AYI NEDJIMI Consultants

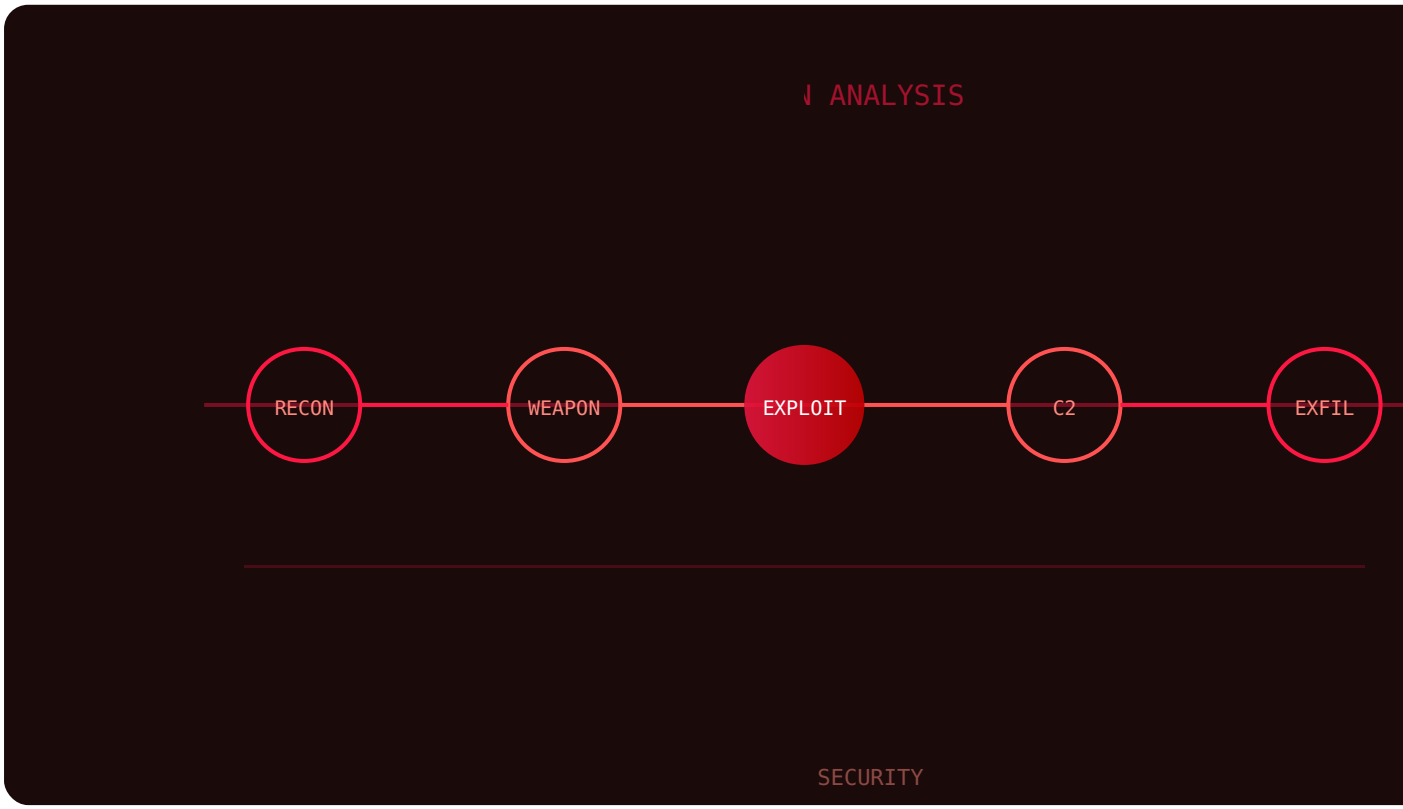
Qualification PASSI ANSSI : Devenir Prestataire d'Audit

Catégorie : Conformité Lecture : 14 min Publié le : 08/03/2026 Auteur : Ayi NEDJIMI

Guide complet qualification PASSI ANSSI : référentiel, 5 portées d'audit, processus de qualification, exigences auditeurs, dossier de candidature.

