LE PREMIER MINISTRE

REPUBLIQUE TOGOLAISE
Travail-Liberté-Patrie

ARRETE N° 2025-002 /PMRT
portant adoption modèle de qualification des prestataires de service de confiance en cybersécurité

LE PREMIER MINISTRE,

Vu la constitution du 06 mai 2024 ;

Vu la loi n° 2018-026 du 07 décembre 2018 sur la cybersécurité et la lutte contre la cybercriminalité modifiée par la loi n° 2022-009 du 24 juin 2022 ;

Vu le décret n° 2019-022/PR du 13 février 2019 portant attributions, organisation et fonctionnement de l'Agence nationale de la cybersécurité ;

Vu l'arrêté n° 2022-040/PMRT du 29 juin 2022 portant adoption des règles de cybersécurité en République togolaise ;

Vu le décret n° 2022-09/PR du 25 août 2022 relatif à la qualification des prestataires de services de confiance de cybersécurité et des produits de sécurité et à l'agrément des centres d'évaluation ;

Vu le décret n° 2024-040/PR du 1er août 2024 portant nomination du Premier ministre ;

Vu le décret n° 2024-041/PR du 20 août 2024 portant composition du gouvernement ;

Vu le procès-verbal de la réunion du Comité stratégique de l'Agence nationale de la cybersécurité (ANCy), en sa séance du 02 décembre 2024 ;

ARRETE :

Article 1er : Objet

Le présent arrêté porte adoption du modèle de qualification des prestataires de service de confiance en cybersécurité en République togolaise.

Article 2 : Application

Les ministres, chacun en ce qui le concerne, veillent à l'application des dispositions du présent arrêté par les administrations et les opérateurs de services essentiels (OSE) relevant de leur ressort.

Article 3 : **Exécution**

Le Directeur général de l'Agence nationale de la cybersécurité (ANCy), est chargé de l'exécution du présent arrêté qui sera publié au Journal officiel de la République togolaise.

Fait à Lomé, le 31 JAN 2025

Le Premier ministre

SIGNE

Victoire S. TOMEGAH-DOGBE

Pour ampliation,
Le Ministre,
Secrétaire général du Gouvernement

Christian Eninam TRIMUA

ANCy
Agence Nationale de la Cybersécurité

RÉPUBLIQUE TOGOLAISE

MODELE DE QUALIFICATION

Prestataires de Service de Confiance en Cybersécurité (PSCC)

Version 1.0 du 31 JAN 2025

www.ancy.gouv.tg

Premier Ministre	
Comité Stratégique	Agence Nationale de la Cybersécurité (ANCy)

HISTORIQUE DES VERSIONS			
DATE	VERSION	EVOLUTION DU DOCUMENT	REDACTEUR
31/01/2025	1.0	Première version applicable	ANCy

Les commentaires sur le présent document sont à adresser à :

Agence Nationale de la Cybersécurité

63, Boulevard du 13 janvier, Nyékonakpoè

07 BP 7878 Lomé – TOGO

Téléphone : +228 70 60 60 83 / 97 52 58 58

secretariat.ancy@ancy.gouv.tg

Table des matières

FICHE SYNTHETIQUE

1. Définition et objectifs du modèle

Le modèle de qualification des prestataires de services de confiance en cybersécurité vise à identifier et encadrer les entités habilitées à fournir des services critiques dans le domaine de la cybersécurité. Ces services incluent la détection des incidents, la réponse aux incidents, l'intégration de solutions sécurisées, et d'autres prestations spécialisées.

2. Objectifs principaux

- **Renforcer la confiance** des parties prenantes (administrations, entreprises, OSE) envers les prestataires ;
- **Garantir la qualité et la sécurité** des services rendus ;
- **Encourager le développement des compétences locales** et l'hébergement national des infrastructures critiques.

3. Types de prestataires visés

Les prestataires ciblés par ce modèle incluent :

a. **Prestataires de Détection des Incidents de Sécurité (PDIS)** : chargés de surveiller les réseaux et de détecter les menaces en temps réel ;

b. **Prestataires de Réponse aux Incidents de Sécurité (PRIS)** : spécialisés dans la gestion des incidents, la remédiation et le rétablissement des services après une cyberattaque ;

c. **Prestataires d'Intégration, d'Administration et de Maintenance Sécurisées (PIAMS)** : responsables de l'implémentation, de la configuration et de la maintenance des solutions et systèmes de cybersécurité ;

d. **Prestataires d'Accompagnement et de Conseil en Cybersécurité (PACC)** : Fournissent des services de conseil stratégique, d'audit, de gestion des risques et d'élaboration de politiques de sécurité adaptées aux besoins des clients ;

e. **Prestataires d'Audit de la Sécurité des Systèmes d'Information (PASSI)** : spécialisés dans la réalisation d'audits techniques et organisationnels des systèmes d'information. Leur rôle est de

détecter les vulnérabilités, évaluer les niveaux de conformité aux standards de sécurité, et proposer des recommandations pour améliorer la résilience des infrastructures numériques.

4. Exigences générales pour la qualification

Pour être qualifiés, les prestataires doivent satisfaire aux conditions suivantes :

Critères administratifs et organisationnels

- **Enregistrement légal** : être une entité dûment enregistrée en tant que personne morale ou physique ;
- **Localisation** : héberger tous les équipements et données associés à leurs services au Togo, sauf dérogation approuvée ;
- **Personnel technique** : employer 100 % de personnel togolais pour les activités techniques.

Critères techniques

- Démontrer une **expertise avérée** dans le domaine de prestation déclaré ;
- Utiliser des outils et méthodologies conformes aux normes internationales (ISO/IEC 27001, 27035, etc.) ;

Critères éthiques

- Adhérer à un **code de déontologie**, garantissant la confidentialité, l'impartialité et la transparence dans leurs opérations ;
- S'engager à signaler tout conflit d'intérêt ou limitation technique.

Critères de continuité et de sécurité

- Garantir la **résilience opérationnelle** et la continuité des services, même en cas de crise ;
- Respecter les exigences de sécurité nationale définies par l'ANCy.

5. Processus de qualification

Le processus de qualification suit les étapes suivantes :

Soumission de la demande

- Le prestataire soumet un dossier de candidature comportant :
    - Les documents administratifs (registre de commerce, statuts, etc.) ;
    - Une description des services et infrastructures proposés ;
    - Les qualifications et certifications des employés.

Évaluation documentaire

- L'ANCy examine la complétude du dossier et vérifie la conformité aux critères requis.

Audit sur Site

- Une inspection est effectuée pour :
    - Évaluer les infrastructures techniques ;
    - S'assurer du respect des standards de sécurité et de confidentialité.

Décision de qualification

- À l'issue de l'évaluation, l'ANCy :
    - Accorde la qualification pour une durée de 3 ans ;
    - Rejette la demande, en précisant les motifs.

Suivi et renouvellement

- Les prestataires qualifiés sont soumis à un suivi périodique pour vérifier leur conformité continue ;
- Ils doivent renouveler leur qualification avant son expiration.

6. Obligations des prestataires qualifiés

Une fois qualifiés, les prestataires doivent :

- Respecter le **champ d'application défini dans leur qualification** ;
- Maintenir leurs infrastructures et compétences au niveau requis ;
- Informer immédiatement l'ANCy de tout changement pouvant affecter leur qualification (ex. : changement d'outils, perte de certification, etc.) ;
- Collaborer aux audits réguliers réalisés par l'ANCy.

7. Bénéfices de la qualification

Pour les prestataires :

- **Renforcer leur crédibilité** auprès des clients ;
- Accéder au marché sensible des OSE nécessitant des services qualifiés.

