



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secrétariat général
de la défense
et de la sécurité nationale

*Agence nationale de la sécurité
des systèmes d'information*

PRESTATAIRES D'AUDIT DE LA SECURITE DES SYSTEMES D'INFORMATION

Référentiel d'exigences

Version 1.0 du 31 octobre 2011

Sommaire

1.	Introduction	3
1.1.	Contexte réglementaire	3
1.2.	Contexte technique	3
1.3.	Objet du document.....	3
1.4.	Terminologie.....	4
1.5.	Structure du document	5
2.	Activités d’audit visées par le référentiel	5
2.1.	Audit d’architecture	5
2.2.	Audit de configuration	6
2.3.	Audit de code source	6
2.4.	Tests d’intrusion	6
2.5.	Audit organisationnel.....	6
3.	Qualification des prestataires d’audit	6
3.1.	Modalités de la qualification	6
3.2.	Portée de la qualification	7
4.	Exigences relatives au prestataire d’audit	7
4.1.	Exigences générales.....	7
4.2.	Charte d’éthique.....	8
4.3.	Gestion des ressources et des compétences	9
4.4.	Protection de l’information du prestataire d’audit.....	10
5.	Exigences relatives aux auditeurs	10
5.1.	Aptitudes générales.....	10
5.2.	Expérience	11
5.3.	Aptitudes et connaissances spécifiques aux activités d’audit.....	11
5.4.	Engagements.....	11
6.	Exigences relatives au déroulement d’un audit	11
6.1.	Convention d’audit	12
6.2.	Préparation et déclenchement de l’audit.....	13
6.3.	Exécution de l’audit	14
6.4.	Exigences spécifiques aux activités d’audit	14
6.4.1.	Audit d’architecture.....	15
6.4.2.	Audit de configuration	15
6.4.3.	Audit de code source	16
6.4.4.	Tests d’intrusion	16
6.4.5.	Audit organisationnel	17
6.5.	Elaboration du rapport d’audit.....	17
6.6.	Conclusion de l’audit	18
7.	Références documentaires	19
7.1.	Textes réglementaires	19
7.2.	Normes et documents techniques	19
7.3.	Autres références documentaires.....	19
Annexe A : Recommandations à l’intention des commanditaires d’audits		20
7.4.	Recommandations générales	20
7.5.	Types d’audit recommandés par l’ANSSI.....	21
Annexe B : Liste détaillée des compétences techniques et organisationnelles d’un prestataire d’audit.....		22
A.	Compétences techniques.....	22
B.	Compétences organisationnelles.....	22
8.	Annexe C : Echelle de classification des vulnérabilités.....	24

1. Introduction

1.1. Contexte réglementaire

L'ordonnance n° 2005-1516 du 8 décembre 2005, relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives, introduit la notion de prestataires de services de confiance (PSCO), publics ou privés, et prévoit qu'ils peuvent obtenir une qualification attestant de leur conformité aux règles du référentiel général de sécurité (RGS) qui leur sont applicables. La version 1.0 du RGS, approuvée par arrêté du Premier ministre le 6 mai 2010, permet la qualification de deux catégories de PSCO : les prestataires de services de certification électronique et les prestataires de services d'horodatage électronique.

Afin d'enrichir les prestations de services contribuant à la sécurisation des systèmes d'information sujettes à la qualification selon le schéma décrit au chapitre IV du décret n° 2010-112 du 2 février 2010 pris pour l'application des articles 9, 10 et 12 de l'ordonnance précitée, l'ANSSI a élaboré un référentiel d'exigences à l'intention des prestataires de services qui réalisent des audits de la sécurité des systèmes d'information des autorités administratives.

1.2. Contexte technique

Les avantages et gains associés à la dématérialisation des processus et documents, aux échanges par voie électronique ainsi que l'interconnexion des systèmes d'information à Internet ne sont plus à démontrer mais ne sont pas sans risques. En effet, les points d'interconnexion avec l'extérieur (et en particulier les téléservices) sont autant d'accès qu'un attaquant externe à l'organisme peut tenter d'utiliser pour s'introduire au sein même du système d'information de l'organisme, pour dérober, dénaturer ou encore détruire son patrimoine informationnel. Les attaquants sont parfois des utilisateurs autorisés à accéder au système d'information (exemples : salariés, stagiaires, prestataires de l'organisme). Il convient de prendre en considération cette source de menace.

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 et de contribuer ainsi à l'élévation de son niveau de sécurité, en vue, notamment, de son homologation de sécurité.