Qualification PASSI ANSSI : Devenir Prestataire d'Audit constitue un enjeu majeur pour les professionnels de la sécurité informatique et les équipes techniques. Guide complet qualification PASSI ANSSI : référentiel, 5 portées d'audit, processus de qualification, exigences auditeurs, dossier de candidature. Ce guide détaillé sur passi qualification anssi prestataire audit propose une méthodologie structurée, des outils éprouvés et des recommandations opérationnelles directement applicables. L'objectif est de fournir aux praticiens — consultants, ingénieurs sécurité, administrateurs systèmes — les connaissances et les techniques nécessaires pour aborder ce sujet avec rigueur. Chaque section s'appuie sur des retours d'expérience terrain et intègre les évolutions les plus récentes du domaine. Les recommandations présentées sont adaptées aux environnements d'entreprise et tiennent compte des contraintes opérationnelles réelles.

1. Introduction : la qualification PASSI dans l'écosystème cyber français



Dans un marché de la cybersécurité en pleine expansion, la **qualification PASSI** (Prestataires d'Audit de la Sécurité des Systèmes d'Information) délivrée par l'**ANSSI** (Agence Nationale de la Sécurité des Systèmes d'Information) constitue le label de confiance le plus exigeant pour les prestataires d'audit de sécurité en France. Créée dans le cadre du **Référentiel Général de Sécurité (RGS)**, elle garantit aux commanditaires -- administrations, OIV (Opérateurs d'Importance Vitale) et grandes entreprises -- que le prestataire respecte des exigences strictes en termes de compétences, de méthodologie, de confidentialité et de qualité. Ce guide approfondi examine en detail les aspects fondamentaux et avances de Qualification PASSI ANSSI, en proposant une analyse structuree et documentee des enjeux actuels. Les professionnels y trouveront des recommandations concretes, des methodologies eprouvees et des retours d'experience terrain directement applicables en environnement de production.

Points cles :

- 1. Introduction : la qualification PASSI dans l'écosystème cyber français
- 2. Contexte réglementaire et positionnement de la qualification
- 3. Les 5 portées de la qualification PASSI
- 4. Processus de qualification : de la candidature à la décision
- 5. Exigences du référentiel PASSI

En 2026, la qualification PASSI prend une dimension nouvelle avec l'entrée en vigueur de la directive NIS 2. Les entités essentielles et importantes soumises à NIS 2 devront faire réaliser des audits de sécurité par des prestataires qualifiés. Le marché accessible aux prestataires PASSI s'élargit donc considérablement, au-delà du périmètre historique des OIV et des administrations. Parallèlement, le règlement DORA renforce les exigences d'audit pour le secteur financier, créant une demande supplémentaire en prestations qualifiées. Pour plus d'informations, consultez les ressources de ANSSI.

Obtenir la qualification PASSI est un projet structurant pour un cabinet de conseil ou une ESN. Le processus est exigeant -- il faut compter 12 à 24 mois de préparation, un investissement significatif en ressources humaines et un engagement fort de la direction. Mais le retour sur investissement est substantiel : accès aux marchés publics à exigence PASSI, crédibilité renforcée, différenciation concurrentielle et accès aux missions les plus sensibles. Pour plus d'informations, consultez les ressources de MITRE ATT&CK.

Ce guide détaille l'ensemble du processus : référentiel PASSI, les 5 portées d'audit, les exigences techniques et organisationnelles, le dossier de candidature, l'audit de qualification, le maintien de la qualification et les qualifications complémentaires (PRIS, PDIS). Il intègre des retours d'expérience concrets pour aider les prestataires à préparer efficacement leur démarche.

