ANSSI
AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION
CÔTE D'IVOIRE

# RÉFÉRENTIEL D'EXIGENCES RELATIF À L'AGRÉMENT DES PRESTATAIRES D'AUDIT DE SÉCURITE DES SYSTÈMES D'INFORMATION

www.anssi.gouv.ci

# RÉFÉRENCES

| Descriptif du Document | |
|---|---|
| Titre du document : | ANSSI – Référentiel d'exigences des PASSI |
| Version du document : | 1.0 |
| Classification | **Public** |
| Statut du document : | En cours / Revu / **Validé** |
| Auteur : | **ANSSI/PEC/DAC** |

| Mise à jour | | |
|---|---|---|
| **Version** | **Date** | **Motif et nature de la modification** |
| 1.0 | 04/02/2026 | Création et diffusion du document |
| | | |

## NIVEAUX DE CONFIDENTIALITE ANSSI

| N° | LIBELLÉ | DESCRIPTION | ☑ CONFIDENTIALITÉ DU DOCUMENT |
|---|---|---|---|
| [1] | **Public** | Informations pouvant être partagées sans risque pour l'ANSSI ou ses partenaires. | ☑ |
| [2] | **Interne** | Informations de fonctionnement non critiques et non sensibles réservées à l'usage interne de l'ANSSI. Informations nécessitant une gestion contrôlée. | |
| [3] | **Confidentiel** | Informations sensibles dont la divulgation pourrait nuire ou compromettre l'ANSSI, ses employés ou ses partenaires. | |
| [4] | **Hautement Confidentiel** | Informations critiques liées à des opérations sensibles ou des partenaires stratégiques qui, en cas de divulgation, pourraient causer des dommages graves à l'ANSSI ou à ses parties prenantes. | |
| [5] | **Classifié** | Informations extrêmement sensibles dont la divulgation peut entraîner des dommages graves, catastrophiques ou irréversibles à la sécurité nationale, à des partenaires ou à l'agence elle-même. | |

# TABLE DES MATIÈRES

# PARTIE 1 : GÉNÉRALITES

# 1. INTRODUCTION

L'audit de sécurité des systèmes d'information est un moyen d'éprouver et d'évaluer le niveau de sécurité d'un système d'information. Il permet de mettre en évidence les forces, mais surtout les faiblesses et les vulnérabilités du système d'information. Ses conclusions permettent d'identifier des axes d'amélioration, de proposer des recommandations et de contribuer ainsi à l'élévation de son niveau de sécurité. Il devient donc impératif que les administrations privées et les organismes publics mettent à jour leur système d'information en procédant à la réalisation d'audits de sécurité de leurs systèmes d'information.

Conformément aux dispositions du décret n°2021-917 du 22 décembre 2021, définissant les procédures d'audit, de contrôle et de certification des systèmes d'information, les organismes du secteur public ainsi que les entreprises privées opérant sur le territoire national sont tenus de faire auditer régulièrement leurs systèmes d'information par des prestataires de services d'audit agréés par l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI).

Ce décret précise en son article 5 que les missions d'audit de sécurité sont effectuées par l'ANSSI elle-même. Toutefois, l'article 6 prévoit que l'ANSSI peut déléguer ces missions à des Prestataires d'Audit de Sécurité des Systèmes d'Information (PASSI), dûment agréés selon les conditions fixées par elle.

Cette disposition confère à l'ANSSI la possibilité de recourir à un réseau de prestataires spécialisés pour assurer la couverture des besoins nationaux en matière d'audit, dans le respect des exigences de qualité et de conformité.

## 2. OBJECTIF DU DOCUMENT

Le présent référentiel a pour objet de définir, de manière précise et exhaustive, l'ensemble des exigences à satisfaire par tout prestataire candidat à l'agrément en tant que Prestataire d'Audit de la Sécurité des Systèmes d'Information (PASSI) auprès de l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI).

Il constitue le document de référence officiel encadrant le processus d'évaluation des prestataires, en fixant :

- Les critères d'éligibilité administratifs, légaux, organisationnels, et techniques ;
- Les compétences minimales attendues du personnel impliqué dans les audits ;
- Les méthodologies et outils conformes aux bonnes pratiques et aux exigences du Référentiel Général de Sécurité des Systèmes d'Information (RGSSI) ;
- Les garanties de qualité, de confidentialité et d'intégrité des prestations d'audit ;
- Les engagements déontologiques visant à préserver l'indépendance, l'objectivité et la neutralité des évaluations.

Ce référentiel vise donc à instaurer un cadre unifié et exigeant, garantissant la qualité et la fiabilité des audits, la protection des organisations et la confiance numérique au niveau national.

## 3. CHAMP D'APPLICATION

Le présent référentiel s'applique à l'ensemble des candidats à l'agrément PASSI, à l'ANSSI qui est l'autorité compétente et l'évaluateur, ainsi qu'aux organismes soumis à l'obligation d'audit.

## 4. CADRE LEGAL, REGLEMENTAIRE ET NORMATIF

La gouvernance de la sécurité des systèmes d'information en Côte d'Ivoire est régie par un ensemble de textes juridiques nationaux et des normes internationales. Ces instruments constituent la base légale et normative qui encadre la sécurisation des transactions électroniques, ainsi que la mise en œuvre des bonnes pratiques de sécurité.

