**ROYAUME DU MAROC**
**ADMINISTRATION DE LA DÉFENSE NATIONALE**
**DIRECTION GÉNÉRALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION**

# REFERENTIEL D'EXIGENCES RELATIF A LA QUALIFICATION DES PRESTATAIRES D'AUDIT DE LA SECURITE DES SYSTEMES D'INFORMATION

# Informations

**PERSONNES AYANT CONTRIBUÉ À LA RÉDACTION DE CE DOCUMENT :**

| Rédigé par | Version | Date |
|---|---|---|
| DGSSI | 1.1 | 01/10/2021 |

**ÉVOLUTION DU DOCUMENT :**

| Version | Date | Nature des modifications |
|---|---|---|
| 1.0 | 11/2018 | Version initiale |
| 1.1 | 10/2021 | - |

**PUBLIC CONCERNÉ PAR CE DOCUMENT :**

| |
|---|
| Infrastructure d'importance vitale |
| Organisme évaluateur |
| Prestataire d'audit de la sécurité des systèmes d'information |

**POUR TOUTE REMARQUE :**

| Contact | Email |
|---|---|
| DGSSI | contact@dgssi.gov.ma |

## SOMMAIRE


1. Contexte et objectifs ..... 4
2. Activités d'audit concernées par la qualification ..... 4
3. Déroulement du processus de qualification des prestataires d'audit ..... 4
4. Exigences relatives au prestataire d'audit ..... 4
4.1. Statut juridique ..... 4
4.2. Références ..... 5
4.3. Respect de la déontologie ..... 5
4.4. Protection de l'information ..... 5
4.5. Gestion des ressources et des compétences ..... 5
4.6. Référentiels et Méthodologie ..... 6
5. Exigences relatives au déroulement d'une prestation d'audit ..... 6
5.1. Etablissement du contrat d'audit ..... 6
5.2. Préparation et déclenchement de la prestation ..... 6
5.3. Exécution de la prestation ..... 7
5.4. Exigences techniques à respecter lors de l'audit par le prestataire ..... 7
5.4.1. Audit d'architecture ..... 7
5.4.2. Audit de configuration ..... 7
5.4.3. Audit de code source ..... 8
5.4.4. Tests d'intrusion ..... 8
5.4.5. Audit organisationnel et physique ..... 9
5.4.6. Audit d'un système industriel ..... 9
5.5. Restitution ..... 9
5.6. Elaboration du rapport d'audit ..... 9
5.7. Clôture de la prestation ..... 10
6. Exigences et niveaux de qualification des auditeurs ..... 11
6.1. Aptitudes générales ..... 11
6.2. Engagements ..... 11
6.3. Formation, Expérience et niveaux de qualification ..... 11
6.4. Aptitudes spécifiques ..... 12

# 1. Contexte et objectifs

Conformément aux dispositions du décret n° 2-21-406 pour l'application de la loi n° 05-20 relative à la cybersécurité, les entités et infrastructures d'importance vitale disposant de systèmes d'information sensibles doivent mener des audits périodiques de leurs systèmes par des prestataires d'audit qualifiés par la direction générale de la sécurité des systèmes d'information (DGSSI).

L'objectif de ce document est de regrouper les exigences à respecter par les prestataires d'audit en vue d'être qualifiés par cette direction.

Ce système de qualification constitue un gage de confiance pour confier des missions d'audit aux prestataires qualifiés. Il s'appuie sur la vérification d'un certain nombre de critères attestant, notamment :

- des références des prestataires dans le domaine;
- de la qualification de leurs ressources humaines;
- de l'efficacité et l'adéquation des méthodes et outils utilisés;
- de l'organisation du travail et le respect des règles déontologiques et de sécurité.

# 2. Activités d'audit concernées par la qualification

Sont concernés par la qualification, six domaines d'audit tels que définis dans l'annexe 2 du décret n° 2-21-406 précité, et qui sont :

- Audit organisationnel et physique ;
- Audit d'architecture ;
- Audit de configuration ;
- Tests d'intrusions ;
- Audit du code source ;
- Audit des systèmes industriels.

