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	Mise en conformité avec les dispositions de la loi n° 05.20 relative à la cybersécurité et son décret d'application n° 2-21-406

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 8
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 10
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 :

- avoir des politiques de sécurité des systèmes d'information, définies, approuvées par la direction, diffusées et communiquées aux salariés et aux tiers concernés par les prestations d'audit ;
- 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 son système d'information en prenant en considération les aspects énumérés en annexe.

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. - Disposer d'un minimum de deux années d'expérience dans le domaine des systèmes d'information. - Disposer d'un minimum de deux années d'expérience dans le domaine de la sécurité des systèmes d'information. - 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. - Disposer d'un minimum de quatre années d'expérience dans le domaine des systèmes d'information. - Disposer au minimum de quatre années d'expérience dans le domaine de la sécurité des systèmes d'information. - 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. - 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 :
    - 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.

ANNEXE : EXIGENCES LIEES A LA SECURITE DU SYSTEME D'INFORMATION DU PRESTATAIRE

I- SECURITE PHYSIQUE DES LOCAUX DU PRESTATAIRE

- Le prestataire doit définir les périmètres de sécurité physique servant à protéger les zones contenant l'information sensible et les moyens de traitement de l'information reliés aux audits.
- Le prestataire doit concevoir et appliquer des mesures de sécurité physique aux bureaux, aux salles et aux équipements hébergeant le système d'information.
- L'accès aux zones internes de travail doit reposer sur un dispositif de contrôle d'accès physique afin de s'assurer que seules les personnes autorisées y ont accès.
- Aucun visiteur externe ne doit être autorisé à accéder aux zones restreintes sans être accompagné et chaque visite doit être justifiée et consignée. Une traçabilité des accès des visiteurs externes aux zones restreintes doit être mise en place. L'autorisation formelle d'accès doit être fournie au cas par cas par le prestataire qui documente sa décision et prend la responsabilité formelle de cette autorisation.
- Le prestataire doit déterminer des règles de sécurité physiques et environnementales pour protéger le matériel contre les dangers environnementaux et les possibilités d'accès non autorisé.
- Une procédure doit être en place pour s'assurer qu'aucun matériel, information ou logiciel ne peuvent pas être sortis des locaux sans autorisation préalable.
- Le prestataire doit détruire physiquement les supports de stockage contenant de l'information confidentielle ou protégée par le droit d'auteur, ou bien détruire, supprimer ou écraser cette information en privilégiant les techniques rendant l'information d'origine irrécupérable plutôt qu'en utilisant la fonction standard de suppression ou de formatage.
- En plus de sécuriser l'effacement des disques, le prestataire doit s'assurer que le chiffrement intégral des disques réduise le risque de divulgation de l'information confidentielle lorsque le matériel est mis au rebut ou remis en service, en respectant les exigences suivantes :
    - Le processus de chiffrement est suffisamment fort et couvre l'intégralité du disque (y compris les espaces perdus, les fichiers d'échange, etc.) ;
    - Les clés de chiffrement sont suffisamment longues pour résister aux attaques par force brute au meilleur état de l'art ;
    - Les clés de chiffrement demeurent confidentielles (jamais stockées sur le même disque).