Point clé : La qualification PASSI n'est pas une certification ISO. C'est une reconnaissance étatique délivrée par l'ANSSI après un audit approfondi des compétences et des processus du prestataire. Elle engage la responsabilité de l'agence et offre un niveau de confiance supérieur.

Prérequis de cet article

Cet article s'adresse aux dirigeants de cabinets de cybersécurité, aux responsables qualité et aux auditeurs souhaitant comprendre ou préparer la qualification PASSI. Pour les aspects techniques des audits, consultez nos articles sur l'exploitation Kerberos Active Directory et les techniques d'escalade de privilèges Linux.

Notre avis d'expert

L'audit de conformité n'est utile que s'il débouche sur des actions correctives concrètes et mesurables. Nos missions d'accompagnement privilégient l'approche par les risques plutôt que la conformité checkbox, ce qui garantit une amélioration réelle de la posture de sécurité.

2. Contexte réglementaire et positionnement de la qualification

2.1 Le Référentiel Général de Sécurité (RGS)

Le **RGS**, institué par l'ordonnance n° 2005-1516 du 8 décembre 2005, définit les règles de sécurité que doivent respecter les systèmes d'information des autorités administratives. Son décret d'application (n° 2010-112 du 2 février 2010) prévoit la qualification des produits et prestataires de services de confiance. C'est dans ce cadre que l'ANSSI a créé la qualification PASSI.

Le RGS impose aux administrations de recourir à des prestataires qualifiés pour certaines prestations de sécurité. Cette obligation a été étendue aux **OIV** par la Loi de Programmation Militaire (LPM) de 2013, qui impose aux opérateurs d'importance vitale de faire auditer leurs SIIV (Systèmes d'Information d'Importance Vitale) par des prestataires PASSI qualifiés.

2.2 L'ANSSI : autorité de qualification

L'ANSSI agit en tant qu'**autorité nationale de qualification** pour les prestataires de services de sécurité. À ce titre, elle :

- Définit les référentiels de qualification (PASSI, PRIS, PDIS, SecNumCloud)
- Évalue les dossiers de candidature des prestataires
- Missionne un **organisme d'évaluation** (COFRAC ou accrédité) pour réaliser l'audit de qualification
- Prononce la décision de qualification (ou de refus)
- Réalise des audits de surveillance pendant la durée de la qualification
- Publie la liste des prestataires qualifiés sur son site officiel

En mars 2026, l'ANSSI recense environ **55 prestataires PASSI qualifiés** en France, un chiffre relativement stable qui témoigne du niveau d'exigence de la qualification. Parmi eux figurent des acteurs majeurs du marché (Wavestone, Orange Cyberdefense, Thales, Capgemini) mais aussi des structures plus petites et spécialisées.

2.3 Impact de NIS 2 sur la demande de prestations PASSI

La transposition de la directive NIS 2 en droit français élargit considérablement le périmètre des entités soumises à des obligations de cybersécurité. Alors que NIS 1 concernait environ 300 opérateurs en France, NIS 2 s'applique à plus de **15 000 entités** (essentielles et importantes). Nombre d'entre elles devront faire réaliser des audits de sécurité, créant une demande croissante en prestataires qualifiés.

Comment démontrez-vous l'accountability exigée par le RGPD en cas de contrôle ?

3. Les 5 portées de la qualification PASSI

Le référentiel PASSI définit **5 portées d'audit** distinctes. Un prestataire peut candidater pour une ou plusieurs portées. Chaque portée correspond à un type d'audit spécifique, avec des compétences et des méthodologies associées :

3.1 Portée 1 : Audit organisationnel et physique

L'audit organisationnel évalue la gouvernance de la sécurité, les politiques, les processus et la conformité aux référentiels (ISO 27001, RGPD, réglementations sectorielles). Il couvre la gestion des risques, la classification des données, la gestion des accès, la sensibilisation des collaborateurs, la sécurité physique des locaux et les plans de continuité d'activité (PRA/PCA). Les auditeurs doivent posséder une expertise en gouvernance de la sécurité et maîtriser les référentiels normatifs.