# 3. Déroulement du processus de qualification des prestataires d'audit

Le processus de qualification se déroule en deux étapes avec l'obligation de valider une phase pour passer à la suivante, comme indiqué ci-après :

**Etape 1 - Pré-qualification :** consiste en l'analyse des éléments constituant le dossier de la demande de qualification conformément à l'article 21 du décret n° 2-21-406 précité.

**Etape 2 – Qualification :** consiste en l'évaluation :

- des auditeurs et leur attribuer un niveau de qualification conformément au paragraphe 6.3 du présent référentiel ;
- des processus de l'entreprise (veille, formation et maintien des compétences, gestion des ressources, moyens de travail et outils etc.) ;
- de la sécurité des locaux et du système d'information du prestataire d'audit ;
- des méthodologies de travail et des outils utilisés.

# 4. Exigences relatives au prestataire d'audit

## 4.1. Statut juridique

- Le prestataire doit être une entité dotée d'une personnalité morale de droit marocain ;
- Le prestataire doit être spécialisé dans l'audit de la sécurité des systèmes d'information ou disposer, en son sein, d'une structure organisationnelle dédiée à cette activité.

## 4.2. Références

- Le prestataire doit avoir des références connues sur le marché, relatives à des prestations d'audit de la sécurité des systèmes d'information, en particulier dans chacun des domaines de qualification faisant l'objet de sa demande.

## 4.3. Respect de la déontologie

- Le prestataire doit disposer d'une charte d'éthique et la faire appliquer. Cette charte doit notamment indiquer que :
  - ✓ les prestations sont réalisées avec loyauté, discrétion et impartialité ;
  - ✓ seules les méthodes, outils et techniques validés par le prestataire sont utilisés ;
  - ✓ aucune divulgation d'informations obtenues ou générées dans le cadre de leurs activités n'est autorisée sans accord préalable du commanditaire ;
  - ✓ tout contenu manifestement illicite découvert durant une prestation doit immédiatement être signalé au commanditaire ;
  - ✓ les auditeurs s'engagent à respecter la législation et la réglementation nationale en vigueur ainsi que les bonnes pratiques liées à leurs activités d'audit.
- Le prestataire doit s'assurer, pour chaque prestation, que les auditeurs désignés ont les qualités et les compétences requises.

## 4.4. Protection de l'information

Le prestataire doit protéger les informations sensibles relatives à la prestation, et notamment les preuves, les constats et les rapports. Il doit à cet effet :

- Maîtriser le circuit de production documentaire ;
- Tracer la diffusion des documents et s'assurer de la faire via des canaux sécurisés ;
- Avoir des processus clairs concernant la sauvegarde et la destruction des données ;
- Assurer la sécurité de ses locaux et de son système d'information.

## 4.5. Gestion des ressources et des compétences

- Le prestataire doit employer un nombre suffisant d'auditeurs, de responsables d'équipe d'audit pour assurer totalement les activités d'audit pour lesquels il demande d'être qualifié ;
- Le prestataire doit s'assurer du maintien à jour des compétences de ces auditeurs dans les domaines d'audits pour lesquels ils sont employés. Il doit disposer à cet effet d'un processus de formation continue et permettre à ses auditeurs d'assurer une veille technologique ;
- Le prestataire doit, en matière de recrutement, procéder à une vérification des formations, compétences et références professionnelles des auditeurs candidats et de la véracité de leur curriculum vitae ;
- Le prestataire est responsable des méthodes, outils (logiciels ou matériels) et techniques utilisés par ses auditeurs et de leur bonne utilisation (précautions d'usage, maîtrise de la configuration, etc.) pour la réalisation de la prestation. Pour cela, le prestataire doit assurer une veille technologique sur leur mise à jour et leur pertinence (efficacité et confiance) ;
- Le prestataire doit disposer des licences valides des outils (logiciels ou matériels) utilisés pour la réalisation de la prestation ;
- Le prestataire doit mettre en place un processus de sensibilisation des auditeurs à la législation en vigueur sur le territoire national, applicable à leurs missions ;
- Le prestataire doit avoir une relation d'emploi stable avec les auditeurs concernés par le processus de qualification (contrat de travail de droit marocain) et avoir élaboré un processus disciplinaire formel à l'intention des auditeurs ayant enfreint les règles de

sécurité ou la charte d'éthique.

