Procédure de Planification, Mise en œuvre et Rapport des PASSI

Propriétés du document :

Version :	3.0
Niveau de confidentialité :	Protégé
Type de document :	Procédure
Approuvé par :	RST

Historique des versions :

Version	Date	Auteur	Changement
0.1	26/04/2017	JAL	Création
0.2	08/05/2017	JAL	Modification
1.0	11/05/2017	RST	Approbation
1.1	23/09/2017	JAL	Change organisation name
2.0	23/09/2017	PDE	Approval
2.1	05/05/2023	GCA	Mise à jour en fonction du règlement 8.0
3.0	15/05/2023	RST	Approbation

Table des matières

1. Sujet

Cette procédure définit les exigences à considérer pour le processus de certification relatif au programme spécifique aux Prestataires d'Audit de la Sécurité des Systèmes d'Information (ci-après « PASSI ») afin d'assurer que l'ensemble des tâches sont réalisées de manière complète, consistante et conforme aux exigences d'accréditation.

2. Périmètre

Cette procédure couvre les activités de planification, d'exécution et de formalisation des audits pour tout type d'audit relatif au programme PASSI, à savoir :

- Etude du dossier de candidature
- Évaluation du siège
- Examens écrits des auditeurs
- Examens oraux des auditeurs
- Évaluation terrain
- Évaluation de surveillance
- Évaluation de renouvellement

3. Définitions et acronymes

Les acronymes utilisés dans le présent document sont les suivants :

- **ANSSI** : Agence Nationale de Sécurité des Système d'Information
- **COFRAC** : Comité Français d'Accréditation
- **ICTS France** : International Certification Trust Services (ICTS) France sàrl
- **PASSI** : Prestataires d'Audit de la Sécurité des Systèmes d'Information
- **RGS** : Référentiel Général de Sécurité
- **SIDR** : Système d'Information de Diffusion Restreinte

4. Vente

4.1. Demande client

La demande de qualification est réalisée par le commanditaire de la qualification en envoyant le formulaire [TEM-44 Formulaire d'application PASSI] complété et signé par mail à sales.france@certi-trust.com

Les éléments à renseigner dans le formulaire sont notamment :

- Le périmètre de la qualification (lieux d'activités et portées d'audit pour lesquelles la qualification est recherchée).
- Des informations générales sur le prestataire candidat, telles que sa dénomination, l'adresse pour chacun des sites considérés dans le périmètre, le contact principal du prestataire candidat, les lois et règlementations applicables.
- Le nombre d'auditeurs candidats pour chaque activité d'audit ainsi que leur rôle (auditeur principal ou auditeur).
- Des informations sur les processus externalisés par l'organisation qui peuvent impacter la conformité aux exigences applicables (par exemple, hébergement externalisé du SI).
- Description générale du système d'information de diffusion restreinte (classe de réseau, ressources techniques, technologie utilisée, etc.).

- Les dates potentielles auxquelles le prestataire candidat souhaiterait être évalué lors des premières étapes (dont la date prévue pour la soumission des documents exigés en vue de l'étude du dossier de candidature ainsi qu'une date souhaitée pour l'évaluation du siège).

Si le prestataire inclus des documents complémentaires à sa demande tel qu'un dossier d'architecture technique (DAT), l'échange des informations doit se faire par une solution qualifiée au niveau de diffusion restreinte.

Certi-Trust accusera réception de la demande de qualification et évaluera le dossier de candidature sous quatre semaines au maximum. Certi-Trust se réserve le droit de ne pas donner suite à une demande de qualification et expliquera sa décision par écrit (par exemple : n'a pas la capacité à répondre à la demande dans un délai raisonnable, conflit d'intérêt, n'a pas les compétences particulières, etc.).

Un prestataire peut demander une qualification pour tout ou partie des activités d'audit. Toutefois, conformément à [PASSI], il ne peut pas demander la qualification pour l'activité de tests d'intrusion seule ou pour l'activité d'audit organisationnel et physique seule.

Un prestataire d'audit peut demander une qualification d'un service d'audit de la sécurité des systèmes d'information interne, c'est-à-dire un service utilisé pour répondre à tout ou partie de ses propres besoins en audit de la sécurité des systèmes d'information. Dans ce cas, le processus de qualification ainsi que les exigences applicables pour obtenir la qualification sont strictement identiques à ceux définis dans le présent règlement avec les adaptations nécessaires (ex : la convention de service n'implique pas nécessairement la refacturation de la prestation mais elle doit inclure les autres éléments tel que décrire le périmètre de l'audit, la liste des intervenants, les clauses relatives à l'éthique, etc.).

En déposant une demande d'application, le prestataire consent que l'ANSSI puisse être informée par Certi-Trust de toute demande de qualification PASSI et des activités d'évaluation.

Il est à noter qu'une demande de qualification PASSI LPM doit être adressée à l'ANSSI. Certi-Trust n'est pas habilité pour traiter une telle demande.

4.2. Préparation et envoi de l'offre

La candidature est étudiée afin de s'assurer que l'ensemble des informations nécessaires ont été renseignées et qu'aucune ambiguïté n'existe. Certi-Trust peut proposer ou demander à formuler des modifications de la demande, si des incohérences sont identifiées. En cas de doute, des informations complémentaires peuvent être demandées au prestataire candidat.

Dans le cas où Certi-Trust n'est pas en mesure de répondre à la demande, une réponse écrite est formulée pour en indiquer les raisons.

Dans le cas où Certi-Trust est en mesure de répondre à la demande, une durée d'évaluation ainsi que les modalités sont déterminées afin de réaliser une proposition commerciale. Afin de préserver l'impartialité et les négociations commerciales sur la durée et/ou la nature des activités d'évaluation, la durée et les modalités de l'évaluation sont déterminées par le responsable de programme et non par un commercial de Certi-Trust.

4.3. Détermination du temps d'évaluation

La matrice ci-dessous précise le temps d'évaluation standard pour les différentes étapes de l'évaluation. Les spécificités pour les différentes activités d'audit sont également précisées.

Les temps d'évaluation définis ci-dessous correspondent au temps passé à distance ou sur le site. Le temps prévu pour la planification, la préparation et l'interface avec le prestataire candidat est inclus. En revanche, le temps nécessaire pour les voyages et le personnel qui n'est pas impliqué dans les activités d'audit ne sont pas inclus.

La matrice est à considérer comme une base de référence, mais qui peut être ajustée en fonction des spécificités du prestataire et du périmètre de l'évaluation.

Tout diminution ou augmentation sur le nombre de jours d'évaluation doit être décidé par le responsable du programme d'évaluation désigné et justifié notamment par les modalités définies ci-dessous. Dans tous les cas, la réduction ne peut excéder 30% du temps d'évaluation standard défini.

Les modalités définies ci-dessous ne couvrent pas l'ensemble des situations et le responsable du programme d'évaluation peut diminuer ou augmenter le temps d'évaluation suivant d'autres critères. Dans tous les cas, toute modification doit être formalisée dans le formulaire de revue de l'application.

Matrice de temps d'évaluation

La charge de travail (sous la forme « évaluateur par jour ») des évaluations de qualification du prestataire candidat est définie par Certi-Trust, conformément aux exigences [QUAL_SERV_PORTEES], en fonction :

- Du nombre d'auditeurs candidats,
- De la portée de la qualification (différentes activités d'audit demandées),
- Du nombre de sites concernés,
- De la classe de réseau du SIDR,
- De critères additionnels (intégration avec d'autres normes, complexité du système d'information, etc.).