3.2 Portée 2 : Audit d'architecture

L'audit d'architecture examine la conception des systèmes d'information : segmentation réseau, topologie, mécanismes de filtrage, chiffrement des flux, architecture de l'annuaire Active Directory, infrastructure cloud, gestion des certificats et PKI. L'auditeur doit être capable d'identifier les faiblesses architecturales qui pourraient être exploitées par un attaquant, même en l'absence de vulnérabilité technique spécifique.

3.3 Portée 3 : Audit de configuration

L'audit de configuration vérifie les paramètres de sécurité des composants du SI : systèmes d'exploitation, serveurs web, bases de données, équipements réseau, firewalls, solutions de virtualisation. Il s'appuie sur des référentiels de durcissement (CIS Benchmarks, guides ANSSI) et identifie les écarts de configuration susceptibles d'être exploités. Pour les environnements VMware ESXi ou Microsoft 365, des référentiels spécifiques s'appliquent.

3.4 Portée 4 : Audit de code source

L'audit de code source combine analyse statique (SAST), revue manuelle du code et identification des vulnérabilités applicatives. Les auditeurs recherchent les injections SQL, les failles XSS, les problèmes de gestion de sessions, les défauts cryptographiques, les vulnérabilités de désérialisation et les configurations dangereuses. La maîtrise de plusieurs langages de programmation et des frameworks de développement sécurisé (OWASP, ISO 27034) est indispensable.

3.5 Portée 5 : Test d'intrusion (pentest)

Le test d'intrusion est la portée la plus demandée. Il consiste à simuler des attaques réelles pour identifier les vulnérabilités exploitables et évaluer l'impact potentiel d'une compromission. Les pentesters qualifiés PASSI doivent maîtriser un large spectre de techniques : escalade de privilèges Windows, exploitation d'Active Directory, attaques réseau, tests d'applications web, ingénierie sociale, et être capables de documenter leurs constats de manière claire et exploitable.

Cas concret
L'entrée en vigueur de NIS2 en octobre 2024 a élargi le périmètre des organisations soumises à des obligations de cybersécurité en Europe. Les secteurs essentiels et importants doivent désormais notifier les incidents significatifs dans les 24 heures et maintenir des mesures de gestion des risques proportionnées.

4. Processus de qualification : de la candidature à la décision

4.1 Vue d'ensemble du processus

Le processus de qualification PASSI se décompose en 7 grandes étapes, sur une durée totale de 12 à 24 mois :

4.2 Le dossier de candidature

Le dossier de candidature PASSI comprend les éléments suivants :

- **Formulaire de candidature ANSSI** : identification du prestataire, portées demandées, périmètre géographique
- **Descriptif de l'organisation** : organigramme, processus qualité, SMSI (Système de Management de la Sécurité de l'Information)
- **CV détaillés des auditeurs** : formation, certifications (OSCP, CEH, GPEN, CISSP, ISO 27001 Lead Auditor...), expérience en audit de sécurité
- **Rapports d'audit exemples** : au minimum 2 rapports anonymisés par portée demandée, démontrant la qualité méthodologique et rédactionnelle
- **Méthodologies d'audit** : description détaillée des méthodologies appliquées pour chaque portée
- **Politique de confidentialité** : procédures de gestion des données sensibles, chiffrement, destruction des données d'audit
- **Assurance RC Professionnelle** : attestation d'assurance couvrant les risques liés aux prestations d'audit
- **Engagement de veille sécuritaire** : processus de veille sur les vulnérabilités et les techniques d'attaque

4.3 L'audit de qualification

L'audit de qualification est réalisé par un **organisme d'évaluation** mandaté par l'ANSSI. Il se déroule sur 2 à 4 semaines et comprend :

- **Revue documentaire** : vérification de la conformité des procédures, méthodologies et livrables au référentiel PASSI
- **Entretiens individuels avec les auditeurs** : évaluation des compétences techniques par des mises en situation et des questions techniques approfondies

