# Procédure de Planification, Mise en œuvre et Rapport des PASSI

## Propriétés du document :

| | |
|---|---|
| **Version :** | 2.0 |
| **Niveau de confidentialité :** | Protégé |
| **Type de document :** | Procédure |
| **Approuvé par :** | RSG |

## 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 | RSG | Approbation |
| 1.1 | 23/09/2017 | JAL | Change organisation name |
| 2.0 | 23/09/2017 | PDE | Approval |

# 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
- Evaluation du siège
- Examens écrits des auditeurs
- Examens oraux des auditeurs
- Evaluation terrain
- Evaluation de surveillance
- Evaluation de renouvellement

# 3. Définitions et acronymes

Les définitions et acronymes utilisés dans le cadre de cette procédure s'appuient sur la norme ISO 19011 ainsi que sur le référentiel d'exigences des PASSI.

# 4. Vente

## 4.1. Demande client

Toutes les demandes doivent être formalisées via le formulaire d'application dédié au programme PASSI par une personne autorisée chez le prestataire candidat. L'objectif du formulaire d'application est d'identifier :

- Le périmètre de la certification (activités 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 pour chaque activité d'audit ainsi que leur rôle (auditeur principal ou auditeur).
- Des informations sur les processus externalisés par le prestataire qui peuvent impacter la conformité aux exigences applicables.
- Description générale du système d'information (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).

La qualification ne peut toutefois être attribuée à un prestataire uniquement sur l'activité de tests d'intrusion ou d'audit organisationnel et physique.

## 4.2. Préparation et envoi de l'offre

Lors de la préparation de l'offre, une visite sur site peut être nécessaire pour obtenir des informations complémentaires. La détermination du temps d'évaluation est de la responsabilité du responsable des programmes d'audit. Le responsable des ventes ne peut soumettre et envoyer l'offre sans avoir obtenu au préalable la détermination du temps d'évaluation.

Un calendrier prévisionnel sera également joint à l'offre et transmis au prestataire candidat.

Après validation et signature de l'offre par l'ensemble des parties, Certi-Trust doit informer l'ANSSI à ce sujet.

## 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.

### *1.1.1. Matrice de temps d'évaluation*

**Etude du dossier de candidature**

Le temps d'évaluation standard pour l'étude du dossier de candidature est de 2 jours.

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

- 0,5 jour :
  - Multiplication des plans d'audit types et des rapports d'audit types
  - Multiplication des processus d'audit et des conventions d'audit types

Les études de dossier de candidature ne font pas l'objet d'évaluation de surveillance ou d'évaluation de renouvellement spécifique. En revanche, dans le cadre de l'évaluation du siège, une attention doit être portée à la mise à jour effective de la documentation.

### Evaluation du siège

Le temps d'évaluation standard pour l'évaluation du siège initiale est de 3 jours soit approximativement :

- 1 jour pour l'évaluation des exigences générales ;
- 1 jour pour l'évaluation de la protection des systèmes d'information utilisé par le prestataire dans le cadre du traitement des informations sensibles relatives aux prestations PASSI ;
- 1 jour pour la préparation à l'évaluation et la rédaction du rapport.

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.

| Activité d'audit | Temps estimé pour l'examen |
|---|---|
| Audit d'architecture | 45 minutes |
| Audit de configuration | 45 minutes |
| Audit de code source | 45 minutes |
| Test d'intrusion | 45 minutes |
| Audit organisationnel et physique | 45 minutes |
| Auditeur principal | 45 minutes |

**Evaluation terrain**
Le temps d'évaluation standard pour l'évaluation terrain initiale est de 4 jours pour chaque activité d'audit. Selon le niveau de complexité de l'audit à observer sur le terrain, le temps d'évaluation peut varier d'une journée (à la hausse ou à la baisse).

**Evaluation de surveillance**
Le temps d'évaluation standard pour l'évaluation de surveillance est de 2 jours.

**Evaluation de renouvellement**
Le temps d'évaluation standard pour l'évaluation de renouvellement est de 3 jours.

**Renouvellement des habilitations des auditeurs**
La durée de validité des habilitations fournies aux auditeurs est de 3 ans. Les habilitations doivent être renouvelées en passant à nouveau les examens écrits et les examens oraux.

## 4.4. Multi-sites

### *1.1.2. 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.

### *1.1.3. 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 peut procéder à une réduction du temps d'audit (si applicable) si le périmètre inclut les activités reliées aux prestations PASSI du prestataire.

Des rapports d'audit intégrés pourront être établis et émis. Une attention particulière devra toutefois être portée afin de s'assurer que l'audit a bien satisfait à l'ensemble des exigences des normes considérées.

Dans le cadre d'une évaluation PASSI d'un prestataire candidat avec un audit de certification ISO 9001 sur le même périmètre, 0,5 jour sera additionné pour l'audit initial. Par contre, les audits de surveillance combinés seront effectués tous les 12 mois au lieu de 18 mois.

Dans le cadre d'une évaluation PASSI d'un prestataire candidat avec un audit de certification ISO/CEI 27001 sur le même périmètre, 1.0 jour sera additionné pour l'audit initial. Par contre, les audits de surveillance combinés seront effectués tous les 12 mois au lieu de 18 mois.

## 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 ici un prestataire déjà qualifié par un autre prestataire de qualification qui souhaite à présent être qualifié chez Certi-Trust.

Un formulaire d'application doit être complété et retourné par le client dans lequel est précisé la qualification existante du client et sa demande de transfert. Le

certificat existant doit également être joint au formulaire complété ainsi que les derniers rapports d'évaluation (étude du dossier, siège et terrain).

Les étapes suivantes doivent être procédées :

- Réaliser le processus standard pour la préparation de l'offre.
- Vérifier que le périmètre de qualification du client est bien celui mentionné dans le formulaire d'application, ainsi que la liste des auditeurs qualifiés du prestataire.
- Valider que le prestataire est enregistré auprès de l'autorité de surveillance (ANSSI en France).
- Confirmer que Certi-Trust est compétent pour évaluer le client suivant le périmètre de qualification défini.
- Vérifier que le certificat est valide, n'est pas expiré et est sous accréditation.
- Vérifier par rapport au cycle de qualification à quel état le client est.
- Définir le programme d'audit en conséquence.