II- EXIGENCES RELIEES A LA GESTION DES ACTIFS ET A LA CLASSIFICATION DE L'INFORMATION

- Le prestataire doit :
  - Identifier les actifs associés à l'information et aux moyens de traitement de l'information utilisées dans le cadre des prestations d'audit ;
  - Dresser et tenir à jour un inventaire de ces actifs ;
  - Disposer des licences valides des outils (logiciels ou matériels) utilisés pour la réalisation de la prestation ;
  - S'assurer que les actifs sont correctement classés et protégés ;
  - Formaliser le processus de fin de mission ou d'emploi pour qu'il inclue la restitution de tous les actifs physiques et électroniques créés, appartenant au prestataire ou lui ayant été confiés ;
  - S'assurer que les données non chiffrées doivent être effacées avant l'envoi en maintenance externe de toute ressource informatique ;
  - S'assurer qu'une personne a la responsabilité d'assurer la gestion du cycle de vie d'un actif de leur acquisition à leur décommissionnement ;
  - S'assurer de l'évaluation de la sensibilité de toute information et du marquage systématique des documents, en fonction du niveau de sensibilité.
- L'utilisateur doit protéger les informations qu'il est amené à manipuler dans le cadre de ses fonctions, selon leur sensibilité et tout au long de leur cycle de vie, depuis leur création jusqu'à leur éventuelle destruction.
- Les postes de travail, y compris dans le cas d'une location, sont fournis à l'utilisateur par l'entité, gérés et configurés sous la responsabilité de l'entité. La connexion d'équipements non maîtrisés, non administrés ou non mis à jour par l'entité, qu'il s'agisse de smartphones, de tablettes, d'équipements informatiques nomades et fixes ou de supports de stockage amovibles, sur des équipements et des réseaux professionnels est interdite ;
- Une procédure de gestion des postes et des supports dans le cadre de départs de personnel ou de réaffectations à de nouveaux utilisateurs doit être mise en place et validée par le RSSI. Elle doit définir les conditions de recours à un effacement des données.

III- EXIGENCES RELIEES A LA CONCEPTION DU SYSTEME D'INFORMATION

- Le prestataire doit disposer d'une cartographie de l'ensemble des systèmes d'information dont il dispose.
- La sécurité des systèmes d'information doit avoir été prise en compte dans toutes les phases de projet de la conception et de la spécification du système d'information jusqu'à son retrait du service.
- Les systèmes d'exploitation déployés doivent faire l'objet d'un support valide de la part d'un éditeur ou d'un prestataire de service. Seuls les services et les applications nécessaires sont installés, de façon à réduire la surface d'attaque. Une attention particulière doit être apportée aux comptes administrateurs.
- Les éléments d'authentification par défaut des composants du système doivent être modifiés dès leur installation et, s'agissant de mots de passe, être conformes aux recommandations précédentes en matière de choix, de dimensionnement et de stockage.
- Le système d'information doit être segmenté selon des zones présentant chacune un niveau de sécurité homogène.
- La configuration standard des ressources informatiques doit être documentée et mise à jour à chaque changement notable.
- Les systèmes d'exploitation et les logiciels doivent faire l'objet d'un durcissement. Les configurations et les mises à jour sont effectuées dans le strict respect des guides d'autorités reconnues ou des procédures écrites du prestataire.

IV- EXIGENCES RELIEES A L'EXPLOITATION DU SYSTEME D'INFORMATION

- Les procédures nécessaires à l'exploitation du système d'information doivent être documentées et mises à disposition de tous les utilisateurs concernés.
- Des procédures écrites doivent être définies pour les actes élémentaires du maintien en condition de sécurité lors des phases de conception, d'évolution, de gestion et de retrait d'un système.
- Une procédure de gestion des changements doit être en place pour assurer un contrôle satisfaisant de tous les changements apportés. Tous les changements relatifs aux procédures de gestion des audits doivent être documentés.
- Les interventions de maintenance sur les ressources informatiques de l'entité doivent être tracées. Les traces doivent rester accessibles durant au moins trois ans.
- L'utilisation de comptes génériques (ex : admin, user) pour les maintenances doit être marginale et ceux-ci doivent pouvoir être rattachés à un nombre limité de personnes physiques.
- Des logiciels de protection contre les codes malveillants doivent être installés sur l'ensemble des serveurs d'interconnexion, des serveurs applicatifs et des postes de travail du prestataire. Les mises à jour des bases antivirales et des moteurs d'antivirus doivent être déployées automatiquement sur les serveurs et les postes de travail par un dispositif prescrit par les services centraux.
- L'ensemble des logiciels utilisés sur le système d'information doit l'être dans une version pour laquelle l'éditeur assure le support et le tient à jour. En cas de défaillance du support, le prestataire doit en étudier l'impact et prendre les mesures adaptées.
- Un processus de gestion des correctifs propre à chaque système ou applicatif doit être défini et adapté aux contraintes et au niveau d'exposition du système. Les correctifs de sécurité des ressources informatiques locales doivent être déployés par l'équipe locale chargée des SI en s'appuyant sur les préconisations et les outils recommandés par les éditeurs.
- Concernant les mises à jour logicielles des équipements administrés, elles doivent être récupérées depuis une source sûre (le site de l'éditeur par exemple), contrôlées puis transférées sur le poste ou le serveur utilisé pour l'administration des services liés au programme d'audit PASSI.
- Chaque système doit disposer de dispositifs de « journalisation » permettant de conserver une trace des événements de sécurité. Ces traces doivent être conservées de manière sécurisée, à travers des mesures conçues pour protéger le moyen de journalisation contre les modifications non autorisées de la journalisation des informations et les dysfonctionnements.
- La journalisation doit permettre d'assurer la traçabilité des événements suivants :
  - L'usage des identifiants utilisateurs ;
  - Les activités du système ;
  - La date, l'heure et les détails relatifs aux événements significatifs, par exemple les ouvertures et fermetures de session ;
  - L'identité ou l'emplacement du terminal si possible et l'identifiant du système ;
  - Les enregistrements des tentatives d'accès au système, réussies et avortées ;

