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 0.9 du 11 mai 2011

PROJET

pour appel à commentaires

51 boulevard de La Tour-Maubourg 75700 PARIS 07 SP

Sommaire

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*

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 au référentiel général de sécurité (RGS). La version en vigueur du RGS ne permet la qualification que de deux types 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 et susceptibles d'être qualifiées selon le schéma décrit au chapitre IV du décret n° 2010-112, dit décret « RGS », du 2 février 2010 pris pour l'application des articles 9, 10 et 12 de l'ordonnance précitée, l'ANSSI élabore un référentiel d'exigences à l'intention des prestataires de services qui réalisent des audits techniques 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 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.

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, par exemple, 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 très critique eu égard aux vulnérabilités qu'elle est susceptible de révéler ainsi qu'à l'exploitation qui pourrait en être faite. De plus, 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 souhaite permettre la qualification, au sens du décret « RGS », des « prestataires d'audit de la sécurité des systèmes d'information ».

A ce titre, le présent référentiel contient les exigences que les prestataires d'audit de la sécurité de systèmes d'information doivent respecter pour être qualifiés au sens du RGS.

Il fournit 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.

Les prestataires qui feront l'objet d'une qualification, attestant de leur conformité aux exigences du présent référentiel, garderont la faculté de réaliser des prestations de services et des activités d'audit en dehors du périmètre pour lequel ils sont qualifiés (cf. chapitre 2.6), mais ne pourront, pour celles-ci, se prévaloir du label. Par ailleurs, le commanditaire d'un audit en dehors de ce périmètre peut sélectionner dans ce référentiel, dans le cadre de son expression de besoin, les exigences pertinentes pour son audit que les prestataires d'audit candidats devront respecter.

1.4. Terminologie

Les définitions ci-dessous sont 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 : tout 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 : sous-ensemble des activités d'audit de la sécurité d'un système d'information correspondant à celles décrites au chapitre 2.

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 client du prestataire d'audit, et qui ordonne l'audit.

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

Périmètre d'audit : environnement physique et logique 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.

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.

Champ de l'audit : étendue et limites de l'audit.

Rapport d'audit : document de synthèse élaboré par le prestataire d'audit à l'issue de l'audit et remis au commanditaire 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 propres à l'audité, 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. L'état de l'art suit une évolution permanente et nécessite que les auditeurs mettent à jour par une veille active leurs compétences et leur méthodologie régulièrement.

1.5. Structure du document

Les exigences du référentiel sont présentées en trois domaines : celles relatives au prestataire d'audit (chapitre 3), celles relatives aux auditeurs (chapitre 4) et celles relatives au déroulement de l'audit (chapitre 5).

L'annexe A détaille les compétences techniques, théoriques et pratiques, que doit posséder le prestataire d'audit.

L'annexe B 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.

2. Activités d'audit visées par le référentiel

Ce chapitre présente les activités d'audit qu'un prestataire d'audit conforme aux exigences du présent référentiel doit être en mesure de proposer au commanditaire de l'audit. Les exigences associées à ces activités sont décrites au chapitre 5. Ce chapitre précise également les activités d'audit non couvertes par le référentiel.

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

2.1. Audit de code source

L'audit de code source consiste en l'analyse de tout ou partie du code source 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 terme de sécurité.

2.2. Audit de configuration

L'audit de configuration a pour vocation de vérifier la mise en œuvre des bonnes pratiques de sécurité dans la configuration des dispositifs matériels et logiciels déployés dans un système d'information. Ces dispositifs peuvent notamment être des équipements réseau, des produits de sécurité, des serveurs, des systèmes d'exploitation ou des applications.

2.3. Audit d'architecture

L'audit d'architecture consiste en la vérification de la prise en compte des bonnes pratiques de sécurité relatives au choix, au positionnement, au déploiement et à la mise en œuvre des dispositifs matériel et logiciels déployés dans un système d'information. L'audit peut être étendu aux interconnexions avec des réseaux tiers, et notamment Internet.