Une proposition commerciale est formulée qui contient la charge de l'évaluation initiale (ou de renouvellement) et de surveillance à 18 mois, sur un cycle de 3 ans. Le renouvellement de l'offre n'est pas tacite après 3 ans. Une nouvelle proposition commerciale doit être reformulée et envoyée par Certi-Trust au prestataire candidat pour signature et validation avant renouvellement du cycle de qualification.

Cette charge peut évoluer tout au long du cycle de qualification en fonction des demandes d'extension ou de réduction de la qualification qui sont formulées.

La durée de chaque activité d'évaluation est indiquée et justifiée dans l'offre commerciale transmise ainsi que le prix facturé pour chacune des activités reliées à la qualification de l'organisme prestataire :

- Étude de recevabilité
- Évaluation siège (revue documentaire)
- Évaluation siège (évaluation sur site)
- Évaluation de prestations témoins

- Évaluation de compétences

Les activités pour une évaluation initiale devraient être de 12 à 14 jours/homme dont 4 à 5 jours/homme d'activité sur site et 4 à 5 jours/homme d'activité de revue documentaire en conformité avec [QUAL_SERV_PORTEES]. L'évaluation de surveillance devrait être d'environ 1/3 de la charge initiale et 2/3 dans le cadre d'une évaluation de renouvellement. En cas de demandes supplémentaires d'activité à sa portée et/ou de sites dans le périmètre de qualification, une demande formelle doit être adressée à Certi-Trust. Une nouvelle offre est alors émise. Il en va de même en cas de changements significatifs, en cours d'évaluation, du site où se déroule les activités du prestataire, du système d'information et/ou de la documentation.

Dans la proposition commerciale, la grille des tarifs applicables aux activités d'évaluation des compétences des auditeurs sont indiquées. Une formule de calcul pour adapter les tarifs peut être inclus pour tenir compte de l'inflation et d'autres facteurs définis avec le prestataire.

L'inscription des auditeurs candidats aux examens écrits et aux examens oraux peuvent faire l'objet d'une demande séparée à Certi-Trust par l'organisme candidat. Une facture est émise par la suite. À la demande du prestataire, un devis peut être émis en amont ou intégrée avec la proposition commerciale.

L'acceptation définitive par Certi-Trust de la demande de qualification est ensuite notifiée au commanditaire lorsqu'un engagement contractuel est conclu et signé entre Certi-Trust et le commanditaire de la qualification

Le temps d'évaluation pourra être revu à la baisse suivant les critères suivants :

- 0,5 jour :
  - Connaissance préalable du prestataire candidat (déjà enregistré pour un autre standard d'audit avec un périmètre contenant les activités de prestataire PASSI du prestataire)
  - Evaluation antérieure du prestataire candidat (déjà enregistré comme PASSI auparavant auprès d'un autre prestataire de certification)
  - Maturité et simplicité du système de management en place (nombre d'auditeurs et de programmes)
- A définir :
  - Intégration de l'évaluation avec une autre norme compatible

Le temps d'évaluation pourra être revu à la hausse suivant les critères suivants :

- 0,5 jour :
  - L'usage d'une autre langue dans le périmètre PASSI en plus du français (langue d'usage obligatoire). Les langues devant être employées durant l'évaluation nécessitent l'intervention d'un interprète ou l'auditeur ne peut pas travailler de manière indépendante ou la documentation est fournie dans plusieurs langues différentes
- A définir :
  - Complexité des méthodes, outils et techniques utilisés dans le cadre des procédures d'exploitation en fonction des activités d'audit incluses dans le périmètre (exemple : activité d'audit de code source est présumée plus complexe à évaluer)
  - Complexité du système de management (situation de risque du système de management, criticité des informations, etc.)
  - Complexité et variété des technologies utilisées au sein du système d'information
  - Variété des processus externalisés
  - Performance auparavant démontrée par le système de management

- Les extensions ou changements demandés sur le périmètre de certification dans le cas des évaluations de surveillance et de renouvellement

Examens écrits

Le temps estimé est à considérer comme le temps maximum pour chaque candidat.

Activité d'audit	Temps estimé pour l'examen
Audit d'architecture	40 minutes
Audit de configuration	40 minutes
Audit de code source	40 minutes
Tests d'intrusion	40 minutes
Audit organisationnel et physique	40 minutes
Principes et méthodologies d'audit	30 minutes

Examens oraux

Le temps estimé est à considérer comme le temps maximum pour chaque candidat est de 30 minutes plus 10 minutes par portée.

4.4. Multi-sites

Eligibilité

Le système de management du prestataire candidat doit être géré de manière centralisée permettant d'avoir un contrôle de la documentation et des changements apportés au système de management ainsi que les activités d'audit interne.

Nombre de jours d'évaluation et échantillonnage

La définition du nombre de jours d'évaluation par site doit être consistent autant que possible avec la matrice ci-dessous :

Evaluation du siège initiale	Site principal + racine carrée du nombre de sites
Evaluation du siège de surveillance	Site principal + 0.6 x racine carrée du nombre de sites
Evaluation du siège de renouvellement	Site principal + 0.8 x racine carrée du nombre de sites

Cet échantillonnage pourra être revu à la hausse ou à la baisse suivant les facteurs suivants :

- Taille et nombre d'employés
- Variété des activités exercées sur les sites

4.5. Intégration de l'évaluation

Dans le cas d'une intégration de l'évaluation avec un autre audit de système de management (ISO 27001, ISO 9001, ISO 22301, etc.), le responsable du

programme d'audit ne peut procéder pas à une réduction du temps d'évaluation sur le PASSI.

4.6. Extension, réduction et changement du périmètre

Un nouveau formulaire d'application doit être complété par le prestataire et retourné à Certi-Trust dans le cas d'une extension, d'une réduction ou d'un changement dans le périmètre.

Une revue devra être réalisée afin d'évaluer le temps d'évaluation nécessaire pour une étude du dossier (si nécessaire) et une évaluation du siège.

Dans le cas d'un ajout d'une activité d'audit, l'évaluation terrain pourra être réalisée durant le cycle de qualification de 3 ans suivant le programme d'audit défini.

4.7. Transfert de qualification d'un prestataire

Le transfert de qualification d'un prestataire concerne un PASSI déjà qualifié par un autre centre d'évaluation, actuellement accrédité par le COFRAC et ainsi qu'habilité par l'ANSSI, qui souhaite à présent être qualifié chez Certi-Trust. Cette règle de transfert ne s'applique pas à un transfert d'un PASSI qui aurait été évalué sur un programme similaire hors de France.

Le commanditaire doit compléter un formulaire de candidature et le retourner à Certi-Trust. Les documents suivants doivent être inclus avec la demande de transfert :

- Formulaire d'application renseigné ;
- Lettre d'intention de transfert signée (modèle en annexe du présent règlement) ;
- Extrait KBis de moins de 3 mois ;
- Attestation de qualification PASSI en date ;
- Liste des auditeurs et copies de leurs attestations de compétence des auditeurs ;
- Rapports d'audit depuis le dernier cycle de qualification (i.e siège, complémentaire siège, témoin et surveillance) et les fiches de non-conformité associée.

Certi-Trust s'engage, dans un délai d'un mois calendaire, à :

- Réaliser le processus standard pour la préparation de l'offre.
- Vérifier que le périmètre de qualification du PASSI est bien celui mentionné dans le formulaire de candidature, ainsi que la liste des auditeurs qualifiés du prestataire.
- Valider que le PASSI a été qualifié par un centre d'évaluation actuellement accrédité par le COFRAC et ainsi qu'habilité par l'ANSSI.
- Vérifier que l'attestation de qualification est valide, n'est pas expirée et est sous toujours accréditation.
- Valider que le PASSI est enregistré auprès de l'ANSSI et que la date d'expiration de sa qualification est supérieure à 3 mois calendaires.
- Confirmer que Certi-Trust est compétent pour évaluer le PASSI suivant le périmètre de qualification défini.
- Vérifier par rapport au cycle de qualification l'état actuel du client.