## 4.8. Transfert de qualification des auditeurs

Dans le cas d'auditeurs préalablement qualifiés chez un prestataire qualifié PASSI qui rejoindraient un autre prestataire qualifié PASSI, les auditeurs seront également amenés à transférer leur habilitation chez Certi-Trust. Dans ce cas, le prestataire devra fournir pour chaque auditeur préalablement habilité les documents suivant :

- Formulaire de candidature
- Curriculum Vitae
- Une attestation de formation en technologie des systèmes d'information et communication et en audit (diplôme, attestation employeur, etc.)
- Toute autre attestation de compétence (exemple : certificat)
- La copie d'une pièce justifiant l'identité du candidat et comportant une photographie
- Une attestation d'emploi ou DUE
- Le certificat de qualification PASSI existant
- Toute preuve permettant de démontrer que l'auditeur a été adéquatement formé aux processus d'audit du prestataire ainsi qu'aux méthodes, techniques et outils utilisés chez son nouvel employeur (le prestataire PASSI qu'il a rejoint).

Il est à noter qu'en aucun cas, un auditeur peut réaliser des audits PASSI à l'extérieur du cadre d'un prestataire PASSI qualifié. Si l'auditeur quitte un prestataire PASSI et ne transfert pas sa qualification chez un autre prestataire qualifié dans une période d'un an, sa qualification sera considérée caduque et le processus de qualification devra être renouvelé.

# 5. Opérations

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

Tous les membres de l'équipe d'évaluation (siège et terrain) doivent :

- Avoir une formation ou un enseignement professionnel équivalent à un niveau universitaire.
- Avoir au moins 4 ans d'expérience dans le domaine des technologies de l'information, dont 2 ans dans un rôle relatif à la sécurité de l'information.
- Avoir au moins 1 an d'expérience dans le domaine de l'audit de sécurité des systèmes d'information.
- Avoir au moins deux années d'expérience dans le domaine des systèmes industriels, pour réaliser l'activité d'audit de la sécurité des systèmes industriels.
- Avoir suivi et réussi une formation de 5 jours dont le sujet couvre les méthodologies d'audit et plus spécifiquement les audits relatifs à la sécurité de l'information.
- Être de nationalité française ou être résident français.
- Ne pas être salarié ou consultant d'un prestataire qualifié PASSI.
- Ne pas être salarié ou consultant d'un prestataire concurrent au prestataire candidat à la qualification.
- Être sensibilisé à la législation en vigueur sur le territoire français et applicable aux différentes missions d'évaluation.
- Avoir une bonne maitrise des bonnes 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 prester des activités d'évaluation.
- Avoir signé l'engagement d'impartialité et d'éthique de Certi-Trust.
- Avoir été approuvé par l'ANSSI.

En fonction des activités d'audit considérées dans le périmètre de qualification, les membres de l'équipe d'évaluation doivent regrouper les compétences requises pour chaque activité. Ces compétences sont listées dans l'annexe 2 du référentiel PASSI et ce pour chaque activité. Par exemple, un membre de l'équipe d'évaluation pourra être compétent pour évaluer les audits organisationnels et physiques et un autre membre de l'équipe d'évaluation pourra être compétent pour évaluer les audits de configuration.

Concernant les membres du jury pour les examens oraux, chaque membre doit :

- Avoir une formation ou un enseignement professionnel équivalent à un niveau universitaire.
- Avoir au moins 4 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 de nationalité française ou être résident français.
- Ne pas être salarié ou consultant d'un prestataire qualifié PASSI.
- Ne pas être salarié ou consultant d'un prestataire concurrent au prestataire candidat à la qualification.
- Avoir une bonne maitrise des bonnes pratiques et méthodologies d'audit décrites dans la norme ISO/CEI 19011 ainsi que du référentiel PASSI.
- Être sensibilisé à la législation en vigueur sur le territoire français et applicable aux différentes missions d'évaluation.
- 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 prester des activités d'évaluation.
- Avoir signé l'engagement d'impartialité et d'éthique de Certi-Trust.
- Avoir été approuvé par l'ANSSI.

Par ailleurs, les membres du jury doivent regrouper les compétences suivantes :

- Avoir au moins 1 an d'expérience dans le domaine de l'audit de sécurité des systèmes d'information.
- Au moins un membre qui possède deux années d'expérience dans chaque activité d'audit parmi lesquelles un candidat sera évalué.
- Avoir une connaissance approfondie de la législation en vigueur sur le territoire français et applicable aux différentes missions d'évaluation.

## 5.2. Planification de l'étude du dossier de candidature

Les objectifs de l'étude du dossier de candidature sont de :

- Prendre connaissance et revoir la documentation du prestataire candidat.
- S'assurer que l'ensemble des documents et preuves requis sont existants et sont appropriés par rapport au périmètre de certification demandé.
- Obtenir toutes les informations nécessaires permettant de planifier au mieux l'évaluation du siège ainsi que les examens écrits.

- S’assurer de la compréhension du prestataire candidat par rapport au processus de certification et des différentes étapes à venir.

Dans le cadre de la réalisation de l’étude du dossier de candidature, une liste des documents devant être revus doit être envoyée au prestataire candidat au PASSI :

- Portée de qualification
- Extrait K-Bis
- Convention d'audit type
- Rapport d'audit type
- Plan d'audit type
- Attestation de responsabilité
- Site Internet
- Formulaire de consentement
- Document de présentation
- Liste des auditeurs candidats
- Liste des responsables d'audit candidats
- Copie pour chaque auditeur ou responsable d’audit candidat de :
    - Formulaire de candidature
    - Curriculum Vitae
    - Une attestation de formation en technologie des systèmes d’information et communication et en audit (diplôme, attestation employeur, etc.)
    - Toute autre attestation de compétence (exemple : certificat)
    - La copie d’une pièce justifiant l’identité du candidat et comportant une photographie
    - Une attestation d’emploi ou DUE
- Attestation d'homologation
- Processus d'audit
- Procès-verbal de destruction type
- Procès-verbal de restitution type
- Procès-verbal de livraison type
- Attestation d'assurance

- Charte d'éthique
- Compte rendu de réunion de lancement type
- Compte rendu de réunion de clôture type
- Fiche d'autorisation type

Après réception et validation que la documentation est complète, Certi-Trust s'engage à terminer l'étude du dossier de candidature dans les 10 jours ouvrés.

## 5.3. Planification de l'évaluation du siège

Les objectifs de l'évaluation du siège sont de :

- Vérifier la mise en œuvre effective des politiques, procédures, modes opératoires, etc. définis par le prestataire candidat pour répondre aux exigences de la qualification.
- Confirmer qu'une analyse de risques a été réalisée par le prestataire candidat sur base des bonnes pratiques reconnues couvrant l'ensemble du périmètre du système d'information.
- S'assurer que des preuves sont disponibles afin de démontrer l'implémentation effective des processus du prestataire candidat en ligne avec ses politiques, objectifs et procédures.
- S'assurer que l'ensemble des critères et exigences de la qualification ont été considérés.