2.4. 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 mises en pratique.

2.5. Tests d'intrusion

Le principe du test d'intrusion est de vérifier l'exploitabilité et l'impact des vulnérabilités découvertes sur le système d'information audité, dans les conditions réelles d'une attaque sur le système d'information, à la place d'un utilisateur malveillant potentiel.

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. En revanche, il s'agit d'une activité qui peut être effectuée en complément des activités décrites dans les chapitres 2.1, 2.2, 2.3 et 2.4 afin d'en améliorer l'efficacité ou de démontrer la faisabilité de l'exploitation des failles et vulnérabilités découvertes à des fins de sensibilisation.

2.6. Activités d'audit non couvertes par le référentiel

Le référentiel ne couvre pas :

- les audits de systèmes d'information traitant d'informations relevant du secret de la défense nationale ;
- les audits de la sécurité physique des locaux ;
- les audits réalisés au titre d'une certification à une norme[2] ;
- les audits de systèmes industriels de type SCADA ;
- les audits isolés de détection (*scan*) de vulnérabilités ;
- les prestations utilisant des méthodes d'ingénierie sociale.

[2] Normes ISO 27001 et 27005 par exemple.

3. Exigences relatives au prestataire d'audit

3.1. Exigences générales

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

a) Le prestataire doit être 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 agit comme prestataire d'audit est considérée comme tel sur la base de sa qualité d'autorité administrative.

b) Le prestataire d'audit réalise ses audits dans le cadre d'une convention d'audit.

c) Le prestataire d'audit assume l'entière 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.

d) 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 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, y compris après la livraison de la prestation.

e) 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.

f) 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 personnel[3], de prêt de main d'œuvre illicite, de propriété intellectuelle[4] et de fraude informatique[5].

g) Le prestataire d'audit doit décrire l'organisation de son activité d'audit.

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

i) Le prestataire d'audit doit décrire ses sources de revenus et être en capacité d'apporter la preuve qu'il est libre de toutes pressions commerciales, financières ou susceptibles de compromettre son impartialité et la qualité de ses prestations.

j) Tous les documents produits par le prestataire d'audit lors des audits doivent être au moins fournis en langue française.

k) Le prestataire d'audit doit s'engager à ce que les audits qu'il effectue soient réalisés en toute impartialité.

[3] 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.

[4] Exemples : licences des logiciels utilisés, des scripts et programmes développés.

[5] Articles 323-1 et suivants du code pénal.

l) Le prestataire d'audit doit être en mesure d'identifier les conflits d'intérêt potentiels relatifs à tout audit envisagé, qu'ils résultent des auditeurs ou des activités antérieures ou prévues du prestataire d'audit, et apporter la preuve de la manière dont il élimine ou limite ce risque au maximum.

m) Le prestataire d'audit ne doit pas divulguer à un tiers d'informations relatives à l'audité, obtenues ou accédées lors d'un audit, sauf autorisation écrite de ce dernier (cf. chapitres 3.2. et 5.3).

n) 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 3.1.d, 3.1.h et 3.1.i ne s'appliquent qu'aux prestataires d'audit privés.

3.2. 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 ;
   - 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 ;
   - les auditeurs signalent au commanditaire de l'audit tout contenu illicite découvert durant l'audit ;
   - les auditeurs s'engagent à respecter la loi et la réglementation en vigueur ainsi que les bonnes pratiques liées à l'audit.

b) Le prestataire d'audit doit faire signer la charte d'audit aux auditeurs qu'il emploie.

3.3. Gestion des ressources et des compétences

a) Le prestataire d'audit doit employer un nombre suffisant d'auditeurs et de responsables d'équipe d'audit 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 compétences techniques et organisationnelles requises.

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 technologique[6].

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 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.