1.3. Objet du document

L'autorité administrative, si elle décide d'externaliser la prestation d'audit de la sécurité de son système d'information, doit attacher le plus grand soin dans le choix du prestataire. En effet, l'activité d'audit est critique eu égard aux vulnérabilités qu'elle est susceptible de révéler ainsi qu'à l'exploitation qui pourrait en être faite. A ce titre, l'autorité administrative auditée doit disposer de garanties sur la compétence du prestataire d'audit et de ses auditeurs, sur la qualité des audits qu'ils effectuent et sur la confiance qu'elle peut leur accorder, notamment en matière

de confidentialité et de déontologie, avant de lui donner accès à son système et aux informations qu'il contient.

C'est dans le but d'identifier de tels prestataires de confiance que l'ANSSI permet la qualification des « prestataires d'audit de la sécurité des systèmes d'information » (PASSI), selon les modalités décrites au chapitre 3.

Ce document n'exclut ni l'application des règles générales imposées aux prestataires d'audit en leur qualité de professionnel et notamment leur devoir de conseil vis-à-vis de leurs clients, ni l'application de la législation nationale et notamment des articles L. 323-1 et suivants du code pénal.

1.4. Terminologie

Les définitions ci-dessous sont notamment issues de la norme ISO 19011, du glossaire du document relatif à la stratégie publique de la France en matière de défense et de sécurité des systèmes d'information et de l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives.

Référentiel : le présent document.

Autorité administrative : sont considérées comme autorités administratives les administrations de l'Etat, 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.

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

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.

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 2.

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

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

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

Prestataire d'audit : organisme réalisant des prestations d'audits de la sécurité des systèmes d'information.

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

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.

Commanditaire de l'audit : organisme ou personne demandant un audit.

Audité : organisme(s) responsable(s) de tout ou partie du système d'information audité¹. Le commanditaire de l'audit peut être l'audité.

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.

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

Rapport d'audit : document de synthèse élaboré par l'équipe d'audit et remis au commanditaire de l'audit 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.

Etat 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.

1.5. Structure du document

Le chapitre 2 décrit les activités d'audit visées par le présent référentiel.

Le chapitre 3 présente les modalités de la qualification, qui atteste de la conformité du PASSI aux exigences qui leurs sont applicables.

Ces exigences sont présentées en trois domaines : celles relatives au prestataire d'audit lui-même (chapitre 4), celles relatives à ses auditeurs (chapitre 5) et celles relatives au déroulement de l'audit (chapitre 6).

L'annexe A donne des recommandations à l'intention des autorités administratives dans le but de les aider à exprimer leurs besoins en termes d'audit et à rédiger d'éventuels appels d'offres.

L'annexe B détaille les exemples des compétences techniques, théoriques et pratiques dont doit disposer un prestataire d'audit pour être qualifié.

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

2. Activités d'audit 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 6.

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

2.1. 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 matériel 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.

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

2.2. 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.

2.3. 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.

2.4. 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.

2.5. Audit organisationnel

L'audit de l'organisation de la sécurité 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, complètent correctement les mesures techniques mises en place, et enfin sont efficacement mises en pratique.

3. Qualification des prestataires d'audit

3.1. Modalités de la qualification

Le Référentiel contient les exigences que les prestataires d'audit de la sécurité de systèmes d'information doivent respecter dans le but d'obtenir la qualification. Il donne également des recommandations afin d'orienter les autorités administratives, et plus généralement les commanditaires d'audits, dans leurs expressions de besoins, et les prestataires d'audit dans les solutions qu'ils leur proposent.

La qualification des prestataires d'audit est réalisée conformément au schéma décrit au chapitre IV du décret n° 2010-112 du 2 février 2010.

Les recommandations sont données à titre de bonnes pratiques et ne feront pas l'objet d'une quelconque évaluation ou vérification en vue de la labellisation.

La procédure d'évaluation de la conformité des prestataires d'audit aux règles du Référentiel qui leur sont applicables fera l'objet de documents complémentaires.

3.2. Portée de la qualification

Le prestataire d'audit peut demander la qualification pour tout ou partie des activités d'audit décrites au chapitre 2. Toutefois, la qualification d'un prestataire d'audit ne portant que sur l'activité de tests d'intrusion ou l'activité d'audit organisationnel n'est pas autorisée, une telle activité étant jugée insuffisante si elle est menée seule.

Le prestataire d'audit respectera en conséquence les exigences du chapitre 6.2 en cohérence avec la portée demandée.

La qualification est accordée notamment au regard de la compétence des auditeurs qui réaliseront les prestations qualifiées. Les auditeurs seront reconnus compétents pour tout ou partie des types d'activité pour lequel le prestataire a demandé la qualification, à l'issue d'un processus d'évaluation par rapport à l'état de l'art. Les auditeurs ainsi que les activités d'audit pour lesquelles ils ont été reconnus compétents sont inscrits dans une liste spécifique.