Cette évaluation fait l'objet d'un plan d'évaluation qui décrit le déroulement des opérations.

Après validation du dossier de candidature, l'évaluation du siège peut être réalisée, sauf exception justifiée, sous 20 jours ouvrés. Passé un délai de 6 mois après l'étude du dossier de candidature, l'ensemble du cycle de qualification doit être renouvelé.

## 5.4. Planification des examens écrits

Les examens écrits ont pour but de valider les compétences et le savoir-faire des auditeurs candidats.

Les examens écrits ont lieu, dans la mesure du possible, en même temps que l'évaluation du siège, mais peuvent être planifiés à tout moment après l'acceptation du dossier de candidature du prestataire. Chaque auditeur candidat doit avoir un dossier complet incluant le formulaire de candidature, un Curriculum Vitae, une attestation de formation en technologie des systèmes d'information et communication et en audit (diplôme, attestation employeur, etc.), toute autre attestation de compétence (exemple : certificat), la copie d'une pièce justifiant l'identité du candidat et comportant une photographie et une attestation d'emploi ou DUE.

L'examen écrit comporte :

- Une partie commune indépendante des activités choisies et portant sur les pratiques et la méthodologie pour la réalisation d'audit selon la norme ISO 19011. Les candidats doivent obtenir un minimum de 18 points sur 30.

- D'autant d'épreuves écrites que d'activités d'audit demandées (tests d'intrusion, audit de code source, audit de configuration, audit d'architecture et audit organisationnel et physique). Les candidats doivent obtenir un minimum de 20 points sur 40.

Des séances publiques sont prévues tous les 3 mois pour passer les examens écrits.

Dans le cas où un examen écrit sur demande est demandé, le prestataire candidat doit réaliser la demande pour au moins 4 examens et une session est programmée sous 10 jours ouvrés. Des exceptions pourront être acceptées avec accord du responsable des ventes et du responsable du programme d'audit.

## 5.5. Planification des examens oraux

Les examens oraux ont pour but de confirmer ou d'infirmer la compétence des auditeurs candidats.

Seuls les auditeurs candidats ayant eu au moins le minimum de points requis lors des examens écrits peuvent passer l'examen oral associé aux domaines réussis. Ainsi, un candidat peut passer un examen oral pour un ou plusieurs domaines, même s'il a échoué certains examens écrits.

Des séances sont prévues tous les 3 mois pour réaliser les examens oraux.

Dans le cas où un examen oral sur demande est demandé, le prestataire candidat doit réaliser la demande pour au moins 4 examens oraux et une session en présence du jury d'experts est programmée sous 30 jours ouvrés. Des exceptions pourront être acceptées avec accord du responsable des ventes et du responsable du programme d'audit.

L'examen oral consiste à évaluer devant un jury d'experts, dûment habilité par Certi-Trust, les éléments suivants :

- Approfondir les compétences démontrées lors des examens écrits et, notamment, les éléments où l'auditeur candidat a échoué ;

- Evaluer 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 ;

- Evaluer le comportement de l'auditeur candidat dans différentes situations caractéristiques d'un audit ;

## 5.6. Planification de l'évaluation terrain

L'évaluation terrain a pour objectif d'observer les activités d'audit du prestataire candidat sur les sites du client de ce dernier afin de valider :

- La réalisation des activités d'audit conformément aux politiques et procédures d'audit définies par le prestataire candidat ;

- Le déroulement du processus d'audit conformément aux exigences définies dans le référentiel PASSI.

Toutes les activités d'audit demandées en qualification ne font pas nécessairement l'objet d'une évaluation terrain lors de la qualification initiale. Il appartient à Certi-Trust de définir la meilleure façon d'observer un maximum d'activités d'audit chez un client du prestataire candidat et ensuite de répartir les évaluations terrains sur les audits de surveillance et/ou de renouvellement de manière à ce que toutes les activités dans la portée soient régulièrement observées.

Les modalités suivantes doivent être respectées :

- L'ensemble des activités d'audit inclus dans le périmètre de qualification doivent être observées. Les évaluations terrains peuvent être équitablement réparties entre l'évaluation initiale et l'évaluation de renouvellement sur le cycle de 3 ans.

- Au moins une évaluation terrain doit être réalisée sous 6 mois suivant le dernier jour de l'évaluation du siège du prestataire candidat.

- L'évaluation terrain s'effectue en conditions réels chez un client du prestataire candidat. Le prestataire doit proposer à Certi-Trust des clients potentiels qui acceptent la présence des évaluateurs durant l'audit ainsi que des dates où sont planifiées ces audits. Le choix de l'évaluation terrain est du ressort de Certi-Trust et est effectué parmi la liste des audits clients de l'organisme candidat. Si le prestataire confirme une date potentielle d'audit dans un horizon de 20 jours ouvrés, Certi-Trust garantie les dates de l'évaluation terrain. À moins de 20 jours ouvrés, la garantie ne s'applique pas.

## 5.7. Planification des évaluations de surveillance

Des évaluations de surveillance doivent être conduites au moins 18 mois après la décision de qualification du prestataire. Pour la première évaluation de surveillance suivant une qualification initiale, l'évaluation de surveillance doit être réalisée pas plus de 18 mois après le dernier jour de la première évaluation terrain réalisée.

Sur base des précédentes évaluations ou d'autres informations portées à la connaissance de Certi-Trust, des évaluations de surveillance pourront être décidées 6 ou 12 mois après la décision de qualification du prestataire.

## 5.8. Planification des évaluations de renouvellement

Des évaluations de renouvellement sont conduites tous les 3 ans après décision de qualification du prestataire.

## 5.9. Extension du périmètre

Toute extension du périmètre de qualification fera l'objet d'une évaluation additionnelle lors de la prochaine évaluation prévue dans le cas de l'ajout d'une activité d'audit ou de l'ajout d'un nouveau site.

Dans le cas de l'ajout d'auditeurs habilités à réaliser des audits pour le prestataire qualifié, une session peut être prévue lors de la prochaine évaluation du siège ou sur demande. Dans le cas d'une session dédiée, le prestataire candidat doit réaliser la demande pour au moins 4 examens et une session est programmée sous 30 jours ouvrés pour l'examen écrit. Des exceptions pourront être acceptées avec accord du responsable des ventes et du responsable du programme d'audit.

Des séances publiques sont prévues tous les 3 mois pour passer les examens écrits.

Concernant l'examen oral, le prestataire candidat doit réaliser la demande pour au moins 4 examens et une session en présence du jury d'experts est programmée sous 30 jours ouvrés. Des exceptions pourront être acceptées avec accord du responsable des ventes et du responsable du programme d'audit.