  - Les enregistrements des tentatives d'accès aux données et autres ressources, réussies ou avortées ;
  - Les modifications apportées à la configuration du système ;
  - L'utilisation des comptes à privilèges ;
  - L'emploi des utilitaires et des applications ;
  - Les fichiers qui ont fait l'objet d'un accès et la nature de l'accès ;
  - Les adresses et les protocoles du réseau ;
  - Les alarmes déclenchées par le système de contrôle d'accès ;
  - L'activation et la désactivation des systèmes de protection, tels que les systèmes antivirus et les systèmes de détection des intrusions ;
  - Les enregistrements des transactions réalisées par les utilisateurs dans les applications.
- Une politique de gestion et d'analyse des journaux de traces des événements de sécurité est définie et mise en œuvre par le RSSI, ceci afin de détecter les erreurs, les dysfonctionnements et les tentatives d'accès illicites survenant sur les éléments qui le composent.
- Les échanges de fichiers entre applications doivent privilégier les protocoles sécurisés (SSL/TLS, SFTP, etc.).
- Afin d'assurer une cohérence dans les échanges entre applications ainsi qu'une traçabilité pertinente des événements techniques et de sécurité, le prestataire assure la synchronisation des horloges de l'ensemble des systèmes de traitement de l'information sur une référence de temps commune (service NTP, Network Time Protocol).
- Une politique de sauvegarde destinée à définir les exigences du prestataire en matière de sauvegarde de l'information, des logiciels et des systèmes doit être définit. Il convient que la politique de sauvegarde définisse les exigences en matière de conservation et de protection des copies de sauvegarde.
- Les impressions d'informations sensibles doivent être effectuées selon une procédure définie préalablement, garantissant un contrôle par l'utilisateur, du déclenchement de l'impression jusqu'à la récupération du support imprimé.