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

4. Exigences relatives au prestataire d'audit

4.1. Exigences générales

Les exigences listées dans ce chapitre portent sur les domaines suivants : juridique, structurel, responsabilité et impartialité du prestataire d'audit.

- b) Le prestataire d'audit doit être une entité ou une partie d'une entité dotée de la personnalité morale de façon à pouvoir être tenu juridiquement responsable de toutes ses activités d'audit.

Une autorité administrative qui réalise des activités d'audit peut être considérée comme un prestataire d'audit.

- c) Le prestataire d'audit réalise ses audits dans le cadre d'une convention d'audit préalablement approuvée par le commanditaire de l'audit. La loi applicable à la convention d'audit est la loi française. La convention d'audit doit être conforme aux exigences du paragraphe 6.1 du Référentiel.

- d) Le prestataire d'audit assume la responsabilité de l'audit qu'il réalise pour le compte du commanditaire de l'audit, en particulier des dommages éventuellement causés au cours de l'audit.

Le prestataire et le commanditaire de l'audit peuvent préciser les modalités de partage des responsabilités au sein de la convention d'audit. Le prestataire peut s'exonérer de tout ou partie de sa responsabilité s'il est avéré que le dommage éventuellement subi par le commanditaire de l'audit résulte d'un défaut d'information de ce dernier.

Il est recommandé que le prestataire d'audit garde, notamment, la responsabilité des actions qu'il effectue lors de l'audit de son propre fait ainsi que de celles pour lesquelles le commanditaire de l'audit ne dispose pas de compétence particulière.

- e) Le prestataire d'audit doit pouvoir apporter la preuve qu'il a évalué les risques résultant de ses activités d'audit et qu'il a pris les dispositions appropriées pour couvrir les risques résultant de ses prestations d'audit. Il met à disposition du commanditaire de l'audit ces éléments de preuve.

Il est, à ce titre, recommandé que le prestataire d'audit souscrive une assurance couvrant les dommages éventuellement causés aux systèmes d'information de ses clients-

- f) Le prestataire d'audit peut sous-traiter une partie de l'audit demandé par le commanditaire de l'audit à un prestataire d'audit qualifié conforme aux exigences qui lui sont applicables du présent référentiel sous réserve que :
- il existe une convention ou un cadre contractuel documentés entre le prestataire d'audit et le sous-traitant ;
 - le recours à la sous-traitance est connu et accepté par le commanditaire et l'audité.
- g) Le prestataire d'audit est tenu de respecter la législation et la réglementation en vigueur sur le territoire français, notamment en matière de traitements de données à caractère personnel², de prêt de main d'œuvre illicite, de propriété intellectuelle³ et de fraude informatique⁴.
- h) Le prestataire d'audit doit décrire l'organisation de son activité d'audit au bénéfice de chaque commanditaire d'audit.
- i) Le prestataire d'audit doit garantir que les informations qu'il fournit, y compris la publicité, ne sont ni fausses ni trompeuses.
- j) Le prestataire s'assure du consentement du commanditaire de l'audit avant toute communication au public d'éléments d'information relatifs à l'audit, à l'audité ou au commanditaire de l'audit, que ces informations soient obtenues lors de l'audit ou non.
- k) Le prestataire d'audit doit s'engager à ce que les audits qu'il effectue soient réalisés en toute impartialité.

Le prestataire d'audit doit être en mesure d'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 de l'audit ou de provoquer des conflits d'intérêts.

- l) Tous les documents produits par le prestataire d'audit lors des audits doivent être au moins fournis en langue française.
- m) Le prestataire d'audit doit réaliser la prestation de manière loyale, en toute bonne foi et dans le respect de l'audité, de son personnel et de ses infrastructures.

Les points 4.1.d, 4.1.g et 4.1.i ne s'appliquent qu'aux prestataires d'audit privés.

4.2. Charte d'éthique

- a) Le prestataire d'audit doit disposer d'une charte d'éthique prévoyant notamment que :
- les prestations d'audit sont réalisées avec loyauté, discrétion, impartialité et indépendance ;

² Loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, loi n° 91-646 du 10 juillet 1991 modifiée sur le secret des correspondances, loi n° 2004-669 du 9 juillet 2004 relative aux communications électroniques et aux services de communication audiovisuelle.

³ Exemples : licences des logiciels utilisés, des scripts et programmes développés.

⁴ Articles 323-1 et suivants du code pénal.

- les auditeurs ne recourent qu'aux méthodes, outils et techniques validés par le prestataire d'audit ;
 - les auditeurs s'engagent à ne pas divulguer d'informations obtenues ou générées dans le cadre des audits sauf autorisation du commanditaire de l'audit ;
 - les auditeurs signalent au commanditaire de l'audit tout contenu manifestement illicite découvert durant l'audit ;
 - les auditeurs s'engagent à respecter la loi, la réglementation en vigueur ainsi que les bonnes pratiques liées à l'audit.
- b) L'ensemble des auditeurs évalués au titre de la qualification du prestataire d'audit doivent signer la charte d'éthique prévue au paragraphe précédent préalablement à la réalisation d'un quelconque audit.

