ROYAUME DU MAROC
ADMINISTRATION DE LA DEFENSE NATIONALE

DIRECTION GENERALE DE LA SECURITE
DES SYSTEMES 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	2.1	11/2025

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
2.0	02/2024	- Réorganisation des chapitres et des sections - Développement du processus de qualification - Intégration d'une nouvelle section sur la gestion de la qualification - Révision des exigences et des niveaux de qualification des auditeurs - Ajustements mineurs
2.1	11/2025	- Révision des critères liés à l'expérience et à l'ancienneté des auditeurs

PUBLIC CONCERNÉ PAR CE DOCUMENT :

Entités et Infrastructures d'importance vitale (cf. loi n° 05.20 relative la cybersécurité)
Prestataires d'audit de la sécurité des systèmes d'information
Organismes d'évaluation

POUR TOUTE REMARQUE :

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

SOMMAIRE

1. Contexte et objectifs

Conformément aux dispositions du décret n° 2-21-406 pris pour l'application de la loi n° 05-20 relative à la cybersécurité, les entités et infrastructures d'importance vitale (IIV) disposant de systèmes d'information sensibles (SIS), de classe A ou de classe B, 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 lesdits prestataires d'audit en vue d'être qualifiés par cette direction générale.

Ce système de qualification constitue un gage de confiance et une garantie de la compétence, l'expertise, l'expérience des PASSI et de la qualité des prestations fournies, leur permettant de réaliser des missions d'audit au profit des entités, au sens de la loi 05-20, et IIV disposant de systèmes d'information sensibles.

Le système de qualification s'appuie sur la vérification d'un certain nombre de critères attestant que le prestataire dispose, notamment :

- d'une expérience et de références suffisantes dans les domaines d'audit de la SSI ;
- de ressources humaines compétentes et qualifiées ;
- de méthodes et outils de travail efficaces et adaptés à l'exercice de ses missions ;
- de méthodologies de travail respectant les règles déontologiques et de sécurité.

2. Activités d'audit concernées par la qualification

Les domaines d'audit objets du système de qualification sont définis au niveau de l'annexe 2 du décret n° 2-21-406 précité. Il s'agit de :

- Audit organisationnel et physique ;
- Audit d'architecture ;
- Audit de configuration ;
- Tests d'intrusion ;
- 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 (02) étapes comme indiqué ci-après :

Etape 1 – Examen du dossier :

Elle consiste en l'analyse des pièces et documents constituant le dossier de la demande de qualification, et ce conformément à l'article 21 du décret n° 2-21-406 précité. La liste de ces pièces et documents est la suivante :

a) Formulaire de la demande de la qualification, selon le modèle publié sur le site web de la DGSSI ;
b) Copie des statuts de la société ;
c) Attestation d'inscription au registre de commerce ;
d) Liste des noms des associés et leurs nationalités ;
e) Copies des pièces d'identité des dirigeants de la société et des membres de ses organes d'administration ;

f) Copies des pièces d'identité des auditeurs proposés ;

g) Note indiquant les moyens humains et techniques de la société ;

h) Copies des casiers judiciaires des auditeurs proposés, établis par l'autorité marocaine compétente ;

i) Curriculums vitae des auditeurs proposés, selon le modèle publié sur le site internet de la DGSSI ;

j) Copies des diplômes et certificats de formation des auditeurs proposés ;

k) Copies des contrats de travail conclus avec les auditeurs proposés ;

l) Copies des attestations de référence, signées et datées, délivrées par les maîtres d'ouvrages au profit desquels ont été réalisées des prestations d'audit de la sécurité des systèmes d'information, et devant indiquer obligatoirement : le nom de l'organisme audité, l'objet précis, la nature et le domaine de l'audit, le périmètre de l'audit, la date de réalisation, le délai d'exécution, le montant de la prestation, le nom, prénom et la qualité du signataire ainsi que ses coordonnées (adresse, n° de téléphone et adresse mail).

m) Document décrivant la méthodologie appliquée pour conduire la prestation d'audit, objet de la demande de qualification.

n) Pour les PASSI ayant été préalablement qualifiés par la DGSSI, la liste détaillée des missions d'audit de sécurité des systèmes d'information réalisées durant les trois dernières années, auprès d'entités soumises à la loi n° 05.20 relative la cybersécurité. Cette liste doit indiquer obligatoirement et pour chaque mission d'audit, les informations suivantes : le nom de l'organisme audité, l'objet, la nature et le domaine de l'audit, le périmètre de l'audit, la date de réalisation de la mission et la liste des auditeurs ayant participé à la mission.