V- EXIGENCES RELIEES AUX CONTROLES D'ACCES

- Après avoir déterminé le niveau de sensibilité, le besoin de diffusion et de partage des ressources, les droits d'accès aux ressources doivent être gérés suivant les principes suivants :
  - Besoin d'en connaître : chaque utilisateur n'est autorisé à accéder qu'aux ressources pour lesquelles on lui accorde explicitement le bénéfice de l'accès ;
  - Besoin d'utiliser : chaque utilisateur n'a accès qu'aux moyens de traitement de l'information (matériel informatique, applications, procédures, salles) dont il a besoin pour accomplir sa tâche ;
  - Moindre privilège : chaque utilisateur accède aux ressources avec le minimum de privilèges lui permettant de conduire les actions explicitement autorisées pour lui.
- À cet effet, une politique explicite de contrôle d'accès aux ressources du PASSI doit être établie, présentant des règles de droit et de restriction d'accès appropriées aux fonctions spécifiques de chaque utilisateur des actifs, avec la quantité de détails et la rigueur des mesures correspondant aux risques associés en matière de sécurité de l'information.
- Cette politique de contrôle d'accès doit tenir compte des exigences suivantes :
  - Exigences en matière de sécurité des applications métier ;
  - Politiques relatives à la diffusion de l'information et aux autorisations, par exemple nécessité de connaître le principe, les niveaux de sécurité de l'information et la classification de l'information ;
  - Cohérence entre la politique des droits d'accès et la politique de classification de l'information des différents systèmes et réseaux ;
  - Législation et obligations contractuelles applicables relatives à la limitation de l'accès aux données ou aux services ;
  - Gestion des droits d'accès dans un environnement décentralisé mis en réseau qui reconnaît tous les types de connexions disponibles ;
  - Cloisonnement des rôles pour le contrôle d'accès, par exemple la demande d'accès, l'autorisation d'accès et l'administration des accès ;
  - Exigences en matière d'autorisation formelle des requêtes d'accès ;
  - Exigences en matière de revue régulière des droits d'accès ;
  - Annulation de droits d'accès ;
  - Archivage des enregistrements de tous les événements significatifs relatifs à l'utilisation et à la gestion des identités des utilisateurs et des informations d'authentification secrètes ;
  - Fonctions avec accès privilégié.
- L'accès à toute ressource non publique doit nécessiter une identification et une authentification individuelle de l'utilisateur. Dans le cas d'accès à des données sensibles, des moyens d'authentification forte doivent être utilisés.
- Les applications manipulant des données sensibles doivent permettre une gestion fine par profils d'accès. Les principes du besoin d'en connaître et du moindre privilège s'appliquent.

- Toute action d'autorisation d'accès d'un utilisateur à une ressource des SI doit s'inscrire dans le cadre d'un processus d'autorisation formalisé, qui s'appuie sur le processus d'arrivée et de départ du personnel.
- Une revue des autorisations d'accès doit être réalisée annuellement sous le contrôle du RSSI, le cas échéant avec l'appui du correspondant local de la SSI.
- Les informations d'authentification (mots de passe d'accès aux SI, clés privées liées aux certificats électroniques, etc.) doivent être considérées comme des données sensibles.
- Les utilisateurs ne doivent pas stocker leurs mots de passe en clair, par exemple dans un fichier, sur leur poste de travail. Les mots de passe ne doivent pas transiter en clair sur les réseaux.
- Chaque compte utilisateur doit être créé avec un mot de passe initial aléatoire unique. Si les circonstances l'imposent, un mot de passe plus simple mais à usage unique peut être envisagé.
- Des moyens techniques permettant d'imposer la politique de mots de passe, par exemple pour s'assurer du respect de l'éventuelle obligation relative à l'usage de caractères spéciaux, doivent être mis en place. A défaut, un contrôle périodique des paramètres techniques relatifs aux mots de passe doit être réalisé.
- Chaque administrateur doit disposer d'un mot de passe propre et destiné à l'administration.
- En cas de départ d'un administrateur disposant de privilèges sur des composants des SI, les comptes individuels dont il disposait doivent être immédiatement désactivés. Les éventuels mots de passe d'administration dont il avait connaissance doivent être changés, par exemple les mots de passe des comptes fonctionnels, des comptes génériques ou des comptes de service utilisés dans le cadre des fonctions de l'administrateur.
- L'accès aux outils et aux interfaces d'administration doit être strictement limité aux personnes habilitées, selon une procédure formelle d'autorisation d'accès. Sauf exception dûment motivée et validée par le RSSI, les utilisateurs n'ont pas de droits d'administration.
- Les opérations d'administration doivent être tracées de manière à pouvoir imputer individuellement les actions d'administration.
- La prise de main à distance d'une ressource informatique locale ne doit être réalisable que par les agents autorisés par l'équipe locale chargée des SI, sur les ressources informatiques de leur périmètre. Des mesures de sécurité spécifiques doivent être définies et respectées.
- La politique de gestion des mots de passe doit être conçue de façon à protéger contre les attaques par essais successifs de mots de passe. Une complexité minimale dans le choix des mots de passe doit être imposée aux utilisateurs.
- La gestion des comptes doit d'appuyer sur une nomenclature adaptée, afin de pouvoir distinguer selon leur usage les comptes d'utilisateur standard, les comptes d'administration (domaine, serveurs, postes de travail) et les comptes de service.
- Les comptes de service doivent faire l'objet d'une restriction des droits, en suivant le principe du moindre privilège.
- Il est nécessaire de désactiver immédiatement, voire de supprimer, les comptes

obsolètes, que ce soient des comptes d'utilisateur (administrateur, service ou utilisateur standard) ou des comptes de machine.