- Loi n°2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel ;
- Loi n°2013-451 du 19 juin 2013 relative à la lutte contre la cybercriminalité ;
- Loi n°2013-546 du 30 juillet 2013 relative aux transactions électroniques ;
- Décret n°2021-915 du 22 décembre 2021 portant adoption de la politique de sécurité des systèmes d'information de l'administration publique ;
- Décret n°2021-916 du 22 décembre 2021 portant adoption du Référentiel Général de Sécurité des Systèmes d'Information (RGSSI) et du Plan de Protection des Infrastructures Critiques (PPIC) ;
- Décret n°2021-917 du 22 décembre 2021 définissant les procédures d'audit, de contrôle et de certification des systèmes d'information ;
- Décret n°2024-958 du 30 octobre 2024 portant création, attributions, organisation et fonctionnement de l'Agence Nationale de la Sécurité des Systèmes d'Information ;
- ISO/IEC 27001:2022, système de management de la sécurité de l'information ;
- ISO/IEC 27002:2022, code de bonnes pratiques pour le management de la sécurité de l'information ;
- ISO/IEC 19011:2018, lignes directrices pour l'audit des systèmes de management.

## 5. DEFINITIONS

Les définitions ci-dessous s'appuient sur la norme ISO19011 et le décret n°2021-917 du 22 décembre 2021 définissant les procédures d'audit, de contrôle et de certification des systèmes d'information, la présente section en propose une version opérationnelle adaptée à l'agrément PASSI.

**Agrément des prestataires** : autorisation délivrée par l'ANSSI à une personne morale en vue de réaliser des missions d'audits de sécurité.

**Analyse des risques** : processus systématique consistant à identifier et à estimer les risques auxquels un système d'information est exposé.

**ANSSI** : Agence Nationale de la Sécurité des Systèmes d'Information.

**Audit** : processus systématique, indépendant et documenté visant à obtenir des preuves d'audit et à les évaluer objectivement pour déterminer le niveau de conformité et de maîtrise des risques.

**Audité** : organisme responsable de tout ou partie du système d'information audité et faisant appel au service d'audit de sécurité des systèmes d'information.

**Auditeur :** membre de l'équipe d'audit chargé de conduire les activités (collecte, tests, analyses, entretiens) et de produire des preuves/constats.

**Certificat** : attestation formelle, délivrée par l'Autorité compétente prouvant qu'une personne physique ou morale remplit les conditions fixées par le référentiel général de sécurité.

**Certification** : processus de délivrance d'un certificat.

**Conflit d'intérêts** : situation dans laquelle des intérêts secondaires peuvent altérer l'indépendance, l'impartialité ou l'objectivité (réels, potentiels ou perçus).

**Confidentialité** : obligation de protéger les informations non publiques obtenues dans le cadre de la mission.

**Correspondant d'audit** : personne désignée chez l'audité pour servir de point de contact principal avec le prestataire lors d'une mission d'audit.

**Constats d'audit** : résultat objectif fondé sur des preuves, décrivant une situation observée (écart, bonne pratique, risque).

**Convention de service** : document contractuel formalisant l'accord entre un prestataire d'audit de sécurité (PASSI) et une organisation auditée, définissant les conditions de réalisation de la prestation d'audit.

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

**Expert technique** : spécialiste intervenant sur des sujets pointus (ex : tests d'intrusion, de configuration, d'architecture, etc.)

**Données sensibles :** l'ensemble des informations dont la divulgation, l'altération ou la destruction non autorisée présente un risque significatif, qu'il s'agisse :

- de données à caractère personnel définies comme sensibles au sens de la loi N° 2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel, notamment les données révélant l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, les données génétiques, biométriques, relatives à la santé, à la vie sexuelle ou l'orientation sexuelle, ainsi que les données relatives aux condamnations pénales et infractions ;
- de données d'importance vitale ou stratégique pour l'État, incluant les informations classifiées (défense nationale, secret défense), les données relatives aux infrastructures critiques, à la sécurité nationale, à la souveraineté économique, aux intérêts fondamentaux de la Nation ou dont la compromission pourrait porter atteinte à la sécurité publique, aux relations internationales ou aux capacités opérationnelles des services de l'État.

**Dossier d'audit :** ensemble des documents/traces (plan, journaux, scripts, captures, échantillons, rapports) conservés avec traçabilité.

**Indépendance :** absence de liens (capitalistiques, contractuels, hiérarchiques, commerciaux) susceptibles d'influencer la mission.

**Impartialité :** absence de biais ou de préférence ; traitement équitable des informations et des parties.

**Méthodologie d'audit :** cadre procédural (préparation, exécution, validation, restitution) conforme au RGSSI et aux bonnes pratiques.

**Périmètre d'agrément :** ensemble des domaines d'audit (organisationnel/physique, architecture & configuration, applications & code, tests d'intrusion, environnements spécifiques) pour lesquels le PASSI est autorisé à intervenir.

**Périmètre d'audit** : environnement physique, logique et organisationnel dans lequel se trouve le système d'information ou la portion du système d'information, sur lequel l'audit est effectué.

**Plan d'audit** : document de mission (objectifs, périmètre, ressources, calendrier, méthodes, règles de test, gestion des risques).

**Prestataire d'audit de sécurité des systèmes d'information (PASSI)** : organisme agréé par l'ANSSI qui fournit des prestations d'audits de sécurité des systèmes d'informations conformes aux exigences règlementaires.

**Preuves d'audit** : information vérifiable (documentaire, technique, observation, entretien, journal, capture) établissant un fait ; doit être adéquate, pertinente et suffisante.

**Rapport d'audit** : document de synthèse élaboré par l'équipe d'audit et remis à l'ANSSI et à l'audité à l'issue de l'audit de sécurité. Il présente les résultats de l'audit et en particulier les vulnérabilités découvertes ainsi que les mesures correctives proposées.

**RE-PASSI** : Référentiel d'Exigences Relatif à l'Agrément des Prestataires d'Audit de la Sécurité des Systèmes d'Information, le présent document.

**Responsable d'équipe :** auditeur senior garant de la méthodologie, de l'indépendance, du planning, de la qualité des livrables et de la relation client.

**Risques** : probabilité qu'une menace donnée exploite une vulnérabilité occasionnant un impact dommageable sur la disponibilité, l'intégrité et la confidentialité d'un système d'information.