4.3. Gestion des ressources et des compétences

- a) Le prestataire d'audit doit employer un nombre suffisant d'auditeurs, de responsables d'équipe d'audit et éventuellement de sous-traitants pour assurer totalement et dans tous leurs aspects les audits pour lesquels il a établi des conventions d'audit avec des commanditaires d'audits.
- b) Le prestataire d'audit doit s'assurer, pour chaque audit, que les auditeurs désignés pour réaliser l'audit ont les qualités et les compétences requises.

Des auditeurs débutants du prestataire d'audit peuvent, au titre de leur formation et de leur montée en compétence, être incorporés à l'équipe d'audit. Ils doivent cependant respecter la charte d'éthique du prestataire ainsi que l'ensemble des obligations contractuelles, réglementaires ou légales imposées aux auditeurs.

- c) Le prestataire d'audit doit s'assurer du maintien à jour des compétences des auditeurs. Pour cela, il doit disposer d'un processus de formation et assurer une veille technologique⁵.
- d) En matière de recrutement, le prestataire d'audit doit procéder à une vérification des formations, qualifications et références professionnelles des auditeurs candidats et de la véracité de leur CV. Le prestataire d'audit peut également demander au candidat une copie du bulletin n° 3 de son casier judiciaire.
- e) Un processus disciplinaire doit être élaboré par le prestataire d'audit à l'intention des salariés ayant enfreint les règles de sécurité ou la charte d'éthique.
- f) Le prestataire d'audit 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...). Pour cela, il doit mettre en œuvre un processus de formation des auditeurs à ses outils et assurer une veille technologique sur leur mise à jour et leur pertinence.
- g) Le prestataire d'audit justifie, au travers des auditeurs évalués au titre de la qualification du prestataire d'audit, qu'il dispose des compétences techniques, théoriques et pratiques, afférentes aux activités d'audit citées aux paragraphes 2.1 à 2.4, couvrant les domaines suivants :
- réseaux et protocoles ;

⁵ 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.

- systèmes d'exploitation ;
- couche applicative ;
- équipements et logiciels de sécurité ;
- développement d'outils utilisés adaptés à la cible auditée dans le cadre des audits ou des tests d'intrusion ;
- techniques d'ingénierie inverse ;
- exigences techniques requises par le Référentiel Général de Sécurité.

Ces domaines sont détaillés en annexe B.

- h) Le prestataire d'audit justifie, au travers des auditeurs évalués au titre de la qualification du prestataire d'audit, qu'il dispose des compétences organisationnelles, théoriques et pratiques, afférentes aux activités d'audit citées au paragraphe 2.5, couvrant les domaines suivants :
- maîtrise des normes relatives à la sécurité des systèmes d'information ;
 - maîtrise des domaines relatifs à l'organisation de la sécurité des systèmes d'information ;
 - maîtrise des pratiques liées à l'audit.

Ces domaines sont détaillés en annexe B.

- i) Le prestataire d'audit justifie, au travers des auditeurs évalués au titre de la qualification du prestataire d'audit, qu'il maîtrise les référentiels et guides relatifs à la sécurité des systèmes d'information.

Ces référentiels et guides sont détaillés en annexe B.

4.4. Protection de l'information du prestataire d'audit

Les informations sensibles relatives aux audits, et notamment les preuves, les constats et les rapports d'audit, doivent être protégés au minimum au niveau Diffusion Restreinte. Le système d'information que le prestataire d'audit utilise pour le traitement de ces informations doit respecter les règles de l'instruction interministérielle relative aux mesures de protection des systèmes d'information traitant d'informations sensibles non classifiées de défense de niveau Diffusion Restreinte et établie par l'ANSSI.

5. Exigences relatives aux auditeurs

5.1. Aptitudes générales

- a) L'auditeur doit disposer des qualités personnelles décrites au chapitre 7.2 de la norme ISO 19011.
- b) L'auditeur doit maîtriser la réglementation applicable aux activités d'audits qu'il met en œuvre (maîtrise de la réglementation spécifique aux types d'audits, à la nature ou au secteur d'activité du commanditaire et de l'audit, etc.).
- c) 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.
- d) L'auditeur met régulièrement à jour ses compétences par une veille active sur celles-ci, sur la méthodologie, les techniques ou les outils utilisés lors des activités d'audit.

Il est recommandé que l'auditeur participe à l'évolution de l'état de l'art par une participation à des événements professionnels de son domaine de compétence, à des travaux de recherche ou la publication d'articles.