- Définir le programme d'évaluation en conséquence.

Dans le cas d'un transfert qui surviendrait durant une démarche initiale de qualification, Certi-Trust peut reconnaître l'étude de recevabilité effectuée par un autre centre d'évaluation. L'évaluation sur site et/ou l'évaluation de prestations témoins peuvent être reconnues comme valides seulement si un rapport d'évaluation a été émis par un centre d'évaluation reconnu par l'ANSSI. Dans tous les cas, l'équipe d'évaluation de Certi-Trust doit alors effectuer une nouvelle revue documentaire. De la même manière, le délai de douze mois pour compléter l'évaluation sera basé sur la date de décision de recevabilité du prestataire.

À l'inverse, si un prestataire PASSI qualifié par Certi-Trust désire changer de centre d'évaluation, le personnel de Certi-Trust s'engage à collaborer avec le prestataire et le nouvel organisme de certification afin de procéder au transfert dans les meilleures conditions.

Concernant les auditeurs, le prestataire PASSI devra fournir pour ceux-ci les mêmes pièces que celles exigées pour l'évaluation de compétence et de savoir-faire, ainsi que l'attestation de compétence en vigueur. Si un auditeur a réussi que l'examen écrit chez un autre certificateur et désire le faire reconnaître, il doit fournir la preuve de réussite de cet examen avant d'être admis à passer un examen oral auprès de Certi-Trust.

5. Opérations

5.1. Sélection de l'équipe en charge de l'évaluation

Tous les membres de l'équipe d'évaluation doivent :

- Avoir été approuvés par l'ANSSI en tant qu'évaluateur technique ou responsable de mission d'évaluation ;
- Avoir une formation ou un diplôme professionnel équivalent à un niveau universitaire et au moins 5 ans d'expérience dans le domaine des technologies de l'information, dont 2 ans dans un rôle relatif à la sécurité de l'information ;
- Être ressortissant d'un des états membres de l'Union européenne ou, dans tous les autres cas, être résident français ;
- Être sensibilisé à la législation en vigueur sur le territoire français et applicable aux différentes missions d'évaluation ;
- Avoir une très bonne maitrise des pratiques et méthodologies d'audit décrites dans la norme ISO/CEI 19011 ainsi que du référentiel PASSI ;
- Se tenir à jour sur les compétences et connaissances nécessaires en matière de sécurité de l'information et d'audit à travers un développement professionnel continu ;
- Avoir un contrat avec Certi-Trust pour la réalisation des activités d'évaluation ;
- Avoir signé l'engagement d'impartialité et d'éthique de Certi-Trust ;
- Avoir signé l'engagement de confidentialité et de secret professionnel.

L'évaluation de qualification initiale est composée de 5 parties :

1. **Étude de recevabilité :** validation que le prestataire candidat répond à certains critères de base du programme et qu'il a transmis à Certi-Trust un dossier suffisamment complet afin d'autoriser le démarrage de l'évaluation.
2. **Évaluation siège (Revue documentaire) :** validation que le corpus documentaire du candidat PASSI, produit tout au long d'une prestation d'audit qualifié, répond aux exigences [PASSI] (contrat, législation, réglementation et impartialité, etc.) et que le candidat est prêt à l'évaluation sur site et éligible à l'évaluation de prestations témoins ;
3. **Évaluation siège (Évaluation sur site) :** vérification sur site de la mise en œuvre effective des procédures, instructions, modes opératoires, outils, etc. définis par le PASSI pour répondre aux exigences de la qualification.
4. **Évaluation de prestations témoins :** valider les niveaux de qualité et de sécurité effectivement atteints par le candidat PASSI lors d'une prestation d'audit réalisée en conditions réelles.
5. **Évaluation de compétence et savoir-faire des auditeurs** : Vérification des compétences des auditeurs candidats sur les portées d'audit auxquels ils candidatent.

5.2. Étude de recevabilité

L'objectif de l'étude de recevabilité est de vérifier si le prestataire a transmis un dossier suffisamment complet afin d'autoriser le démarrage de l'évaluation ainsi que de valider s'il répond à certains critères de base du programme PASSI. La liste des documents à fournir est incluse dans la trame d'évaluation de Certi-Trust (K-bis, convention-type, charte éthique, programme audit…). Celle-ci est fourni en même temps que l'offre commerciale et/ou à la demande.

Certi-Trust s'engage à réaliser, dans un délai de vingt (20) jours ouvrés au maximum, l'étude de recevabilité après réception du dossier et des documents demandés. Elle peut être réalisée sur le site du prestataire ou hors site. Dans le cas d'une exigence à réaliser cette étape sur site, le temps et les frais de déplacement seront facturés au prestataire. Le prestataire doit en préciser la demande lors de la négociation du contrat de qualification. L'étude de recevabilité peut être effectuée par du personnel interne à Certi-Trust, soit par un évaluateur PASSI. Une vérification du dossier sera effectuée. Dans le cas d'un dossier incomplet, une demande de complément d'information peut être exigée.

À l'issue de l'étude de recevabilité, Certi-Trust notifiera le candidat PASSI de son éligibilité à démarrer l'évaluation de sa qualification en faisant parvenir la lettre de décision de recevabilité. Certi-Trust se réserve le droit de notifier également l'ANSSI de la recevabilité du prestataire.

Dans le cas où Certi-Trust conclut que le dossier n'est pas éligible au démarrage de l'évaluation, une réponse écrite sera formulée pour en indiquer les raisons. Lors de l'étude de recevabilité, aucun écart documenté ne sera transmis au prestataire candidat.

5.3. Évaluation Siège (Revue documentaire)

L'objectif de cette première partie de l'évaluation siège est de vérifier que la documentation du candidat est conforme aux exigences [PASSI]. Cette étape doit être réalisée obligatoirement par l'équipe d'évaluateurs qui ont été assignés sur la mission d'évaluation du prestataire candidat.

L'équipe d'évaluateurs peut demander au prestataire de fournir d'autres documents que ceux indiqués dans la Trame d'évaluation de Certi-Trust en vigueur. Le prestataire devrait fournir l'ensemble de la documentation demandée, au moins, vingt jours ouvrés avant la date prévue de l'évaluation sur site ou de l'évaluation d'une prestation témoin. Sans respect de ce délai, le responsable d'évaluation déterminera si l'évaluation documentaire peut être réalisé dans les délais fixés. Sinon, les modalités d'interruption d'une activité en cours de processus de qualification seront appliquées (voir section 4.6 du présent règlement).

Selon les modalités d'accès à la documentation, les vérifications sont réalisées, soit :

- Sur le site du prestataire ;
- Sur le site du centre d'évaluation ;
- Ou une combinaison des deux.

Si le prestataire exige une consultation sur site des documents, des frais de déplacements supplémentaires pourront être facturés en supplément.

Certains documents peuvent contenir des données sensibles et doivent par conséquent être transmis avec des moyens permettant de garantir la confidentialité des informations. Ils doivent être transmis en les chiffrant avec un moyen convenu avec Certi-Trust.

Les documents de niveau Diffusion Restreinte ou supérieur transmis à Certi-Trust doivent être protégés en confidentialité au moyen d'un produit agréé par l'ANSSI au niveau adéquat et utilisé conformément aux conditions d'utilisation figurant dans la décision d'agrément du produit.