**Objectivité** : jugement fondé sur les preuves, exempt d'opinions personnelles.

**Sécurité des systèmes d'information** : processus constituant en la mise en valeur de mesures techniques et organisationnelles visant à assurer qu'un système d'information est capable de résister à des évènements volontaires ou non, susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées ou transmises.

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

**Vulnérabilité** : faiblesse d'un bien ou d'une mesure pouvant être exploitée par une menace ou un groupe de menaces.

# PARTIE 2 : TYPES D'AUDIT ET CATEGORIE D'AGREMENT

# 1. TYPES D'AUDIT

Afin de couvrir l'ensemble des besoins en matière de sécurité des systèmes d'information, le présent référentiel définit différents types d'audit pouvant faire l'objet d'un agrément PASSI. Conformément aux exigences réglementaires, toute demande d'agrément doit inclure l'audit organisationnel et physique ou l'audit de tests d'intrusion.

## 1.1. Audit organisationnel et physique

L'audit organisationnel et physique permet de faire un état des lieux complet de la sécurité du système d'information et d'en identifier les dysfonctionnements et les risques. Il permet ainsi de couvrir l'ensemble du système d'information de l'organisme et de détecter les carences liées aux différents processus de gestion et d'organisation de la sécurité.

## 1.2. Audit de tests d'intrusion

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

Cette activité d'audit peut être réalisée soit depuis l'extérieur du système d'information audité (notamment depuis Internet ou le réseau interconnecté d'un tiers), soit depuis l'intérieur et selon différents modes (boîte noire, boîte grise, boîte blanche).

# 2. CATÉGORIE D'AGRÉMENT

La catégorie d'agrément désigne la classification officielle attribuée à un PASSI, en fonction du domaine d'activité ou du niveau de compétence reconnu par l'ANSSI.

A cet effet, nous avons défini trois niveaux d'exigences dans le RGSSI permettant de définir le degré d'habilitation et de responsabilité accordé aux PASSI :

- Niveau 1 : Concerne les organismes à faible exposition, qui n'exploitent pas de données sensibles.

- Niveau 2 : Concerne les organismes qui traitent des données sensibles dont la compromission aurait un impact limité, sans effet sur l'ordre national.
- Niveau 3 : S'applique aux organismes qui exploitent des données sensibles à caractère vital ou stratégique pour la nation.

Pour mieux encadrer les missions d'audits, le dispositif d'agrément prévoit deux catégories :

- **Catégorie Essentielle** : couvrant les systèmes de niveaux 1 et 2. Les PASSI de cette catégorie sont capables d'intervenir sur des environnements sensibles ou non, sans impact majeur sur la sécurité nationale.
- **Catégorie Critique** : couvrant les systèmes de niveau 3. Les PASSI de cette catégorie sont capables d'intervenir sur des environnements classés critiques.

| Niveau / Catégorie | N1 | N2 | N3 |
|---|---|---|---|
| **Essentielle** | ✓ | ✓ | |
| **Critique** | ✓ | ✓ | ✓ |

Ce dispositif est de nature incrémentielle : un PASSI agréé pour la catégorie Critique est réputé disposer des compétences lui permettant également d'intervenir sur les systèmes de la catégorie Essentielle (N1 et N2).

Lors de sa demande d'agrément, le candidat PASSI doit indiquer les types d'audits qu'il propose (organisationnel et physique ou tests d'intrusion). Toutefois, il convient de préciser qu'un PASSI agréé en catégorie Essentielle pour un type d'audit donné ne pourra pas offrir ce service sur des systèmes de niveau 3.

À l'inverse, un PASSI agréé en catégorie Critique pour un type d'audit donné est habilité à offrir ce service aussi bien sur des systèmes de niveau 3 que sur ceux des niveaux 1 et 2.

Un PASSI agréé en catégorie Essentielle peut soumettre à tout moment une nouvelle demande d'agrément pour la catégorie Critique.

# PARTIE 3 : CRITERES D'EVALUATION DES CANDIDATS PASSI

Cette section établit les critères de conformité que le candidat PASSI doit observer, incluant les aspects organisationnels, administratifs, déontologiques, techniques et liés au personnel, pour assurer la qualité et l'intégrité des audits.

Les critères portant la mention **[CRITIQUE]** doivent être respectés par le candidat PASSI sollicitant un agrément de catégorie critique.

## 1. CRITERES ADMINISTRATIFS ET LEGAUX

1) Le candidat PASSI doit être une entité dotée de la personnalité morale légalement constituée, immatriculée (RCCM), disposant d'un IDU avec statut à jour.
2) Le candidat PASSI doit fournir une attestation de non-redevance ou de régularité fiscale délivrée par la Direction Générale des Impôts.
3) Le candidat PASSI doit justifier la régularité de sa situation vis-à-vis des organismes sociaux (CNPS).
4) Les auditeurs du candidat PASSI doivent avoir un contrat signé conforme au droit ivoirien.
5) Un auditeur pris en consultance ne peut participer à deux missions d'audit se déroulant simultanément pour le compte de PASSI différents.
6) Le candidat PASSI doit disposer d'une assurance de Responsabilité Civile Professionnelle valable 12 mois à partir de la date de dépôt et couvrant les activités d'audit de sécurité du système d'information.
7) Le candidat PASSI doit fournir une attestation sur l'honneur signée du représentant légal en vue de certifier l'absence de tout lien de dépendance ou de conflit d'intérêt avec les entités audités ou l'ANSSI (à retirer à l'ANSSI).
8) Le candidat PASSI doit fournir le casier judiciaire de son représentant légal attestant de l'absence de condamnations.
9) **[CRITIQUE]** Le candidat PASSI doit fournir les deux derniers bilans financiers certifiés ou visés par un expert-comptable/commissaire au compte agréé.
10) **[CRITIQUE]** Le candidat PASSI doit démontrer que son contrôle effectif ne relève d'aucun intérêt étranger et que son capital social est détenu à 100% par des nationaux ivoiriens.
11) **[CRITIQUE]** Le candidat PASSI doit disposer d'une assurance cyber couvrant les éventuels dommages causés lors de l'exécution des activités d'audit.