[6] 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.

f) Le prestataire d'audit est responsable des outils (logiciels ou matériel) 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.

g) Le prestataire d'audit doit s'assurer que les compétences techniques, théoriques et pratiques, de l'ensemble des auditeurs qu'il emploie couvrent les domaines suivants, détaillés dans l'annexe A :

- protocoles et réseaux ;
- systèmes d'exploitation ;
- couche applicative ;
- systèmes de gestion de bases de données ;
- technologies sans-fil ;
- téléphonie ;
- virtualisation ;
- développement d'outils utilisés adaptés à la cible auditée dans le cadre des audits ou des tests d'intrusion ;
- utilisation des outils techniques, matériel et logiciels, mis à disposition par le prestataire d'audit.

Par ailleurs, il est recommandé que le prestataire d'audit dispose de compétences en matière de réseaux de télécommunication.

h) Le prestataire d'audit doit s'assurer que les compétences organisationnelles, théoriques et pratiques, de l'ensemble des auditeurs qu'il emploie couvrent les exigences suivantes :

- maîtrise des référentiels techniques et réglementaires :
  - le RGS et les référentiels cryptographiques associés ;
  - les normes ISO 27001 et ISO 27002 ;
  - les guides et référentiels[7] de l'ANSSI ;
  - les textes réglementaires relatifs à la sécurité des systèmes d'information, aux audits et aux sujets connexes[8].
- 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 ;

[7] 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] 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.

- gestion du plan de continuité de l'activité.

- maîtrise des techniques d'audit :
  - conduite d'entretien ;
  - visite sur site ;
  - analyse documentaire.

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

a) Les informations sensibles relatives aux audits, et notamment les preuves, les constats et les rapports d'audit, doivent être protégés au niveau Diffusion Restreinte. Le système 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 (document en cours de validation).

b) Il est recommandé que le système que le prestataire d'audit utilise pour le traitement des informations évoquées au a) soit certifié selon la norme ISO 27001.

4. Exigences relatives aux auditeurs

4.1. 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 audits.

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.

4.2. Formation et expérience

Il est recommandé que l'auditeur :

- soit issu d'une école d'ingénieur délivrant un diplôme reconnu par la commission des titres d'ingénieur, ou ait suivi un cursus universitaire de niveau Master minimum, avec une spécialisation en informatique ;
- 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.

4.3. Aptitudes et connaissances spécifiques à l'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 5) ;

b) L'auditeur doit disposer de connaissances techniques ou organisationnelles approfondies parmi celles décrites au 3.3.g et détaillées dans l'annexe A ainsi que celles décrites au 3.3.h.

4.4. 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.

5. Exigences relatives au déroulement d'un audit

5.1. Définition de l'audit et de son périmètre

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 (une autorité administrative dans le cadre du RGS). L'annexe B 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 d'audit des recommandations de l'annexe B.

5.2. Exigences relatives 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 ci-dessous.

Les énumérations listées dans les chapitres 5.2.1 à 5.2.5 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.

5.2.1. Audit de code source

a) Le code source doit être fourni 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) Le prestataire d'audit doit, *a minima*, vérifier 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.

c) Le prestataire d'audit doit, *a minima*, rechercher les vulnérabilités suivantes : *cross-site scripting*, injections SQL, *cross-site Request Forgery*, erreurs de logique applicative, débordement de tampon (« *buffer overflow* »), déni de service, exécution de commandes arbitraires, inclusion de fichiers (locaux ou distants), fuites d'informations.

d) 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.

5.2.2. 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.

b) Le prestataire d'audit doit, *a minima*, vérifier la sécurité des configurations :

- des équipements réseau de type commutateurs ou routeurs (règles de filtrage et de configuration de VLAN par exemple) ;
- des équipements de sécurité de type pare-feu ou relais inverse (filtrant ou non) et leurs règles de filtrage ;
- des systèmes d'exploitation ;
- des systèmes de gestion de bases de données ;
- des services réseau classiques : SSH, HTTP, SMTP, DNS... ;
- des serveurs d'applications : JBoss, Apache Tomcat, IBM Websphere... ;
- 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 mots de passe…) ;
- les mécanismes cryptographiques utilisés ;
- les règles de filtrage réseau (entrée, sortie, routage, NAT...) ;
- les bonnes pratiques en matière de segmentation par VLAN ;
- les bonnes pratiques de durcissement des systèmes d'exploitation et des services réseau.