Outre les pièces et documents cités ci-dessus, la DGSSI peut demander tous documents ou informations complémentaires utiles à l'instruction du dossier. Elle peut aussi demander toute explication ou justification, notamment au sujet des statuts de la société, de l'identité des associés, de l'expérience des auditeurs ou des attestations de référence.

L'examen des dossiers des demandes de qualification se fait au vu des conditions et critères ci-dessous :

— Être constitué sous forme de société de droit marocain ;

— Disposer en son sein d'une structure organisationnelle (ex : direction, département, service ou autre avec un responsable nommé à sa tête) dédiée exclusivement à l'audit de la sécurité des systèmes d'information ;

— Justifier d'une expertise avérée et d'une ancienneté suffisante dans les domaines d'audit de la SSI objets de la demande de qualification. Le candidat PASSI doit disposer aussi d'une grande expérience et de références techniques suffisantes en la matière.

— La demande de qualification doit porter au minimum sur trois (03) domaines d'audit et le PASSI doit présenter un nombre suffisant d'auditeurs. Au terme du processus de qualification, la décision de qualification ne peut être accordée que si le PASSI :

- arrive à couvrir au minimum trois domaines d'audit ;
- dispose au minimum de trois auditeurs ayant réussi les évaluations ;
- dispose au minimum d'un auditeur responsable de mission, tel que défini à la section 5.3, ayant réussi les évaluations.

Enfin, et conformément aux dispositions de l'article 20 du décret n° 2-21-406 précité, le candidat PASSI doit, afin de fournir des prestations d'audit de la sécurité des systèmes d'information ayant

la classification « classe A », remplir les conditions suivantes :

- Le capital de la société doit être majoritairement détenu par des marocains ;
- Les auditeurs proposés doivent être de nationalité marocaine.

Etape 2 – Evaluations :

Cette phase, conduite conformément à l'article 22 du décret n° 2-21-406 précité consiste en l'évaluation :

- des processus de l'entreprise (capacités organisationnelles, capacités financières, assurances, veille, formation et maintien des compétences, gestion des ressources, moyens de travail et outils etc.) conformément au chapitre 4 du présent référentiel ;
- des méthodologies de travail et des outils utilisés conformément au chapitre 4 du présent référentiel.
- de la sécurité des locaux et du système d'information du prestataire d'audit, conformément à l'annexe du présent référentiel ;
- des auditeurs et le respect des prérequis pour leur qualification conformément au chapitre 5 du présent référentiel ;

A l'issue des deux étapes et au vu des résultats de l'examen du dossier du candidat et des évaluations précitées, la DGSSI délivre la décision de qualification au PASSI en indiquant notamment :

- La dénomination et l'adresse du siège social du prestataire d'audit ;
- Les domaines d'audit objet de la qualification, en indiquant la classe des systèmes d'information sensibles que le prestataire est autorisé à auditer ;
- La durée de validité de la qualification qui ne doit pas dépasser trois (03) ans ;

La DGSSI délivre également des attestations aux auditeurs ayant réussi les tests d'évaluation. Ces attestations précisent, pour chaque auditeur, le domaine d'audit objet de la qualification, le niveau de qualification, la durée de validité de l'attestation et le rattachement de l'auditeur en question au PASSI qualifié.

Les modalités d'organisation et de déroulement des tests d'évaluation des auditeurs sont fixées par le Règlement d'examen des candidats auditeurs, élaboré par la DGSSI.

Il sied enfin de signaler que lors de la mission d'évaluation, le candidat PASSI doit respecter les délais préalablement convenus avec la DGSSI et l'organisme d'évaluation. Tout dépassement non justifié de ces délais pourrait entraîner la suspension voire l'arrêt de la procédure de qualification. En cas de circonstances exceptionnelles, le candidat doit informer immédiatement la DGSSI et l'organisme d'évaluation de tout retard et proposer des solutions alternatives permettant de maintenir la continuité de la mission d'évaluation.

La DGSSI se réserve le droit de prendre des mesures appropriées, y compris l'arrêt de la qualification, si le candidat ne respecte pas les délais convenus sans justification valable.

En cas de refus de qualification, la DGSSI notifie sa décision au candidat PASSI.

4. Exigences relatives au prestataire d'audit

4.1. 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, avant chaque prestation d'audit, que les auditeurs désignés ont signé la charte d'éthique.

— Le prestataire doit s'assurer, pour chaque prestation d'audit, que les auditeurs désignés ont les qualités et les compétences requises.

4.2. Protection de l'information

Le prestataire doit veiller à la protection de toute information récoltée lors de la prestation d'audit 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 auditeurs, au reste des 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.