- **Observation de missions** : l'évaluateur peut observer une mission d'audit en cours pour vérifier l'application effective des méthodologies déclarées
- **Vérification des environnements techniques** : contrôle des outils d'audit, du laboratoire, des postes de travail sécurisés
- **Audit des processus de gestion** : gestion de projet, communication avec le client, gestion des constats, suivi qualité

Point d'attention : les entretiens techniques
Les entretiens individuels avec les auditeurs sont le point le plus critique de l'audit de qualification. Les évaluateurs posent des questions techniques pointues, spécifiques à chaque portée. Un pentester sera interrogé sur des scénarios d'attaque concrets, les outils utilisés, les méthodologies de contournement des défenses. La préparation de ces entretiens est essentielle.

5. Exigences du référentiel PASSI

5.1 Exigences relatives aux compétences des auditeurs

Le référentiel PASSI impose des exigences strictes sur les compétences des auditeurs :

Critère	Exigence PASSI
Expérience minimale	2 ans d'expérience en audit de sécurité (5 ans recommandés pour les portées pentest et code)
Formation continue	Plan de formation annuel documenté, incluant veille technique et certifications
Habilitation	Capacité à obtenir une habilitation Secret Défense (nationalité française ou EU selon missions)
Certifications	Fortement recommandées : OSCP, GPEN, CEH, CISSP, CISA, ISO 27001 LA (selon portée)
Casier judiciaire	Extrait de casier judiciaire vierge (bulletin n°3)
Effectif minimum	Au moins 2 auditeurs qualifiés par portée pour assurer la continuité de service

5.2 Exigences organisationnelles et processus qualité

Le prestataire PASSI doit démontrer la mise en place d'un **Système de Management de la Sécurité de l'Information (SMSI)** couvrant l'ensemble de ses activités d'audit. Ce SMSI peut s'appuyer sur l'ISO 27001, bien que la certification ISO 27001 ne soit pas formellement exigée. Les éléments attendus incluent :

- **Politique de sécurité** : document approuvé par la direction, révisé annuellement
- **Analyse de risques** : identification et traitement des risques liés aux activités d'audit
- **Gestion de la confidentialité** : chiffrement des données d'audit, clause de confidentialité, destruction sécurisée des données

- **Processus de gestion de projet** : planification, exécution, contrôle qualité et clôture des missions d'audit
- **Revue par les pairs** : chaque rapport d'audit doit être relu par un auditeur n'ayant pas participé à la mission
- **Gestion des incidents** : procédure en cas de découverte d'une vulnérabilité critique en cours d'audit
- **Veille sécuritaire** : processus formalisé de veille sur les vulnérabilités, les techniques d'attaque et les évolutions réglementaires

5.3 Exigences techniques : laboratoire et outils

Le prestataire doit disposer d'un **environnement technique sécurisé** pour la réalisation des audits :

- **Postes d'audit durcis** : chiffrement intégral du disque, authentification forte, pas de données résiduelles entre missions
- **Laboratoire de test** : environnement isolé pour les tests d'exploitation, la validation des vulnérabilités et le développement d'exploits
- **Outils d'audit référencés** : inventaire des outils utilisés, vérification de l'intégrité, mises à jour régulières
- **Infrastructure de communication sécurisée** : échange des rapports et données d'audit par canaux chiffrés
- **Gestion du cycle de vie des données** : procédure d'effacement sécurisé des données d'audit en fin de mission (ou selon la durée de conservation convenue)

Votre conformité ISO 27001 se traduit-elle par une amélioration réelle de votre sécurité ?