Des séances publiques sont prévues tous les 3 mois pour passer les examens oraux.

## 5.10. 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.

## 5.11. 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.

Pour chaque jeu d'examen, des questions sont choisies au hasard par le département administratif en charge de la préparation des jeux d'examen.

Les modalités suivantes doivent s'appliquer :

| **Audit d'infrastructure** | | **Audit de code source** | |
|---|---|---|---|
| **Thèmes** | **Nombre de questions minimum** | **Thèmes** | **Nombre de questions minimum** |
| Réseaux et protocoles | 12 | Couche applicative | 12 |
| Equipements et logiciels de sécurité | 12 | Attaque | 12 |

| Audit organisationnel et physique | | Principes et méthodologies d'audit | |
|---|---|---|---|
| **Thèmes** | **Nombre de questions minimum** | **Thèmes** | **Nombre de questions minimum** |
| Gestion des risques | 4 | Termes et définitions | 3 |
| Sécurité physique | 4 | Principes d'audit | 3 |
| Maitrise du cadre légal et normatif | 3 | Gestion d'un programme d'audit | 3 |
| Maitrise des domaines relatifs à l'organisation de la sécurité des systèmes d'information | 10 | Déclenchement de l'audit et préparation des activités d'audit | 3 |
| | | Réalisation des activités d'audit | 3 |
| | | Rapport d'audit, clôture de l'audit et suivi de l'audit | 3 |
| | | Compétence et évaluation des auditeurs | 3 |

| Audit de configuration | | Tests d'intrusion | |
|---|---|---|---|
| **Thèmes** | **Nombre de questions minimum** | **Thèmes** | **Nombre de questions minimum** |
| Réseaux et protocoles | 4 | Réseaux et protocoles | 4 |

| | | | |
|---|---|---|---|
| Equipements et logiciels de sécurité | 4 | Equipements et logiciels de sécurité | 4 |
| Systèmes d'exploitation | 4 | Systèmes d'exploitation | 4 |
| Techniques d'intrusion | 4 | Couche applicative | 4 |
| Couche applicative | 4 | Attaque | 4 |

Une revue est réalisée par le responsable du programme d'évaluation au moins tous les 6 mois pour assurer la pertinence des questions et alimenter la base de données.

# 6. Evaluation

## 6.1. Général

L'évaluation est effectuée conformément aux normes, guides et autres référentiels de qualification publiés par les autorités administratives nationales ou européennes désignées dans les textes législatifs ou réglementaires en vigueur et relatifs aux services d'audit de la sécurité des systèmes d'information.

L'évaluation consiste en l'examen des compétences et savoir-faire des auditeurs et en l'évaluation de l'organisation et des méthodes de travail du prestataire ainsi que des outils dont il dispose.

## 6.2. Etude du dossier de candidature

Pour réaliser l'étude du dossier de candidature, l'équipe d'évaluation doit compléter le rapport d'étude du dossier de candidature PASSI qui suit la trame d'audit établie par l'ANSSI, dont la dernière version est disponible sur la plateforme de gestion documentaire.

Pour chaque document ou preuve requis, l'équipe d'évaluation doit mentionner l'existence du document ou de la preuve et indiquer si la revue du document ou de la preuve a fait l'objet de commentaire.

L'équipe d'évaluation doit enfin conclure sur la recevabilité du dossier de candidature en statuant sur l'ensemble des documents et preuves revus.

Dans l'absence d'un document ou d'une preuve, l'équipe d'évaluation doit contacter le prestataire candidat et lui indiquer les pièces manquantes au dossier. Dans l'absence d'une réponse sous 20 jours ouvrés, l'étude du dossier de candidature devra être recommencée depuis le début.

Les modalités spécifiques de l'étude du dossier de candidature sont :

- L'étude du dossier de candidature peut être réalisée par un seul membre de l'équipe d'évaluation habilité ou plusieurs membres.

- L’étude du dossier de candidature peut être réalisée sur le site du prestataire candidat ou hors site.

- Dans le cas où l’étude du dossier de candidature est réalisée hors site, l’équipe d’évaluation doit se mettre d’accord avec le prestataire candidat sur le canal de communication à utiliser pour la transmission des documents et des preuves de façon sécurisée.

- Lors de la prise de connaissance et de la revue des documents et des preuves, des questions peuvent s’avérer nécessaires. Le cas échéant, l’équipe d’évaluation contacte le prestataire candidat afin de clarifier les points restés en suspens. Si nécessaire, une réunion spécifique peut être programmée.

- Après l’étude du dossier de candidature, le prestataire candidat sera informé par écrit par Certi-Trust de la recevabilité de son dossier de candidature. Certi-Trust notifiera également l’ANSSI de la recevabilité du prestataire et de son dossier de candidature afin que celui-ci soit enregistré sur la liste de l’ANSSI en tant que « prestataires d’audit de la sécurité des systèmes d’information en cours de qualification ».

## 6.3. Évaluation du siège

Pour réaliser l’évaluation du siège, l’équipe d’évaluation doit suivre le plan d’évaluation établi et se baser sur la trame d’audit établie par l’ANSSI pour couvrir l’ensemble des thématiques.

Un rapport d’évaluation du siège PASSI doit ainsi être complété dans un délai de 10 jours ouvrés après la fin des activités d’évaluation du siège.

Les preuves suivantes sont, entre autres, requises durant l’évaluation du siège afin de s’assurer de la mise en œuvre effective des processus du prestataire candidat :

- Echantillon de conventions d'audit
- Echantillon d'attestations de responsabilité
- Attestation d'assurance
- Analyse de risques
- Contrats de travail
- Echantillon de formulaires de consentement
- Matrice de compétences des auditeurs et des responsables d'audit
- Manuel qualité
- Echantillon de dossiers individuels des auditeurs et des responsables d'audit (contrat de travail, charte d'audit, règlement intérieur, fiches d'entretien individuel, etc.)
- Attestation d'homologation
- Analyse de risques du système d'information

- Politique de sécurité des systèmes d'information (PSSI)
- Procédures d'exploitation
- Plan des locaux
- Liste du personnel
- Contrat de surveillance
- Cartographie du système d'information
- Matrice des flux
- Echantillon de contrats de sous-traitance
- Echantillon de procès-verbaux de destruction
- Echantillon de procès-verbaux de restitution
- Echantillon de procès-verbaux de livraison
- Echantillon de rapports d'audit
- Echantillons de plans d'audit
- Document de présentation
- Base de données des méthodes, outils (logiciels et matériels) et techniques
- Echantillons de comptes rendus de réunions de lancement
- Echantillons de supports de réunions de lancement
- Echantillons de comptes rendus de réunions de clôture
- Echantillons de supports de réunions de clôture
- Echantillon de fiches d'autorisation
- Règlement intérieur
- Echantillon de postes de travail bureautiques
- Echantillon de postes de travail nomades
- Echantillon des licences des outils logiciels
- Echantillon d'enregistrements de plaintes