4.3. Gestion des ressources et des compétences

— 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 doit s'assurer du maintien à jour des compétences de ses 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. Les preuves de compétence doivent être conservées dans les dossiers des auditeurs ;

— Le prestataire est responsable des méthodes, outils (logiciels ou matériels) et techniques utilisées 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, 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 former ses auditeurs sur sa méthodologie et ses processus d'audit. Les preuves de la sensibilisation doivent être conservées dans les dossiers des auditeurs ;

— 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. Les preuves de la sensibilisation doivent être conservées dans les dossiers des auditeurs ;

— 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.

4.4. Référentiels et Méthodologie

— En accord avec le commanditaire de l'audit, le prestataire doit faire usage d'une démarche d'audit éprouvée basée sur des normes et référentiels reconnus (ISO-2700x, ISO 19011, COBIT, ITIL, …) et pertinents à chaque domaine d'audit ;

— Le prestataire doit disposer d'une méthodologie de gestion de travail bien définie. Cette méthodologie doit couvrir au moins la planification et préparation des missions d'audit, la préparation de listes de contrôle (checklist), la collecte des preuves, la qualification des constats, la rédaction des rapports, les modalités de suivi des missions et le contrôle qualité des livrables ;

— 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 de la réglementation, des référentiels et des guides de bonnes pratiques relatifs à la sécurité des systèmes d'information.

4.5. Gestion de la qualification

— Après octroi de la qualification et à la fin de chaque semestre, le prestataire d'audit qualifié est tenu d'élaborer et de transmettre à la DGSSI un rapport faisant état de (i) la liste des missions d'audit, réalisées dans le cadre de la loi n° 05.20 relative la cybersécurité avec indication des auditeurs ayant réalisés ces missions et de (ii) la liste actualisée des auditeurs en activité au sein de la société ;

— Après l'obtention de la qualification, le PASSI peut être soumis avant la fin de la première année de qualification, à un audit de contrôle mené par la DGSSI, afin de s'assurer de la levée des non conformités mineures révélées dans le cadre de l'audit d'évaluation et restées en instance.

— Si le PASSI qualifié ne répond plus à l'un des critères sur la base desquels la qualification lui a été délivrée, la DGSSI le met en demeure de se conformer aux prescriptions y afférentes dans un délai fixé selon l'importance des prescriptions ;

— Si le PASSI qualifié ne défère pas à la mise en demeure, la DGSSI suspend sa qualification, jusqu'à ce qu'il se conforme auxdites prescriptions selon le délai fixé par la Direction Générale, à défaut, la décision de qualification lui est retirée.

— Tout prestataire d'audit qualifié doit informer, sans délai, la DGSSI de toute modification survenue dans les éléments ayant servi de base à la délivrance de sa qualification. À cette fin, le PASSI doit soumettre à la DGSSI un dossier contenant les documents requis :

- Cas de modification de la raison sociale : le formulaire de déclaration de modification (téléchargeable sur le site internet de la DGSSI) ainsi que les pièces et documents « b » et « c » cités au chapitre 3.
- Cas de modification de l'adresse du siège sociale : le formulaire de déclaration de modification (téléchargeable sur le site internet de la DGSSI) ainsi que les pièces et documents « b » et « c » cités au chapitre 3.
- Cas de modification des associes et/ou des parts du capital social : le formulaire de déclaration de modification (téléchargeable sur le site internet de la DGSSI) ainsi que les pièces et documents « b » cités au chapitre 3.
- Cas de départ des auditeurs qualifiés : le formulaire de déclaration de modification (téléchargeable sur le site internet de la DGSSI).

— Les prestataires d'audit qualifiés peuvent modifier la portée de leurs qualifications par l'ajout de nouveaux domaines d'audit et/ou de nouveaux auditeurs. À cette fin, le PASSI doit soumettre à la DGSSI un dossier contenant les documents requis :

  - Cas d'ajout d'un nouveau domaine d'audit : le formulaire de déclaration de modification (téléchargeable sur le site internet de la DGSSI) ainsi que les pièces et documents « l » et « m » cités au chapitre 3.
  - Cas d'ajout d'un auditeur : le formulaire de déclaration de modification (téléchargeable sur le site internet de la DGSSI) ainsi que les pièces et documents « f », « h », « i », « j » et « k » cités au chapitre 3.
  - Cas d'extension des domaines d'audit d'un auditeur : le formulaire de déclaration de modification (téléchargeable sur le site internet de la DGSSI) ainsi que les pièces et documents « i » et « j » cités au chapitre 3.

— Le renouvellement de la qualification du prestataire d'audit de la sécurité des systèmes d'information a lieu dans les mêmes conditions exigées pour son obtention sous réserve du dépôt de la demande dans les (60) soixante jours, avant l'expiration de la décision de qualification.