## 2. CRITERES ORGANISATIONNELS

1) Le candidat PASSI doit mettre en place une organisation interne spécifiquement dédiée aux activités d'audit de sécurité distincte de ses autres services, disposant d'une direction clairement identifiée, de procédures documentées et de ressources humaines qualifiées.
2) Le candidat PASSI doit désigner un Responsable de la Sécurité du Système d'Information (RSSI) rattaché à la Direction Générale.
3) Le candidat PASSI doit adopter et diffuser une politique de sécurité des systèmes d'information.
4) Le candidat PASSI doit mettre en œuvre un processus de gestion des risques appliqué à son propre système d'information.
5) Le candidat PASSI doit définir et appliquer une procédure de gestion des incidents incluant les modalités de notification à l'ANSSI et, le cas échéant, au commanditaire de l'audit.
6) Le candidat PASSI doit définir une politique de gestion et d'analyse des journaux des événements de sécurité.
7) Le candidat PASSI doit documenter une méthodologie d'audit (préparation, cadrage, tests, validation des constats, restitution) et un processus de gestion des preuves.
8) Le candidat PASSI doit maintenir un PCA/PRA couvrant l'indisponibilité des locaux/outils, la perte de données d'audit, les incidents de sécurité et les tests périodiques.
9) Le candidat PASSI doit mettre en place des mécanismes documentés de sauvegarde et de restauration sécurisées des données d'audit.
10) Le PASSI doit assurer des mesures de sécurité physique (contrôle d'accès aux zones sensibles, dispositifs incendie testés régulièrement, stockage et destruction sécurisés des preuves).

## 3. CRITERES DE COMPETENCE DU PERSONNEL

1) Le candidat PASSI doit constituer, pour chaque mission, une équipe d'audit constituée d'au moins deux (2) personnes dont un responsable d'équipe.

2) Les auditeurs du candidat PASSI doivent obligatoirement être certifiés ANSSI (voir Annexe1).

3) Le candidat PASSI doit disposer d'auditeurs compétents dans les domaines pour lesquels il sollicite l'agrément. Ces professionnels doivent démontrer des compétences techniques, théoriques et pratiques dans les activités d'audit de sécurité des systèmes d'information (voir Annexe 2).

4) Le candidat PASSI doit garantir la probité et la confidentialité de ses auditeurs par :

   - La signature d'accords de non-divulgation ;
   - L'élaboration d'un processus disciplinaire en cas d'infraction.

5) Le candidat PASSI doit disposer d'un processus de formation continue et de veille technologique.

6) Le candidat PASSI doit s'assurer que chaque auditeur démontre des compétences techniques, rédactionnelles et communicationnelles en français.

7) Le candidat PASSI s'engage à mobiliser et à renforcer les compétences locales en assurant l'implication significative de professionnels nationaux dans les activités d'audit et les actions de transfert de connaissances.

8) **[CRITIQUE]** Les auditeurs du candidat PASSI doivent justifier d'une ancienneté d'au moins un an au sein de l'organisation du PASSI.

9) **[CRITIQUE]** Le candidat PASSI doit produire un bulletin de casier judiciaire vierge pour chaque membre de l'équipe d'audit.

## 4. CRITERES TECHNIQUES

1) Le candidat PASSI doit conserver, dans des environnements protégés et chiffrés, accessibles uniquement aux personnes autorisées, toutes les données d'audit collectées, produites et échangées.
2) Le candidat PASSI ne doit conserver aucune donnée sensible issue des missions d'audit au-delà des délais contractuels, sauf obligation légale ou réglementaire.
3) Le candidat PASSI doit maintenir à jour une cartographie de son réseau précisant les zones d'adressage IP, les équipements de sécurité et de routage et les interconnexions externes.
4) Le système d'information du candidat PASSI doit disposer de dispositifs de journalisation permettant de conserver une trace des événements de sécurité.

- Gestion des risques

5) Le candidat PASSI doit collecter, analyser et exploiter les informations relatives aux menaces pesant sur la sécurité de l'information (techniques, organisationnelles, humaines ou réglementaires). Ces renseignements doivent être intégrés au processus global de gestion des risques.
6) Le candidat PASSI doit identifier les risques et opportunités pouvant impacter la sécurité de l'information en tenant compte du contexte interne et externe, ainsi que des exigences des parties intéressées.
7) Le candidat PASSI doit définir et appliquer un processus d'appréciation des risques formel : identification, analyse (probabilité/impact), et évaluation.
8) Le candidat PASSI doit établir et maintenir un processus de traitement des risques identifiés.

- Contrôle d'accès

9) Le candidat PASSI doit mettre en place un processus de gestion du cycle de vie des identités numériques : création, modification, suspension et suppression. Chaque identité doit être unique et associée à un utilisateur ou à un système identifiable.
10) Le candidat PASSI doit définir des règles précises pour attribuer les droits d'accès en fonction des besoins métiers et du principe du moindre privilège.

11) Le candidat PASSI doit strictement contrôler l'utilisation des programmes capables de contourner et compromettre les mesures de sécurité (ex. éditeurs de registre, outils de diagnostic).

12) Le candidat PASSI doit contrôler et limiter aux personnes autorisées, l'accès au code source des applications et aux outils de développement.

- Gestion des actifs

13) Le candidat PASSI doit établir et maintenir à jour un inventaire complet et à jour de ses actifs informationnels et physiques impliqués dans les activités d'audit, incluant notamment les données, équipements, logiciels, services, infrastructures.

14) Le candidat PASSI doit maintenir un inventaire à jour des outils d'audit (logiciels/matériels) avec licences ou autorisations d'usage valides.