- Afin d'empêcher la réutilisation des empreintes d'un compte d'utilisateur local d'une machine à une autre, il faut soit utiliser des mots de passe différents pour les comptes locaux d'administration, soit interdire la connexion à distance via ces comptes.

VI- EXIGENCES RELIEES A LA SECURITE DES RESEAUX INFORMATIQUES

- Les auditeurs PASSI ne doivent avoir accès qu'au réseau et aux services en réseau pour lesquels ils ont spécifiquement reçu une autorisation. Pour ce faire, le prestataire doit mettre en œuvre une politique d'utilisation des services en réseau qui soit cohérente avec sa politique de contrôle d'accès.
- Cette politique relative à l'utilisation des réseaux et des services en réseau doit couvrir, à minima :
  - Les réseaux et les services en réseau pour lesquels l'accès a été accordé ;
  - Les procédures d'autorisation désignant les personnes autorisées à accéder à tels ou tels réseau et service en réseau ;
  - Les procédures et mesures de gestion destinées à protéger l'accès aux connexions réseau et aux services en réseau ;
  - Les moyens utilisés pour accéder aux réseaux et aux services en réseau (par exemple, aux réseaux privés virtuels ou à des réseaux sans fil) ;
  - Les exigences d'authentification de l'utilisateur pour l'accès à différents services en réseau ;
  - La surveillance de l'utilisation faite de ces services en réseau.
- Le principe de défense en profondeur doit être respecté pour la sécurité des réseaux du prestataire, en particulier par la mise en œuvre successive de « zones démilitarisées » (DMZ), d'environnements de sécurité en zone d'hébergement, de machines virtuelles ou physiques dédiées, de réseaux locaux virtuels (VLAN) appropriés, d'un filtrage strict des flux applicatifs et d'administration.
- Seuls les équipements gérés et configurés par les équipes informatiques habilitées peuvent être connectés au réseau local du prestataire.
- Toute interconnexion entre les réseaux locaux du prestataire et d'un réseau externe (réseau d'un tiers, Internet, etc.) doit être réalisée via les infrastructures maîtrisées du prestataire.
- Dans l'optique de réduire les possibilités offertes à un attaquant, les connexions des machines du réseau interne vers l'extérieur doivent être filtrées.
- Les accès à Internet passent obligatoirement à travers des passerelles maîtrisées du prestataire. Dès lors que des informations sensibles doivent transiter sur des réseaux non maîtrisés, il convient de les protéger spécifiquement par un chiffrement adapté.
- Dans le cas où le prestataire partage des locaux avec des entités externes, des mesures de cloisonnement des ressources informatiques doivent être mises en place.
- Le déploiement de réseaux sans fil doit faire l'objet d'une analyse de risques spécifique. Les protections intrinsèques étant insuffisantes, des mesures complémentaires doivent être prises dans le cadre de la défense en profondeur. En particulier, une segmentation du réseau doit être mise en place de façon à limiter à un périmètre déterminé les conséquences d'une intrusion depuis la voie radio. À défaut de mise en œuvre de mesures spécifiques, le déploiement de réseaux sans fil sur des SI manipulant des données sensibles est proscrit.
- Le prestataire doit implanter des mécanismes de protection contre les attaques sur les couches basses. Une attention particulière doit être apportée à l'implantation des

protocoles de couches basses, de façon à se prémunir des attaques usuelles par saturation ou empoisonnement de cache. Cela concerne, par exemple, le protocole ARP.