Pour les clients (OSE, administrations, entreprises) :

- Bénéficier de **services fiables et conformes** aux standards de sécurité ;
- Réduire les risques liés à l'externalisation des activités de cybersécurité.

Pour l'État :

- Assurer la **protection des infrastructures critiques** et des données sensibles ;
- Promouvoir le développement des compétences locales en cybersécurité.

Conclusion

Le modèle de qualification des prestataires de services de confiance en cybersécurité établit un cadre essentiel pour structurer l'écosystème national de cybersécurité. En fixant des exigences rigoureuses et des processus de validation, il contribue à la fois à renforcer la souveraineté numérique du Togo et à garantir une protection efficace contre les cybermenaces.

ANCy
Agence Nationale de la Cybersécurité
Tél: 97 52 58 58 / 70 60 60 83 Lomé - TOGO

1. INTRODUCTION GENERALE

1.1. OBJECTIF DU MODELE ET DOMAINE D'APPLICATION

Le présent document présente le cadre de référence pour la qualification des Prestataires de services de confiance en cybersécurité, notamment les étapes du processus de qualification d'un service par l'ANCy. Ce Modèle a pour vocation de cadrer et organiser les activités de qualification selon une politique, des procédures et des documents de travail bien déterminés.

Ce document s'applique à toutes les demandes de qualification pour les services, ci-après, qui s'inscrivent dans le cadre de l'application des documents de référence :

- D'audit de la sécurité des systèmes d'information ;
- De détection des incidents de sécurité ;
- De réponse aux incidents de sécurité ;
- D'intégration, d'administration et de maintenance sécurisées ;
- D'accompagnement et conseils en cybersécurité.

Les Prestataires de services de confiance en cybersécurité sont tenus de respecter les règles générales qui leur sont imposées en leur qualité de professionnels, notamment celles inscrites dans la législation nationale, le code d'éthique et les bonnes pratiques.

1.2. DOCUMENTS DE REFERENCE

La qualification des services de confiance en cybersécurité au Togo est encadrée par les textes listés ci-dessous de manière non-exhaustive, désignés ci-après les « Documents de référence ».

Le présent Modèle de qualification s'applique en complément des Documents de référence dont il n'exclut pas l'application. Ce document n'exclut pas non plus l'application des règles générales imposées aux Prestataires en leur qualité de professionnels, et notamment leur devoir de conseil.

1.2.1. Textes législatifs et règlementaires

- La loi n° 2018-026 du 07 décembre 2018 sur la cybersécurité et la lutte contre la cybercriminalité, modifiée par la loi n° 2022-009 du 24 juin 2022 ;
- Le décret n° 2019-022/PR du 13 février 2019 portant attributions, organisation et fonctionnement de l'ANCy ;

- Le décret n° 2019-095/PR du 08 juillet 2019 relatif aux opérateurs de services essentiels, aux infrastructures essentielles et aux obligations y afférentes ;
- Le décret n° 2022-09/PR du 25 août 2022 relatif à la qualification des Prestataires de services de confiance de cybersécurité et des produits de sécurité et à l'agrément des centres d'évaluation ;
- L'arrêté n° 2022-040/PRMT du 29 juin 2022 portant adoption des règles de cybersécurité en République togolaise ;

Ces documents sont disponibles sur les sites web de l'ANCy et du CERT.tg.

1.2.2. Textes de l'ANCy

- Décision ANCy portant liste des pays tiers de confiance ;
- Déclaration de la politique de qualification ;

  REF : Déclaration de la politique de qualification de l'ANCy

Ces documents sont disponibles auprès de l'ANCy ou communiqués par l'ANCy sur demande.

1.3. IDENTIFICATION DU DOCUMENT ET DATE D'APPLICATION

Le présent document est dénommé « Modèle de qualification des Prestataires de services de confiance en cybersécurité ».

Il peut être identifié par son nom, sa référence, son numéro de version et sa date de mise à jour.

Ce document est applicable à compter de sa publication.

Il est élaboré, mis à jour et publié par l'ANCy, qui précisera les modalités de transition et la date d'effet pour chaque mise à jour.

1.4. ACTEURS DU PROCESSUS DE QUALIFICATION

Les acteurs intervenant dans le processus de qualification au Togo sont :

- Le Comité stratégique de l'ANCy ;
- Le Directeur général de l'ANCy ;
- Le Responsable de la qualification de l'ANCy ;

ANCy Agence Nationale de la Cybersécurité
Tél: 97 52 58 58 / 70 60 60 83 Lomé - TOGO

- L'évaluateur ;
- Le Candidat à la qualification ;
- Le Prestataire de services de confiance en cybersécurité qualifié.
- Sur sollicitation ou validation par l'ANCy, toute autre personne ressource le cas échéant.

1.5. PRESTATIONS VISEES PAR LE REFERENTIEL DE QUALIFICATION

1.5.1. Services d'audit de la sécurité des systèmes d'information

❖ **Audit organisationnel**

L'audit de l'organisation de la sécurité permet de réaliser un état des lieux exhaustif du niveau de sécurité de l'ensemble du système d'information sur les volets organisationnels, procéduraux et technologiques.

❖ **Audit physique et environnemental**

L'audit environnemental et physique permet de s'assurer que les aspects physiques de la sécurité du système d'information sont correctement couverts.

❖ **Audit des architectures**

L'audit d'architecture consiste à contrôler la conformité du choix, du déploiement et de la mise en œuvre d'un système d'information, notamment les dispositifs matériels et logiciels, à des référentiels ou standards internationaux et aux exigences et règles internes d'une entité. L'audit peut être étendu aux interconnexions avec des réseaux tiers, et notamment Internet.

❖ **Audit des configurations**

L'audit de configuration consiste à vérifier la mise en œuvre de pratiques de sécurité conformes à des référentiels ou des standards internationaux et aux exigences et règles internes d'une entité en matière de configuration des dispositifs matériels et logiciels déployés dans un système d'information.

❖ **Audit de code source**

L'audit de code source consiste en l'analyse de tout ou partie du code source ou des conditions de compilation d'une application en vue d'y découvrir des vulnérabilités, liées à de mauvaises pratiques de programmation ou des erreurs de logique, qui pourraient avoir un impact en matière de sécurité.

❖ **Audits intrusifs**

Les tests d'intrusion permettent de découvrir des vulnérabilités sur le système d'information audité et de vérifier leur exploitabilité et leur impact, dans les conditions réelles d'une attaque sur le système d'information, à la place d'un potentiel attaquant. Ces tests peuvent être réalisés en interne (à partir du système d'information) ou en externe.

- **Audit des systèmes industriels SCADA**

L'audit des systèmes industriels est une spécialisation des audits de vulnérabilités qui évalue et traite les questions de sécurité relatives aux systèmes industriels. La connaissance des technologies spécifiques à la production industrielle est souvent primordiale dans ce type d'audit.

1.5.2. Services de détection des incidents de sécurité

- **Détection des incidents**

C'est l'ensemble des moyens techniques et organisationnels visant à détecter et évaluer un incident de sécurité à partir d'événements recueillis ainsi que le stockage et l'archivage des incidents dans le but d'améliorer le processus de détection.

- **Gestion des événements**

C'est l'ensemble des moyens techniques et organisationnels assurant la collecte et l'enregistrement des événements liés à la sécurité.

- **Gestion des notifications**

C'est l'ensemble des moyens techniques et organisationnels permettant de communiquer à une entité l'état des incidents de sécurité détectés sur son système d'information ainsi que le stockage de ces incidents.