15) Le candidat PASSI doit garantir l'utilisation responsable et éthique de ses outils, maintenus dans des versions à jour.

16) Le candidat PASSI doit classifier les informations selon leur sensibilité et les besoins de confidentialité, d'intégrité et de disponibilité. Cette classification s'applique également aux données et preuves issues des missions d'audit réalisées.

17) Le candidat PASSI doit définir et appliquer des procédures pour le marquage des informations selon leur niveau de classification.

18) Le candidat PASSI doit définir, formaliser et diffuser une politique d'utilisation acceptable des systèmes et actifs informationnels, précisant la responsabilité des utilisateurs, les règles d'usage et les conditions d'utilisations hors site (postes portables, VPNs, supports amovibles, etc.).

19) Le candidat doit s'assurer que tous les accès à distance à son système d'information sont réalisés via des réseaux privés virtuels (VPN) de confiance configurée selon les recommandations de sécurité en vigueur.

20) Le candidat PASSI doit encadrer les postes de travail utilisés dans le cadre des missions d'audit par des règles de sécurité garantissant la protection des informations. Ces postes doivent faire l'objet de mises à jour régulières, être protégés par des dispositifs antiviraux, un verrouillage automatique des sessions et une limitation stricte des privilèges d'accès.

21) Le candidat PASSI doit encadrer l'ensemble du cycle de vie des supports de stockage : acquisition, utilisation, transport, archivage et destruction et protéger les supports contenant des données sensibles contre tout accès, perte ou divulgation non autorisée.

22) Le candidat PASSI doit assurer la destruction physique ou logique des supports contenant des informations confidentielles ou protégées, au moyen de techniques garantissant l'impossibilité de toute récupération ultérieure.

23) Le candidat PASSI doit définir et appliquer un processus formalisé de restitution des actifs physiques et électroniques du personnel en fin de mission ou de contrat. Ce processus doit prévoir, l'effacement sécurisé des données et la vérification de la restitution effective de tout équipement utilisé.

- Cryptographie

24) Le candidat PASSI doit définir, documenter et appliquer une politique cryptographique garantissant la mise en œuvre de mécanismes de chiffrement robustes, fondés sur des algorithmes éprouvés et des longueurs de clé adéquates.

- Relation avec les fournisseurs

25) Le candidat PASSI doit encadrer l'acquisition, l'utilisation et la cessation des services cloud selon ses exigences de sécurité de l'information (authentification, chiffrement, localisation, sauvegarde, réversibilité, etc.).

- Gestion des incidents

26) Le candidat PASSI doit établir et mettre en œuvre un Plan de Réponse aux Incidents (PRI) décrivant les rôles, responsabilités, procédures, outils et canaux de communication nécessaires à la gestion des incidents de sécurité.

27) Le candidat PASSI doit mettre en place des procédures de collecte et de conservation des preuves numériques (forensic) garantissant leur intégrité et leur authenticité.

## 5. CRITERES DEONTOLOGIQUES

1) Le candidat PASSI doit s'abstenir d'auditer un périmètre sur lequel il a fourni conseil, intégration, infogérance ou remédiation.
2) Le candidat PASSI ne doit pas recommander d'éditeurs et d'intégrateurs informatiques.
3) Le candidat PASSI doit fonder ses constats sur des preuves suffisantes, pertinentes, adéquates et pratiquer la validation contradictoire avant rapport final.
4) Le candidat PASSI doit s'assurer du consentement de l'audité avant toute communication d'informations liées aux activités d'audit à un tiers et veiller à anonymiser les informations communiquées lorsque cela est nécessaire.
5) Le candidat PASSI doit fournir le service de manière impartiale, en toute bonne foi et dans le respect de l'audité, de son personnel et de son infrastructure.
6) Le candidat PASSI doit disposer d'une charte d'éthique couvrant les engagements suivants : loyauté, impartialité, respect des règles légales et réglementaires, confidentialité stricte, signalement de contenu illicite, interdiction de cadeaux/avantages (à retirer à l'ANSSI).
7) Le candidat PASSI doit faire signer et appliquer la charte d'éthique par ses auditeurs.

# PARTIE 4 : DISPOSITIONS APPLICABLES AU PRESTATAIRE AGREE ET A LA CONDUITE DES AUDITS

Cette section présente les obligations du PASSI agréé et les exigences à respecter lors de la préparation, de la réalisation et de la clôture des audits.

Les exigences portant la mention **[CRITIQUE]** doivent être respectés par tout PASSI agréé dans la catégorie critique.

## 1. OBLIGATIONS DU PASSI AGREE

1) Le PASSI doit réaliser ses prestations uniquement dans les types d'audit et catégories pour lesquels il a obtenu l'agrément délivré par l'ANSSI.

2) En cas de sous-traitance, le PASSI doit recourir exclusivement à un PASSI lui-même agréé ANSSI, dont la catégorie couvre le niveau d'organisme concerné. Seuls des sous-traitants agréés peuvent intervenir dans la réalisation des missions d'audit.

3) En cas de besoin d'intervention sur un domaine non couvert par son agrément, le PASSI doit en informer l'audité et orienter ce dernier vers l'ANSSI pour une meilleure prise en charge.

4) Le PASSI doit transmettre à l'ANSSI, dans les délais convenus, un exemplaire complet et fidèle du rapport d'audit conforme aux modèles et formats définis par l'ANSSI, exclusivement via les canaux sécurisés approuvés.

5) Le PASSI doit transmettre, dans les délais convenus, un exemplaire complet et fidèle de son rapport d'activité annuelle relatif aux activités d'audit réglementaire, exclusivement via les canaux sécurisés approuvés. Ce rapport présente notamment :

    - Le chiffre d'affaires annuel et les effectifs du personnel d'audit ;
    - Le volume et la typologie des missions réalisées ;
    - Les actions de formation et d'amélioration continue menées ;
    - Les perspectives et évolutions prévues pour l'année suivante.