5. Exigences et niveaux de qualification des auditeurs

5.1. Aptitudes générales

— Les auditeurs doivent posséder les qualités personnelles tel que décrites dans la norme ISO 19011 précitée, notamment :

  - L'autonomie ;
  - Le sens d'observation ;
  - L'esprit de synthèse et perspicacité (bonne compréhension des situations et bonne manière de tirer les conclusions) ;
  - La rigueur et le 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.

5.2. Engagements

— Les auditeurs doivent avoir un contrat de droit marocain avec le prestataire d'audit qualifié ;

— Les auditeurs doivent signer la charte d'éthique élaborée par le prestataire et s'engagent 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.

- L'impartialité : Les auditeurs ne peuvent exécuter des missions d'audit, auprès d'un commanditaire, entrainant un conflit d'intérêt. Ils doivent conduire leurs missions de manière objective et indépendante, en veillant à ne pas compromettre leur intégrité en raison d'intérêts personnels ou financiers.

5.3. Formation, Expérience et niveaux de qualification

— Les auditeurs doivent avoir reçu une formation de base en technologies des systèmes d'information.

— Les auditeurs proposés doivent justifier d'une ancienneté suffisante au sein de la société afin d'assurer une bonne connaissance de ses activités et de ses processus internes ;

— Ils doivent maîtriser les bonnes pratiques et la méthodologie d'audit décrite dans la norme ISO19011 précitée ;

— Ils doivent disposer des compétences requises pour l'exercice de sa mission, notamment celles spécifiques à leur domaine d'audit tel que spécifié dans la section 5.4 ;

— Ils doivent 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	— Être diplômé en technologies de l'information ; — Disposer de certificats en relation avec le domaine de la sécurité des SI ; — Disposer d'un minimum de trois (03) années d'expérience dans les domaines des systèmes d'information et de la sécurité des systèmes d'information ; — Justifier de l'exécution d'un minimum de six (06) différentes missions se rapportant aux domaines d'audit objet de la demande de qualification ; — Pour le domaine des tests d'intrusion, disposer d'un minimum d'une (01) années d'expérience.
Responsable de mission	— Être diplômé en technologies de l'information ; — Disposer de certificats en relation avec le domaine de la sécurité des SI ; — Disposer au minimum de quatre (04) années d'expérience dans le domaine de la sécurité des systèmes d'information ; — Disposer d'un minimum de cinq (05) années d'expérience dans le domaine des systèmes d'information ; — Justifier de l'exécution d'un minimum de dix (10) 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.

5.4. Aptitudes spécifiques

Les compétences décrites dans le présent chapitre font l'objet d'une évaluation individuelle conformément aux modalités fixées par le Règlement d'examen des candidats auditeurs PASSI, élaboré par la DGSSI.
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 ou équivalent ;
- 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 ;
- Norme ISO27005 ou équivalent
- Politique de sécurité des systèmes d'information ;
- Gestion des actifs
- 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 et connaissances de base dans les systèmes de lutte contre l'incendie, conditionnement d'air, vidéosurveillance et leur maintenance.

— Maîtrise des pratiques liées à l'audit :
- Conduite d'entretien ;
- Visite sur site ;
- Analyse documentaire.
- Echantillonnage
- Rédaction des constats et des rapports

Les certifications professionnelles ci-après représentent un plus :

— ISO19011, 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.
- Connaissance de base en cryptographie
- Gestion des identités et des accès
- Compétences en programmation et automatisation (Automatisation et script) pour évaluer rapidement de grandes configurations et connaissance des outils d'automatisation

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 ;
- Outils de Gestion des vulnérabilités, gestion des incidents et SIEM

— 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 et outils de test 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 :

— SCADA (Supervisory Control and Data Acquisition) / HMI (Human Machine Interface)

— 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 ;
- Firewalls industriels.

— Connaissances des outils de gestion de la sécurité des systèmes industriels :
- Simulateurs et testeurs de sécurité industriels ;
- Outils d'analyse de flux de données ;
- Gestion des vulnérabilités, gestion des incidents et SIEM.

6. Exigences relatives au déroulement d'une prestation d'audit

Les étapes que doivent suivre les prestataires d'audit, lors de l'exécution d'une mission d'audit de la sécurité des SIS, sont définies comme suit :

— étape 1: établissement d'un contrat d'audit ;

— étape 2: préparation et déclenchement de la prestation d'audit ;

— étape 3: exécution de la prestation d'audit de la sécurité des SIS ;

— étape 4: restitution des résultats ;

— 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.

6.1. Etablissement du contrat d'audit

— Le prestataire doit établir un contrat de service avec le commanditaire avant l'exécution de la prestation devant tenir compte à minima des dispositions de l'article 29 du décret n° 2-21-406 pris pour l'application de la loi 05-20 ;

— Les niveaux de qualification et les domaines d'audit 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 d'audit.