1.5.3. Services de réponse aux incidents de sécurité

- **Réponse et traitement des incidents dits de niveau 3**

La réponse aux incidents dits de niveau 3 consiste en la recherche d'indicateurs de compromission permettant une analyse approfondie des résultats pour déceler la présence d'éventuels signes de compromission. Elle permet d'analyser ces données dans le but de recueillir, préserver, examiner et présenter des preuves numériques.

1.5.4. Services d'intégration, d'administration et de maintenance sécurisées

Les services d'administration englobent les opérations telles que l'installation, la suppression, la modification et la consultation d'un système intégré dans le système d'information et qui nécessitent des opérations de maintenance étant donné qu'ils sont susceptibles d'altérer le fonctionnement ou la sécurité du système d'information.

1.5.5. Services d'accompagnement et de conseil en cybersécurité

Les services d'accompagnement et de conseil en cybersécurité regroupent un ensemble d'activités visant à identifier, d'une part les mesures de sécurité (organisationnelles, physiques et techniques) à mettre en place en priorité et d'autre part, à définir la manière dont elles doivent être appliquées.

Ces services permettent à une entité de renforcer sa posture de cybersécurité par la sensibilisation du personnel, l'évaluation et la certification des compétences, tout en bénéficiant de conseils d'experts dans les démarches de gestion des risques et la gestion des incidents.

1.6. NOTIONS GENERALES DE QUALIFICATION

La qualification des prestaires des services de confiance en cybersécurité et des produits de sécurité est une mission de l'ANCy, prévue à l'article 4 du décret n° 2019-022/PR du 13 février 2019 portant attributions, organisation et fonctionnement de l'ANCy. La qualification a pour objectif de mettre à la disposition de l'administration, des opérateurs de services essentiels, et de toutes autres personnes, des services et produits répondant à leurs besoins en matière de sécurité des systèmes d'information.

La qualification en cybersécurité au Togo implique que l'État togolais recommande des services ou des produits de cybersécurité spécifiques qui ont été soigneusement évalués et validés par l'Agence Nationale de la Cybersécurité (ANCy), l'autorité compétente en matière de sécurité des infrastructures essentielles et des systèmes d'information dans le pays.

La qualification vise à garantir la conformité des services ou produits de cybersécurité aux critères établis par l'ANCy en matière de sécurité et de performance à travers les référentiels d'exigences de chaque prestation. Elle témoigne également de la compétence des Prestataires de services et de l'engagement des fournisseurs de produits à respecter des critères de confiance, permettant une confiance des utilisateurs de ces services ou produits.

Enfin, la qualification vise à renforcer la protection des systèmes informatiques et des données sensibles contre les menaces cybernétiques au Togo.

1.7. DEFINITIONS

Les termes suivants utilisés dans le présent document auront la signification indiquée ci-dessous :

1.7.1. Candidat à la qualification

La personne physique ou morale demandant la qualification d'un service. Il s'agit du Prestataire de services qui fournit le service pour lequel la qualification est demandée.

1.7.2. Centre d'évaluation

Tout organisme agréé par l'ANCy pour effectuer des tests de produits de sécurité et/ou des Prestataires de services de confiance en cybersécurité.

1.7.3. Client final

C'est la partie qui requiert les services de confiance en cybersécurité en faisant appel à un Prestataire de services de confiance en cybersécurité qualifié par l'ANCy. Il peut s'agir d'une structure du secteur public, d'un OSE, etc.

1.7.4. Décision de qualification

La décision émanant de l'ANCy concernant l'octroi ou le refus de qualification à un Candidat à la qualification.

1.7.5. Décision de suspension ou de retrait de la qualification

La décision émanant de l'ANCy prononçant la suspension ou le retrait de la qualification octroyée à un Prestataire de services de confiance en cybersécurité qualifié, en cas de manquement aux dispositions légales et règlementaires applicables, aux conditions et réserves fixées par la décision de qualification ou en cas de changement des circonstances de droit ou de fait dans lesquelles le Prestataire a été qualifié.

1.7.6. Déclaration de la politique de qualification

La politique de qualification traduit l'engagement de la direction générale de l'ANCy à satisfaire les exigences des intervenants dans le schéma de qualification et veiller à améliorer en permanence l'efficacité du système de qualification des Prestataires de services de confiance de cybersécurité, et ce par la mise à disposition des moyens et ressources nécessaires en vue de l'atteinte des objectifs visés.

1.7.7. Évaluateur

L'évaluateur peut être :

- L'ANCy ; ou
- Un centre d'évaluation agréé par l'ANCy et agissant comme délégataire de celle-ci, conformément aux articles 11 et suivants du décret n°2022-090 du 25 août 2022 relatif à la qualification des Prestataires de services de confiance de cybersécurité et des produits de sécurité et à l'agrément des centres d'évaluation.

1.7.8. Opérateur de services essentiels

Tout opérateur, public ou privé, offrant des services essentiels au fonctionnement de la société ou de l'économie et dont la continuité pourrait être gravement affectée par des incidents touchant les réseaux de communications électroniques ou systèmes d'information nécessaires à la fourniture desdits services.

1.7.9. Portée de la qualification

C'est l'étendue ou la gamme des activités, des services, des produits ou des systèmes pour lesquels une qualification spécifique est demandée ou accordée.

1.7.10. Prestataire de services de confiance en cybersécurité ou Prestataire de services de confiance de cybersécurité

Toute personne fournissant des services qui contribuent à la sécurité des systèmes d'information.

1.7.11. Prestataire de services de confiance en/de cybersécurité qualifié par l'ANCy

Prestataire fournissant des services qui contribuent à la sécurité (i) des systèmes d'information de l'administration ou des opérateurs de services essentiels et (ii) de tout matériel, logiciel ou système d'information destiné à traiter des informations couvertes par le secret de la défense nationale.

1.7.12. Produit de sécurité

Tout dispositif, matériel ou logiciel, mettant en œuvre des fonctions qui contribuent à la sécurité des systèmes d'information de l'administration publique ou des opérateurs de services essentiels et de tout matériel, logiciel ou système d'information destiné à traiter des informations couvertes par le secret de la défense nationale.

1.7.13. Rapport d'évaluation

Le document présentant les résultats de l'évaluation d'un service de confiance pour les besoins de la qualification.

1.7.14. Responsable de la qualification

Il s'agit de la personne chargée au sein de l'ANCy, d'examiner les différentes étapes du processus de qualification et de proposer au directeur général de l'ANCy les décisions de qualification.

1.7.15. Service essentiel

Tout service essentiel pour la sûreté publique, la défense nationale, la stabilité économique, la sécurité nationale, la stabilité internationale, et pour la pérennité et la restauration du cyberespace critique.

1.7.16. Suivi de la qualification

Processus de vérification visant à s'assurer après chaque décision d'octroi de la qualification, que les critères sur la base desquels la qualification a été attribuée sont toujours respectés.

2. PROCESSUS DE QUALIFICATION

2.1. INTRODUCTION

2.1.1. Étapes clés

Le processus de qualification démarre dès réception par l'ANCy du dossier de demande de qualification **(REF Dossier de demande de qualification)** adressé par le Candidat à la qualification.

Il se répartit en trois étapes clés :

- **Étape 1 : Demande de qualification**
- **Étape 2 : Évaluation des Prestataires**
- **Étape 3 : Décision de qualification**

Un processus de suivi est ensuite mis en place pour assurer le maintien de la qualification.