### 4.6. Référentiels et Méthodologie

- Le prestataire doit faire preuve d'usage d'une démarche d'audit éprouvée basée sur des normes et référentiels reconnus (ISO-2700x, ISO 19011, COBIT, ITIL, …) ;
- Méthodologie de gestion projet ;
- Le prestataire justifie, au travers des auditeurs évalués au titre de la qualification, qu'il dispose des compétences techniques, théoriques et pratiques, afférentes aux activités d'audit qu'il exerce ainsi que de la maîtrise des référentiels et guides de bonnes pratiques relatifs à la sécurité des systèmes d'information.

## 5. Exigences relatives au déroulement d'une prestation d'audit

Les exigences auxquelles doivent se conformer les prestataires sont regroupées dans les différentes étapes du déroulement d'un audit, à savoir :

- étape 1: établissement d'un contrat d'audit ;
- étape 2: préparation et déclenchement de la prestation ;
- étape 3: exécution de la prestation ;
- étape 4: restitution ;
- étape 5: élaboration du rapport d'audit ;
- étape 6: clôture de la prestation.

D'une manière générale, le déroulement de l'audit doit respecter les dispositions de la norme ISO 19011- Lignes directrices pour l'audit des systèmes de management.

### 5.1. Etablissement du contrat d'audit

- Le prestataire doit établir un contrat de service avec le commanditaire avant l'exécution de la prestation conformément aux dispositions de l'article 29 du décret n°2-21-406 précité.
- Les niveaux de qualification des auditeurs exigés par le commanditaire de l'audit doivent être scrupuleusement respectés.
- Le contrat doit être signé par un représentant légal du commanditaire et du prestataire.

### 5.2. Préparation et déclenchement de la prestation

- Le prestataire doit nommer un responsable d'équipe parmi ses auditeurs ayant le niveau de qualification « Auditeur Senior » (voir paragraphe 6.3) pour tout audit qu'il effectue.
- 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 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'entité auditée, 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.
- Les objectifs, le champ, les critères et le planning de l'audit doivent être définis entre le prestataire et le commanditaire, en considération des contraintes d'exploitation du système d'information de l'entité auditée. Ces éléments doivent figurer dans le contrat d'audit ou dans le plan d'audit.
- En fonction de l'activité d'audit, l'équipe d'auditeurs doit obtenir, au préalable, toute la documentation existante de l'entité auditée (e.g. : politique de sécurité, analyse des risques, procédures d'exploitation de la sécurité, etc.), relative à la cible auditée dans l'objectif d'en faire une revue.
- L'audit ne doit débuter qu'après une réunion formelle au cours de laquelle les représentants habilités du prestataire et ceux de l'entité auditée confirment leur accord sur l'ensemble des

modalités de la prestation.

- Le prestataire doit sensibiliser avant l'audit son client sur l'intérêt de sauvegarder et préserver les données, applications et systèmes présents sur les machines auditées.
- Au préalable, et dans le cas spécifique des tests d'intrusion, une fiche d'autorisation doit être signée par le commanditaire, l'entité auditée et d'éventuelles tierces parties. Elle précise en particulier :
    - ✓ la liste des cibles auditées (adresses IP, noms de domaine, etc.);
    - ✓ la liste des adresses IP de provenance des tests ;
    - ✓ la date et les heures exclusives des tests ;
    - ✓ la durée de l'autorisation.

## 5.3. Exécution de la prestation

- Le responsable d'équipe d'audit doit tenir informé le commanditaire des vulnérabilités critiques découvertes au cours de l'audit. Il doit rendre compte immédiatement à l'entité auditée 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.
- L'audit doit être réalisé dans le respect des personnels et des infrastructures physiques et logiques de l'entité auditée.
- Les constatations et observations effectuées par les auditeurs doivent être factuelles et basées sur la preuve.
- 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'entité auditée, dans le respect des clauses de confidentialité fixées dans le contrat d'audit.
- 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.
- Les constats d'audit doivent être documentés, tracés, et conservés, par le prestataire, durant toute la durée de l'audit.
- Le prestataire et les auditeurs doivent prendre toutes les précautions utiles pour préserver la confidentialité des documents et informations relatives à l'entité auditée.
- Les actions et résultats des auditeurs du prestataire sur le système d'information audité, ainsi que leurs dates de réalisation, devraient être tracés. Ces traces peuvent par exemple servir à identifier les causes d'un incident technique survenu lors de l'audit.