6.2. Préparation et déclenchement de la prestation

— Le prestataire est tenu de ne faire intervenir que des auditeurs ayant obtenus la qualification de la DGSSI pour effectuer les prestations d'audit de la sécurité des SIS ;

— Le prestataire d'audit doit désigner, parmi ses auditeurs qualifiés, un auditeur ayant le niveau de qualification de responsable de mission (conformément à la section 5.3) pour tout audit qu'il effectue.

— L'auditeur responsable de mission doit constituer une équipe d'auditeurs ayant les compétences adaptées à la nature de l'audit.

— L'auditeur responsable de mission élabore un plan d'audit qui couvre en particulier les points suivants :

- les objectifs, champs et critères de l'audit, le périmètre technique et organisationnel de la prestation d'audit ;
- 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 ;
- 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 d'audit et l'entité auditée, 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.

6.3. Exécution de la prestation

— L'auditeur responsable de mission 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 à l'auditeur responsable de mission, 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 appartenant à l'entité auditée.

— Les actions et résultats des auditeurs 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.

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

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.

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.

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.

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.

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.

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.

6.5. Restitution

— Dès la fin de l'audit, et sans attendre que le rapport d'audit soit achevé, l'auditeur responsable de mission doit informer 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, dès leur détection, et décrit les recommandations associées.

6.6. Elaboration du rapport d'audit

— A la fin de la mission, le prestataire d'audit doit remettre au commanditaire le rapport final d'audit accompagné de tous les documents et supports y afférents. Le PASSI ne doit garder aucune copie des documents fournis par le commanditaire d'audit pour les besoins de la mission d'audit (rapports, documents et supports fournis) et ce conformément à l'article 32 du décret précité ;

— Le prestataire d'audit doit veiller à la confidentialité du rapport d'audit et ce conformément à l'article 22 de la loi n° 05.20 relative à la cybersécurité ;

— 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 de mission 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.

— Le prestataire d'audit doit mentionner dans son rapport et informer le commanditaire de l'obligation, pour ce dernier, de conserver le rapport d'audit et les documents y afférents pendant une durée de trois (03) ans au moins.

— Il est recommandé que le prestataire d'audit, informe le commanditaire de l'obligation de transmettre le rapport d'audit à la DGSSI.

6.7. Clôture de la prestation

— Il est recommandé qu'une réunion de clôture de l'audit soit organisée avec le commanditaire 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.

— Toutes les traces, relevés de configuration, informations ou documents relatifs au système d'information audité obtenus par le prestataire doivent être restitués au commanditaire ou, sur sa demande, détruits conformément à la convention d'audit. Le cas échéant, l'auditeur responsable de mission produit un procès-verbal de destruction de ces données qu'il remet au commanditaire en 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 suivi afin de vérifier si les mesures correctives proposées lors de l'audit ont été correctement mises en œuvre.

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

I- Conception du système d'information

— Le prestataire doit évaluer les risques relatifs à l'ensemble de ses systèmes d'information.

— La sécurité des systèmes d'information doit être 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 compétent. 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.

— 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.

— Le prestataire doit disposer d'une cartographie de l'ensemble des systèmes d'information dont il dispose.

— Le prestataire doit avoir un schéma simplifié du réseau (ou cartographie réseau) représentant les différentes zones IP et le plan d'adressage associé, les équipements de routage et de sécurité (pare-feu, relais applicatifs, etc.) et les interconnexions avec l'extérieur (Internet, réseaux privés, etc.) et les partenaires. Ce schéma doit être maintenu à jour et permettre également de localiser les serveurs détenteurs d'informations sensibles du PASSI.

II- Gestion des actifs et classification de l'information

— Le prestataire d'audit doit :

- Etablir et maintenir à jour un inventaire des ressources informatiques sous sa responsabilité, en s'appuyant sur un outillage adapté. Cet inventaire est tenu à la disposition de la DGSSI en cas de besoin de coordination opérationnelle. Il comprend la liste des « briques » matérielles et logicielles utilisées ainsi que leurs versions exactes. Il est constitué d'une base de données de configuration, maintenue à jour et tenue à la disposition du RSSI. L'historique des attributions des biens inventoriés doit être conservé dans le respect de la réglementation en vigueur ;
- Identifier les actifs associés à l'information et aux moyens de traitement de l'information utilisées dans le cadre des prestations d'audit ;
- Disposer des licences valides des outils (logiciels ou matériels) utilisés pour la réalisation de la prestation ;
- Classifier l'ensemble des actifs informationnels selon des échelles définies et assurer leur protection depuis leur création jusqu'à leur éventuelle destruction ;
- Formaliser et mettre en place le processus de restitution, en fin de mission ou d'emploi, des actifs physiques et électroniques, appartenant au prestataire d'audit ou lui ayant été confiés ;
- S'assurer que les données non chiffrées doivent être effacées d'une manière sécurisée avant l'envoi en maintenance externe de toute ressource informatique.