Étape 1 : Demande de qualification

Cette étape se décompose en plusieurs sous étapes :

a. Le Candidat à la qualification constitue un dossier de demande de qualification, qui comporte la demande de qualification ainsi que l'ensemble des pièces requises listées sur le site internet de l'ANCy tel que prévu au point 2.2.1. La demande de qualification est adressée au directeur général de l'ANCy.

b. Le directeur général de l'ANCy procède à la désignation d'un Responsable de qualification chargé d'instruire la demande de qualification.

c. Le responsable de qualification de l'ANCy effectue une première analyse du dossier en vue de s'assurer de sa complétude (vérifier qu'il comporte bien l'ensemble des pièces requises et que celles-ci sont conformes) d'une part, et du respect de l'ensemble des critères d'acceptation de la demande de qualification listés au point 2.2.2, d'autre part. Le Responsable de qualification peut dans ce cadre solliciter le Candidat à la qualification pour un complément d'informations. Le Responsable de qualification rend compte de l'analyse préliminaire effectuée au directeur général de l'ANCy.

d. Si le dossier est jugé complet et conforme, le directeur général de l'ANCy prend une décision d'acceptation de la demande de qualification et de lancement de la phase d'évaluation du Candidat à la qualification, en vue de lui délivrer une qualification.

e. Dans le cas contraire, L'ANCy notifie au Candidat à la qualification de l'échec du processus de qualification, avec précision des motifs pour lesquels il ne peut être qualifié.

f. La décision de l'ANCy intervient dans un délai d'un (01) mois suivant la date de réception du dossier de demande complet ; ce délai peut être prorogé d'un (01) mois.

Étape 2 : Évaluation des Prestataires

L'évaluation vise à s'assurer que le Candidat à la qualification respecte les règles prévues par les référentiels du/des services pour lequel/lesquels la qualification est demandée, et en particulier qu'il dispose du personnel compétent, des moyens techniques et des locaux adéquats pour fournir le (s) service (s) concerné (s).

Les travaux d'évaluation sont réalisés par l'ANCy elle-même, ou sur délégation de l'ANCy, par des centres d'évaluation qu'elle agrée, selon la procédure d'agrément des centres d'évaluation.

L'ANCy fait réaliser une enquête administrative sur le Candidat à la qualification afin d'évaluer la confiance.

L'ANCy ou le cas échéant le centre d'évaluation saisi par le Candidat à la qualification, émet un rapport d'évaluation de ce Candidat à la qualification dans un délai de deux (02) mois suivant la décision de lancement de la phase d'évaluation. Ce délai peut être prorogé de deux (02) mois.

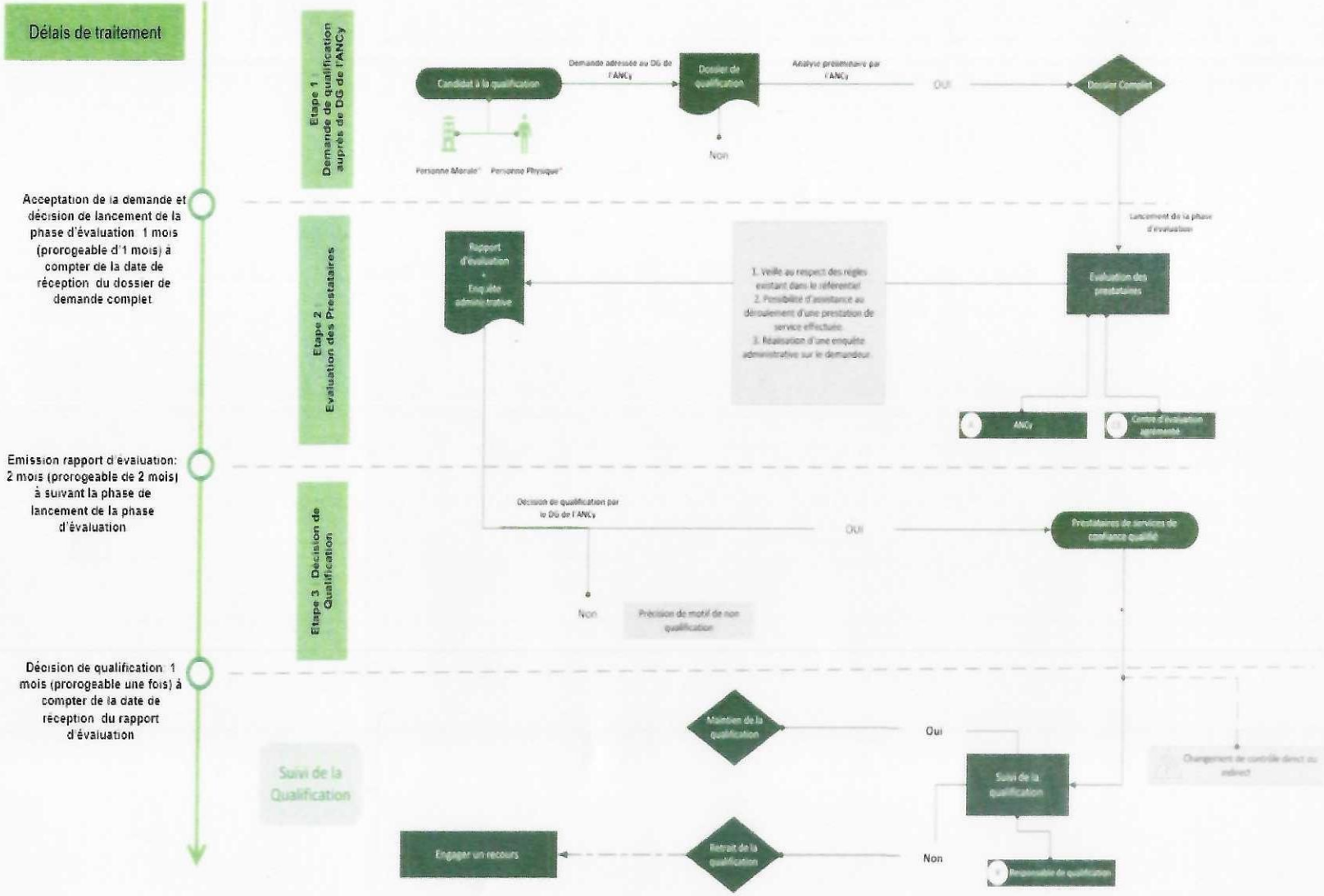
Étape 3 : Décision de qualification

Le directeur général de l'ANCy, prend une décision définitive d'octroi de qualification ou de refus de qualification, conformément aux dispositions du point 2.4., après soumission au comité stratégique.

La décision de qualification est notifiée au Candidat à la qualification.

La qualification est octroyée pour une durée maximale de trois (03) ans. Le Candidat à la qualification peut à l'échéance, en demander le renouvellement pour la même durée en déposant une nouvelle demande de qualification auprès de l'ANCy (06) mois avant l'expiration de la qualification.

2.1.2. Schéma de qualification



2.1.3. Portées de la qualification

La portée de la qualification visée est définie par le Candidat à la qualification dans sa demande de qualification.

La portée de la qualification d'un service est constituée de la famille de services de confiance en cybersécurité et du cadre règlementaire auquel se réfère la qualification, complétés le cas échéant, et selon la famille de services, de la liste des activités faisant l'objet de la qualification.