- Lorsque l'utilisation de protocoles de routage dynamique est nécessaire, celle-ci doit s'accompagner de la mise en place d'une surveillance des annonces de routage et de procédures permettant de réagir rapidement en cas d'incidents.
- Le protocole de routage dynamique de type IGP doit être activé exclusivement sur les interfaces nécessaires à la construction de la topologie du réseau et désactivé sur le reste des interfaces. La configuration du protocole de routage dynamique doit systématiquement s'accompagner d'un mot de passe de type MESSAGEDIGEST- KEY.
- Lors de la mise en place d'une session EGP avec un pair extérieur sur un média partagé, cette session doit également s'accompagner d'un mot de passe de type MESSAGE-DIGEST-KEY.
- Les mots de passe par défaut doivent être impérativement modifiés, de même que les certificats. Les dispositions nécessaires doivent être prises auprès des fournisseurs de façon à pouvoir modifier les certificats installés par défaut.
- Les équipements de réseaux, comme les routeurs, doivent faire l'objet d'un durcissement spécifique comprenant notamment, outre le changement des mots de passe et des certificats, la désactivation des interfaces et des services inutiles ainsi que la mise en place de mécanismes de protection du plan de contrôle.
- De façon à garantir un niveau de sécurité satisfaisant face aux attaques informatiques, des mécanismes de filtrage et de cloisonnement doivent être mis en œuvre.

VII- EXIGENCES RELIEES A LA SECURITE DES POSTES DE TRAVAIL

- Les postes de travail utilisés dans le cadre du programme PASSI doivent être sous le contrôle du prestataire.
- Une procédure de SSI doit définir les règles concernant le traitement à appliquer aux informations ayant été stockées ou manipulées sur des postes réaffectés.
- La gestion des privilèges des utilisateurs sur leurs postes de travail doit suivre le principe du moindre privilège : chaque utilisateur ne doit disposer que des privilèges nécessaires à la conduite des actions relevant de sa mission.
- Les privilèges d'accès des administrateurs doivent être utilisés uniquement pour les actions d'administration le nécessitant. Si une délégation de privilèges sur un poste de travail est réellement nécessaire pour répondre à un besoin ponctuel de l'utilisateur, celle-ci doit être tracée, limitée dans le temps et retirée à échéance.
- Dans la mesure du possible, les données traitées par les auditeurs doivent être stockées sur des espaces dédiées sur le réseau PASSI, eux-mêmes sauvegardés selon les exigences des entités et en accord avec les règles de sécurité en vigueur.
- Un moyen de chiffrement reconnu par une autorité légitime et soutenu par des algorithmes de chiffrement, des longueurs des clés et des pratiques d'utilisation conformes aux bonnes pratiques doit être mis à la disposition des utilisateurs et des administrateurs afin de chiffrer les données sensibles stockées sur les postes de travail.
- Le cycle de vie de ce moyen de chiffrement doit être soutenu par une politique relative à l'utilisation, la protection - y compris du matériel physique utilisé pour générer, stocker et archiver les clés - et la durée de vie des clés cryptographiques qui y sont associées, depuis leur génération jusqu'à leur destruction en passant par leur stockage, leur archivage, leur extraction, leur attribution et leur retrait. Les clés secrètes et privées devront être protégées contre toute utilisation ou divulgation non autorisée.
- Les accès à distance aux SI de l'entité (accès dits « nomades ») doivent intervenir via des réseaux privés virtuels (VPN) de confiance conformes aux recommandations d'une autorité légitime.
- Un pare-feu local conforme aux recommandations d'une autorité légitime doit être installé sur les postes nomades. Afin de rendre plus difficile ce déplacement latéral de l'attaquant, il est nécessaire d'activer le pare-feu local des postes de travail au moyen de logiciels intégrés (pare-feu local Windows) ou spécialisés.
- Lors de l'utilisation de postes nomades, le prestataire veille particulièrement à ce que les informations liées à l'activité d'audit ne soient pas compromises. La politique en matière de postes nomades doit ainsi envisager :
    - Les mesures de protection contre la perte ou le vol, en particulier en cas d'usage des postes nomades dans des moyens de transports, des hôtels ou des salles de réunions ;
    - L'enregistrement des appareils mobiles ;
    - Les exigences liées à la protection physique ;
    - Les restrictions liées à l'installation de logiciels ;
    - Les exigences liées aux versions logicielles des appareils mobiles et à l'application de correctifs ;

- Les restrictions liées aux connexions à des services d'information ;
- Les contrôles d'accès ;
- Les techniques cryptographiques ;
- La protection contre les logiciels malveillants ;
- La désactivation, l'effacement des données ou le verrouillage à distance ;
- Les sauvegardes ;
- L'utilisation des services web et des applications web.