— Les informations sensibles relatives aux audits, et notamment les preuves, les constats et les rapports d'audit, doivent être protégés au minimum au niveau Diffusion Restreinte.

— 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 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.

— Des mesures doivent être mises en œuvre afin de garantir la protection des informations sensibles en termes de confidentialité et d'intégrité. A défaut d'utilisation d'un réseau homologué, ces informations doivent être chiffrées à l'aide d'un moyen de chiffrement labellisé.

— La sensibilité de toute information doit être évaluée. Le marquage systématique des documents, en fonction du niveau de sensibilité, est fortement recommandé.

III- Sécurité physique des locaux du prestataire d'audit

— Le prestataire d'audit 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 d'audit doit déterminer et appliquer des règles de sécurité physiques et environnementales aux bureaux, aux salles et aux équipements hébergeant le système d'information pour protéger le matériel contre les dangers environnementaux et les possibilités d'accès non autorisé. Ces règles doivent être justifiées dans son évaluation des risques de sécurité de l'information.

— L'installation de matériel de protection contre le feu est obligatoire. Des procédures de réaction à un incendie sont définies et régulièrement testées. Les salles techniques doivent être propres. Aucun carton, papier ou autre matière inflammable ne doit être entreposé dans ces locaux.

— L'accès aux zones internes (autorisées uniquement au personnel du centre informatique ou aux visiteurs accompagnés) et restreintes (autorisées aux seules personnes habilitées ou aux visiteurs accompagnés) doit reposer sur un dispositif de contrôle d'accès physique. Ce dispositif doit s'appuyer sur des produits de sécurité labellisés, lorsqu' ils sont disponibles, et être maintenu en condition de sécurité de façon rigoureuse.

— La délivrance des moyens d'accès physique doit respecter un processus formel permettant de s'assurer de l'identité de la personne et s'appuyer sur le processus d'arrivée et de départ du personnel. Le personnel autre que celui explicitement autorisé ou habilité mais néanmoins appelé à intervenir dans les zones internes ou restreintes (entretien ou réparation des bâtiments ou des équipements non informatiques, nettoyage, visiteurs) accède à ces zones sous surveillance permanente et systématique.

— 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 et ces traces doivent être conservés pendant un an, dans le respect de la réglementation protégeant les données personnelles. L'autorisation formelle d'accès doit être fournie au cas par cas par le prestataire d'audit qui documente sa décision et prend la responsabilité formelle de cette autorisation.

— Tout accès au réseau installé dans une zone d'accueil du public doit être filtré ou isolé du reste du réseau informatique du Prestataire d'audit.

— Il convient de protéger le câblage du réseau contre les dommages et les interceptions des communications qu'ils transmettent. En complément, les panneaux de raccordements et les salles des câbles doivent être placés en dehors des zones d'accueil du public et leur accès doit être contrôlé.

— Un découpage des sites en zones physiques de sécurité doit être effectué, en liaison avec le RSSI, les correspondants locaux de la SSI et les services chargés de l'immobilier, de la sécurité et des moyens généraux. Pour chaque zone de sécurité, des critères précis d'autorisation d'accès sont établis.

— Dans le cas où un Prestataire d'audit partage des locaux avec des Prestataires, des mesures de cloisonnement des ressources informatiques doivent être mises en place. Les mesures prises doivent être validées par la DGSSI si elles ne sont pas physiques.

— Dans l'objectif d'empêcher la perte, l'endommagement, le vol ou la compromission des actifs et l'interruption des activités de l'organisation, le mobilier de sécurité doit être adéquat.

— Une procédure de sortie des actifs 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 d'audit 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 d'audit 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).

— Une climatisation proportionnée aux besoins énergétiques du système informatique doit être installée. Des procédures de réaction en cas de panne, connues du personnel, doivent être élaborées et vérifiées annuellement. Ces dispositions visent à prévenir toute surchauffe des équipements, pouvant engendrer une perte du service voire une détérioration du matériel.

IV- <u>Sécurité Organisationnelle</u>

— Le Prestataire d'audit établit une PSSI, validée par la direction. Une structure de pilotage de la PSSI est définie. Cette structure est chargée de sa mise en place, de son évolution, de son suivi et de son contrôle.

— Une organisation dédiée à la SSI est déployée au sein de la Direction en charge des prestations PASSI. Cette organisation définit les responsabilités internes et à l'égard des

tiers, les modalités de coordination avec les autorités externes ainsi que les modalités d'application des mesures de protection. Des procédures d'application des mesures sont écrites et portées à la connaissance de tout le personnel du Prestataire d'audit.