Services	PRESTATAIRE	Cadre réglementaire	Référentiels Exigences	Charge d'évaluation en H/J	Durée de la qualification
Audit de la sécurité des systèmes d'information	Personne morale ou physique	Décret n° 2022-09/PR du 25 août 2022	Référentiel PA	15 jours	3 ans
Détection des incidents de sécurité	Personne morale	Décret n° 2022-09/PR du 25 août 2022	Référentiel DI	25 jours	3 ans
Réponse aux incidents de sécurité	Personne morale	Décret n° 2022-09/PR du 25 août 2022	Référentiel RI	20 jours	3 ans
Intégration, Administration et maintenance sécurisées	Personne morale	Décret n° 2022-09/PR du 25 août 2022	Référentiel MS	25 jours	3 ans
Accompagnement et conseil en cybersécurité	Personne morale ou physique	Décret n° 2022-09/PR du 25 août 2022	Référentiel Conseil	15 jours	3 ans

2.1.4. Confidentialité

Conformément à l'article 19 du décret n° 2019-022/PR du 13 février 2019 portant attributions, organisation et fonctionnement de l'ANCy, les agents de l'ANCy sont tenus au secret professionnel indépendamment des règles instituées dans le code pénal togolais, et notamment son article 176.

Par ailleurs, l'article 177 du code pénal togolais punit la publication ou la diffusion de papiers ou enregistrements privés sans l'accord de leurs auteurs.

L'ANCy bénéficie des mesures de protection et de sécurité élevées, tant en termes de protection des locaux et des systèmes d'information que d'habilitation des personnels.

À ce titre, les informations échangées dans le contexte de la qualification d'un service sont traitées avec une confidentialité appropriée. L'ANCy leur réserve un traitement selon des règles de protection adéquates.

Tous les documents confidentiels transmis à l'ANCy bénéficient de mesures de confidentialité au moyen d'outils définis entre l'ANCy et l'expéditeur.

2.1.5. Frais et coûts

Les coûts associés aux travaux d'évaluation incombent entièrement au demandeur. Le montant de l'évaluation est établi après discussion entre le candidat et l'ANCy ou son délégataire.

2.1.6. Réclamations

Toute personne dispose du droit de déposer auprès de l'ANCy une réclamation contre un service qualifié ou son Prestataire.

Toute réclamation doit être adressée à l'ANCy sous format écrit par voie postale ou par voie électronique, aux adresses ci-dessous :

Par voie postale : 63 Bd du 13 Janvier, Nyékonakpoe. 07 BP 7878 Lomé – TOGO

Par voie électronique : secretariat.ancy@ancy.gouv.tg ou toute autre adresse électronique indiquée par l'ANCy.

Les réclamations sont traitées dans le cadre du suivi de la qualification par le Responsable qualification en application des dispositions énoncées à la Section 2.5 du présent document. Le responsable qualification peut dans ce cadre, inviter le plaignant à exposer les motifs de sa réclamation ou convoquer le Prestataire pour recueillir des informations supplémentaires.

Si l'instruction de la réclamation révèle qu'au moins l'un des critères de qualification énoncés au point 2.4.2 n'est pas respecté, le directeur général de l'ANCy peut après avis du comité stratégique, prendre une décision de suspension ou de retrait de la qualification.

2.1.7. Recours

Le Candidat à la qualification ou un Prestataire de services de confiance qualifié par l'ANCy peut engager un recours gracieux ou contentieux, en cas de refus de la demande de qualification ou en cas de décision de suspension ou de retrait de la qualification.

Le recours gracieux est déposé auprès de l'ANCy, et doit être formulé dans un délai d'un (01) mois à compter de la date de la décision faisant l'objet du recours.

Le recours est envoyé par voie électronique ou postale aux adresses ci-dessous :

Par voie postale : 63 Bd du 13 Janvier, Nyékonakpoè. 07 BP 7878 Lomé – TOGO

Par voie électronique : secretariat.ancy@ancy.gouv.tg ou toute autre adresse électronique indiquée par l'ANCy.

Le recours gracieux formé auprès de l'ANCy n'est pas suspensif de la décision de qualification.

La personne désignée au sein de l'ANCy pour le traitement des recours gracieux peut solliciter des informations complémentaires du Candidat à la qualification ou du Prestataire de services de confiance qualifié quant à la motivation de son recours.

L'ANCy dispose d'un délai de deux (02) mois à compter de la réception du recours gracieux pour rendre sa décision.

À l'issue de ce délai, ou si la décision rendue par l'ANCy ne le satisfait pas, le Candidat à la qualification ou le Prestataire de services de confiance en cybersécurité qualifié dispose du droit de saisir les juridictions nationales compétentes dans le cadre d'un recours contentieux dans un délai de trois (3) mois à compter de la notification de la décision de rejet.

2.1.8. Interruption du processus de qualification

Le processus de qualification peut être interrompu dans l'un des cas suivants :

- Le dossier de demande de qualification n'est pas complet et le Candidat à la qualification n'a pas fourni le complément d'informations sollicité par l'ANCy dans un délai d'un (01) mois ;
- Le dossier de demande de qualification est complet, mais l'ANCy a des motifs justifiant que le Candidat à la qualification ne peut être qualifié et s'abstient de lancer la phase d'évaluation ;

- Le Candidat à la qualification ne respecte pas un engagement pris dans le dossier de demande de qualification ;

La décision d'interruption du processus de qualification est prononcée de manière unilatérale par l'ANCy. Elle est notifiée dans un délai raisonnable au Candidat à la qualification par tout moyen laissant trace écrite.

En cas d'interruption du processus de qualification, le Candidat à la qualification peut soumettre ultérieurement une nouvelle demande de qualification pour le même service si le motif d'interruption de la première demande a été corrigé.

2.2. DEMANDE DE QUALIFICATION

2.2.1. Contenu du dossier de demande de qualification

Le dossier de demande de qualification est composé d'une liste des documents ainsi que d'un formulaire de demande de qualification **REF : Formulaire de demande de qualification**, publiés sur le site de l'ANCy et incluant :

a. Une demande écrite adressée au directeur général de l'ANCy ;
b. La description des services sur lesquels porte la demande et la démonstration qu'ils sont susceptibles de répondre aux besoins de sécurité des systèmes d'information des administrations et des opérateurs de services essentiels ;
c. L'organisation, les procédures et les méthodes mises en place par le Prestataire pour fournir les services ;
d. Les conditions satisfaisantes d'accès aux locaux, aux personnels et aux moyens techniques du Prestataire.

2.2.2. Critères d'acceptation de la demande de qualification

Les critères d'acceptation de la demande de qualification sont :

- Le dossier de demande de qualification est complet ;
- Le dossier de demande de qualification est envoyé par voie postale ou électronique à l'ANCy aux adresses ci-dessous :

- Par voie postale : 63 Bd du 13 Janvier, Nyékonakpoè. 07 BP 7878 Lomé – TOGO
- Par voie électronique : secretariat.ancy@ancy.gouv.tg ou toute autre adresse électronique indiquée par l'ANCy.

- Le service répond aux besoins (i) de la sécurité nationale, de l'administration publique ou des opérateurs de services essentiels dans le cadre de la Loi n° 2018-026 du 07 décembre 2018 sur la cybersécurité et la lutte contre la cybercriminalité modifiée et ses textes d'application ; et (ii) de la sécurité dans les transactions électroniques dans le cadre de la loi n°2017-07 du 22 juin 2017 relative aux transactions électroniques et ses textes d'application ;
- La portée de la qualification demandée est cohérente avec les objectifs et fonctions de sécurité du service ;
- Le Candidat à la qualification est en mesure de respecter l'ensemble des engagements pris dans le dossier de demande de qualification.

2.2.3. Décision d'acceptation ou de refus de la demande de qualification

2.2.3.1. Acceptation

Lorsque les critères d'acceptation sont remplis et que sur la base de la recommandation du Responsable de qualification, le directeur général de l'ANCy, prend une décision d'acceptation de la demande de qualification. Cette décision est notifiée au Candidat à la qualification par voie électronique ou postale, et est prise dans un délai d'un (1) mois suivant la date de réception du dossier de demande de qualification complet. Ce délai peut être prolongé d'un (1) mois.