- Lorsqu'il est nécessaire d'utiliser des supports amovibles, il convient de contrôler le transfert de l'information sur ces supports en documentant les procédures et les niveaux d'autorisation. Des procédures de gestion des supports amovibles doivent être mises en œuvre conformément au plan de classification adopté par le prestataire, notamment en mettant en œuvre les exigences suivantes :
  - Le prestataire doit rendre impossible toute récupération du contenu d'un support réutilisable devant être retiré de son SI, si ce contenu n'est plus indispensable ;
  - Le retrait des supports du prestataire doit exiger une autorisation formelle et le prestataire doit garder un enregistrement de ces retraits pour en assurer la traçabilité ;
  - Tous les supports qui sont utilisés dans le cadre d'un audit PASSI doivent être conservés dans un environnement sûr, sécurisé et conforme aux spécifications du fabricant ou d'une autorité légitime ;
  - Des techniques cryptographiques doivent être mises en œuvre protéger les données figurant sur le support amovible ;
  - Diverses copies de données de valeur doivent être conservées sur des supports séparés pour réduire les risques concomitants d'endommagement ou de perte de données ;
  - Un registre des supports amovibles doit être maintenus ;
  - Le prestataire ne doit activer les lecteurs de supports amovibles que si l'activité d'audit le nécessite.
- Seuls les supports de stockage amovibles (clés USB et disque durs externes, notamment) fournis aux auditeurs par le prestataire peuvent être utilisées. Ceux-ci doivent être sécurisés selon un standard reconnu par une autorité légitime.
- Un filtrage par le pare-feu doit être en place afin de bloquer l'accès aux ports d'administration par défaut des postes de travail (ports TCP 135, 445 et 3389 sous Windows, port TCP 22 sous Unix), excepté depuis les ressources explicitement identifiées (postes d'administration et d'assistance utilisateur, éventuels serveurs de gestion requérant l'accès à des partages réseau sur les postes, etc.).
- Une analyse des flux entrants utiles (administration, logiciels d'infrastructure, applications particulières, etc.) doit être menée par le pare-feu pour définir la liste des autorisations à configurer. Il est préférable de bloquer l'ensemble des flux par défaut et de n'autoriser que les services nécessaires depuis les équipements correspondants (« liste blanche »).
- Le pare-feu doit également être configuré pour journaliser les flux bloqués, et ainsi identifier les erreurs de configuration d'applications ou les tentatives d'intrusion.

- Pour les postes de travail nomades manipulant des données sensibles, un filtre de confidentialité doit être fourni et être positionné sur l'écran dès lors que le poste est utilisé en dehors du bureau du prestataire.
- Des règles de configuration des interfaces de connexion sans fil (Wifi, Bluetooth, 30, etc.), permettant d'interdire les usages non maîtrisés et d'éviter les intrusions via ces interfaces, doivent être définies et appliquées. Les interfaces sans fil ne doivent être activées qu'en cas de besoin.
- Des règles doivent être en place pour limiter les applications installées et modules optionnels des navigateurs web aux seuls nécessaires
- Des règles doivent être en place pour chiffrer les partitions où sont stockées les données des utilisateurs
- Des règles doivent être en place pour désactiver les exécutions automatiques (autorun).
- En cas de dérogation nécessaire aux règles de sécurité globales applicables aux postes, ceux-ci doivent être isolés du système PASSI (s'il est impossible de mettre à jour certaines applications nécessaires pour un audit technique par exemple).
- Des règles doivent être mises en place permettant d'interdire l'exécution de programmes sur les périphériques amovibles (par exemple, « Applocker » sous Windows ou des options de montage « noexec » sous Unix).