## 5.4. Exigences techniques à respecter lors de l'audit par le prestataire

### 5.4.1. Audit d'architecture

- Le prestataire doit procéder à la revue des documents suivants lorsqu'ils existent :
    - ✓ schémas d'architectures de niveau 2 et 3 du modèle OSI ;
    - ✓ matrices de flux ;
    - ✓ règles de filtrage ;
    - ✓ configuration des équipements réseau (routeurs et commutateurs) ;
    - ✓ interconnexions avec des réseaux tiers ou Internet ;
    - ✓ analyses de risques système ;
    - ✓ documents d'architecture technique liés à la cible.
- Le prestataire doit pouvoir organiser des entretiens avec le personnel concerné par la mise en place et l'administration de la cible auditée, notamment en ce qui concerne les procédures d'administration.

### 5.4.2. Audit de configuration

- Les éléments de configuration des cibles auditées doivent être fournis au prestataire. Ils peuvent être récupérés manuellement ou automatiquement, à partir d'un accès privilégié sur les cibles auditées, sous la forme de fichiers de configuration ou de captures d'écran. Cette action peut être entreprise directement par l'auditeur après accord de l'entité auditée. Il est recommandé

que le prestataire vérifie, conformément à l'état de l'art ou aux exigences et règles spécifiques de l'entité auditée, 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.

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

### 5.4.3. Audit de code source

- Le code source, la documentation relative à la mise en œuvre, les méthodes et rapports de tests et l'architecture du système d'information audité doivent être fournis au prestataire ainsi que la configuration des éléments de compilation et d'exécution, dans les limites des droits dont disposent le commanditaire et l'entité auditée.
- 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.
- Il est recommandé que l'audit de code fasse préalablement l'objet d'une analyse de la sécurité de l'application auditée afin de limiter l'audit aux parties critiques de son code.
- Il est recommandé que le prestataire vérifie la sécurité des parties du code source relatives :
  - ✓ aux mécanismes d'authentification ;
  - ✓ aux mécanismes cryptographiques ;
  - ✓ à la gestion des utilisateurs ;
  - ✓ au contrôle d'accès aux ressources ;
  - ✓ aux interactions avec d'autres applications ;
  - ✓ aux relations avec les systèmes de gestion de bases de données ;
  - ✓ à la conformité à des exigences de sécurité relative à l'environnement dans laquelle est déployée l'application.
- Il est recommandé que le prestataire cherche 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.
- 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.

### 5.4.4. Tests d'intrusion

- L'équipe d'audit en charge de la réalisation d'un test d'intrusion sur une cible donnée peut effectuer une ou plusieurs des phases suivantes :
  - ✓ phase boîte noire : l'auditeur ne dispose d'aucune autre information que les adresses IP et URL associées à la cible auditée. Cette phase est généralement précédée de la découverte d'informations et l'identification de la cible par interrogation des services DNS, par le balayage des ports ouverts, par la découverte de la présence d'équipements de filtrage, etc.;
  - ✓ phase boîte grise : les auditeurs disposent des connaissances d'un utilisateur standard du système d'information (authentification légitime, poste de travail « standard », etc.). Les identifiants peuvent appartenir à des profils d'utilisateurs différents

afin de tester des niveaux de privilèges distincts ;

- ✓ phase boîte blanche : les auditeurs disposent du maximum d'informations techniques (architecture, code source, contacts téléphoniques, identifiants, etc.) avant de démarrer l'analyse. Ils ont également accès à des contacts techniques liés à la cible. Si plusieurs de ces prestations sont effectuées, il est recommandé de préserver l'ordre d'exécution décrit ci-dessus.