2.2.3.2. Rejet

Lorsqu'au moins un des critères d'acceptation de la demande de qualification n'est pas respecté, le directeur général de l'ANCy sur la base de la recommandation du Responsable de la qualification, rejette la demande de qualification.

L'ANCy informe le Candidat à la qualification du rejet de sa demande de qualification, et la lui notifie par voie postale ou électronique. Les motifs du rejet de la demande de qualification sont exposés dans la décision de rejet.

Cette décision est prise dans un délai d'un (1) mois suivant la date de réception du dossier de demande de qualification complet. Ce délai peut être prolongé d'un (1) mois.

Les décisions de rejet de demande de qualification peuvent faire l'objet d'un recours formé par le Candidat à la qualification conformément au point 2.1.7.

2.3. ÉVALUATION DES PRESTATAIRES

2.3.1. Approche de l'évaluation

Le Candidat à la qualification détermine avec l'évaluateur :

- Les services à évaluer ;
- Les conditions d'accès à ses locaux, personnels et moyens techniques ;
- Le programme de travail du centre d'évaluation concerné ainsi que les délais nécessaires pour réaliser l'évaluation ;
- Les conditions dans lesquelles sera protégée la confidentialité des informations traitées dans le cadre de l'évaluation.

À cet égard, le Candidat à la qualification met à la disposition de l'ANCy et, le cas échéant, du centre d'évaluation concerné tous les documents nécessaires à l'évaluation, leur permettant d'accéder à ses locaux, à ses moyens techniques, et de rencontrer son personnel.

2.3.2. Tâches d'évaluation

Les tâches d'évaluation qui peuvent être réalisées dans le cadre du processus de qualification d'un service sont listées ci-après de manière non exhaustive.

L'évaluateur peut ajourner une évaluation de sa seule initiative, après en avoir informé préalablement le Candidat à la qualification, lorsqu'il estime que les conditions d'évaluation ne sont pas satisfaisantes.

Les travaux d'évaluation sont régis par un contrat qui définit clairement les droits et obligations du Candidat à la qualification et de l'évaluateur ainsi que les coûts associés.

❖ **Évaluation de la conformité du service aux référentiels d'exigences**

Le but est de vérifier que le service est conforme et respecte toutes les exigences des référentiels applicables à la portée de qualification sollicitée par le Candidat à la qualification.

❖ **Évaluation de la confiance**

Le but est de vérifier, dans le cadre des Documents de référence, et conformément à l'article 4 du décret n°2022-090 du 25 août 2022, que le personnel du Candidat à la qualification est compétent, et notamment que le comportement des personnes physiques ou morales impliquées dans la fourniture du service est compatible et en adéquation avec les missions de fourniture des services à qualifier.

2.3.3. Évaluateurs et travaux d'évaluation

Les travaux d'évaluation sont réalisés par l'ANCy elle-même, ou sur délégation de l'ANCy, par des centres d'évaluation qu'elle agréé conformément aux dispositions légales et règlementaires applicables.

Dans le dernier cas, l'ANCy en informe le demandeur, qui choisit un centre d'évaluation agréé afin de se soumettre à son évaluation.

L'ANCy dispose du droit de demander à assister aux travaux dévaluation lorsqu'ils sont menés par un centre d'évaluation, ou d'obtenir des informations sur leur déroulement.

2.3.4. Modalités relatives aux rapports d'évaluation

❖ **Contenu des rapports d'évaluation**

L'ANCy ou le cas échéant, le centre d'évaluation saisi par le Candidat à la qualification, émet un rapport d'évaluation à la suite de la phase d'évaluation.

Le rapport d'évaluation détaille les différentes tâches d'évaluation réalisées, les résultats obtenus, ainsi que les vulnérabilités et les non-conformités identifiées par rapport aux exigences du référentiel. De plus, il inclut, le cas échéant, des mesures préconisées pour corriger ces vulnérabilités et non-conformités.

Lorsque les travaux d'évaluation sont menés par un centre d'évaluation agréé, l'ANCy peut demander au centre d'évaluation concerné de modifier ou compléter son rapport d'évaluation, ou de mener des travaux complémentaires.

Les rapports d'évaluation sont strictement confidentiels.

❖ **Transmission des rapports d'évaluation**

Si l'évaluation est effectuée par un centre d'évaluation agréé, le rapport d'évaluation est transmis par voie électronique ou postale à l'ANCy aux adresses ci-après :

- Par voie postale : 63 Bd du 13 Janvier, Nyékonakpoè. 07 BP 7878 Lomé – TOGO
- Par voie électronique : secretariat.ancy@ancy.gouv.tg ou toute autre adresse électronique indiquée par l'ANCy.

❖ Confidentialité et protection des rapports d'évaluation

Les rapports d'évaluation renferment des informations sensibles concernant le Candidat à la qualification et les services de confiance. Ces documents sont susceptibles de contenir des informations dont la révélation est réprimée par la loi, y compris en matière de défense nationale. En conséquence, les rapports d'évaluation revêtent un caractère strictement confidentiel.

Pour garantir l'authenticité des rapports d'évaluation et prévenir toute altération de leur contenu, l'évaluateur peut utiliser tout moyen d'authentification convenu entre les parties prenantes, sous réserve des standards de sécurité et de vérifiabilité appropriés.

Lorsque les conditions techniques et réglementaires de mise en œuvre de la signature électronique, telles que définies par la loi n°2017-07 relative aux transactions électroniques et ses textes d'application, seront réunies, l'authentification par une signature électronique de type avancé sera privilégiée.

❖ Propriété et langue des rapports d'évaluation

Des clauses de titularité peuvent être insérées dans les rapports d'évaluation. Ces clauses sont définies contractuellement entre le Candidat à la qualification et l'évaluateur.

Les clauses de titularité ne sauraient cependant constituer un obstacle à la détention et à la conservation sans limite de temps ou de diffusion au sein de l'ANCy des copies des rapports d'évaluation.

Les rapports d'évaluation sont rédigés en langue française.

❖ Délais

Le rapport d'évaluation doit être émis dans un délai de deux mois suivant la décision de lancement de la phase d'évaluation conformément aux dispositions de l'article 6 du décret n°2022-90 du 25 août 2022. Ce délai peut être prorogé de deux (2) mois.

2.4. DECISION DE LA QUALIFICATION

2.4.1. Instruction

L'instruction de la décision de qualification est menée par le Responsable de la qualification.

Le Responsable de la qualification instruit la décision de qualification conformément aux critères de qualification listés au point 2.4.2. Cette phase vise à vérifier que l'ensemble des critères de qualification sont respectés, puis à proposer au directeur général de l'ANCy une décision de qualification.

Le responsable de qualification vérifie notamment que :

- L'approche de l'évaluation a été respectée ;
- L'ensemble des travaux d'évaluation ont été bien menés en conformité avec les tâches d'évaluation (périmètre, méthodologie, etc.) ;
- Le rapport d'évaluation a été transmis à l'ANCy ;
- L'enquête administrative a été effectuée ;
- L'ensemble des engagements pris dans le dossier de demande de qualification a été respecté.

2.4.2. Critères de qualification

Les critères de qualification désignent l'ensemble des exigences et des conditions établies pour évaluer et déterminer si un Prestataire de services répond aux standards requis pour être qualifié à délivrer une prestation en rapport avec les services de confiance.

Les critères de qualification sont relatifs à la robustesse d'un service et à la confiance accordée au Prestataire du service.