### *1.1.4. Réunion d'ouverture*

Une réunion d'ouverture doit être tenue et les participants enregistrés. L'objectif de la réunion d'ouverture est de fournir une description succincte à le prestataire candidat du déroulement des activités d'évaluation du siège. La réunion d'ouverture doit inclure :

- Présentation des participants et une description succincte de leurs rôles ;
- Confirmation du périmètre de la certification ;
- Confirmation du plan d'évaluation (y compris le type et le périmètre de l'évaluation, les objectifs et les critères), des modifications éventuelles et des autres dispositions importantes, comme la date et l'heure de la réunion de clôture, des réunions intermédiaires entre l'équipe d'évaluation et la direction du prestataire candidat ;
- Confirmation des circuits de communication officiels entre l'équipe d'évaluation et le prestataire candidat ;
- Confirmation de la disponibilité des ressources et de la logistique nécessaire à l'équipe d'évaluation ;
- Confirmation des points relatifs à la confidentialité ;
- Confirmation des procédures d'hygiène, d'urgence et de sécurité pour l'équipe d'évaluation ;
- Confirmation de la disponibilité, des rôles et de l'identité des guides et des observateurs ;
- Méthode utilisée pour rendre compte des constats d'évaluation y compris leur classement ;
- Informations sur les conditions dans lesquelles il peut être mis fin à l'évaluation prématurément ;
- Confirmation que le responsable de l'équipe d'évaluation et l'équipe d'évaluation, qui représentent le prestataire de certification, sont responsables de l'évaluation et de l'exécution du plan d'évaluation, y compris des activités et des cheminements d'évaluation ;
- Confirmation du statut des constats de la revue ou de l'évaluation précédente, le cas échéant ;
- Méthodes et procédures utilisées pour conduire l'évaluation sur la base d'un échantillonnage ;
- Confirmation de la langue à utiliser pendant l'évaluation ;
- Confirmation du fait que, pendant l'évaluation, le prestataire candidat sera tenu informé de l'avancement de l'évaluation ;
- Opportunité du prestataire candidat de poser des questions.

### *1.1.5. Évaluation du siège*

Lors de l'évaluation du siège, l'équipe d'évaluation doit s'assurer que l'ensemble des exigences listées dans la trame d'audit sont couvertes. Ces exigences couvrent notamment les aspects suivant :

- L'organisation et la structure du prestataire candidat ;
- Les dispositions relatives à l'éthique et l'impartialité ;
- La gestion de la qualité et des compétences des auditeurs et des responsables d'audit et son suivi ;
- Les dispositions relatives à la gestion des employés (recrutement, processus disciplinaire) ;
- Processus d'audit incluant les modalités relatives à la convention d'audit, les modalités de sous-traitance, le respect de la réglementation et de la législation, les dispositions relatives aux documents de l'organisation auditée, les dispositions relatives à la détermination de l'équipe d'audit, les méthodes, outils et techniques utilisés, la planification de l'audit, le déroulement de l'audit en fonction du type d'activité, le rapport d'audit, etc. ;
- L'homologation du système d'information au niveau « Diffusion Restreinte » ;
- La Politique de sécurité du système d'information de niveau Diffusion Restreinte ;
- Les mesures relatives à la sécurité physique ;

- Les mesures relatives à la sécurité logique du système d'information de niveau Diffusion Restreinte ;
- Les mesures relatives à la sécurité des postes bureautiques et nomades ;
- Les mesures relatives à la sécurité des documents et des médias de stockage.

### *1.1.6. La réunion de clôture*

Une réunion de clôture doit être tenue et les participants enregistrés. L'objectif de la réunion de clôture est de présenter les conclusions de l'évaluation, y compris les constats relatifs à la qualification du prestataire candidat. La réunion de clôture doit inclure :

- Notifier au prestataire candidat que les preuves d'évaluation obtenues étaient fondées sur un échantillon d'informations, introduisant, de ce fait, un élément d'incertitude ;
- La méthode et le délai utilisés pour rendre compte, y compris le classement des constats d'évaluation ;
- Le processus du prestataire de certification pour le traitement des non-conformités, incluant toutes les conséquences relatives à la qualification du prestataire candidat ;
- Le délai dans lequel le prestataire candidat doit soumettre un plan de correction et une action corrective pour toute non-conformité identifiée pendant l'évaluation ;
- Les activités post-évaluation du prestataire de certification ;
- Des informations sur les processus de traitement des plaintes et des appels.
- Planifier la suite des activités d'évaluation PASSI, dont les examens oraux et l'évaluation terrain.

## 6.4. Examens écrits

Chaque examen écrit doit être surveillé par une personne désignée et habilitée par Certi-Trust.

L'examen écrit se déroule comme suit :

- La personne en charge de la surveillance vérifie l'identité de chaque auditeur candidat, lui fait signer la liste de présence et lui donne le(s) examen(s) écrit(s) qui ont été demandés dans le formulaire de candidature.

- Lorsque chaque auditeur candidat a reçu ses examens écrits, la personne en charge de la surveillance rappelle les règles à respecter dans le cadre de l'examen (interdiction d'utiliser un appareil mobile, interdiction de communiquer avec les autres auditeurs candidats, interdiction de quitter la salle).

- La personne en charge de la surveillance autorise les auditeurs candidats à débuter l'examen écrit.

- La personne en charge de la surveillance informe les auditeurs candidats de la fin du délai imparti pour compléter l'examen écrit et récupère les copies complétées.

- La personne en charge de la surveillance range les copies complétées dans une enveloppe dédiée et transmet l'enveloppe au responsable du programme PASSI.

- Une correction des copies (anonymisées) est réalisée par un membre de l'équipe d'évaluation.

- Un membre de l'équipe administration envoie les résultats des examens écrits à chaque auditeur candidat dans un délai de 10 jours ouvrés suivant l'examen.

- En cas de succès, Certi-Trust invitera le candidat à s'inscrire aux examens oraux. En cas d'échec, un auditeur peut repasser à nouveau l'examen écrit après un délai minimal de 2 semaines.