6) Le PASSI doit informer l'ANSSI, sans délai, de tout incident de sécurité ayant pu impacter la confidentialité, l'intégrité ou la disponibilité des informations traitées ou des outils utilisés dans le cadre de ses missions.

7) Le PASSI doit notifier à l'ANSSI toute modification substantielle de son organisation pouvant impacter le maintien de son agrément (changement de gouvernance, réorganisation interne, perte de personnel clé, etc.).

8) Le PASSI doit se soumettre aux audits de contrôle et d'évaluation organisés par l'ANSSI et fournir aux auditeurs mandatés toutes les informations, documents et accès nécessaires.

9) Le PASSI doit fournir aux auditeurs mandatés par l'ANSSI l'ensemble des informations, documents et accès nécessaires pour mener à bien le contrôle.

10) Tout refus, entrave, ou dissimulation d'information lors d'un audit de contrôle constitue un manquement pouvant entraîner la suspension ou le retrait de l'agrément.

11) Le PASSI doit participer activement aux ateliers, réunions et sessions de formation organisés ou mandatés par l'ANSSI, et veiller à ce que ses représentants désignés relaient en interne les informations issues de ces sessions.

## 2. EXIGENCES RELATIVES AU DEROULEMENT DE LA PRESTATION D'AUDIT

1) La définition du périmètre et des objectifs de la prestation d'audit relève de la responsabilité de l'audité et du PASSI, sous réserve du contrôle de l'ANSSI.

2) Le PASSI doit définir et communiquer à l'audité les conditions nécessaires à la réalisation de la prestation, et s'assurer que celui-ci met à disposition un environnement de travail conforme à ces exigences.

3) Le PASSI doit vérifier que le système audité et ses dépendances externes sont correctement identifiés.

4) Le PASSI doit s'assurer que la prestation est adaptée au contexte et aux objectifs de sécurité ; le cas échéant, il en informe l'audité avant exécution.

### 2.1. Établissement de la convention

5) Le PASSI doit établir une convention de service avec l'audité avant l'exécution de la prestation, signée par les représentants légaux de l'audité et du PASSI (à retirer à l'ANSSI).

#### 2.1.1. Méthodes de la prestation

La convention de service doit :

a) Définir le périmètre, la démarche générale, les activités et modalités de la prestation (objectifs, champs et critères de l'audit, jalons, livrables attendus en entrée et prérequis) ;

b) Préciser les livrables attendus en sortie, les réunions d'ouverture et de clôture, les publics cibles, leur niveau de sensibilité ;

c) Décrire les moyens techniques (matériel et outils) et organisationnels mis en œuvre par le PASSI dans le cadre de sa prestation ;

d) Préciser les méthodes de communication qui seront employées lors de la prestation entre le PASSI et l'audité ;

e) Prévoir les moyens humains, matériels, logistiques et techniques devant être mis à disposition pour la mission ;

f) Préciser la titularité des éléments protégés par la propriété intellectuelle (outils développés, indicateurs de compromission, rapport) ;

g) Préciser les actions interdites sans autorisation expresse de l'audité et les modalités associées ;

h) Définir les moyens de traçabilité entre audité, PASSI et supports soumis à analyse ;

i) En cas de test d'intrusion, préciser les moyens de remédiation et les personnes à contacter en cas d'incident.

### 2.1.2. Organisation

La convention de service doit :

a) Préciser le nom du correspondant d'audit en charge chez l'audité, et mettre en relation le PASSI avec les différents correspondants impliqués ;

b) Préciser les noms, rôles, responsabilités des personnes impliquées, ainsi que les droits de chaque partie :

Droits du PASSI

- Accéder aux locaux, aux systèmes, aux documents de preuve ;
- Poser des questions utiles à la mission ;
- Présenter ses conclusions de manière objective et indépendante ;

Droits de l'audité

- Être informé de la méthodologie et du calendrier de l'audit ;
- Formuler des observations sur les constats présentés.

c) Stipuler que seuls des auditeurs liés contractuellement au PASSI et signataires de sa charte d'éthique peuvent intervenir.

### 2.1.3. Responsabilités

La convention de service doit stipuler que :

a) Le PASSI ne réalisera la prestation qu'après la signature de la convention de service ;

b) Tout manquement constaté à la convention doit être signalé par chaque partie ;

c) En cas de manquement grave constaté lors de la prestation, le PASSI ou l'audité doivent en informer l'ANSSI. Ces manquements peuvent entraîner des sanctions à l'encontre de l'auteur du manquement.

d) Les actions du PASSI doivent rester strictement conformes aux objectifs définis ;

e) L'audité garantit qu'il dispose de l'ensemble des droits de propriété et d'accès sur les actifs concernés par la prestation (systèmes d'information, supports matériels, etc.).

f) L'audité garantit d'avoir recueilli l'accord des éventuels tiers, notamment de ses prestataires ou de ses partenaires, dont les systèmes d'information entreraient dans le périmètre ;

g) L'audité autorise provisoirement le PASSI, aux seules fins de réaliser la prestation, à accéder et à se maintenir dans tout ou partie du périmètre et d'effectuer des traitements sur les données hébergées, quelle que soit la nature de ces données ;

h) Chaque partie doit respecter les responsabilités et précautions d'usage définies dans la convention, afin de préserver la confidentialité des informations traitées et la sécurité du système audité.

### 2.1.4. Confidentialité

La convention de service doit :

a) Prévoir la non-divulgation à un tiers de toute information relative à l'audit et à l'audité sans autorisation écrite ;

b) Préciser les informations que l'audité autorise le PASSI à conserver après la prestation, ainsi que les modalités de leur destruction en cas de refus formel et écrit ;

c) Stipuler que les informations conservées doivent être anonymisées et décontextualisées.