5.2. Expérience

L'auditeur doit avoir reçu une formation en technologie des systèmes d'information et de communication et en audit.

Il est recommandé que l'auditeur :

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

Ces recommandations ne sont pas cumulatives.

5.3. 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 ISO 19011 et être en mesure de réaliser des audits conformément aux exigences relatives au déroulement d'une prestation d'audit (cf. chapitre 6).
- b) L'auditeur doit être compétent dans au moins une des activités d'audit décrites au chapitre 2 pour lesquelles le prestataire d'audit demande la qualification. Pour cela, l'auditeur doit disposer de connaissances techniques ou organisationnelles approfondies dans au moins un des domaines cités dans les paragraphes 4.3.g et 4.3.h.

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

- c) Le responsable d'audit doit disposer des compétences de gestion d'équipe nécessaire à la constitution adéquate de l'équipe d'audit par rapport aux objectifs visés dans la convention d'audit.

5.4. Engagements

- a) L'auditeur doit avoir un contrat avec le prestataire d'audit.
- b) L'auditeur doit avoir signé la charte d'éthique élaborée par le prestataire d'audit.
- c) L'auditeur s'engage à subir une évaluation personnelle de ses compétences au titre de la procédure de qualification du prestataire d'audit dont il dépend.
- d) Il est recommandé que le commanditaire de l'audit ait la capacité à révoquer un auditeur qui ne disposerait pas des compétences attendues.

6. Exigences relatives au déroulement d'un audit

La définition du périmètre de l'audit et la description de l'audit attendu, formulées généralement dans un appel d'offres, sont du ressort du commanditaire de l'audit. L'annexe A du référentiel fournit des recommandations de l'ANSSI à cet effet.

Bien que le prestataire d'audit 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 de l'audit des recommandations issues de l'annexe A.

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

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

Le prestataire d'audit s'assure que l'audit est adapté au contexte et aux objectifs souhaités par le commanditaire de l'audit.

A défaut, le prestataire d'audit en informe le commanditaire de l'audit préalablement à l'audit.

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

- établissement de la convention d'audit ;
- préparation et déclenchement de l'audit ;
- exécution de l'audit (les exigences spécifiques à chacune des activités d'audit sont listées) ;
- élaboration du rapport d'audit ;
- conclusion de l'audit.

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

6.1. Convention d'audit

a) La convention établie entre le prestataire d'audit et le commanditaire de l'audit doit :

- décrire le périmètre et les modalités de l'audit (jalons, livrables attendus en entrée, livrables prévus en sortie, objectifs, champs et critères de l'audit...) ;
- préciser les noms, rôles, responsabilités et le besoin d'en connaître des personnes désignées par le prestataire d'audit, le commanditaire de l'audit et l'audité ;
- prévoir que l'audit ne peut débuter sans une autorisation formelle du commanditaire de l'audit ;
- préciser les actions qui ne peuvent être menées sur le système d'information à auditer ou sur les données recueillies sans autorisation expresse du commanditaire de l'audit et éventuellement accord ou présence de l'audité, ainsi que leurs modalités (mise en œuvre, personnes présentes, durée, plage horaire, exécutant, description des données sensible et des actions autorisées...) ;
- préciser les dispositions d'ordre logistique mises à disposition du prestataire d'audit par l'audité (moyens matériels, humains, techniques...) ;
- inclure les clauses relatives à l'éthique du prestataire d'audit ;
- prévoir la non divulgation à un tiers, par le prestataire d'audit et par les auditeurs, de toute information relative à l'audit et à l'audité, sauf autorisation écrite ;
- stipuler que le prestataire d'audit ne fait pas intervenir d'auditeur n'ayant pas de relation contractuelle avec lui, n'ayant pas signé sa charte d'éthique ou ayant fait l'objet d'une inscription au bulletin n° 3 du casier judiciaire en lien avec les systèmes d'information ;
- prévoir une clause relative aux risques potentiels liés à la prestation, notamment en matière de disponibilité (déni de service lors du *scan* de vulnérabilités d'une machine ou d'un serveur par exemple) ;
- préciser si le prestataire d'audit dispose d'une assurance couvrant les dommages éventuellement causés lors de la réalisation des activités d'audit et, le cas échéant, la surface de couverture de celle-ci ;

- définir les règles de titularité des éléments protégés par la propriété intellectuelle tels que les outils développés spécifiquement pour l'audit ;
 - prévoir les livrables ainsi que leurs modalités de restitution.
- b) Le prestataire d'audit peut sous-traiter une partie de l'audit demandé par le commanditaire de l'audit à un prestataire d'audit qualifié conforme aux exigences du présent référentiel sous réserve que :
- il existe une convention ou un cadre contractuel documentés entre le prestataire d'audit et le sous-traitant ;
 - le recours à la sous-traitance est connu et accepté par le commanditaire et l'audité.
- c) Il est recommandé que la convention prévoie une procédure de recueil du consentement des audités pour la réalisation de l'audit.