## 6.5. Examens oraux

Chaque examen oral est réalisé en présence d'au moins 3 membres habilités par Certi-Trust à faire partie du jury d'évaluation. A chaque session, le jury se concerte pour nommer un responsable du jury. Le responsable du jury est chargé de compléter le rapport sur le déroulement de la session d'examens ainsi que de transmettre à Certi-Trust les fiches d'évaluation.

Les membres du jury doivent avoir l'expertise, de manière regroupée, pour chaque activité d'audit dont le niveau de compétence devra être évalué sur la session.

Une copie des examens écrits des auditeurs candidats doit être transmise aux membres du jury.

L'examen oral se déroule comme suit :

- Chaque auditeur candidat se présente tour à tour face au jury.

- Une session est réalisée pour chaque activité d'audit pour laquelle l'auditeur s'est porté candidat.

- Les membres du jury remplissent leur grille d'évaluation de manière indépendante.

- Les grilles d'évaluation sont envoyées au responsable du programme d'audit chez Certi-Trust par le responsable du jury à la fin de la session d'examen.

- La moyenne des notes attribuées dans chaque catégorie est réalisée pour chaque auditeur candidat et pour chaque activité d'audit. Si la note générale dépasse ou est égale à 4.5, l'auditeur candidat sera qualifié.

- Le département administratif envoie les résultats des examens oraux à chaque auditeur candidat dans un délai de 10 jours ouvrés suivant l'examen.

- En cas de succès, un certificat de compétence sera transmis à chaque auditeur. En cas d'échec, un auditeur peut repasser à nouveau l'examen après un délai minimal de deux semaines.

## 6.6. Evaluation terrain

Lors de l'évaluation terrain, le(s) membre(s) de l'équipe d'évaluation doit participer au minimum à :

- La réunion d'ouverture

- Une journée complète d'activité d'audit
- La réunion de clôture

Le(s) membre(s) de l'équipe d'évaluation doit observer l'auditeur ou les auditeurs afin de s'assurer notamment de :

- Le respect de la charte d'éthique
- L'établissement de scénarios de menace suivant les vulnérabilités détectées
- Le respect de la PSSI du prestataire qualifié
- Le respect des bonnes pratiques en matière d'audit telles qu'édictées dans ISO 19011
- Le respect du référentiel PASSI
- Le respect des processus d'audit du prestataire qualifié

L'évaluation terrain fait l'objet d'un rapport qui est soumis au prestataire candidat dans un délai de 5 jours ouvrés à partir du dernier jour de l'évaluation terrain. En plus de ce rapport, une fiche d'évaluation sur le(s) auditeur(s) ayant participé à l'audit PASSI est réalisée ainsi que la trame d'audit PASSI de l'ANSSI.

## 6.7. Evaluation de surveillance

L'évaluation de surveillance consiste à réaliser une évaluation du siège afin de valider les éléments suivants :

- Le respect de l'ensemble des exigences applicables au prestataire qualifié ;
- La mise en œuvre des actions correctives pour lever les non-conformités de l'évaluation précédente ;
- Les éventuelles modifications apportées au prestataire qualifié, aux méthodes et aux ressources ;
- Le respect des exigences stipulées par Certi-Trust ;
- L'utilisation de la marque ;
- Les réclamations et plaintes à l'encontre du prestataire ;
- Le maintien des compétences des auditeur ;
- Le maintien à niveau des méthodes, outils et techniques utilisés.

Les modalités suivantes s'appliquent :

- 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.

En fonction des résultats de ces évaluations, la qualification peut être maintenue sans réserve, maintenue sous réserve, suspendue ou retirée. L'évaluation de surveillance fait l'objet d'un rapport d'évaluation.

## 6.8. Evaluation de renouvellement

L'évaluation de renouvellement consiste à réaliser une évaluation du siège afin de valider les éléments suivants :

- Vérifier la mise en œuvre toujours effective des politiques, procédures, modes opératoires, etc. définis par le prestataire candidat pour répondre aux exigences de la qualification.
- Le respect de l'ensemble des exigences applicables au prestataire qualifié ;
- La performance du système de management sur le cycle de qualification ;
- La mise en œuvre des actions correctives pour lever les non conformités de l'évaluation précédente ;
- Les éventuelles modifications apportées au prestataire qualifié, aux méthodes et aux ressources ;
- Le respect des exigences stipulées par Certi-Trust ;
- L'utilisation de la marque ;
- Les réclamations et plaintes à l'encontre du prestataire ;
- Le maintien des compétences des auditeur ;
- Le maintien à niveau des méthodes, outils et techniques utilisés ;
- S'assurer que l'ensemble des critères et exigences de la qualification sont toujours considérés.

Les modalités suivantes s'appliquent :

- 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 n'est pas renouvelée.
- Dans le cas où la qualification n'est pas renouvelée, une nouvelle demande enregistrée au maximum 6 mois après la décision de non-renouvellement fera l'objet d'une nouvelle évaluation du siège et des évaluations terrains. Passé ce délai, le cycle complet d'évaluation doit être réalisé.

Concernant le renouvellement de la qualification des auditeurs, chaque auditeur doit passer à nouveau les examens écrits puis les examens oraux sur les activités d'audit pour lesquelles il a été préalablement qualifié afin de renouveler sa qualification pour 3 ans.

## 6.9. Evaluation de suivi

L'objectif des évaluations de suivi est de vérifier si les non-conformités majeures relevées lors d'une précédente évaluation ont bien été clôturées. Le temps

nécessaire pour l'évaluation de suivi dépend du nombre et de la nature des non-conformités majeures soulevées.

L'évaluateur principal détermine un plan et le type de suivi qui est nécessaire de mettre en œuvre (sur site ou hors site). Une évaluation de suivi hors site peut être réalisée dans le cas où des preuves documentées peuvent être envoyées à l'évaluateur principale et que ces preuves sont des éléments suffisants pour s'assurer de la clôture effective de la non-conformité majeure.

Dans le cas où l'évaluation de suivi ne peut être réalisée sous 3 mois après l'évaluation du siège, une nouvelle évaluation du siège partielle doit être réalisée (au minimum la moitié du temps prévu pour l'évaluation du siège initiale). Si l'évaluation de suivi n'est pas réalisée sous 6 mois, un cycle complet d'évaluation doit être réalisé à nouveau.

### 6.10. Evaluation spécifique

Des évaluations spécifiques peuvent être réalisées dans le cas où un changement significatif intervient chez le prestataire qualifié ou en fonction de plaintes ou d'appels réalisées contre le prestataire qualifié qui nécessiteraient une évaluation spécifique ou toute autre raison qui amènerait Certi-Trust à juger de la nécessité de réaliser une évaluation spécifique.