❖ **Les Critères relatifs à la robustesse du service**

Ils sont mis en évidence à travers les résultats des travaux qui attestent que :

- Le service résiste au niveau de menace correspondant à la portée de qualification demandée ;
- Le service est conforme aux référentiels d'exigences applicables à la portée de qualification demandée ;
- Le service respecte les exigences techniques et réglementaires ainsi que les différents référentiels d'exigences des Prestataires de confiance en cybersécurité de l'ANCy.

❖ **Les Critères relatifs à la confiance concernant le Prestataire de services de confiance en cybersécurité**

Ils sont mis en évidence comme suit :

- Le processus de qualification d'un service a été respecté ;
- Le Candidat à la qualification respecte ses engagements pris dans le dossier de demande de qualification ;
- Les résultats de l'enquête administrative menée par l'ANCy, ont permis de vérifier que le comportement des personnes physiques ou morales impliquées dans la fourniture du service est compatible avec les missions de fourniture d'un service qualifié.

2.4.3. Contenu de la décision de qualification

La décision de qualification est prise par le directeur général de l'ANCy.

La décision de qualification est émise sur la base du rapport d'évaluation, des résultats de l'enquête administrative, et au vu des recommandations faites par le Responsable de la qualification.

La décision de qualification est prise dans un délai d'un (01) mois suivant la date de réception du rapport d'évaluation. Ce délai peut être prorogé une fois pour la même durée.

La qualification est octroyée pour une durée maximale de trois (03) ans. L'ANCy fixe dans la décision de qualification la durée de validité de la qualification, les conditions et les éventuelles restrictions d'utilisation

Le prestataire de services de confiance peut, en demander le renouvellement pour la même durée en déposant une nouvelle demande de qualification auprès de l'ANCy. La demande de renouvellement de la qualification devra être déposée par le prestataire dans un délai minimum de six (06) mois précédant l'échéance de la qualification en cours, et selon les formes et modalités prévues pour les demandes initiales de qualification.

2.4.4. Octroi de la qualification

Lorsque l'ensemble des critères de qualification listés au point 2.4.2 sont respectés, le directeur général de l'ANCy, prend une décision d'octroi de la qualification au prestaire de services de confiance en cybersécurité.

La qualification peut être octroyée pour la portée demandée par le Prestataire dans le dossier de demande de qualification, ou pour une portée de qualification inférieure à celle demandée lorsqu'au moins un des critères de qualification n'est pas respecté.

Le Prestataire de services de confiance en cybersécurité obtient le statut de Prestataire de services de confiance en cybersécurité qualifié.

Lorsqu'une décision d'octroi de la qualification pour la portée de qualification demandée est prononcée, le service obtient le statut « qualifié ». La décision de qualification est notifiée au Prestataire de services de confiance et précise les services qualifiés. Cette décision est publiée sur le site de l'ANCy.

Cette qualification est personnelle et ne peut être louée, cédée ou transférée à un tiers.

Les Prestataires de services de confiance de cybersécurité qualifiés établis dans un pays étranger reconnu par l'ANCy peuvent bénéficier d'une reconnaissance accordée par le Directeur Général de l'ANCy après avis favorable du comité stratégique de l'ANCy.

2.4.5. Refus de la qualification

Lorsqu'au moins un des critères de qualification n'est pas respecté, le directeur général de l'ANCy prend une décision de refus de qualification et précise au Candidat à la qualification les motifs pour lesquels il ne peut être qualifié.

2.5. SUIVI DE LA QUALIFICATION

Le suivi de la qualification intervient dans le cadre du contrôle par l'ANCy des Prestataires de services de confiance en cybersécurité qualifiés. Le suivi vise et permet à l'ANCy de s'assurer à tout moment après la décision d'octroi de la qualification, que le Prestataire de services de confiance qualifié respecte les règles au vu desquelles il a été qualifié, et que les critères qui ont conduit à l'attribution de la qualification sont toujours respectés.

Le suivi repose notamment sur les éléments relatifs à la sécurité et à la pérennité du service indiqués par le Prestataire de services de confiance qualifié, conformément aux engagements qu'il a pris au titre du dossier de demande de qualification.

Outre les informations fournies lors de la demande de qualification, le suivi de la qualification s'appuie également sur les évolutions de l'état de l'art identifiées par l'ANCy, ainsi que sur les éventuelles non-conformités signalées par un tiers.

2.5.1. Instruction

Dans le cadre de l'instruction du suivi de la qualification, le Responsable de la qualification peut convoquer le Prestataire de services de confiance en cybersécurité qualifié ou lui demander de modifier ou de compléter les informations transmises à l'ANCy le cas échéant.

L'ANCy peut également à tout moment, après en avoir informé préalablement le Prestataire de services de confiance en cybersécurité qualifié par écrit, contrôler ou faire contrôler par un Evaluateur, les critères de qualification définis au point 2.4.2.

Le Responsable de la qualification invite le Prestataire de services de confiance en cybersécurité et l'Évaluateur à présenter les résultats des contrôles au cours d'une ou plusieurs réunions, et peut demander à l'évaluateur d'apporter des modifications à son rapport, le compléter, ou mener des travaux complémentaires.

À la fin de l''instruction, le Responsable qualification propose au directeur général de l'ANCy une décision de qualification parmi celles définies au point 2.5.3.

2.5.2. Critères de suivi de la qualification et de la sécurité du service qualifié

Conformément à ses engagements pris dans le dossier de demande de qualification, le Prestataire de services de confiance qualifié s'oblige à informer sans délai l'ANCy, par voie postale ou électronique de :

- **Tout incident impactant ou susceptible d'impacter** :

- Le service qualifié et particulièrement les systèmes d'information impliqués dans l'administration, l'exploitation, la maintenance, ou le support technique du service qualifié ;

- Les données sensibles relatives aux utilisateurs du service qualifié, que ces données soient à caractère personnel ou non.

Le Prestataire de services de confiance en cybersécurité constitue à cet égard une déclaration d'incident en vue de déclarer l'incident concerné. La déclaration d'incident est effectuée à partir du formulaire mis à la disposition du public par l'ANCy à travers le site du CERT.tg et est effectuée conformément à la procédure y décrite.

La déclaration d'incident dans le cadre du suivi de la sécurité d'un service ne se substitue pas aux éventuelles autres obligations légales et règlementaires auxquelles le Prestataire de services de confiance qualifié en cybersécurité pourrait être tenu en vertu des documents de référence ou des bonnes pratiques en vigueur au Togo.

❖ **Tout changement de l'environnement du service qualifié :**

- Tout changement important lié au Prestataire de services de confiance en cybersécurité, ou à ses sous-traitants de premier rang, notamment ceux à qui serait confiée une activité jugée suffisamment sensible par l'ANCy ou un volume d'activités suffisamment important. Les changements visés peuvent être relatifs à la cessation d'activité, le changement de propriétaire, d'organisation, de structure juridique, de locaux, etc.
- Toute perte des compétences indispensables à l'exercice des activités couvertes par la qualification, suite à des mouvements de personnel notamment.
- Tout arrêt de la commercialisation ou du support, aussi bien en termes de maintenance corrective que de support utilisateurs, du service qualifié.

De façon plus générale, le Prestataire de services de confiance en cybersécurité qualifié s'oblige à informer l'ANCy sans délai, de toute modification des circonstances sur la base desquelles il a été qualifié.

2.5.3. Décision de qualification dans le cadre du suivi de la qualification

L'ANCy peut dans le cadre du suivi de la qualification, prononcer des décisions de maintien ou de suspension ou retrait de la qualification. Ces décisions font l'objet d'une notification aux Prestataires de services de confiance en cybersécurité qualifiés.