— Une note d'organisation fixe la répartition au sein de chaque Prestataire d'audit et au niveau local des responsabilités et rôles en matière de SSI.

— Tout Prestataire d'audit doit disposer d'un référent en Sécurité des Systèmes d'Information qui sera soutenu par la direction ou par une instance décisionnelle spécialisée selon le niveau de maturité de la structure.

— Une attention particulière doit être portée au recrutement des personnes clés de la SSI : RSSI ou référent SSI et administrateurs de sécurité. Les RSSI et leurs correspondants locaux doivent être spécifiquement formés à la SSI. Les administrateurs des SI doivent être régulièrement sensibilisés aux devoirs liés à leur fonction et doivent veiller à respecter ces exigences dans le cadre de leurs activités quotidiennes.

— Ce référent devra être connu de tous les utilisateurs et sera le premier contact pour toutes les questions relatives à la sécurité des systèmes d'information. Il sera en charge de :

  - La définition des règles à appliquer selon le contexte ;
  - La vérification de l'application des règles ;
  - La sensibilisation des utilisateurs et définition d'un plan de formation des acteurs informatiques ;
  - La centralisation et traitement des incidents de sécurité constatés ou remontés par les utilisateurs.

— Ce référent devra être formé à la sécurité des systèmes d'information et à la gestion de crise.

— Chez les Prestataires d'audit de taille plus importante, ce référent peut être désigné pour devenir le relais du RSSI. Il pourra par exemple signaler les doléances des utilisateurs et identifier les thématiques à aborder dans le cadre des sensibilisations, permettant ainsi d'élever le niveau de sécurité du système d'information au sein de l'organisme.

— Le référent SSI ou le RSSI coordonne les actions permettant l'intégration des clauses liées à la SSI dans tout contrat ou convention impliquant un accès par des tiers à des informations ou à des ressources informatiques.

— Une charte SI, récapitulant les mesures pratiques d'utilisation sécurisée des ressources informatiques et élaborée sous le pilotage de la chaîne fonctionnelle de la SSI, est communiquée à l'ensemble des agents du Prestataire d'audit. Cette charte doit être opposable juridiquement et, si possible, intégrée au règlement intérieur du Prestataire d'audit. Le personnel non permanent (stagiaires, intérimaires, prestataires) est informé de ses devoirs dans le cadre de son usage des SI.

— Chaque utilisateur doit être régulièrement informé des exigences de sécurité le concernant. Il doit être formé à l'utilisation des outils de travail conformément aux règles édictées au niveau de la charte SI.

— Toutes les personnes manipulant des informations sensibles doivent le faire avec une attention particulière, dans le respect des textes en vigueur. Les sanctions éventuelles s'appliquant aux cas de négligence ou de malveillance leur sont rappelées.

— Une procédure permettant de gérer les arrivées, les mutations et les départs des collaborateurs doit être formalisée et appliquée strictement. Cette procédure doit couvrir au minimum :

  - La gestion et la révocation des comptes et des droits d'accès aux SI, y compris

pour les partenaires et les prestataires externes ;

- La gestion du contrôle d'accès aux locaux ;
- La gestion des équipements mobiles ;
- La gestion du contrôle des habilitations.

— Un tableau de bord de la SSI est mis en place et tenu à jour. Il fournit au RSSI et aux autorités une vision générale du niveau de sécurité et de son évolution, rendant ainsi plus efficace le pilotage de la SSI. Au niveau stratégique, le tableau de bord de la SSI permet de suivre l'application de la politique de sécurité et de disposer d'éléments propres à qualifier les ressources devant être allouées à la SSI. Au niveau du pilotage, la mise en place de ce tableau de bord permet de contrôler la réalisation d'objectifs opérationnels, d'améliorer la qualité de service et de détecter au plus tôt les retards dans la réalisation de certains objectifs de sécurité.

V- Contrôles d'accès

— 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 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.

— L'appartenance aux groupes du domaine ADMINISTRATEURS DE L'ENTREPRISE et ADMINISTRATEURS DU DOMAINE n'est nécessaire que dans de très rares cas. Les opérations les plus courantes doivent être effectuées avec des comptes du domaine membres des groupes locaux d'administration des ordinateurs ou ayant une délégation d'administration.

— Les mots de passe des comptes de service sont souvent inscrits en dur dans des applications ou dans des systèmes. Cette mauvaise pratique ne permet pas d'être en mesure de changer ces mots de passe, par exemple en urgence. Il est ainsi nécessaire de veiller à pouvoir maîtriser leur utilisation.

— 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.

— 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.

— 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 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- Exploitation du système d'information

— Les procédures nécessaires à l'exploitation du système d'information doivent être documentées et mises à disposition de tous les utilisateurs concernés.