- Le prestataire et le commanditaire doivent, préalablement à tout test d'intrusion, définir un profil d'attaquant simulé.
- Le prestataire doit avoir un contact permanent avec l'entité auditée et l'auditeur doit prévenir le commanditaire et l'entité auditée avant toute action qui pourrait entraîner un dysfonctionnement, voire un déni de service de la cible auditée.
- 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'entité auditée. L'absence de tentative d'exploitation de telles vulnérabilités doit être indiquée et justifiée dans le rapport d'audit.
- Les vulnérabilités non publiques découvertes lors de l'audit doivent être communiquées à la DGSSI.

### 5.4.5. Audit organisationnel et physique

- Le prestataire doit analyser l'organisation de la sécurité des systèmes d'information sur la base des référentiels techniques et réglementaires en accord avec les réglementations et méthodes applicables dans le domaine d'activité de l'entité auditée.
- L'audit organisationnel et physique doit permettre de mesurer la conformité du système d'information audité par rapport aux référentiels et identifier les écarts présentant les vulnérabilités majeures du système audité.
- L'audit organisationnel et physique peut intégrer l'analyse des éléments liés à la sécurité des aspects physiques des systèmes d'information et notamment la protection des locaux hébergeant les systèmes d'information et les données de l'entité auditée ou le contrôle d'accès de ces locaux.

### 5.4.6. Audit d'un système industriel

- Le prestataire doit réaliser les activités suivantes sur le périmètre du système industriel et le cas échéant de son centre de contrôle :
  -audit de l'architecture ;
  -audit de configuration des composants ;
  -audit organisationnel et physique ;
- Le prestataire doit pouvoir organiser des entretiens avec le personnel concerné par la sécurité du système industriel, notamment le responsable de la sécurité des systèmes d'information (RSSI), le responsable opérationnel du système et le cas échéant, les correspondants techniques.
- Il est recommandé au prestataire de sensibiliser le commanditaire aux risques de la réalisation de tests d'intrusion sur un environnement comportant des systèmes industriels.

## 5.5. Restitution

Dès la fin de l'audit, et sans attendre que le rapport d'audit soit achevé, le responsable d'équipe d'audit doit informer l'entité auditée et le commanditaire des constats et des premières conclusions de l'audit.

Le cas échéant, il présente les vulnérabilités majeures et critiques qui nécessiteraient une action rapide et décrit les recommandations associées.

## 5.6. Elaboration du rapport d'audit

- Le prestataire doit, pour toute prestation, élaborer un rapport d'audit et le transmettre au commanditaire.
- Le prestataire doit mentionner explicitement dans le rapport d'audit si la prestation réalisée est une prestation qualifiée.

- Le rapport d'audit doit contenir en particulier :
  - ✓ une synthèse, compréhensible par des non experts, qui précise :
    - le contexte et le périmètre de la prestation;
    - les vulnérabilités critiques, d'origine technique ou organisationnelle, et les mesures correctives proposées ;
    - l'appréciation du niveau de sécurité du système d'information audité par rapport à l'état de l'art et en considération du périmètre d'audit.
  - ✓ un tableau synthétique des résultats de l'audit, qui précise :
    - la synthèse des vulnérabilités relevées, classées selon une échelle de valeur ;
    - la synthèse des mesures correctives proposées, classées par criticité et par complexité ou coût estimé de correction ;
  - ✓ lorsque réalisés, une description du déroulement linéaire des tests d'intrusion et de la méthodologie employée pour détecter les vulnérabilités et, le cas échéant, les exploiter;
  - ✓ une analyse de la sécurité du système d'information audité, qui présente les résultats des différentes activités d'audit réalisées.
- Le rapport d'audit doit être adapté en fonction de l'activité d'audit réalisée par le prestataire.
- 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.
- Chaque vulnérabilité doit être associée à une ou plusieurs recommandations adaptées au système d'information de l'entité auditée. Les recommandations décrivent les solutions permettant de résoudre temporairement ou définitivement la vulnérabilité et d'améliorer le niveau de sécurité.
- Le rapport d'audit peut également présenter des recommandations générales non associées à des vulnérabilités et destinées à conseiller l'entité auditée pour les actions liées à la sécurité de son système d'information qu'il entreprend.
- Le rapport d'audit doit mentionner les réserves relatives à l'exhaustivité des résultats de l'audit (liées aux délais alloués, à la disponibilité des informations demandées, à la collaboration de l'entité auditée, etc.) ou à la pertinence de la cible auditée.
- Le rapport d'audit doit mentionner les noms et coordonnées des auditeurs, responsables d'équipe d'audit et commanditaires de l'audit.
- Le rapport d'audit doit mentionner s'il s'agit d'une prestation d'audit qualifiée et préciser les activités d'audit associées.