6.2. Préparation et déclenchement de l'audit

- a) Le prestataire d'audit 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. Il peut incorporer à l'équipe d'audit des auditeurs débutants, au titre de leur formation et de leur montée en compétence sous réserve du respect des obligations décrites au paragraphe 4.3 b) alinéa 2.
- c) Le responsable d'équipe d'audit doit, dès le début de la préparation de l'audit, établir un contact avec les personnes responsables de l'audit chez l'audité. Ce contact, formel ou informel, a notamment pour objectif d'établir les circuits de communication et de préciser les modalités d'exécution de l'audit.
- d) Le responsable d'audit s'assure auprès du commanditaire et de l'audité que les représentants légaux des entités impactées par l'audit ont été préalablement averties 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 d'audit et le commanditaire de l'audit, en considération des contraintes d'exploitation du système d'information de l'audité. Ces éléments doivent figurer dans la convention 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 (exemples : politique de sécurité, analyse des risques, procédures d'exploitation de la sécurité...) de l'audité 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 d'audit 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 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 de l'audit, l'audité et d'éventuelles tierces parties. Elle précise en particulier :
 - la liste des cibles auditées (adresses IP, noms de domaine...) ;
 - la liste des adresses IP de provenance des tests ;
 - la date et les heures exclusives des tests ;
 - la durée de l'autorisation.

6.3. Exécution de l'audit

- a) Le responsable d'équipe d'audit doit tenir informé le commanditaire de l'audit 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 d'audit, durant toute la durée de l'audit.
- g) Le prestataire d'audit 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 d'audit 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.
- i) 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 de l'audit des constats et des premières conclusions de l'audit, ainsi que, le cas échéant, des vulnérabilités majeures et critiques qui nécessiteraient une action rapide ainsi que des recommandations associées.

6.4. Exigences spécifiques aux activités d'audit

Lorsqu'elles sont demandées par le commanditaire de l'audit, les activités d'audit réalisées par le prestataire d'audit doivent être conformes aux exigences précisées dans les chapitres 6.4.1 à 6.4.5.

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

Remarques :

- les activités techniques décrites dans les paragraphes 6.4.1 à 6.4.4 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 6.4.1 à 6.4.5 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.

6.4.1. Audit d'architecture

- a) Le prestataire d'audit 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 d'audit 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.

6.4.2. Audit de configuration

- a) Les éléments de configuration des cibles auditées doivent être fournis au prestataire d'audit. 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 d'audit 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.
- c) Le prestataire d'audit doit, à l'issue de l'audit de la configuration effectuer des recommandations sur :
- les mécanismes d'authentification (robustesse des dispositifs...) ;
 - les mécanismes cryptographiques utilisés ;

- les règles de filtrage réseau (entrée, sortie, routage, NAT...);
- les bonnes pratiques en matière de segmentation (VLAN...);
- les bonnes pratiques de durcissement des systèmes d'exploitation, des configurations des serveurs applicatifs et des services d'infrastructure.

6.4.3. *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 d'audit ainsi que la configuration des éléments de compilation et d'exécution, dans les limites des droits dont disposent le commanditaire de l'audit 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 audité afin de limiter l'audit aux parties critiques de son code.
- d) Il est recommandé que le prestataire d'audit vérifie la sécurité des parties du code source relatives à :
 - l'authentification ;
 - la gestion des utilisateurs ;
 - le contrôle d'accès aux ressources ;
 - les interactions avec d'autres applications ;
 - les relations avec les systèmes de gestion de bases de données ;
 - la conformité à des exigences de sécurité relative à l'environnement dans laquelle est déployée l'application.
- e) Il est recommandé que le prestataire d'audit 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.

6.4.4. *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 audité. 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... ;
 - phase *boîte grise* : les auditeurs disposent des connaissances d'un utilisateur standard du système d'information (authentification légitime, poste de travail « standard »...). 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...) 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 d'audit et le commanditaire doivent, préalablement à tout test d'intrusion, définir un profil d'attaquant simulé.
- c) Le prestataire d'audit doit avoir un contact permanent avec l'audité et l'auditeur doit prévenir le commanditaire de l'audit 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 au CERTA (<http://www.certa.ssi.gouv.fr>).

6.4.5. *Audit organisationnel*

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

L'audit organisationnel 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.