5.2.3. Audit d'architecture

a) Le prestataire d'audit doit procéder à la revue des documents suivants :

- 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 ;
- documents d'architecture technique liés à la cible.

b) Le prestataire d'audit peut 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.

5.2.4. Audit organisationnel

a) 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 utilisant les techniques d'audit décrits au 3.3.h.

5.2.5. Tests d'intrusion

a) L'équipe d'audit en charge de la réalisation d'un test d'intrusion sur une cible donnée devrait effectuer les phases suivantes et dans l'ordre indiqué :

- 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... ;
- 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.

b) 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.

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

5.3. 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, les 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 sans autorisation expresse du commanditaire de l'audit, ainsi que leurs modalités (mise en œuvre, personnes présentes, durée, exécutant…) ;
- 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 ayant fait l'objet d'une condamnation pour fraude informatique, n'ayant pas de relation contractuelle avec lui ou n'ayant pas signé sa charte d'éthique ;
- 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) ;

- définir les règles de titularité des éléments protégés par la propriété intellectuelle tels que les outils développés spécifiquement pour l'audit.

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

5.4. 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.

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'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.

e) 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.

f) En fonction de l'activité d'audit, l'équipe d'auditeurs doit obtenir, le cas échéant, avant le début même de l'audit, 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.

g) 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.

h) Le prestataire doit sensibiliser son client sur l'intérêt de sauvegarder et préserver les données présentes sur les machines auditées.

i) 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.

5.5. Exécution de l'audit

a) Le responsable d'équipe d'audit doit tenir informé le commanditaire de l'audit des vulnérabilités majeures 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) Les constatations et observations effectuées par les auditeurs doivent être factuelles et basées sur la preuve.

c) Les auditeurs doivent rendre compte des constats d'audit au responsable d'équipe d'audit, lequel peut en avertir sans délai sa hiérarchie ainsi que l'audité.

d) Les constats d'audit doivent être documentés, tracés, et conservés.

e) Les actions susceptibles d'entraîner une compromission d'informations sensibles ou un déni de service doivent être effectuées en présence de l'audité.

f) 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.

g) 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.

5.6. Restitution

Dès la fin de l'audit, et sans attendre que le rapport d'audit soit achevé, le responsable d'équipe d'audit doit restituer à l'audité et au commanditaire de l'audit les constats et les premières conclusions de l'audit, ainsi que, le cas échéant, les vulnérabilités majeures et critiques qui nécessiteraient une action rapide ainsi que les recommandations associées.

5.7. 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 contenir en particulier :

- une synthèse, compréhensible par des non experts, qui précise :
  - le contexte et le périmètre de l'audit[9] ;
  - les vulnérabilités critiques, d'origine technique ou organisationnelle, et les mesures correctives proposées ;
  - l'appréciation du niveau de sécurité global du système d'information audité.
- un tableau synthétique des résultats de l'audit, qui précise :
  - la synthèse des vulnérabilités relevées, classées selon l'échelle de valeur décrite au 5.7.c) ;
  - 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.

[9] 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.

c) 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 ; autrement dit en fonction du risque qu'elles font peser sur le système d'information et 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.

La difficulté 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 :

- *Faible* : pas de conséquence directe sur la sécurité du système d'information audité ;
- *Modéré* : conséquences isolées sur des points précis du système d'information audité ;
- *Important* : 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 les risques inhérents aux vulnérabilités découvertes, en fonction de leur difficulté d'exploitation et de leur impact présumé :

Difficulté d'exploitation **Impact**	**Difficile**	**Elevée**	**Modérée**	**Facile**
Faible	*Mineur*	*Mineur*	*Important*	*Majeur*
Modéré	*Mineur*	*Important*	*Important*	*Majeur*
Important	*Important*	*Majeur*	*Majeur*	*Critique*
Critique	*Important*	*Majeur*	*Critique*	*Critique*

d) Il doit être mentionné dans le rapport d'audit les réserves relatives à l'exhaustivité des résultats de l'audit (liées aux délais contraints de l'audit, à la disponibilité des informations demandées…).