## 5.7. Clôture de la prestation

- Il est recommandé qu'une réunion de clôture de l'audit soit organisée avec le commanditaire et l'entité 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. Elle est également l'occasion d'expliquer les recommandations complexes et, éventuellement, de proposer d'autres solutions plus aisées à mettre en œuvre.
- Le responsable d'équipe d'audit doit demander à l'entité 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 de tout problème postérieur à l'audit.
- Toutes les traces, relevés de configuration, informations ou documents relatifs au système d'information audité obtenus par le prestataire doivent être restitués à l'entité auditée ou, sur sa demande, détruits conformément à la convention d'audit. Le cas échéant, le responsable d'audit produit un procès-verbal de destruction de ces données qu'il remet à l'entité auditée et précisant les données détruites et leur mode de destruction.
- Afin qu'il puisse s'assurer de la pertinence des mesures correctives mises en œuvre pour corriger les vulnérabilités découvertes lors de l'audit, le commanditaire peut demander au prestataire la fourniture des développements spécifiques autonomes réalisés lors de l'audit pour

valider les scénarios d'exploitation des vulnérabilités. Ces développements peuvent être fournis sous la forme de scripts ou de programmes compilés, accompagnés de leur code source, ainsi que d'une brève documentation de mise en œuvre et d'utilisation. Les modalités relatives à cette mise à disposition sont précisées dans la convention.

- La prestation est considérée comme terminée lorsque toutes les activités prévues ont été réalisées et que le commanditaire a reçu et attesté, formellement et par écrit, que le rapport d'audit est conforme aux objectifs visés dans la convention.
- Il est recommandé que le prestataire propose au commanditaire d'effectuer ultérieurement un audit de validation afin de vérifier si les mesures correctives proposées lors de l'audit ont été correctement mises en œuvre.

# 6. Exigences et niveaux de qualification des auditeurs

## 6.1. Aptitudes générales

- Les auditeurs doivent posséder les qualités personnelles tel que décrites dans la norme ISO 19011 précitée, notamment :
  - ✓ Autonomie ;
  - ✓ Sens d'observation ;
  - ✓ Esprit de synthèse et perspicacité (bonne compréhension des situations et bonne manière de tirer les conclusions) ;
  - ✓ Rigueur et sens de responsabilités ;
- Ils doivent maîtriser la législation et la réglementation en vigueur sur le territoire national et applicable à leurs missions ;
- Ils doivent disposer de qualités rédactionnelles et de synthèse et savoir s'exprimer à l'oral de façon claire et compréhensible ;
- Ils doivent régulièrement mettre à jour leurs compétences conformément aux processus de formation et de veille du prestataire.

## 6.2. Engagements

- L'auditeur doit avoir un contrat avec le prestataire ;
- Il doit avoir signé la charte d'éthique élaborée par le prestataire et s'engage à respecter ses clauses, notamment :
  - ✓ L'objectivité : les auditeurs présentent de façon impartiale, honnête et précise leurs constatations et font part de l'évaluation avec sincérité, probité et intégrité ;
  - ✓ La confidentialité : les auditeurs s'engagent à préserver les informations obtenues ou générées dans le cadre des audits et à ne les divulguer que sur demande et/ou autorisation du commanditaire de l'audit ;
  - ✓ La compétence : les auditeurs ne s'engagent que sur des missions d'audit pour lesquelles ils ont les compétences requises et réalisent les audits dans le strict respect des bonnes pratiques professionnelles ;
  - ✓ L'approche fondée sur la preuve : Les auditeurs ne peuvent baser leurs conclusions sur des préjugés ou des opinions. Ils s'attachent aux faits constatés et indiscutables.