6.5. Elaboration du rapport d'audit

- a) Pour tout audit, le prestataire d'audit doit établir un rapport d'audit.
- b) Le rapport d'audit doit être adapté en fonction de l'activité d'audit réalisée par le prestataire d'audit.
- c) Le rapport d'audit doit contenir en particulier :
 - une synthèse, compréhensible par des non experts, qui précise :
 - o le contexte et le périmètre de l'audit⁶ ;
 - o les vulnérabilités critiques, d'origine technique ou organisationnelle, et les mesures correctives proposées ;
 - o 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 :
 - o la synthèse des vulnérabilités relevées, classées selon une échelle de valeur ;
 - o la synthèse des mesures correctives proposées, classées par criticité et par complexité ou coût estimé de correction ;

⁶ Compte tenu du fait que le commanditaire 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.

- 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) 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 C. A défaut, le prestataire d'audit doit être en mesure de proposer une échelle pertinente.
- e) Il doit être mentionné dans le rapport d'audit les réserves relatives à l'exhaustivité des résultats de l'audit (liées aux délais alloués à l'audit, à la disponibilité des informations demandées...) ou à la pertinence de la cible auditée.
- f) Le rapport d'audit mentionne les noms et coordonnées des auditeurs, responsables d'équipe d'audit et commanditaires de l'audit.

6.6. Conclusion de l'audit

- a) Une réunion de clôture de l'audit doit être organisée avec le commanditaire de l'audit et l'auditée 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.
- b) Le responsable d'équipe d'audit doit demander à l'auditée 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 d'audit de tout problème postérieur à l'audit.
- c) Toutes les traces, relevés de configuration, informations ou documents relatifs au système d'information audité obtenue par le prestataire d'audit doivent être restitués à l'auditée ou, sur sa demande, détruits. Le cas échéant, le responsable d'audit produit un procès verbal de destruction de ces données qu'il remet à l'auditée 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 de l'audit peut demander au prestataire d'audit 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 script 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 d'audit.
- e) L'audit est considéré comme terminé lorsque toutes les activités prévues ont été réalisées et que le commanditaire de l'audit a reçu et attesté que le rapport d'audit est conforme aux objectifs visés dans la convention d'audit.
- f) Il est recommandé que le prestataire d'audit propose au commanditaire de l'audit 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.

7. Références documentaires

7.1. Textes réglementaires

Ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives.

Décret n° 2010-112 du 2 février 2010 pris pour l'application des articles 9, 10 et 12 de l'ordonnance n° 2005-1516.

Arrêté du 6 mai 2010 portant approbation du référentiel général de sécurité et précisant les modalités de mise en œuvre de la procédure de validation des certificats électroniques <http://www.ssi.gouv.fr/rgs>.

Instruction interministérielle – Recueil de mesures de protection des systèmes d'information traitant d'informations sensibles non classifiées de défense de niveau Diffusion Restreinte, version du 28 avril 2011.

7.2. Normes et documents techniques

Norme internationale ISO/IEC 17020 :1998 : Critères généraux pour le fonctionnement de différents type d'organismes procédant à l'inspection.

Norme internationale ISO/IEC 19011 :2002 : Lignes directrices pour l'audit des systèmes de management de la qualité ou de management environnemental.

Norme internationale ISO/IEC 27001 : 2005 : Techniques de sécurité – Systèmes de gestion de la sécurité de l'information – Exigences.

Norme internationale ISO/IEC 27002 : 2005 : Techniques de sécurité – Code de bonne pratique pour la gestion de la sécurité de l'information.

Guides de l'ANSSI et notamment les guides « Sécurité de l'externalisation » et « Javasec », publiés sur <http://www.ssi.gouv.fr> .

Guides et documentation de l'*Open Web Application Security Project* (OWASP).

Guides de développement sécurisé Microsoft <http://msdn.microsoft.com/fr-fr/library/ms954624.aspx>

Guides de développement sécurité Java <http://www.oracle.com/technetwork/java/seccodeguide-139067.html>

7.3. Autres références documentaires

Défense et sécurité de l'information – Stratégie publique (de la France) – Glossaire

Publié sur <http://www.ssi.gouv.fr>.

Les règles d'hygiène informatique promues par l'ANSSI.

Annexe A : Recommandations à l'intention des commanditaires d'audits

Cette annexe liste les recommandations de l'ANSSI à l'intention des autorités administratives, et plus généralement des commanditaires d'audits, dans le cadre de la passation de marchés publics, ainsi qu'aux prestataires d'audit dans le cadre de leur devoir de conseil.

L'ANSSI peut être consultée pour participer à la définition du cahier des charges des audits faisant l'objet d'un appel d'offres.

