
- 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.

III.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 ;
- 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).

III.3. Compétences requises pour l'audit de systèmes industriels

L'auditeur de configuration de systèmes industriels doit de plus disposer 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.

IV. Auditeur de code source

IV.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, 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.

IV.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).

IV.3. Compétences requises pour l'audit de systèmes industriels

L'auditeur de code source d'applications présentes dans des systèmes industriels doit de plus disposer 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) ;

V. Auditeur en tests d'intrusion

V.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.

V.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).

V.3. Compétences requises pour l'audit de systèmes industriels

L'auditeur en tests d'intrusion de systèmes industriels doit de plus disposer 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.

VI. Auditeur en sécurité organisationnelle et physique

VI.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 ;
- 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.

VI.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[7].
- maîtrise des domaines relatifs à l'organisation de la sécurité des systèmes d'information :
    - analyse des risques ;
    - politique de sécurité des systèmes d'information ;
    - chaines de responsabilités en sécurité des systèmes d'information ;
    - sécurité liée aux ressources humaines ;
    - gestion de l'exploitation et de l'administration du système d'information ;
    - contrôle d'accès logique au système d'information ;
    - développement et maintenance des applications ;
    - gestion des incidents liés à la sécurité de l'information ;
    - gestion du plan de continuité de l'activité ;
    - sécurité physique.
- maîtrise des pratiques liées à l'audit :
    - conduite d'entretien ;
    - visite sur site ;
    - analyse documentaire.

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).

VI.3. Compétences requises pour l'audit de systèmes industriels

L'auditeur en sécurité organisationnelle et physique doit être familier avec les sujets suivants :

- normes de sécurité fonctionnelle telle que l'IEC 61508 ;
- architectures fonctionnelles à base de PLC ;

[7] 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.

- 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) 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 pas suffisante pour bénéficier d'une prestation qualifiée, le commanditaire doit donc également exiger une prestation qualifiée.

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

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

f) 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.

g) 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.

h) 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.

Il est possible pour un commanditaire de recourir à un prestataire qualifié après s'être assuré que ce dernier dispose des habilitations de défense adéquates si nécessaire.

i) La qualification d'un prestataire n'atteste pas de sa capacité à accéder ou à détenir des articles contrôlés de la sécurité des systèmes d'information (ACSSI) [II_910].

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.

j) 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.

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[8]) en l'absence du titulaire du matériel ou sans son accord explicite.

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

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. 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) ;
  - 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 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*[9]	*Important*	*Important*	*Majeur*
Majeur	*Important*	*Majeur*	*Majeur*	*Critique*
Critique	*Important*	*Majeur*	*Critique*	*Critique*

[9] 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*.