6. Maintien et renouvellement de la qualification

6.1 Durée et cycle de la qualification

La qualification PASSI est délivrée pour une durée de **3 ans**. Pendant cette période, le prestataire doit :

- Se soumettre à des **audits de surveillance annuels** par l'organisme d'évaluation
- Notifier l'ANSSI de tout changement significatif (départ d'un auditeur qualifié, changement d'organisation, incident de sécurité)
- Maintenir les compétences de ses auditeurs à jour (formations, certifications, veille)
- Documenter et analyser les retours clients sur les prestations réalisées
- Maintenir son SMSI opérationnel et effectuer les revues de direction annuelles

Le **renouvellement** de la qualification nécessite un nouvel audit de qualification complet, à initier au moins 6 mois avant l'expiration. Le processus est similaire à la qualification initiale, mais tient compte du retour d'expérience accumulé.

6.2 Causes de retrait ou suspension de la qualification

L'ANSSI peut suspendre ou retirer la qualification en cas de :

- Non-conformité majeure constatée lors d'un audit de surveillance
- Incident de sécurité grave impliquant les données d'un commanditaire
- Perte de compétences (départ massif d'auditeurs qualifiés sans remplacement)
- Manquement grave à la déontologie ou à la confidentialité
- Non-notification d'un changement significatif à l'ANSSI

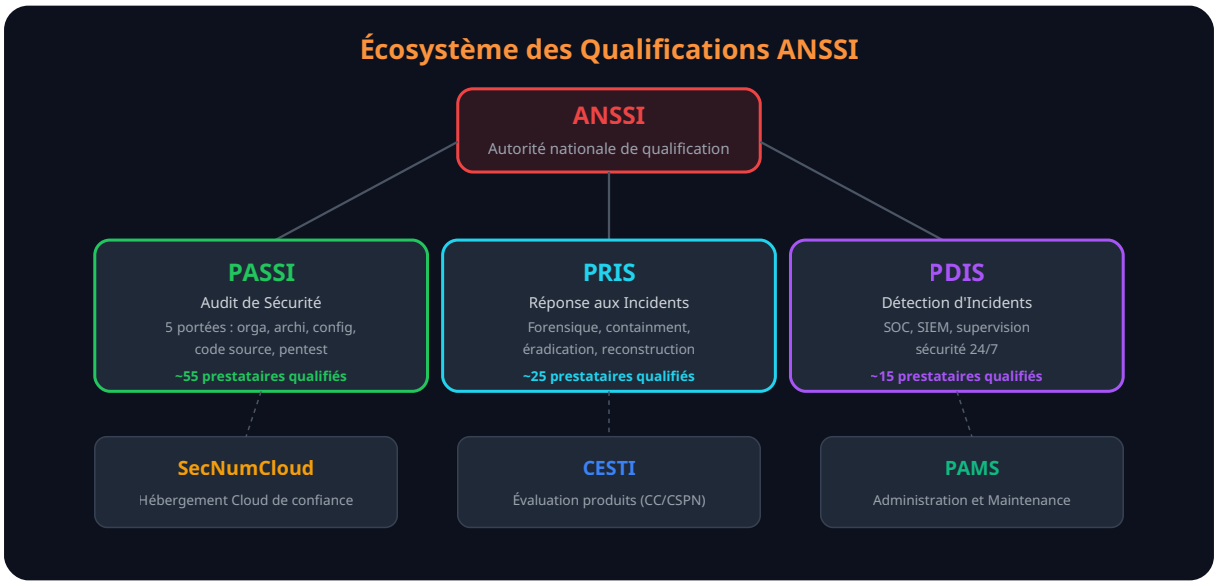
7. Qualifications complémentaires : PRIS et PDIS

7.1 PRIS : Prestataires de Réponse aux Incidents de Sécurité

La qualification **PRIS** concerne les prestataires de réponse aux incidents et de forensique numérique. Elle est complémentaire à la PASSI et couvre la détection, l'analyse, le confinement et l'éradication des incidents de sécurité. Les prestataires PRIS sont mobilisés lors de compromissions avérées, notamment par les OIV et les administrations.