7.4. Recommandations générales

- a) Il est recommandé que le prestataire puisse fournir des références permettant d'estimer de sa compétence : références clients, participation à des programmes de recherche...
- b) Les audits devraient être le plus exhaustif possible, tout en tenant compte des contraintes temporelles et budgétaires allouées à l'audit.
- c) 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.
- d) 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...
 - 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...
- e) Il est préférable de réaliser les tests d'intrusions 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.
- f) La définition du périmètre d'un audit doit être basée sur une analyse préalable des risques « métier » de l'audit. Il est recommandé au commanditaire de l'audit d'indiquer les éléments les plus sensibles de la cible auditée au prestataire d'audit.
- g) Il est recommandé que le commanditaire de l'audit 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.).
- h) 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 à tout audit.

7.5. Types d'audit recommandés par l'ANSSI

- a) L'ANSSI recommande aux commanditaires et aux prestataires d'audit de la sécurité des systèmes d'information 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).
 - *audit d'un centre serveur* :
 - audit d'architecture réseau (liaison entre les différentes zones et entités, filtrage) ;
 - audit de configuration (équipements réseau et de sécurité, serveurs d'infrastructure) ;
 - audit organisationnel.
 - *audit d'un réseau bureautique* :
 - audit d'architecture réseau ;
 - audit de configuration (équipements réseau, serveurs bureautique, serveurs AD) ;
 - audit organisationnel.
 - *audit d'une plate-forme de téléphonie* :
 - audit d'architecture ;
 - audit de configuration (équipements réseau et de sécurité, IPBX, téléphones).
 - *audit d'une plate-forme de virtualisation* :
 - audit d'architecture ;
 - audit de configuration (équipements réseau et de sécurité, systèmes de virtualisation).
- 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...).
- 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 B : Liste détaillée des compétences techniques et organisationnelles d'un prestataire d'audit

A. Compétences techniques

Les éléments suivants sont inclus dans les domaines cités dans la règle 4.3.g :

- réseaux et protocoles :
 - o protocoles réseau et infrastructures ;
 - o protocoles applicatifs courants et service d'infrastructure ;
 - o configuration et sécurisation des principaux équipements réseau du marché ;
 - o réseaux de télécommunication ;
 - o technologie sans fil ;
 - o téléphonie ;
- systèmes d'exploitation (environnement et durcissement) :
 - o architectures Microsoft ;
 - o systèmes UNIX/Linux ;
 - o solution de virtualisation.
- couche applicative :
 - o méthodes d'intrusion dans le contexte d'applications web ;
 - o guides et principes de développement sécurité ;
 - o applications de type client/serveur ;
 - o langages de programmation dans le cadre d'audits de code ;
 - o mécanismes cryptographiques ;
 - o socle applicatif :
 - serveurs web,
 - serveurs d'application,
 - systèmes de gestion de bases de données ;
- équipements et logiciels de sécurité :
 - o pare-feu ;
 - o système de sauvegarde ;
 - o système de stockage mutualisé ;
 - o serveurs mandataires inverses ;
 - o détection et prévention d'intrusion (réseau et hôte) ;
 - o logiciels de sécurité côté poste client.

B. Compétences organisationnelles

Les éléments suivants sont inclus dans les domaines cités dans la règle 4.3.h :

- maîtrise des référentiels techniques :
- maîtrise du cadre normatif :
 - o les normes ISO/IEC 27001 et ISO 27002 ;

- les textes réglementaires relatifs à la sécurité des systèmes d'information, aux audits et aux sujets connexes⁷ ;
- maîtrise des domaines relatifs à l'organisation de la sécurité des systèmes d'information :
 - analyse des risques ;
 - politique de sécurité des systèmes d'information ;
 - chaînes de responsabilités en sécurité des systèmes d'information ;
 - sécurité liée aux ressources humaines ;
 - gestion de l'exploitation et de l'administration 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.

C. Connaissances des référentiels

Les éléments suivants sont inclus dans les domaines cités dans la règle 4.3.i :

- maîtrise du RGS et des référentiels cryptographiques associés ;
- maîtrise des guides et référentiels⁸ de l'ANSSI.

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.

⁸ Méthode de gestion de risques EBIOS 2010, guide pour l'élaboration d'une PSSI, guide d'élaboration de tableaux de bord SSI, guide d'intégration de la SSI dans les projets, guide relatif à la maturité SSI, guide de l'externalisation. Tous ces guides sont publiés sur <http://ssi.gouv.fr>.

8. Annexe C : 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 entraîner 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	Difficile	Elevée	Modérée	Facile
Impact				
Mineur	<i>Mineur</i>	<i>Mineur</i>	<i>Important</i>	<i>Majeur</i>
Important	<i>Mineur</i>	<i>Important</i>	<i>Important</i>	<i>Majeur</i>
Majeur	<i>Important</i>	<i>Majeur</i>	<i>Majeur</i>	<i>Critique</i>
Critique	<i>Important</i>	<i>Majeur</i>	<i>Critique</i>	<i>Critique</i>