### 2.1.5. Lois et réglementations

La convention de service doit :

a) Être rédigée en français ;

b) Stipuler que seule la version française fait foi, notamment dans le cadre d'un litige ;

c) Stipuler que la législation applicable à la convention de service est la législation ivoirienne ;

d) Préciser les moyens techniques et organisationnels mis en œuvre par le PASSI pour se conformer à la législation ivoirienne applicable, notamment celle concernant la protection des données à caractères personnel ;

e) Définir la durée de conservation des informations liées à la prestation, notamment les évènements collectés et les failles de sécurité détectées. Si besoin, une distinction de la durée de conservation peut être faite en fonction du type d'information. La durée de conservation est de trois (03) ans après la restitution du rapport d'audit, sous réserve de la législation et de la réglementation en vigueur. Cette conservation s'effectue pour des besoins de contrôle de l'ANSSI.

### 2.1.6. Livrables

La convention de service doit préciser que tous les livrables produits par le PASSI au titre de la prestation sont fournis en langue française sauf cas contraire sous demande formelle et écrite par l'audité.

### 2.1.7. Agrément

La convention de service doit :

a) Indiquer que la prestation réalisée est une prestation réglementaire et inclure l'attestation d'agrément du PASSI ;

b) Indiquer que les auditeurs disposent d'une attestation individuelle de compétence pour les activités d'audit et inclure ces attestations.

## 2.2. Préparation et déclenchement de la prestation

6) Le responsable d'équipe d'audit doit, dès le début de la préparation de l'audit, établir un contact avec l'audité. Ce contact formel, a pour objectif de mettre en place les circuits de communication, de décision et de préciser les modalités d'exécution de la prestation.

7) Le responsable d'équipe d'audit doit obtenir du correspondant d'audit la liste des points de contact nécessaires à la réalisation de la prestation.

8) Le responsable d'équipe d'audit élabore un plan d'audit. Ce plan d'audit couvre en particulier les points suivants :

   - Les objectifs, champs et critères de l'audit, ;
   - Le périmètre technique et organisationnel de la prestation ;
   - Les dates et lieux où seront menées les activités d'audit ;
   - 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.

9) Les objectifs, le champ, les critères et le calendrier de l'audit doivent être définis entre le PASSI et l'audité, en considération des contraintes d'exploitation du système d'information de l'audité. Ces éléments doivent figurer dans la convention d'audit et dans le plan d'audit.

10) En fonction de l'activité d'audit, l'équipe d'auditeurs doit obtenir, au préalable, toute la documentation existante de l'audité (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.

11) L'audit ne doit débuter qu'après une réunion formelle d'ouverture réunissant les représentants habilités du PASSI et de l'audité, afin de valider l'ensemble des modalités de la prestation. Son but est de :

   - Valider le plan d'audit préétablit ;
   - Exposer le planning prévisionnel de l'audit ;
   - Présenter les activités d'audit qui seront menées ;
   - Confirmer les circuits de communication ;
   - Fournir des clarifications sur les éventuelles ambiguïtés existantes.

L'ANSSI doit préalablement être informée de la tenue de la réunion et peut y être représentée pour s'assurer du respect des exigences. Suite à cette réunion, un compte rendu doit être rédigé et signé par le PASSI et l'audité.

12) Le PASSI doit sensibiliser avant l'audit, l'audité sur l'intérêt de sauvegarder et préserver les données, applications et systèmes présents sur les machines auditées.

13) Au préalable, et dans le cas spécifique des tests d'intrusion, un plan de test doit être signé par l'audité et d'éventuelles tierces parties. Il 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.

**Les livrables de cette phase :**

- La note de cadrage (à retirer à l'ANSSI) ;
- Le compte rendu de la réunion d'ouverture ;
- Le planning prévisionnel ;
- Le plan de test (si applicable).

## 2.3. Exécution de la prestation

14) Le responsable d'équipe d'audit doit tenir informé l'audité des vulnérabilités critiques découvertes au cours de l'audit. Il doit rendre compte immédiatement à l'audité de tout élément constaté présentant un risque immédiat et significatif, et dans la mesure du possible, lui proposer des mesures permettant de lever ce risque.

15) L'audit doit être réalisé dans le respect du personnel et des infrastructures physiques et logiques de l'audité.

16) Les constatations et observations effectuées par les auditeurs doivent être factuelles et basées sur la preuve.

17) Les auditeurs doivent rendre compte des constats d'audit au responsable d'équipe d'audit, lequel peut en avertir sur-le-champ sa hiérarchie et l'audité, dans le respect des clauses de confidentialité mentionnées dans la convention de service.

18) Le système d'information audité doit retrouver un état dont la sécurité n'est pas dégradée par rapport à l'état initial.

19) Les constats d'audit doivent être documentés, tracés et conservés par le PASSI durant toute la durée de l'audit.

20) Le PASSI et les auditeurs doivent prendre toutes les précautions utiles pour préserver la confidentialité des documents et informations relatives à l'audité.

21) Les actions et résultats des auditeurs du PASSI 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.

22) **[CRITIQUE]** Le PASSI doit stocker localement (sur le territoire national) les preuves et livrables issues des audits. En cas de recours à des outils hébergés hors du territoire national, toutes les données d'audits devront être archivées localement puis supprimées des serveurs à la fin de l'audit.

## 2.4. Restitution

23) Dès la fin de la mission d'audit, une restitution préliminaire des constats et vulnérabilités détectées doit être réalisée, présidée par le responsable d'audit, au cours d'une réunion de clôture.

### 2.4.1. Synthèse, plan d'action et recommandations

- Les documents résultant de la phase d'exécution doivent être soigneusement archivés. Ces documents se déclinent comme suit :
    - Les fiches de constat (à retirer à l'ANSSI) dûment remplies qui comportent essentiellement :
        - Les constats des auditeurs ;
        - Les commentaires des audités relatifs au point précédent.
    - Une grille d'évaluation des niveaux de maturité par rapport aux objectifs de sécurité initialement définis doit être remplie (à retirer à l'ANSSI) ;
    - Les relevés techniques, à savoir :
        - Les fichiers contenant les résultats des scans de sécurité ;
        - Le rapport d'analyse des vulnérabilités ;
        - Les échantillons du trafic capturé.