5.8. Conclusion de l'audit

a) Une réunion de clôture de l'audit doit être organisée suite à la livraison du rapport d'audit. Cette réunion permet de présenter la synthèse du rapport d'audit, des démonstrations d'exploitation de certaines failles, et d'organiser un jeu de questions / réponses.

b) Le responsable d'équipe d'audit doit faire signer à l'audité un document attestant de l'intégrité et du bon fonctionnement du système d'information qui a été audité, 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 obtenues par le prestataire d'audit doivent être restituées à l'audité ou, sur sa demande, détruites.

d) Le prestataire d'audit doit fournir, à la fin de l'audit, les développements spécifiques 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.

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 approuvé le rapport d'audit.

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

6. Références documentaires

6.1. 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 (en cours de validation).

6.2. Normes et documents techniques

Norme internationale ISO 17021 : Evaluation de la conformité, exigences pour les organismes procédant à l'audit et à la certification de systèmes de management.

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

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

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

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

6.3. Autres références documentaires

Défense et sécurité de l'information – Stratégie publique (de la France) – Glossaire
Publié sur http://www.ssi.gouv.fr.

7. Annexe A : Liste détaillée des compétences techniques d'un prestataire d'audit

Les éléments suivants sont donnés dans le but de décrire précisément les exigences requises au titre de la règle 3.3.g) :

- Protocoles et réseaux :
  - protocoles réseau et infrastructures (TCP/IP, mécanismes de routage, IPsec, MPLS, …) ;
  - protocoles applicatifs courants (HTTP, SMTP, DNS, FTP, LDAP, SSH, protocoles Microsoft, …) ;
  - configuration et sécurisation des principaux équipements réseau du marché (pare-feu, commutateurs, routeurs, relais inverses).
- Systèmes d'exploitation (environnement et durcissement) :
  - architectures Microsoft (domaines Active Directory, principaux mécanismes de sécurité Windows, GPO, …)
  - systèmes UNIX/Linux ;
- Couche applicative :
  - méthodes d'intrusion dans le contexte d'applications web et principales vulnérabilités rencontrées (injections SQL, Cross-Site Scripting, erreurs de logiques, etc.) ;
  - guides et principes de développement sécurité, tels que ceux produits par la communauté de l'Open Web Application Security Project, OWASP, Microsoft ou Oracle ;
  - audit d'applications lourdes de type client/serveur ;
  - langages de programmation dans le cadre d'audits de code (PHP, Java, ASP.NET, C, C++...).
- Systèmes de gestion de bases de données :
  - configuration et durcissement des solutions du marché (Oracle, Microsoft SQL Server, MySQL, PostgreSQL, …) ;
  - techniques d'intrusion sur les SGBD (exécution de requêtes, élévation de privilèges, rebond).
- Technologies sans-fil :
  - 802.11 (Wi-Fi).
- Téléphonie :
  - Audits de PABX ;
  - ToIP (IPBX, protocoles de VoIP).
- Virtualisation
  - configuration et durcissement des solutions du marché (VMware, Citrix (Xen), VirtualBox, KVM, Hyper-V) ;
  - architecture des plates-formes de virtualisation.

Les compétences théoriques et pratiques des auditeurs du prestataire d'audit permettant de couvrir le domaine technique facultatif lié aux réseaux de télécommunications recommandées au paragraphe 3.3.g sont les suivantes :

- Architectures des réseaux de télécommunication ;
- Protocoles SS7 / SIGTRAN ;
- GSM, GPRS, UMTS...

8. Annexe B : 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.

8.1. 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 du commanditaire de 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...

e) Il est préférable de réaliser les audits 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.

8.2. 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 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

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*

51 boulevard de La Tour-Maubourg 75700 PARIS 07 SP