La revue documentaire doit être terminée, au plus tard, 10 jours ouvrés avant les dates planifiées de l'évaluation du siège sur site. Si certains points significatifs n'ont pas pu être évalués dans les délais, le responsable de la mission d'évaluation peut prendre la décision d'annuler l'évaluation sur site et proposé de nouvelles dates pour la suite de l'évaluation.
À l'issue de l'évaluation documentaire, Certi-Trust notifiera le candidat PASSI de son éligibilité à poursuivre les étapes de l'évaluations siège sur site et l'évaluation de la prestation témoin. La liste des non-conformités constatées est transmise, mais il n'y a pas de rapport émis lors de la revue documentaire.

Dans le cas que l'équipe d'évaluation formule une recommandation négative à la poursuite aux étapes subséquentes de l'évaluation, le candidat devra mettre à jour son corpus documentaire et resoumettre ses documents à Certi-Trust. L'offre commerciale sera mise à jour et une nouvelle évaluation documentaire sera à effectuer. Les évaluations de compétence des auditeurs peuvent continuer, même si le prestataire candidat n'est pas encore considéré éligible aux évaluations siège et témoin.

5.4. Évaluation siège (Évaluation sur site)

La deuxième partie de l'évaluation siège se déroule obligatoirement sur le site du prestataire et consiste à vérifier :

- La mise en œuvre effective des politiques, procédures, méthode, etc. définies par le candidat PASSI pour répondre aux exigences de la qualification ;
- L'homologation du système d'information en support des prestations PASSI pour le traitement d'information Diffusion Restreinte, ainsi que sa conformité aux exigences [II901] ;
- S'assurer que l'ensemble des critères et exigences de la qualification ont été considérés.

Le déroulement de l'évaluation sera décrit dans un plan d'évaluation qui sera envoyé par le responsable de mission préalablement à l'évaluation au moins 10 jours ouvrés avant les dates prévues.

Si cette étape n'est pas réalisée dans un délai de 6 mois après l'évaluation documentaire, la revue documentaire doit être renouvelée. Si cette étape n'est pas réalisée dans un délai de 12 mois, l'ensemble de l'évaluation est à reprendre et devra être l'objet d'un nouveau contrat de qualification.

5.5. Évaluation de prestations témoins

L'évaluation de prestations témoins a pour objectif d'observer les activités d'audit du candidat PASSI lors de la réalisation d'une prestation afin de valider :

- La réalisation des activités d'audit conformément aux politiques et procédures d'audit définies par le candidat ;
- Le déroulement du processus d'audit conformément aux exigences définies dans [PASSI].

Une majorité des portées d'audit incluses dans le périmètre de qualification doivent être observées durant une évaluation initiale lors d'une ou plusieurs évaluations témoins. Il n'y a pas d'observation de prestations témoins lors d'une évaluation de surveillance.
L'évaluation de prestations témoins s'effectue en conditions réelles dans les locaux du candidat PASSI et/ou chez un client du candidat PASSI. Il est du ressort du prestataire de s'assurer de la coopération d'un client témoin à accepter la présence des évaluateurs de Certi-Trust en tant qu'observateurs.

Le prestataire doit proposer à Certi-Trust des clients potentiels qui acceptent la présence des évaluateurs durant l'audit ainsi que des dates auxquelles sont planifiés ces audits. Afin d'être potentiellement retenue en tant que prestation témoin, les activités d'audit doivent être d'au moins 12 jours/homme et représenter un niveau de complexité suffisamment élevés pour être représentatif des portées à évaluer. Le choix final de la prestation à évaluer est du ressort de Certi-Trust. Le candidat PASSI doit confirmer les dates de la prestation 20 jours ouvrés avant celle-ci. Dans le cas contraire, Certi-Trust ne pourra pas garantir sa présence.

L'observation de la prestation témoin s'effectue en deux phases. Lors de la première visite, les évaluateurs doivent assister à la réunion d'ouverture de l'audit (et non pas à une réunion de cadrage préliminaire à l'audit). Aussi, les évaluateurs doivent observer les auditeurs réalisant des activités de démarrage d'audit (Entretien, collecte de fichiers de configuration, préparation de test d'intrusion, etc.). Également, une période sera consacrée

lors de cette première visite, sans la présence du client, pour valider les activités de préparation de l'audit (établissement de la convention d'audit, constitution de l'équipe d'audit, contact avec l'audité, élaboration du plan d'audit et revue documentaire).

Lors de la deuxième visite, qui a lieu quand les activités d'exécution de l'audit sont terminées (incluant le rapport d'audit par l'équipe du prestataire), les évaluateurs assistent à la réunion de clôture de la mission d'audit (et non à la réunion de restitution). Également, une période sera consacrée avec l'équipe d'audit, sans la présence du client, pour évaluer le bon déroulement de l'audit selon la démarche du référentiel PASSI (collecte d'information, analyse et évaluation des preuves recueillis, élaboration des constats, réunion de restitution ainsi que la préparation du rapport d'audit). Lors de cette session, les évaluateurs feront des entretiens et analyseront les preuves et enregistrements reliées à la réaliser de l'audit. Ainsi, cette dernière session d'évaluation doit avoir lieu avant la destruction ou la restitution des informations audités au client.

Si l'évaluation de prestations témoins n'est pas terminé dans un délai de 12 mois après l'étude de recevabilité, l'ensemble du cycle de qualification doit être renouvelé.

5.6. Évaluation de compétence et savoir-faire des auditeurs

L'évaluation de compétence et savoir-faire des auditeurs a pour objectifs de valider que les auditeurs candidats ont les connaissances et les techniques nécessaires à la réalisation de prestations qualifiées. L'évaluation comporte un examen écrit et un examen oral.
Les 5 portées évaluées sont :

1. Audit d'architecture ;
2. Audit de configuration ;
3. Audit de code source ;
4. Tests d'intrusion ;
5. Audit organisationnel et physique.

Chaque auditeur peut postuler pour une ou plusieurs des 5 portées. Après une évaluation initiale des compétences, un auditeur peut postuler pour ajouter une ou plusieurs portées supplémentaires.

Seulement un prestataire sous contrat avec Certi-Trust peut inscrire des candidats aux examens. Les auditeurs sous contrat d'un autre centre d'évaluation ne peuvent pas s'inscrire, sauf dans le cadre d'une démarche de transfert de qualification du prestataire.
Le prestataire doit désigner un référent en tant que point de contact sur le programme PASSI. Seul le référent ou des personnes autorisées par lui peuvent inscrire un candidat aux examens. Également, c'est le référent qui se porte garant que le candidat est bien un employé du prestataire et qu'il répond aux critères [PASSI] et des critères supplémentaires formulés par Certi-Trust. Les critères sont les suivants.

- Un auditeur candidat devrait justifier, au minimum, de deux ans d'expérience de travail ainsi que d'avoir participé à 4 missions reliées aux activités d'une portée demandée ayant un total cumulé de plus de 20 jours.
- Un candidat au rôle de responsable de mission d'audit devrait justifier, au minimum, de quatre ans d'expérience de travail significatif ainsi que d'avoir participé à 7 missions reliées aux activités d'une portée demandée ayant un total cumulé de plus de 35 jours dont 15 jours à titre de responsable de mission.

Le prestataire PASSI doit fournir à Certi-Trust une liste des candidats auditeurs avec les portées postulées ainsi que leur email professionnel. Certi-Trust se réserve le droit d'effectuer des demandes d'informations complémentaires sur l'expérience d'un candidat ainsi que des pièces justificatives (CV, copies de diplômes et certificats professionnels, attestation d'emploi, registre d'audit, etc.).