- Les résultats des tests techniques d'audit sont composés principalement de :
  - La liste des vulnérabilités (réseaux, systèmes, applicatives, etc.) ;
  - La liste des anomalies de configuration des équipements (configuration des firewalls et des équipements réseaux).

- Les enregistrements de la phase d'exécution de l'audit doivent être évalués, analysés et consolidés par l'équipe d'audit. Cette consolidation est réalisée à travers les actions suivantes :
  - Présentation des constats fiables et pertinents, formulés clairement, de manière synthétique ;
  - Validation des conclusions d'audit ;
  - Préparation des recommandations ;
- Le PASSI est invité à rédiger un rapport de synthèse sur sa mission d'audit. Cette synthèse doit être révélatrice des défaillances constatées et des recommandations suggérées.

### 2.5. Élaboration du rapport et clôture d'audit

24) Le PASSI doit rédiger et assumer la responsabilité du rapport d'audit, lequel doit contenir les éléments exigés par le présent référentiel. Ce rapport est présenté à la direction de l'organisme audité lors de la réunion de clôture, afin d'en exposer les résultats et de répondre aux éventuelles questions.

25) Le PASSI est tenu d'assurer la confidentialité durant l'élaboration, la conservation et la transmission du rapport.

26) Le rapport d'audit doit être adapté en fonction du type d'audit réalisée par le PASSI.

27) Le PASSI doit informer l'audité que ce dernier doit transmettre le rapport d'audit à l'ANSSI.

28) Le PASSI doit préciser dans le rapport et rappeler à l'audité, son obligation de conservation du rapport pour une durée de trois (03) années.

29) Le rapport d'audit doit mentionner les noms et coordonnées des auditeurs, responsables de mission et du commanditaire de l'audit.

30) Le rapport d'audit doit être validé et signé par les deux parties, transmis par l'audité, par lettre recommandée avec accusé de réception à l'ANSSI, dans un

délai de dix (10) jours ouvrés à compter de la date de clôture de l'audit, et estampillé de la mention « Confidentiel ».

31) Le PASSI transmet le procès-verbal de la réunion de clôture et le rapport d'audit à l'ANSSI sous les mêmes conditions que l'audité.

### 2.5.1. Contenu du rapport d'audit

Le rapport d'audit doit comporter :

- Un résumé exécutif, à destination des dirigeants, qui présente :
  - La description de la démarche méthodologique utilisée ;
  - L'avis global sur le niveau de conformité observé à l'issue de l'audit (organisationnel, physique et/ou technique) ;
  - Le contexte et le périmètre de la prestation ;
  - Les points forts et faibles des mesures de sécurité observées ;
  - La synthèse des risques critiques identifiés et des recommandations prioritaires à mettre en œuvre immédiatement ;
  - La synthèse des vulnérabilités détectées, classées selon un niveau de sévérité, en fonction de leur impact sur la sécurité du système d'information et de leur difficulté d'exploitation.
- Un tableau synthétique des résultats d'audit, qui présente :
  - La synthèse des conformités et non-conformités relevées ;
  - La grille d'évaluation des niveaux de maturité par domaine.
- Une analyse détaillée des constats qui présente pour chaque domaine :
  - Le niveau de conformité observé (conformité, conformité partielle, non-conformité) ;
  - Les risques identifiés, leur impact, leur facilité d'exploitation et leur criticité ;
  - Les recommandations associées, accompagnées de la complexité et de la priorité de remédiation.
- Lorsque des tests d'intrusion sont réalisés, le rapport doit présenter :
  - La méthodologie employée pour l'identification et, le cas échéant, pour l'exploitation des vulnérabilités ;

- Les résultats détaillés des analyses de tests d'intrusion et de vulnérabilités.

- Une conclusion récapitulative pouvant inclure les axes de collaboration futurs.
- Les annexes, comprenant notamment :
  - Le planning des entretiens et des tests d'intrusion ;
  - La liste des documents reçus ;
  - Les différentes prises de vues accompagnant les constats ;
  - La liste des acronymes.

**Les livrables de cette phase :**

- Le rapport d'audit de sécurité comprenant notamment :
  - Un résumé exécutif ;
  - La description méthodologique ;
  - Des tableaux synthétiques de résultats ;
  - Le détail de l'analyse par constat et/ou les résultats des tests d'intrusion.
- Le procès-verbal de la réunion de clôture, signé par les parties prenantes, attestant de la présentation et de la validation des résultats.

### 2.6. Certification

32) Sur la base des conclusions de l'audit et en cas de conformité ou de non-conformité mineure, le PASSI formule une recommandation de certificat de sécurité sous réserve de validation de l'ANSSI.

33) La recommandation de certification ne peut être émise que sur la base de preuves objectives suffisantes attestant que le système de sécurité de l'information de l'audité est conforme aux exigences applicables du RGSSI, et que les dispositifs de revue de direction et d'audit interne sont établis, opérationnels, efficaces et durablement maintenus.

**Retrouvez nous sur notre site et nos différents canaux digitaux:**

**www.anssi.gouv.ci**

ANSSI
AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION
CÔTE D'IVOIRE

PLCC
Plateforme de Lutte Contre la Cybercriminalité
ANSSI CÔTE D'IVOIRE

UPINP
UNITÉ DE PROTECTION DES INFRASTRUCTURES NUMÉRIQUES PRIVILÉGIÉES
CÔTE D'IVOIRE

CI-CERT
COMPUTER EMERGENCY RESPONSE TEAM
ANSSI CÔTE D'IVOIRE

CÔTE D'IVOIRE TRAFIC

ALERTES 100