— Ces 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, elles doivent en outre prendre en considération les résultats de l'évaluation des risques.

— Toute l'intervention d'un sous-traitant ou d'un expert pour le compte du Prestataire d'audit dans le domaine des SI doit être encadrée par des clauses de sécurité au niveau d'une charte Prestataire. Ces clauses spécifient les mesures SSI que le prestataire doit respecter dans le cadre de ses activités.

— Tout contrat d'hébergement détaille les dispositions mises en œuvre pour prendre en compte la SSI. Ce sont notamment les mesures prises pour assurer le maintien en condition de sécurité des systèmes et permettre une gestion de crise efficace (conditions d 'accès aux journaux, mise en place d'astreintes, etc.).

— 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 du Prestataire d'audit 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.

— Concernant les informations sensibles, déterminer sur quels composants du système d'information elles se localisent (bases de données, partages de fichiers, postes de travail, etc.). Ces composants devront faire l'objet de mesures de sécurité spécifiques pouvant porter sur la sauvegarde, la journalisation, les accès, etc. 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 pendant un an, 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'identification 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.

VII- Sécurité des réseaux informatiques

— D'une manière générale, l'architecture des infrastructures des centres informatiques est conçue de façon à satisfaire l'ensemble des besoins en disponibilité, confidentialité, traçabilité et intégrité. Le principe de défense en profondeur doit être respecté, 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.

— 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.

— 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 d'audit.

— 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 d'audit 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.

— 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 d'audit 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 d'audit. Dès lors que des informations sensibles doivent transiter sur des réseaux non maîtrisés, il convient de les protéger spécifiquement par un chiffrement adapté.

— 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 d'audit 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.

— Le réseau de stockage et de sauvegarde pour les besoins des centres informatiques repose sur une architecture consacrée.

VIII- <u>Sécurité des postes de travail et des supports amovibles</u>

— Les postes de travail utilisés dans le cadre du programme PASSI doivent être sous le contrôle du prestataire d'audit.

— Une procédure de SSI doit définir les règles à appliquer au niveau des postes de travail, des postes nomades et des supports amovibles. Les règles concernant le traitement à appliquer aux informations ayant été stockées ou manipulées sur des postes réaffectés doivent être intégrées.

— 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 du Prestataire d'audit 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 du Prestataire d'audit (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 d'audit 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.

— 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 d'audit.

— 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).

— Les postes de travail sont fournis à l'utilisateur par le Prestataire d'audit, gérés et configurés sous la responsabilité du Prestataire d'audit. La connexion d'équipements non maîtrisés, non administrés ou non mis à jour par le Prestataire d'audit, 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 référent SSI ou le RSSI. Elle doit définir les conditions de recours à un effacement sécurisé des données.

— L'accès au compte de l'administrateur local sur les postes de travail doit être strictement limité aux équipes en charge de l'exploitation et du support sur ces postes de travail.

— Une procédure formalisée de configuration des postes de travail est établie par chaque Prestataire d'audit, conformément aux normes et exigences applicables.

— La configuration des interfaces de connexion sans fil doit interdire les usages dangereux de ces interfaces.

— Le stockage local d'information sur les postes de travail nomades doit être limité au strict nécessaire. Les informations sensibles doivent être obligatoirement chiffrées par un moyen de chiffrement labellisé.

— Le partage de répertoires ou de données hébergées localement sur les postes de travail n'est pas autorisé.

— Dans le cas où des données doivent être stockées localement sur le poste de travail, des moyens de synchronisation ou de sauvegarde doivent être fournis aux utilisateurs.

— Les données présentes sur les postes partagés (portable de prêt, par exemple) doivent être supprimées entre deux utilisations, dès lors que les utilisateurs ne disposent pas du même besoin d'en connaître.

— Un câble physique de sécurité doit être fourni avec chaque poste portable. Les utilisateurs doivent être sensibilisés à son utilisation

— 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 d'audit, notamment en mettant en œuvre les exigences suivantes :

  - Le prestataire d'audit 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 d'audit doit exiger une autorisation formelle et le prestataire d'audit 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 d'audit 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 d'audit peuvent être utilisées. Ceux-ci doivent être sécurisés selon un standard reconnu par une autorité légitime.

IX- Gestion des incidents

— Le prestataire d'audit 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 d'audit 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 d'audit 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 ;
- 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 d'audit 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 référent SSI ou le RSSI doit être informé par les opérations de tout incident de sécurité et contribue si nécessaire à la qualification de l'incident et au pilotage de son traitement. Tout incident de sécurité, même apparemment mineur, dont l'impact dépasse ou est susceptible de dépasser le SI du Prestataire d'audit, doit faire l'objet d'un compte-rendu à la DGSSI.