Seul un candidat employé du prestataire peut obtenir le statut d'auditeur. Néanmoins, un prestataire peut présenter un candidat, non-employé, au passage d'un examen sous la condition d'être lié par une promesse d'embauche. En cas de réussite d'examen, les résultats seront communiqués au prestataire, mais aucune attestation de compétence ne sera délivrée tant que le candidat n'est pas à l'emploi de celui-ci. Si le candidat n'est pas à l'emploi du prestataire dans un délai de six mois après la notification de ses résultats d'examens, les résultats seront considérés comme caduques.

Il est à noter qu'un candidat est autorisé à postuler uniquement pour une attestation de compétence de responsable de mission d'audit sans autre portée d'audit. Il doit réussir l'examen « Principes et méthodologie d'audit » ainsi que l'oral sur la portée « Responsable d'audit ». En cas de réussite, il peut participer et diriger une mission d'audit qualifié (planification de l'audit, conduite des réunions, présentation des constats, etc.). Cependant, il ne peut pas effectuer des activités d'audit reliées à une portée spécifique telle que la collecte d'information et l'analyse des preuves recueillies.

Certi-Trust peut émettre une facture pour chaque candidat et un devis préalable sur demande. Le candidat est alors convoqué à un examen écrit après paiement des frais d'inscription et de validation du dossier de l'auditeur par Certi-Trust.

Les examens écrits sont organisés par Certi-Trust à la demande en intra. Le prestataire candidat doit réaliser une demande à Certi-Trust et une session sera proposée sous 10 jours ouvrés. Ils peuvent se tenir dans les locaux du prestataire, dans les locaux de Certi-Trust ou dans des locaux à accès publics. Les sessions d'examen sont toujours organisées sous la supervision d'un surveillant d'examen agréé par Certi-Trust.

Si une session est organisée chez un prestataire, la salle doit être réservée exclusivement pour le passage des examens durant la période. Dans le cas ou moins de 5 examens sont commandés, un prix forfaitaire peut être facturé au client correspondant au prix-liste de maximum 5 examens, permettant de couvrir les frais incompressibles d'une surveillance de session d'examen. Il est à noter que si aucune session publique n'est prévue dans les trois mois, Certi-Trust ne facture aucun frais supplémentaire pour le passage d'examen en intra (même pour un seul examen).

Des séances publiques peuvent être prévues pour passer les examens écrits. Dans ce cas, Certi-Trust annonce les dates au moins 20 jours ouvrés en avance. Certi-Trust se réserve le droit d'annuler une session d'examen planifiée jusqu'à une semaine avant l'examen, si moins de quatre candidats sont inscrits.

L'examen écrit contient :

- Un tronc commun, « Principes et méthodologie d'audit », identique pour toutes les portées candidatées, permettant d'évaluer les connaissances du candidat des pratiques et méthodes pour la réalisation d'audit conforme à [ISO19011].
    - La réussite de cet examen est obligatoire pour l'ensemble des auditeurs et responsables d'audit.
    - Aucune attestation de compétence d'une portée d'audit ne sera émise sans la réussite préalable de cet examen.
    - Un candidat ayant déjà réussi l'examen dans le présent cycle de qualification n'a pas à repasser cet examen quand il postule pour une nouvelle portée.

- Une partie spécifique pour chaque portée candidatée permettant d'évaluer les connaissances techniques du candidat dans chacun des domaines.

Le candidat réussit s'il obtient une note supérieure ou égale à 15/30 pour l'examen « Principes et méthodologie d'audit » et 24/40 pour chaque portée candidatée.
Les copies sont anonymisées et corrigées par un évaluateur indépendant. Dans le cas que la note est qu'à un écart de 5% de la note de passage, une correction est effectuée par un deuxième évaluateur afin de valider la note finale.

Le résultat « réussite » ou « échec » sera communiqué au référent du prestataire et non au candidat directement. En aucun cas, le candidat ne peut pas avoir accès à ses copies d'examen.

En cas d'échec aux examens écrit, le candidat pourra se représenter ultérieurement après un délai minimal de deux semaines suivant la réception de son résultat.

Seuls les auditeurs candidats ayant eu, au moins, le minimum de points requis lors des examens écrits peuvent se présenter à l'examen oral associé aux domaines ainsi réussis. Ainsi, un candidat peut passer un examen oral pour un ou plusieurs domaines, même s'il a échoué certains autres examens écrits. Un candidat auditeur ne peut pas s'inscrire à un examen oral avant d'avoir été validé à l'écrit.

L'examen oral doit permettre au jury :

- D'approfondir les compétences démontrées lors des examens écrits et, notamment, les éléments où l'auditeur candidat a échoué ;
- D'évaluer les expressions orales de l'auditeur candidat et sa capacité à exprimer clairement et de manière synthétique une réponse à une question posée par le jury ;
- D'évaluer le comportement de l'auditeur candidat dans différentes situations caractéristiques d'un audit ;

Le candidat aura un examen oral incluant l'évaluation de chaque portée à laquelle il candidate. La durée minimale d'un oral est de 30 minutes pour la première portée (qui inclus la partie sur la connaissance du référentiel, la démarche d'audit et les exigences réglementaires) plus 10 minutes par portée supplémentaire.

Les sessions sont organisées environ 2 à 4 semaines après l'annonce des résultats des examens écrits. Certi-Trust organise les oraux sur demande et en mode continue. Les oraux sont organisés en Webconférence sur une base individuelle. Une proposition de date et d'heure de passage est adressée directement au candidat par email.

Dans le cas d'une session d'oraux demandée en présentiel, Certi-Trust garanti la constitution d'un jury dans un délai maximum de 20 jours ouvrés après l'inscription des candidats. Certi-Trust se réserve le droit d'annuler une session d'examen planifiée jusqu'à une semaine avant l'examen, si moins de quatre candidats sont inscrits.

Le candidat est évalué par un jury composé d'au moins deux évaluateurs de Certi-Trust. La composition du jury sera communiquée au candidat par email et/ou avec sa fiche de convocation. Il est de la responsabilité du candidat de faire part à Certi-Trust, par écrit, d'un possible conflit d'intérêts avec l'un des jurés pressentis pour participer à ce jury.

Les 5 critères d'évaluation utilisés lors des oraux sont :

1. Expertise démontrée sur les activités d'audit reliées à la portée des domaines appliqués par le candidat

2. Capacité de mise en situation entre la théorie et la pratique
3. Capacité d'analyse reliée à l'activité d'audit
4. Capacité à formuler des recommandations reliées à l'activité d'audit
5. Capacité d'expression orale et de vulgarisation

Le candidat est noté de 1 à 4 pour chaque critère selon l'échelle suivante :

1. N'a pas su démontrer un niveau d'expertise suffisant
2. Présente des faiblesses
3. A su démontrer un niveau d'expertise suffisant
4. A su démontrer un excellent niveau d'expertise

Une note de 1 ou 2 sur la validation d'expertise d'une portée entraine de facto un avis défavorable sur la portée en question. Une note de 1 ou 2 sur plus de deux des autres critères entraine de facto un avis défavorable sur l'ensemble des portées à évaluer.

Pour chaque candidat, le prestataire recevra un résultat de réussite ou d'échec. Par suite de la prise de décision, Certi-Trust émettra, sous 10 jours ouvrés, une attestation de compétence mentionnant la ou les portées qui seront validées pour chaque candidat. En cas d'échec, un auditeur peut repasser à nouveau l'examen après un délai minimal de 2 semaines de carence.

L'attestation de compétence est valable 3 ans à partir de la date de décision. Dans le cas d'extension à d'autres portées, la date de fin de validité de l'attestation reste inchangée. À l'issue des 3 ans, le candidat devra repasser l'ensemble de l'évaluation de compétence et savoir-faire des auditeurs (examens écrit et l'oral).