7.2 PDIS : Prestataires de Détection des Incidents de Sécurité

La qualification **PDIS** s'adresse aux prestataires opérant des services de détection (SOC, SIEM, NDR). Elle garantit que le prestataire dispose des compétences et des processus nécessaires pour détecter les incidents de sécurité dans les systèmes de ses clients. PDIS et PASSI sont souvent détenues par les mêmes acteurs, offrant une couverture complète du cycle audit/détection/réponse.



8. Le marché de l'audit qualifié en France

8.1 État des lieux du marché PASSI

Le marché de l'audit de sécurité qualifié PASSI en France connaît une croissance soutenue, portée par les exigences réglementaires croissantes et la prise de conscience des risques cyber :

- **Volume de marché :** estimé à 450-600 millions d'euros en 2026 pour les prestations d'audit qualifié (audit OIV, administrations, NIS 2)
- **Croissance :** +15 à 20 % par an, tirée par NIS 2 et DORA
- **Tension sur les compétences :** pénurie de pentesters et auditeurs qualifiés, avec des taux journaliers en hausse
- **Concentration :** les 10 premiers prestataires PASSI captent environ 70 % du marché, mais les acteurs spécialisés se positionnent sur des niches à forte valeur ajoutée

8.2 Positionnement stratégique pour un prestataire

Pour un cabinet de cybersécurité, la qualification PASSI ouvre l'accès à des marchés significatifs :

- **Marchés publics :** de nombreux marchés d'audit exigent la qualification PASSI comme critère d'éligibilité
- **OIV et SIIV :** les audits des systèmes d'importance vitale ne peuvent être réalisés que par des prestataires PASSI
- **Entités NIS 2 :** les entités essentielles privilégient de plus en plus les prestataires qualifiés
- **Secteur financier (DORA) :** les tests TLPT exigent des compétences de niveau PASSI
- **Crédibilité :** la qualification PASSI est un argument commercial majeur, y compris pour les clients du secteur privé non réglementé

Conseil stratégique : commencer par les portées les plus accessibles
Si votre cabinet débute dans la qualification PASSI, il est recommandé de commencer par les portées **audit de configuration** et **test d'intrusion**, qui sont les plus demandées et pour lesquelles il est plus facile de démontrer des compétences établies. Les portées **audit organisationnel** et **audit d'architecture** peuvent être ajoutées dans un second temps lors d'une extension de périmètre.

9. Retour d'expérience : les clés du succès

9.1 Les erreurs fréquentes à éviter

Sur la base de notre expérience et des retours de prestataires qualifiés, voici les erreurs les plus fréquentes :

- **Sous-estimer la charge de préparation :** la qualification PASSI n'est pas un simple exercice documentaire. Il faut 12 à 24 mois de préparation sérieuse, avec un investissement significatif en temps et en ressources.

- **Négliger les rapports exemples :** les rapports d'audit fournis dans le dossier sont scrutés par les évaluateurs. Ils doivent être d'une qualité irréprochable : méthodologie rigoureuse, classification des constats, recommandations concrètes et priorisées.
- **Miser sur un auditeur unique par portée :** le référentiel exige une continuité de service. Si votre unique auditeur qualifié quitte l'entreprise, la qualification est en péril. Prévoyez au moins 2 auditeurs par portée.
- **Négliger la sécurité interne :** le prestataire PASSI doit montrer l'exemple en matière de sécurité. Un SMSI insuffisant ou des pratiques de sécurité internes faibles sont rédhibitoires.
- **Ignorer la dimension commerciale :** obtenir la qualification est une chose, la rentabiliser en est une autre. Préparez votre stratégie commerciale en amont (réponses aux marchés publics, partenariats, communication).