## 6.3. Formation, Expérience et niveaux de qualification

- L'auditeur doit avoir reçu une formation de base en technologies des systèmes d'information.
- Il doit maîtriser les bonnes pratiques et la méthodologie d'audit décrite dans la norme ISO19011 précitée ;
- Il doit disposer des compétences requises pour l'exercice de sa mission, notamment celles spécifiques à son domaine d'audit tel que spécifié dans le paragraphe 6.4 ;
- Il doit justifier d'un certain nombre d'années d'expérience et de connaissances selon les niveaux de qualification demandés et qui sont définis comme suit :

| Niveaux de qualification | Description |
|---|---|
| Auditeur Junior | - Diplômé en technologies de l'information.<br>- Disposer d'un minimum de deux années d'expérience dans le domaine des systèmes d'information.<br>- Disposer d'un minimum de deux années d'expérience dans le domaine de la sécurité des systèmes d'information.<br>- Justifier de l'exécution d'un minimum de 20 jours d'audits sécurité sur au moins 4 différentes missions se rapportant aux domaines d'audit objet de la demande de qualification. |
| Auditeur Senior | - Diplômé en technologies de l'information.<br>- Disposer d'un minimum de deux années d'expérience dans le domaine des systèmes d'information.<br>- Disposer au minimum de deux années d'expérience dans le domaine de la sécurité des systèmes d'information.<br>- Justifier l'exécution d'un minimum de 35 jours d'audits sécurité sur au moins 7 différentes missions se rapportant aux domaines d'audit objet de la demande de qualification.<br>- Justifier des connaissances en termes de planification, de gestion d'équipe d'audit et de reporting. |

## 6.4. Aptitudes spécifiques

Les compétences spécifiques attendues du personnel du prestataire au regard des différents domaines d'audit sont comme suit :

**Audit Organisationnel et physique :**

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

- Cadre référentiel et normatif :
  - ✓ Directive Nationale de la sécurité des systèmes d'information ;
  - ✓ Normes ISO 27001 et ISO 27002 ;
  - ✓ Textes réglementaires relatifs à la sécurité des systèmes d'information, aux audits et aux sujets connexes ;
- Domaines relatifs à l'organisation de la sécurité des systèmes d'information :
  - ✓ analyse des risques ;
  - ✓ politique de sécurité des systèmes d'information ;
  - ✓ chaines de responsabilités en sécurité des systèmes d'information ;

- ✓ sécurité liée aux ressources humaines ;
- ✓ gestion de l'exploitation et de l'administration du système d'information ;
- ✓ contrôle d'accès logique au système d'information ;
- ✓ développement et maintenance des applications ;
- ✓ gestion des incidents liés à la sécurité de l'information ;
- ✓ gestion du plan de continuité de l'activité ;
- ✓ sécurité physique.

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

Les certifications professionnelles ci-après représentent un plus :

- ISO 27001, 27002 et 27005 Lead Auditor ;
- CISA, CGEIT, COBIT, ITIL.

**Audit de configuration :**

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

- Equipements réseau et protocoles :
  - ✓ Protocoles réseau et infrastructures ;
  - ✓ Protocoles applicatifs courants et service d'infrastructure ;
  - ✓ Configuration et sécurisation des principaux équipements réseau du marché ;
  - ✓ Réseaux de télécommunication ;
  - ✓ Technologie sans fil ;
  - ✓ Téléphonie.
- Equipements de sécurité :
  - ✓ Pare-feu ;
  - ✓ Système de sauvegarde ;
  - ✓ Système de stockage mutualisé ;
  - ✓ Logiciels de sécurité côté poste client.
- Systèmes d'exploitation :
  - ✓ Architectures Microsoft ;
  - ✓ Systèmes UNIX/Linux ;
  - ✓ Solution de virtualisation.
- Couche applicative :
  - ✓ Guides et principes de développement sécurité ;
  - ✓ Applications de type Web ou client/serveur ;
  - ✓ Mécanismes cryptographiques (SSL, VPN, etc..);
  - ✓ Socle applicatif :
    - Serveurs web,
    - Serveurs d'application,
    - Systèmes de gestion de base de données.
- Environnements de virtualisation.