Un prestataire a un délai de 20 jours ouvrés pour faire appel de la décision du jury au nom de l'un de ses candidats et obtenir les procès-verbaux de son examen oral et écrit. Seul le référent chez le prestataire peut en effectuer la demande. Toute réclamation concernant cette décision se fera le processus d'appel décrit à la section 4.8.4 de ce règlement. À l'issue d'une période supplémentaire de 3 mois (90 jours calendaires), Certi-Trust n'a plus l'obligation de conserver les copies des examens et des enregistrements associés à l'exception des attestations de compétence. Certi-Trust se réserve le droit de conserver des copies anonymisées des données des examens pour des fins de formations internes et de statistiques.

Les attestations de compétence des auditeurs étant liées au PASSI, si un auditeur quitte son employeur qualifié PASSI, il perd automatiquement sa qualification et devra repasser l'ensemble de l'évaluation de compétence des auditeurs dans le cadre de son nouvel emploi.

Le non-respect des engagements pris par un candidat dans le dossier d'inscription peut amener Certi-Trust à retirer l'attestation de compétences.

Il est à noter qu'aucun résultat d'examens ne sera communiqué par téléphone.

noter qu'aucun résultat d'examens ne sera communiqué par téléphone.

5.7. Décision de qualification

Les rapports d'évaluation et les résultats des examens des auditeurs constituent les éléments pris en considération pour prendre une décision de qualification. Elles ne présument ni ne constituent la décision de qualification elle-même.

La décision de qualification peut être prise quant à elle par le Certification Manager, Directeur du Centre d'évaluation ou le Directeur Général de Certi-Trust. Si l'un de ces derniers est impliqué dans le processus d'évaluation, la décision sera prise par une autre personne autorisée. Le comité d'impartialité et d'éthique de Certi-Trust peut être sollicité à tout moment de ce processus pour fournir un avis non contraignant relatif à la prise de décision de qualification.

5.7.1 Décision initiale

Lorsque le prestataire candidat PASSI a réalisé l'évaluation siège, une évaluation de prestations témoins et qu'au moins un auditeur a reçu une attestation de compétence pour chaque portée demandée, une décision peut alors être rendue, qui soit :

- Un refus de qualification, si :
  - Le rapport fait apparaître au moins une non-conformité majeure.
  - L'évaluation n'a pas permis d'observer la totalité des exigences du référentiel.
- Une qualification sous réserves, si :
  - Les rapports font apparaître un nombre important de non-conformités mineures qui, cumulés, peuvent mettre en cause la validité de la qualification.
  - Les propositions de mesures correctives et préventives du candidat non-conformités mineures ne permettent pas de lever le doute sur la future conformité du PASSI.
- Une qualification sans réserve, si :
  - Le rapport n'a pas fait apparaître de non-conformité majeure.
  - Les propositions de mesures correctives et préventives du candidat aux non-conformités mineures permettent de lever tout doute quant au degré de conformité du PASSI vis-à-vis des exigences du référentiel.

Dans le cas d'une décision de refus ou d'une qualification sous réserves, une évaluation complémentaire devra être effectuée dans les six mois suivant la décision. Passé ce délai de six mois, l'ensemble du processus de qualification sera à recommencer depuis le début. Lorsqu'une décision de qualification est prise, une attestation de qualification est produite et envoyée au PASSI, mentionnant l'ensemble des portées qualifiées. La durée de validité de la qualification est de 3 ans à compter de la date de décision. Les décisions de qualification seront transmises à l'ANSSI sous un délai de 10 jours ouvrés au maximum.

À chaque nouvelle portée acquise, une attestation de qualification sera réémise, tout en conservant sa date de validité initiale.

5.7.2 Décision pour donner suite à une évaluation de surveillance, de renouvellement ou complémentaire

À la réception d'un rapport d'évaluation de surveillance, de renouvellement ou complémentaire, une décision sera prise et communiquée au prestataire. Elle peut consister en :

- Le retrait de la qualification du PASSI
- La suspension de la qualification du PASSI
- Le maintien avec réserve du PASSI
- Le maintien sans réserve du PASSI

S'il y a une modification à la portée de qualification, la décision de qualification sera transmise à l'ANSSI sous un délai de 10 jours ouvrés au maximum.

5.7.3 Suspension - retrait de la qualification

Les raisons suivantes peuvent faire l'objet d'une suspension ou d'un retrait de la qualification :

- Actions curatives et actions correctives non implémentées dans le temps imparti ;
- Utilisation impropre de l'attestation de qualification, du logo ou tout autre symbole au regard de la Politique d'utilisation de la marque Certi-Trust ;
- Le prestataire a manqué à ses obligations financières par rapport à Certi-Trust ;
- Le prestataire a lui-même demandé le retrait de sa qualification ;
- Le prestataire n'a plus suffisamment de compétence à disposition en nombre suffisant dans une activité d'audit. Il doit maintenir, au moins, un auditeur qualifié par portée ;
- Le prestataire a enfreint les conditions contractuelles ou le Règlement de Qualification ;
- Le prestataire n'a pas fait preuve de diligence pour faire respecter les conditions générales pour les examens d'évaluation de compétences par ses auditeurs et employés.
- Le prestataire est incapable ou ne veut pas/plus assurer la conformité avec les versions revues du référentiel. Le délai pour s'y conformer sera notifié lors de la publication d'une nouvelle version ;
- Une plainte sérieuse et étayée par des preuves tangibles ou un nombre important de plaintes similaires, basées sur des éléments factuels démontrables, ont été reçues par Certi-Trust qui indiquent que le prestataire ne maintient pas son système de management ou ne respecte pas les exigences de qualification ;
- Le prestataire n'a pas permis à Certi-Trust de réaliser les évaluations de surveillance suivant la fréquence définie ;
- Le prestataire n'a pas réalisé de prestation qualifiée depuis sa dernière évaluation sachant que ce dernier doit effectuer, à minima, une prestation qualifiée tous les 18 mois et une prestation qualifiée par portée tous les 36 mois ;
- Les conditions d'exécution du schéma de qualification ou un texte règlementaire l'impose ;
- Des travaux de mise en conformité, par suite d'une modification des exigences de qualification, n'ont pas été réalisés avant la date d'échéance requise.

La décision de suspension, ou le retrait, de la qualification est prise par le Certification Manager, par le Directeur du centre d'évaluation et/ou le Directeur Général de Certi-Trust. La décision de suspension ou du retrait de la qualification ainsi que les raisons qui l'ont motivée est notifiée par écrit au PASSI de même qu'à l'ANSSI dans un délai de 10 jour ouvré après qu'elle a eu été prise.

Dans le cas où le prestataire n'a plus aucun auditeur sur une portée, cela entraine immédiatement une décision de suspension de la qualification sur la portée en question sans mettre en cause nécessairement la qualification du prestataire. Si le prestataire n'a pas fait valider au moins un nouvel auditeur sur la portée en question dans un délai maximal de 6 mois après la date de départ du dernier auditeur sur une portée, une décision de retrait de la qualification sera prise concernant cette portée. Dans cette situation, une nouvelle attestation de qualification sera réémise au prestataire indiquant les portées restantes et celle-ci sera envoyée à l'ANSSI.

Lors d'une décision de suspension, la durée de celle-ci ne peut excéder six mois. Passé ce délai et sans réaction du PASSI aux sollicitations écrites de Certi-Trust, ou si les actions permettant de lever la suspension n'ont pas été menées et contrôlées par une évaluation complémentaire, la décision de retrait de la qualification pourra être prise.

À la suite d'un retrait complet de sa qualification, le PASSI devra repasser l'ensemble du processus de qualification s'il veut réobtenir une nouvelle qualification. Il devra par ailleurs démontrer que les causes qui ont amené au retrait ne peuvent plus se reproduire.