Le responsable du programme d'évaluation doit évaluer le besoin de réaliser ce type d'évaluation ainsi que sa durée en fonction des raisons qui ont amené Certi-Trust à réaliser cette évaluation.

Avant de réaliser cette évaluation spécifique, le prestataire qualifié doit formaliser son accord par écrit.

Un rapport d'évaluation doit être réalisé.

### 6.11. Evaluation à court préavis

Des évaluations à court préavis peuvent être nécessaires afin d'investiguer suite à une plainte ou un appel notamment. Dans tous les cas, le prestataire qualifié sera notifié à l'avance des conditions selon lesquelles l'évaluation à court préavis sera menée et est tenu de proposer des dates d'audit sous 15 jours. Une attention particulière devra être donnée à la sélection de l'équipe d'évaluation.

# 7. Non-conformité et actions correctives

### 7.1. Général

Chaque non-conformité soulevée doit être référencée par rapport à la clause du référentiel PASSI où l'absence de conformité a été détectée. Quand un nombre important de non-conformités mineures est soulevé par rapport à une clause du référentiel PASSI, l'évaluateur principal doit éventuellement considérer l'écart comme une non-conformité majeure.

Afin de clôturer les non-conformités, le prestataire et l'évaluateur principal doivent se mettre d'accord sur l'action curative à mener ainsi que l'action corrective

permettant de prévenir contre une future occurrence. Ces actions devront être vérifiées par l'évaluateur.

Concernant les observations et les opportunités d'amélioration, le prestataire est libre de mettre en place ou non une action permettant de clôturer le point soulevé. Pour les observations, une attention particulière devra toutefois être donnée à l'évolution de la faiblesse identifiée afin de s'assurer que le point ne doit pas être remonté en tant que non-conformité mineure.

## 7.2. Catégorisation des constats

### *1.1.7. Non-conformité majeure*

Une non-conformité majeure correspond à l'incapacité d'implémenter ou de se conformer à une ou plusieurs clauses du référentiel PASSI. Cette incapacité se traduit par un doute significatif sur le fait que les mesures et contrôles mis en place permettent de répondre à une exigence du référentiel ce qui remet en cause le système dans son ensemble.

### *1.1.8. Non-conformité mineure*

Une non-conformité mineure correspond à une faiblesse sur quelques aspects d'une clause du référentiel PASSI qui se traduit par un doute sur le fait que les mesures et contrôles mis en place permettent de répondre entièrement à une exigence du référentiel ce qui remet en cause un processus au sein du système.

### *1.1.9. Observation*

Une observation correspond à une faiblesse sur un aspect d'une clause du référentiel PASSI qui pourrait se traduire dans le futur par un doute sur le fait que les mesures et contrôles mis en place permettent de répondre entièrement à une exigence du référentiel ce qui remet en cause un processus au sein du système. Ce constat doit être considéré comme un point d'attention pour le prestataire dans le futur.

### *1.1.10. Opportunité d'amélioration*

Une opportunité d'amélioration correspond à une possibilité pour le prestataire d'améliorer l'efficacité d'un processus en place. Ce constat ne remet pas en cause la conformité ou l'existence des contrôles et mesures au sein d'un processus.

### *1.1.11. Rapport de non-conformité*

| **RAPPORT DE NON-CONFORMITE** | | | |
|---|---|---|---|
| **A compléter par Certi-Trust** | **DATE** | **Société** | **NC ID** |
| | A compléter | A compléter | A compléter |
| | | **Norme/référentiel :** A compléter | |
| | **Processus / thème :** | A compléter | |
| | **Exigence de la norme ou du référentiel :** A compléter | | **Clause :** A compléter |
| | **Description de la non-conformité** | | |

<table>
<tr><td rowspan="5"></td><td colspan="4">A compléter</td></tr>
<tr><td>Niveau (Majeure / Mineure)</td><td>Evaluateur principal</td><td>Evaluateur</td><td>Représentant du prestataire</td></tr>
<tr><td>A compléter</td><td rowspan="3">A compléter</td><td rowspan="3"></td><td rowspan="3">A compléter</td></tr>
<tr><td>A compléter avant</td></tr>
<tr><td>A compléter</td></tr>
<tr><td rowspan="6">A compléter par le prestataire</td><td colspan="4">Analyse de la cause (Qu’est-ce qui n’a pas fonctionné permettant à la non-conformité de se produire ?)</td></tr>
<tr><td colspan="4">A compléter</td></tr>
<tr><td colspan="4">Action curative et action corrective (Ce qui est mis en place pour résoudre le problème et pour prévenir son occurence)</td></tr>
<tr><td colspan="4">Action curative : A compléter<br><br>Action corrective : A compléter</td></tr>
<tr><td rowspan="2"></td><td>Date</td><td colspan="2">A compléter</td></tr>
<tr><td>Représentant du prestataire</td><td colspan="2">A compléter</td></tr>
<tr><td rowspan="3">A compléter par Certi-Trust</td><td rowspan="2">Vérification de l’action curative et de l’action corrective (ou de son plan)</td><td>Date</td><td>Statut</td><td>Evaluateur principal</td></tr>
<tr><td>A compléter</td><td>A compléter</td><td>A compléter</td></tr>
<tr><td>Commentaire de l’évaluateur (incluant les preuves vérifiées)</td><td colspan="3">A compléter</td></tr>
</table>

### *1.1.12. Suivi et clôture des non-conformités majeures*

Des actions curatives doivent être menées immédiatement par le prestataire et Certi-Trust doit être notifiée sous 30 jours des actions correctives envisagées et initiées.

Une évaluation de suivi sera menée sous 90 jours afin de vérifier les actions menées, l’efficacité de celles-ci et de déterminer si la qualification peut être octroyée ou confirmée.

La clôture des non-conformités majeures doit être documentée dans le rapport de non-conformité.

Si la non-conformité majeure ne peut être clôturée sous 90 jours, le processus d’évaluation est finalisé et la qualification n’est pas octroyée.

Dans le cas d'une non-conformité majeure soulevée lors d'une évaluation de surveillance ou de renouvellement ne pouvant être clôturée sous 90 jours, la qualification doit être suspendue et éventuellement retirée.

#### *1.1.13. Suivi et clôture des non-conformités mineures*

Des actions curatives doivent être menées immédiatement par le prestataire et Certi-Trust doit être notifiée sous 30 jours des actions correctives envisagées et initiées.

Une évaluation de suivi sera menée lors de la prochaine évaluation de surveillance ou de renouvellement, si le plan d'action a été jugé efficace, afin de vérifier les actions menées et l'efficacité de celles-ci. Dans le cas contraire, la non-conformité mineure doit être considérée à présent comme une non-conformité majeure.