**Audit des architectures**

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

- réseaux et protocoles :
  - ✓ Protocoles réseau et infrastructures ;
  - ✓ Protocoles applicatifs courants et service d'infrastructure ;
  - ✓ Configuration et sécurisation des principaux équipements réseau du marché ;
  - ✓ Réseaux de télécommunication ;

- ✓ Technologie sans fil ;
- ✓ Téléphonie.

- équipements et logiciels de sécurité :
  - ✓ Pare-feu ;
  - ✓ Système de sauvegarde ;
  - ✓ Système de stockage mutualisé ;
  - ✓ Dispositifs de chiffrement des communications ;
  - ✓ Serveurs d'authentification ;
  - ✓ Serveurs mandataires inverses ;
  - ✓ Solutions de gestion de la journalisation ;
  - ✓ Équipements de détection et prévention d'intrusion ;
- Techniques et outils pour établir des :
  - ✓ cartographies fonctionnelles, techniques et applicatives ;
  - ✓ Schémas d'architecture ;
  - ✓ Architectures hautement disponibles et redondantes ;
  - ✓ mécanismes de défense en profondeur.

Les certifications professionnelles ci-après représentent un plus :

- ISSAP (Information Systems Security Architecture Professional);
- SABSA certifications for Security Architects (Foundation, Practitioner, Master).

**Tests d'intrusion**

L'auditeur en tests d'intrusion doit disposer de compétences approfondies dans les domaines techniques suivants :

- réseau et protocoles :
  - ✓ Protocoles réseau et infrastructures ;
  - ✓ Protocoles applicatifs courants et service d'infrastructure ;
  - ✓ Technologie sans fil ;
- équipements de sécurité :
  - ✓ pare-feu ;
  - ✓ dispositif de chiffrement des communications ;
  - ✓ serveur d'authentification ;
  - ✓ solution de gestion de la journalisation ;
  - ✓ équipement de détection et prévention d'intrusion ;
  - ✓ logiciels de sécurité côté poste client.
- systèmes d'exploitation :
  - ✓ systèmes Microsoft;
  - ✓ Systèmes UNIX/Linux ;
  - ✓ Solutions de virtualisation.
- couche applicative :
  - ✓ Applications de type Web ou client/serveur ;
  - ✓ Langages de programmation utilisés pour la configuration (ex : scripts, filtres WMI, etc.) ;
  - ✓ Mécanismes cryptographiques (SSL, VPN, etc..);
  - ✓ Socle applicatif :
    - Serveurs web,
    - Serveurs d'application,
    - Systèmes de gestion de base de données.
- techniques d'intrusion.

Les certifications professionnelles ci-après représentent un plus :

- CEH (Certified Ethical Hacking) ou équivalent (CPTE de mile2, CSSP…) ;
- OSCP (Offensive Security Certified Professional);
- GIAC Penetration Tester (GPEN) ;
- GIAC Web Application Penetration Tester (GWAPT) ;
- GIAC Exploit Researcher and Advanced Penetration Tester (GXPN).

**Audit du code source**

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

- couche applicative :
  - ✓ guides et principes de développement sécurité ;
  - ✓ architectures applicatives (client/serveur, n-tiers, etc.) ;
  - ✓ langages de programmation ;
  - ✓ mécanismes cryptographiques ;
  - ✓ mécanismes de communication (internes au système et par le réseau) et protocoles associés ;
  - ✓ socle applicatif :
    - o serveurs web ;
    - • serveurs d'application ;
    - • systèmes de gestion de bases de données ;
    - • progiciels ;
- attaques :
  - ✓ principes et méthodes d'intrusion applicatives ;
  - ✓ contournement des mesures de sécurité logicielles ;
  - ✓ techniques d'exploitation de vulnérabilités et d'élévation de privilèges.

**Audit des systèmes industriels**

L'auditeur des systèmes industriels doit disposer, en plus des compétences concernant les architectures et les configurations des systèmes d'information conventionnels ou de gestion, de compétences approfondies dans les domaines techniques suivants :

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