La suspension ou le retrait de la qualification entraînent la résiliation du droit d'utilisation de la marque et des attestations associés à la qualification. Le PASSI n'est dès lors plus autorisé à utiliser la marque PASSI de Certi-Trust ni à faire la promotion de sa qualification. Dans le cas d'un retrait, le PASSI doit retourner immédiatement à Certi-Trust toutes les attestations qui lui ont été délivrés et apporter la preuve de la destruction de tous les éléments associés à ces documents numériques.

Les attestations de compétences des auditeurs peuvent également leur être retirées si les ceux-ci ne respectent pas les engagements pris lors de leur inscription. Ces engagements sont décrits dans l'annexe à ce règlement « Conditions générales pour les examens d'évaluation des compétences ».

5.8. Évaluation en cours de cycle

5.8.1 Évaluations de surveillance

Une évaluation de surveillance est réalisée 18 mois après la prise de décision de la qualification. La fréquence des surveillances peut être augmentée par Certi-Trust (6 ou 12 mois), en fonction des résultats des évaluations précédentes ou sur demande de l'ANSSI ou encore dans le cas de réclamations à l'encontre du PASSI. La durée de l'évaluation est conforme à [QUAL_SERV_PORTEES].

L'objectif de cette évaluation est de vérifier que le PASSI est toujours conforme aux exigences de qualification et en particulier :

- La conformité dans le temps de l'ensemble des exigences applicables, et ce quelles que soit les modifications apportées à l'organisation, aux méthodes et aux ressources du PASSI (incluant son système d'information de diffusion restreinte) ;
- La mise en œuvre du plan d'action correctif et préventif proposé par le PASSI pour lever les non-conformités de l'évaluation précédente ;
- Le respect des exigences règlement de qualification et d'usage de la marque Certi-Trust ;
- Le maintien des compétences des auditeurs et du niveau des outils ;
- La réalisation d'au moins une prestation d'audit qualifiée depuis la dernière évaluation (évaluation initiale ou de renouvellement).

Dans le cadre des évaluations de surveillance, les modalités suivantes s'appliquent :

1. **Étude de recevabilité :** il n'y a pas d'étude de recevabilité à réaliser à moins d'une demande d'extension de portées.
2. **Évaluation siège (Revue documentaire) :** 10 jours avant l'évaluation siège, le prestataire doit faire parvenir à l'équipe d'évaluation le corpus documentaire accompagné d'un résumé des changements depuis la dernière évaluation. Les évaluateurs vont procéder à la revue documentaire, au minimum, sur les documents ayant fait l'objet de changements significatifs (hors corrections éditoriales). Cependant, il n'y a pas de rapports ou de retour formel de la revue documentaire au prestataire au préalable à l'évaluation sur site ;

3. **Évaluation siège (Évaluation sur site) :** vérification sur site de la mise en œuvre effective des procédures, instructions, modes opératoires, outils, etc. définis par le PASSI pour répondre aux exigences de la qualification ainsi que l'évaluation du système d'information de diffusion restreinte. Un échantillonnage des exigences seront revues incluant, au minimum, un tiers de celles-ci.
4. **Évaluation de prestations témoins :** à moins d'une extension de portées, il n'y a pas d'observation de prestations témoins prévues lors des surveillances.
5. **Évaluation de compétence et savoir-faire des auditeurs** : il n'y a pas de réévaluation de la compétence et du savoir-faire des auditeurs à prévoir obligatoirement lors de l'évaluation de surveillance. Cependant, le prestataire peut profiter d'une évaluation de surveillance pour présenter des candidats aux examens écrits et oraux.

Il est à noter que si le prestataire qualifié n'est pas en mesure de présenter au moins une prestation effectuée selon les dispositions qualifiées depuis sa dernière évaluation, la qualification est suspendue tant que le prestataire n'est pas en mesure de présenter une prestation sous qualification. Dans un délai de 6 mois après cette notification, si le prestataire n'est pas en mesure de présenter une prestation qualifiée, la qualification est retirée et l'ensemble du processus de qualification est à recommencer.

Après chaque évaluation de surveillance, un rapport sera produit et une nouvelle prise de décision effectuée.

5.8.2 Évaluations de renouvellement

Une évaluation de renouvellement est réalisée 36 mois après la date de décision de qualification. Ses modalités sont similaires à celles d'une évaluation initiale sans l'étape d'étude de recevabilité et sa durée est conforme à [QUAL_SERV_PORTEES].

Dans le cadre des évaluations de renouvellement, les modalités suivantes s'appliquent :

1. **Étude de recevabilité :** il n'y a pas d'étude de recevabilité à réaliser à moins d'une demande d'extension de portées.
2. **Évaluation siège (Revue documentaire) :** 20 jours avant l'évaluation siège, le prestataire doit faire parvenir à l'équipe d'évaluation le corpus documentaire accompagné d'un résumé des changements depuis la dernière évaluation. Une nouvelle revue documentaire complète sera réalisée par l'équipe d'évaluateurs ;
3. **Évaluation siège (Évaluation sur site) :** vérification sur site de la mise en œuvre effective des procédures, instructions, modes opératoires, outils, etc. définis par le PASSI pour répondre aux exigences de la qualification ainsi que l'évaluation du système d'information de diffusion restreinte. L'ensemble des exigences du référentiel PASSI seront revues.
4. **Évaluation de prestations témoins :** valider les niveaux de qualité et de sécurité effectivement atteints par le candidat PASSI lors d'une prestation d'audit réalisée en conditions réelles.
5. **Évaluation de compétence et savoir-faire des auditeurs** : il n'y a pas de réévaluation de la compétence et du savoir-faire des auditeurs à prévoir obligatoirement. Cependant, le renouvellement des attestations de compétences des auditeurs doit avoir lieu dans le délai maximum de 36 mois.

Le prestataire devra démontrer qu'au moins une prestation par portée qualifiée a été réalisée sous qualification au cours du cycle écoulé depuis la dernière évaluation de renouvellement ou de l'évaluation initiale ainsi qu'au moins une prestation a eu lieu depuis la dernière évaluation de surveillance. Dans le cas contraire, la PASSI dispose de 6 mois pour justifier à Certi-Trust de la réalisation d'un audit qualifié sur les portées manquantes

sans dépasser le délai de validité de la qualification. Passé cette période, une décision de suspension de qualification sur la ou les portées concernées pourra être prise.
Après chaque évaluation de renouvellement, un rapport sera produit et une nouvelle prise de décision effectuée.

5.8.3 Évaluations complémentaires

Une évaluation complémentaire, à la charge du PASSI, doit être programmée suite à une évaluation initiale, de surveillance ou de renouvellement dans les cas suivants :

- Lorsque des non-conformités majeures sont identifiées ;
- Quand des plans d'action pour de nombreuses non-conformités doivent être mis en œuvre ;
- Suite à la notification par le PASSI d'importantes modifications intervenues dans sa structure, son organisation ou ses moyens;
- À la suite d'une plainte à l'encontre du PASSI;
- A la demande de l'ANSSI ;
- Aux fins de lever une suspension de qualification.

Après chaque évaluation complémentaire, un rapport sera produit et une nouvelle prise de décision effectuées.

5.9. Base de données de qualification

La base de données des prestataires qualifiées est tenue à jour par le département Certification de Certi-Trust. Par ailleurs, l'ANSSI tient à jour la liste officielle des prestataires qualifiées sur son site internet.

5.10. Gestion des examens et base de données des questions

L'examen sur les principes et méthodologies d'audit comporte 30 questions (toutes des QCM).