9.2 Les facteurs clés de succès

- **Engagement de la direction :** la qualification PASSI est un projet d'entreprise qui nécessite un soutien fort de la direction (budget, temps, priorité).
- **Qualité des auditeurs :** investissez dans la formation et la certification de vos auditeurs. Les compétences techniques sont le premier critère d'évaluation.
- **Rigueur méthodologique :** documentez tout, formalisez vos processus, appliquez-les systématiquement. La cohérence entre ce qui est décrit et ce qui est fait est vérifiée.
- **Capitalisation :** chaque mission d'audit doit alimenter votre base de connaissances, améliorer vos méthodologies et enrichir votre outillage.
- **Anticipation du renouvellement :** dès la qualification obtenue, planifiez le maintien (audits de surveillance, formation continue, amélioration continue du SMSI).

Pour approfondir ce sujet, consultez notre outil open-source iso27001-toolkit qui facilite l'accompagnement à la certification ISO 27001.

10. Checklist de préparation PASSI : les 25 points essentiels

Utilisez cette checklist pour évaluer votre niveau de préparation à la qualification PASSI :

Organisation et gouvernance

- Un responsable de projet qualification est nommé et dispose du temps nécessaire
- La direction a validé le budget et le planning de qualification
- Un SMSI est en place et opérationnel (politique, analyse de risques, procédures)
- Les processus de gestion de projet d'audit sont documentés et appliqués
- Un processus de revue par les pairs est systématiquement appliqué aux rapports

Compétences et ressources humaines

- Au moins 2 auditeurs qualifiés sont identifiés par portée demandée
- Les CV des auditeurs sont à jour (formations, certifications, expérience)
- Un plan de formation annuel est défini et budgété
- Les auditeurs disposent des certifications recommandées (OSCP, GPEN, CISSP, etc.)
- Un processus de veille technique est en place (CVE, advisories, techniques d'attaque)

Méthodologies et livrables

- Les méthodologies d'audit sont documentées pour chaque portée demandée
- Au moins 2 rapports d'audit exemples de qualité sont disponibles par portée
- Les rapports suivent un format structuré (contexte, méthodologie, constats, recommandations)
- La classification des constats est formalisée (criticité, impact, exploitabilité)
- Les recommandations sont concrètes, priorisées et adaptées au contexte du commanditaire

Sécurité et confidentialité

- Les postes d'audit sont durcis et chiffrés
- Un laboratoire de test isolé est disponible
- Les données d'audit sont chiffrées en transit et au repos
- Un processus de destruction sécurisée des données est en place
- Les engagements de confidentialité sont signés par tous les auditeurs

Aspects administratifs

- L'assurance RC Pro est souscrite et couvre les risques liés aux audits
- Les extraits de casier judiciaire des auditeurs sont à jour
- La capacité d'habilitation Secret Défense est vérifiée pour les auditeurs
- Le formulaire de candidature ANSSI est complété
- Le planning de préparation à l'audit de qualification est établi

Sources et références : CNIL · ANSSI

Questions frequentes

Comment mettre en place Qualification PASSI ANSSI dans un environnement de production ?

La mise en place de Qualification PASSI ANSSI en production necessite une planification rigoureuse, incluant l'evaluation des prerequis techniques, la definition d'une architecture cible, des tests de validation approfondis et un plan de deploiement progressif avec des points de controle a chaque etape.

Pourquoi Qualification PASSI ANSSI est-il essentiel pour la securite des systemes d'information ?

Qualification PASSI ANSSI constitue un element fondamental de la securite des systemes d'information car il permet de reduire significativement la surface d'attaque, d'ameliorer la detection des menaces et de renforcer la posture globale de securite de l'organisation face aux cybermenaces actuelles.

Quel est le délai réaliste pour se mettre en conformité avec Qualification PASSI ANSSI : Devenir Prestataire d'Audit ?

Comptez entre 6 et 18 mois selon la maturité de votre SI. Les entreprises qui partent de zéro doivent prévoir 12 mois minimum avec un accompagnement externe dédié.

Ayi NEDJIMI Consultants — Expert cybersécurité offensive & intelligence artificielle

ayinedjimi-consultants.fr · ayi@ayinedjimi-consultants.fr