La clôture des non-conformités mineures doit être documentée dans le prochain rapport d'évaluation.

# 8. Décision de qualification

## 8.1. 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.

## 8.2. Revue technique et décision de qualification

#### *1.1.14. Etape 1*

L'étape 1 consiste à une revue administrative. L'ensemble des documents sont revues par un membre du département administratif ou par le Certification Manager afin de s'assurer qu'ils sont entièrement complétés. La checklist de revue des rapports d'évaluation est utilisée à cet effet.
Dans le cas où un problème est détecté, une note (appelée Deviation Note) est émise et notifiée au responsable de l'équipe d'évaluation et au responsable du programme pour analyse et action.

#### *1.1.15. Etape 2*

L'étape 2 consiste à une revue technique. Les rapports d'évaluation et la checklist de revue sont soumis au responsable du programme d'évaluation ou au Certification Manager pour revue technique afin de s'assurer que les informations fournies par l'équipe d'évaluation sont suffisantes par rapport aux exigences du référentiel et du programme (incluant par exemple les preuves revues pour clôturer les non-conformités).
Dans le cas où un problème est détecté, une note (appelée Deviation Note) est émise et notifiée au responsable de l'équipe d'évaluation pour analyse et action.

### *1.1.16. Etape 3*

L'étape 3 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 et 2 avant de prendre sa décision et de décider de la qualification ou non du prestataire.
Cette décision est formalisée sur la checklist de revue.
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 de Certi-Trust doit revoir les rapports et prendre la décision de qualification. Ce changement est tracé sur la checklist de revue.

### *1.1.17.Etape 4*

L'étape 4 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.

## 8.3. Préparation du certificat et envoi

Des certificats 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 le certificat :

- Sélectionner le bon modèle de certificat.
- 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 certificat 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 le certificat 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'un certificat. Le certificat 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, le certificat doit être émis à nouveau au Directeur qui doit signer le certificat. Une signature électronique ou une image peuvent être utilisées.

Le certificat 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.

Le certificat est conservé dans le dossier du prestataire.

## 8.4. Qualification des auditeurs et attestation de compétence

Pour réussir leurs **examens écrits**, chaque auditeur candidat doit :

- Obtenir un minimum de 18 points sur 30 sur la partie commune relative aux méthodologies d'audit.

- Obtenir un minimum de 20 points sur 40 sur chaque activité d'audit demandé.

Les résultats sont fournis à l'auditeur candidat dans un délai de 10 jours ouvrés.

Pour réussir leurs **examens oraux**, chaque auditeur candidat doit :

- Obtenir au moins la moyenne sur chaque session demandée.

Les points sont calculés suivant les notes attribuées par chaque membre du jury. La moyenne de ces notes est réalisée sur chaque thématique évaluée. La moyenne générale est ensuite calculée afin de décider de la qualification ou non de l'auditeur sur l'activité d'audit.

Les résultats sont fournis à l'auditeur candidat dans un délai de 10 jours ouvrés.

Après réussite des examens écrits et oraux pour une activité d'audit, l'auditeur reçoit également une attestation de compétence. Celle-ci contient :

- Nom et prénom de l'auditeur

- Prestataire PASSI auquel il est rattaché
- Périmètre de qualification (activité(s) d'audit)

L'attestation de compétence est valable 3 ans à compter de la date de la session pour l'examen oral. Afin de renouveler sa qualification, l'auditeur doit à nouveau passer les examens écrits et oraux.

## 8.5. Changement dans le certificat

Le prestataire peut demander un changement dans le certificat pour les raisons suivantes :

- Changement dans l'actionnariat ou la propriété
- Changement de nom du prestataire
- Changement de siège social
- Modification du périmètre (activités d'audit, site)

Dans le cas d'une modification du périmètre, le processus décrit dans le chapitre 4.6 doit être suivi avant toute modification.

Dans le cas d'un changement de nom ou de siège social, le prestataire doit fournir un registre (extrait K-Bis) attestant du changement. Le certificat peut ensuite être émis.

## 8.6. Publicité de la qualification

La base de données des prestataires qualifiées doit être tenue à jour chez Certi-Trust. L'ANSSI tient à jour sur son site internet la liste officielle des prestataires qualifiées.

En cas de changements du statut du prestataire (suspension, retrait, extension, radiation), Certi-Trust doit notifier dans les plus brefs délais l'ANSSI.

Le statut de qualification d'un prestataire peut être demandé par email et une réponse doit être fournie.

## 8.7. Suspension, retrait ou annulation de la qualification

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

- Actions curatives et actions correctives non implémentées dans le temps imparti.
- Utilisation impropre du certificat, du logo ou tout autre symbole au regard de la Politique d'utilisation de la marque de certification de Certi-Trust.
- Le prestataire a manqué à ses obligations financières par rapport à Certi-Trust.

- Le prestataire a demandé à annuler sa qualification.
- Le prestataire n'a plus suffisamment de compétence à disposition en nombre suffisant dans une activité d'audit.
- Le prestataire a enfreint les conditions contractuelles ou le Règlement de Qualification de Certi-Trust.
- Le prestataire n'est pas capable ou ne veut pas assurer la conformité avec les versions revues du référentiel.
- Une plainte sérieuse ou un nombre important de plaintes ont été faites et indiquent que le prestataire ne maintient pas son système de management.
- Le prestataire n'a pas permis à Certi-Trust de réaliser les évaluations de surveillance suivant la fréquence définie.
- Le prestataire n'a pas presté d'audit sous qualification PASSI depuis sa dernière évaluation.

Le Certification Manager doit décider des actions à mener, en accord avec le responsable du programme d'évaluation. Si des actions sont attendues de la part du prestataire, une lettre formelle doit être envoyée au prestataire en indiquant un délai de réponse de 2 semaines et des échéances précises pour chaque action.

Si la réponse du prestataire est satisfaisante et que les actions ont été menées en conséquence, une lettre indiquant la clôture du problème doit être envoyée au prestataire.

Dans l'absence de réponse sous 2 semaines ou si la réponse n'est pas satisfaisante ou si les actions n'ont pas été menées, une décision de suspension ou de retrait doit être décidée et être notifiée formellement au prestataire.

Le prestataire a le droit de faire appel pour toutes les décisions réalisées par Certi-Trust. Une copie de la procédure d'appel doit être fournie sur demande.

Le département administratif est responsable de mettre à jour la base de données des prestataires qualifiées suivant les décisions de suspension, retrait ou d'annulation.

Les attestations de compétences peuvent être retirées si les auditeurs ne respectent pas les engagements pris lors de leur inscription et décrits dans le formulaire de candidature.