VIII- EXIGENCES RELIEES A LA GESTION DES INCIDENTS

- Le prestataire doit mettre en place des procédures spécifiant quand et comment il convient de contacter les autorités compétentes.
- À cet effet et dans le cas où le prestataire dispose d'une équipe chargée de la réponse aux incidents liés à la sécurité de l'information, l'appréciation et la décision peuvent être transmises à cette équipe en vue de leur confirmation ou d'une nouvelle appréciation. Dans tous les cas, le prestataire doit enregistrer les conclusions de l'appréciation et la décision de manière détaillée en vue de contrôles ou de références ultérieurs.
- Les procédures de signalement doivent définir comment il convient de signaler dans les meilleurs délais les incidents liés à la sécurité de l'information (par exemple, en cas de suspicion de violation de la loi).
- La réponse aux incidents doit comporter :
  - Le recueil de preuves aussitôt que possible après l'incident;
  - Une analyse scientifique de la sécurité de l'information, le cas échéant (voir 16.1.7);
  - Une remontée d'informations, le cas échéant;
  - L'assurance que toutes les tâches concernant la réponse sont correctement journalisées en vue d'une analyse ultérieure;
  - La communication de l'existence d'un incident lié à la sécurité de l'information ou de tout détail pertinent qui s'y rapporte aux autres personnes internes et externes ou aux organisations ayant besoin d'en connaître;
  - Le traitement de la ou des failles constatées dans la sécurité de l'information causant ou contribuant à l'incident;
  - Une fois que l'incident a été résolu avec succès, la clôture formelle de l'incident et son enregistrement.
- Les exigences en matière de procédures de gestion des incidents doivent contenir, à minima, les éléments suivants :
  - Le prestataire doit établir des responsabilités de gestion pour garantir que les procédures suivantes sont développées et communiquées de manière adéquate au sein de l'organisation :
    - ✓ Procédures de planification et de préparation des réponses aux incidents;
    - ✓ Procédures de surveillance, de détection, d'analyse et de signalement des événements et des incidents liés à la sécurité de l'information;
    - ✓ Procédures de journalisation des activités de gestion des incidents;
    - ✓ Procédures de traitement des preuves scientifiques;
    - ✓ Procédures d'appréciation et de prise de décision relatives aux événements liés à la sécurité de l'information et d'appréciation des failles liées à la sécurité de l'information;
    - ✓ Procédures de réponse, incluant les procédures de remontée d'information, de récupération contrôlée de l'incident et de communication aux organisations ou aux personnes internes ou extérieures à l'organisation;
  - Les procédures établies doivent garantir :
    - ✓ Qu'un personnel compétent au sein de l'organisation traite les questions relatives aux incidents liés à la sécurité de l'information;
    - ✓ Qu'un point de contact pour la détection et le signalement des incidents liés à la

sécurité existe;

- ✓ Que des contacts appropriés sont entretenus avec les autorités, les groupes d'intérêts externes ou les forums qui traitent des questions relatives aux incidents liés à la sécurité de l'information.

- Les procédures de signalement doivent également prévoir :
  - ✓ Des formulaires spécifiques destinés à faciliter le signalement, récapitulant toutes les actions à mettre en œuvre lorsqu'un événement lié à la sécurité de l'information est détecté;
  - ✓ La procédure à engager lorsqu'un événement lié à la sécurité de l'information se produit, à savoir: noter immédiatement tous les détails (par exemple le type de non-conformité ou de défaillance, le dysfonctionnement constaté, les messages apparaissant à l'écran) et en informer immédiatement le responsable servant de point de contact et n'exécuter que des actions concertées;
  - ✓ Une référence à un processus disciplinaire formel pour les salariés ayant enfreint les règles de sécurité;
  - ✓ Des processus de retour d'information adéquats, afin de communiquer les détails de la résolution du problème aux personnes ayant signalé un événement, une fois que le problème a été réglé et clôturé.

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