Concernant les examens sur les activités d'audit, chaque examen doit comporter 30 questions, dont 25 QCM et 5 questions ouvertes. Pour chaque activité d'audit, une base de données des questions regroupe un ensemble de questions (QCM et questions ouvertes) qui peuvent servir pour générer un jeu d'examen. Les examens doivent être approuvés par l'ANSSI.

6. Non-conformité et actions correctives

Tous les écarts relevés par rapport à des exigences de qualification font l'objet d'une fiche de non-conformité. Les niveaux de ces écarts sont évalués en fonction du risque causé par l'écart. La classification de la criticité des non-conformités est effectuée par le Responsable d'évaluation en accord avec les membres de l'équipe d'évaluation.
Une non-conformité est classée majeure lorsque, sur la base d'évidences objectives, de l'un ou plusieurs des critères suivants :

- Il y a un risque significatif pour la conformité de la prestation aux exigences de qualification ;
- Il y a non-respect systématique ou répété d'une exigence spécifiée ;
- Il y a un risque significatif pour la sécurité de l'information.

Une non-conformité qui n'est pas classée majeure est classée mineure. Une non-conformité mineure correspond à une faiblesse sur le respect d'une exigence et qui se traduit par un doute sur le fait que les mesures mises en place permettent de répondre entièrement à une exigence.

Dans le cadre de ce programme, il n'est pas permis aux évaluateurs de rédiger des opportunités d'amélioration. Un évaluateur pourra expliquer à un commanditaire et/ou au prestataire les raisons justifiant une non-conformité ainsi que l'exigence associée. Cependant, il ne pourra pas prodiguer de conseils sur les moyens à prendre pour la clôturer.

Les non-conformités sont présentées en réunion de clôture de l'évaluation. Le PASSI dispose de 10 jours ouvrés à l'issue de réunion, pour proposer au responsable d'évaluation, les mesures correctives immédiates qu'il va mettre en œuvre, une analyse de la cause racine de l'écart, ainsi que les actions permettant de corriger les causes de celui-ci. Chaque action proposée devra contenir un délai raisonnable de mise en œuvre. Le responsable d'évaluation, en accord avec les membres de l'équipe d'évaluation, doit valider le plan d'action dans les 10 jours ouvrés. En cas de désaccord sur le plan d'action, le PASSI dispose de 10 jours pour proposer un nouveau plan d'action. Passé ce délai ou si le responsable d'évaluation estime que le plan d'action n'est toujours pas suffisant, la procédure de qualification est arrêtée ou la procédure de suspension de la qualification est engagée.

La clôture d'une non-conformité majeure est réalisée lors d'une évaluation complémentaire. La clôture d'une non-conformité mineure est réalisée lors de la prochaine évaluation de surveillance ou de renouvellement. La clôture d'une non-conformité doit être documentée dans sa fiche d'écart.

Lors d'une évaluation de surveillance ou de renouvellement, toute non-conformité mineure dont le plan d'action validé n'aura pas été mis en œuvre sera réévaluée en non-conformité majeure.

7. Décision de qualification

7.1. Général

L'évaluateur principal est responsable pour soumettre l'ensemble des documents d'évaluation (plans, rapports, notes) au responsable des programmes d'audit de Certi-Trust. C'est ce dernier qui sera responsable de transmettre les documents d'évaluation demandés par l'ANSSI.

Les rapports sont revus à différents niveaux.

7.2. Revue technique et décision de qualification

Etape 1

L'étape 1 consiste à une revue du dossier L'ensemble des documents sont revues par le directeur du centre d'évaluation ou par le Certification Manager afin de s'assurer qu'ils sont entièrement complétés.

Dans le cas où un problème est détecté, un email est envoyé au responsable de l'équipe d'évaluation pour analyse et action afin de soumettre le dossier corrigé à nouveau.

Etape 2

L'étape 2 consiste à la décision de qualification. Les rapports d'évaluation sont revus par le Certification Manager, ainsi que les points relevés lors de l'étape 1 avant de prendre sa décision et de décider de la qualification ou non du prestataire.

Le Certification Manager peut être amené à demander des informations complémentaires à l'équipe d'évaluation.

Pour les évaluations de surveillance, cette étape n'est pas nécessaire.

Dans le cas où le Certification Manager est impliqué dans l'évaluation ou qu'un conflit d'intérêt aurait été détecté par rapport au prestataire, un Directeur du centre d'évaluation de Certi-Trust doit revoir les rapports et prendre la décision de qualification.

Etape 3

L'étape 3 consiste à initier les actions par le département administratif suite à la décision de qualification ou non :

- Préparer le certificat comme défini ci-dessous
- Mettre à jour la base de données des prestataires qualifiés
- Mettre à jour le dossier du prestataire avec l'ensemble des informations recueillies durant le processus d'évaluation
- Vérifier qu'aucune des règles de Certi-Trust n'ont été omises.

7.3. Préparation des attestations et envoi

Des attestation de qualification et de compétence sont émis suite à une évaluation initiale, une extension du périmètre sous qualification, une évaluation de renouvellement ou suite à un changement sur les détails du prestataire (nom, adresse, etc.).

Les certificats font l'objet d'un identifiant unique, commençant par C-, avec ensuite la référence du programme (ici « PASSI »), le mois et l'année de l'émission du certificat, un numéro indiquant si le client est le prestataire évaluée (0) ou si le client est différent du prestataire évalué (1 puis incrémentation séquentielle) suivi enfin par le code client. Exemple pour une évaluation réalisée en mai 2017 où le client était le prestataire évalué : C-PASSI-072017-0CLIENTCODE.

Le département administratif prépare l'attestation :

- Sélectionner le bon modèle de l'attestation.
- Indiquer la date de début de qualification (correspondant au dernier jour de la dernière évaluation terrain) et indiquer la date d'expiration 3 ans plus tard.
- Dans le cas d'un transfert de qualification, la date d'expiration doit être la même que pour le précédent certificat émis. Le responsable du programme doit donner ses instructions dans ce type de cas.
- Dans le cas d'un renouvellement, le numéro de l'attestation ne change pas. Dans le cas où un écart existe entre le premier cycle et le second cycle, un nouveau numéro de certificat doit être généré.
- Indiquer le nom du prestataire, son siège social, son adresse, le référentiel (incluant sa version), le périmètre de qualification et tout autre site inclus.
- Le responsable du programme d'évaluation doit revoir l'attestation et le soumettre au Directeur pour signature.
- Dans le cas où le prestataire demande des certificats séparés pour chacun des sites, le périmètre et l'ensemble des sites doivent être mentionnés. Pour chaque certificat, un suffixe est ajouté (A, B, C, etc.).
- Dans le cas d'une évaluation intégrée, des certificats séparés doivent être émis.
- Dans le cas d'une modification du certificat (changement de nom, etc.), un suffixe (R1, etc.) est rajouté au numéro de certificat. Les dates d'émission et d'expiration ne doivent pas changer.

Le Directeur n'a pas autorité pour rejeter l'émission d'une attestation. L'attestation peut être retourné au Certification Manager en indiquant les raisons. Ce dernier doit revoir les raisons et investiguer dans ce sens. Si le Certification Manager estime que les raisons ne sont pas fondées, l l'attestation doit être émis à nouveau au Directeur qui doit signer l'attestation. Une signature électronique ou une image peuvent être utilisées.

L’attestation est envoyé au prestataire auprès du contact désigné ainsi qu’à l’ANSSI avec l’ensemble des rapports d’évaluation réalisées et ne doit pas être envoyé à une autre personne sans l’approbation écrite du prestataire.

L’attestation de qualification ainsi que les attestation de compétence sont conservées dans le dossier du prestataire.