Lorsqu'une décision d'octroi de la qualification pour une portée de qualification inférieure à celle demandée, de refus ou de retrait de la qualification, ou de maintien de la qualification avec modification est prononcée, les motifs de cette décision sont exposés dans la notification.

❖ **Décision de maintien de la qualification**

La décision de qualification peut être prononcée avec le maintien de la qualification, sans modification ou avec modification.

- **Maintien de la qualification sans modification** : Le directeur général de l'ANCy sur proposition du Responsable de la qualification, maintient la qualification du service sans modifier ni la portée de la qualification, ni la durée de validité de la qualification, ni les conditions et éventuelles restrictions d'utilisation du service, lorsque l'ensemble des critères de qualification définis au point 2.4.2 sont toujours respectés.
- **Maintien de la qualification avec modification** : le directeur général de l'ANCy sur proposition du Responsable de la qualification, peut maintenir la qualification en réduisant la portée de qualification ou en modifiant la durée de validité de la qualification, les conditions et éventuelles restrictions d'utilisation du service lorsqu'au moins un des critères de qualification définis au point 2.4.2 n'est plus respecté.

❖ **Décision de suspension ou retrait de la qualification**

Le directeur général de l'ANCy, après avis du comité stratégique, peut dans les hypothèses ci-dessous, après que le Prestataire de services de confiance en cybersécurité a pu faire valoir ses observations, suspendre ou mettre un terme à la qualification :

- Manquement par le Prestataire de services de confiance en cybersécurité aux dispositions légales et règlementaires applicables ;
- Manquement par le Prestataire de services de confiance en cybersécurité aux conditions et réserves fixées par la décision de qualification ;
- Changement de circonstances de droit ou de fait dans lesquelles le Prestataire de services de confiance en cybersécurité a été qualifié, notamment tout changement de contrôle direct ou indirect du Prestataire de services de confiance en cybersécurité qualifié, sans l'approbation préalable de l'ANCy.

Le directeur général de l'ANCy sur proposition du Responsable de la qualification, retire également la qualification lorsqu'au moins un des critères de qualification définis au point 2.4.2 n'est plus respecté.

Lorsqu'une décision de retrait de la qualification est prononcée, le service perd son statut « qualifié » et la promotion du fait que le service est « qualifié » n'est plus autorisée.

2.6. RECONNAISSANCE DES QUALIFICATIONS OBTENUES A L'ETRANGER

Les Prestataires de services de confiance en cybersécurité qualifiés établis dans un pays étranger reconnu par l'ANCy peuvent bénéficier d'une reconnaissance accordée par le Directeur Général de l'ANCy après avis favorable du comité stratégique de l'ANCy.

Le processus de reconnaissance des Prestataires de services de confiance en cybersécurité qualifiés à l'étranger démarre dès réception par l'ANCy du dossier de demande de reconnaissance (**Dossier de demande de reconnaissance)** adressé par le Prestataire de services de confiance en cybersécurité qualifié à l'étranger.

Le dossier de demande de reconnaissance est composé d'une liste de documents ainsi que d'un formulaire de demande de reconnaissance **REF : Formulaire de demande de reconnaissance,** publiés sur le site de l'ANCy, et inclut :

a. Une demande écrite de reconnaissance adressée au directeur général de l'ANCy ;
b. Une copie de la décision de qualification obtenue à l'étranger ainsi que les coordonnées de l'organisme ayant délivré la qualification ;
c. Une description des services sur lesquels porte la demande, l'organisation, les procédures et les méthodes mises en place par le Prestataire pour fournir les services ;
d. Les conditions satisfaisantes d'accès aux locaux, aux personnels et aux moyens techniques du Prestataire.

Le processus de reconnaissance de la qualification se répartit en trois étapes clés :

- **Étape 1 : Demande de reconnaissance**

La demande de reconnaissance contient une description des services sur lesquels porte la qualification.

Elle contient par ailleurs la démonstration que le service répond aux besoins (i) de la sécurité nationale, des administrations ou des opérateurs de services essentiels dans le cadre de la Loi n° 2018-026 du 07 décembre 2018 sur la cybersécurité et la lutte contre la cybercriminalité modifiée et ses textes d'application ; et (ii) du Décret 2022-090 relatif à la qualification des produits de sécurité, des prestataires

de services de confiance, à l'agrément des centres d'évaluation, ou de sécurité dans les transactions électroniques dans le cadre de la loi n°2017-07 relative aux transactions électroniques et ses textes d'application.

La demande de reconnaissance de qualification contient par ailleurs l'engagement du Prestataire de services de confiance en cybersécurité qualifié à l'étranger de respecter l'ensemble des exigences légales et règlementaires en vigueur au Togo.

❖ **Étape 2 : Examen de la demande**

L'examen de la demande vise à vérifier les conditions dans lesquelles la qualification a été accordée dans le pays tiers, compte tenu des caractéristiques de la prestation à délivrer.

L'ANCy vérifie notamment :

- L'authenticité de la qualification obtenue, telle qu'elle est attestée par l'organisme qui l'a décerné ;
- Le service répond aux besoins (i) de la sécurité nationale, des administrations ou des opérateurs de services essentiels dans le cadre de la loi n° 2018-026 du 07 décembre 2018 modifiée sur la cybersécurité et la lutte contre la cybercriminalité et ses textes d'application ; et (ii) de la sécurité dans les transactions électroniques dans le cadre de la loi n°2017-07 relative aux transactions électroniques et ses textes d'application ;
- La portée de la qualification demandée est cohérente avec les objectifs et fonctions de sécurité du service ;
- Le Prestataire de services de confiance en cybersécurité dispose de procédures de suivi des compétences et de formation en adéquation avec la portée de la qualification sollicitée ;
- Le Prestataire de services de confiance en cybersécurité est en mesure de respecter l'ensemble des engagements pris dans le dossier de demande de reconnaissance ;
- La preuve que le Prestataire qualifié dispose de mécanismes permettant de garantir la confidentialité, la fiabilité et la sécurité des informations ainsi que l'impartialité des services.

❖ **Étape 3 : Décision de reconnaissance de qualification**

Le directeur général de l'ANCy, prend une décision de reconnaissance de qualification ou de refus de reconnaissance au Prestataire de services de confiance qualifié à l'étranger, après avis du comité stratégique.

La décision de reconnaissance de la qualification est notifiée au Prestataire de services de confiance.

La reconnaissance de qualification est octroyée pour une durée maximale de trois (03) ans. Le prestataire peut à l'échéance, en demander le renouvellement pour la même durée en déposant une nouvelle demande de reconnaissance de qualification auprès de l'ANCy. La demande de renouvellement de la reconnaissance devra être déposée par le prestataire dans un délai minimum de six (06) mois précédant l'échéance de la décision de reconnaissance en cours, et selon les formes et modalités prévues pour les demandes initiales de reconnaissance de qualification.

3.EXIGENCES LIEES A LA QUALIFICATION DES PRESTATAIRES DE SERVICES DE CONFIANCE EN CYBERSECURITE

3.1. EXIGENCES COMMUNES

3.1.1. Protection de l'information

Le Prestataire de services de confiance en cybersécurité doit tout mettre en œuvre pour protéger les informations collectées dans le cadre des services de confiance offerts. Ces informations comprennent les informations fournies par le Client final et celles collectées par d'autres moyens techniques et qui sont contenues dans le périmètre de ces services.

Les prestataires de services de réponse aux incidents (PRIS), de détection des incidents de sécurité (PDIS), et d'intégration et de maintenance sécurisée (PIAMS) sont tenus d'héberger au Togo l'ensemble de leurs équipements ainsi que les données associées à leurs activités.

Cependant, l'Agence Nationale de la Cybersécurité (ANCy) peut exceptionnellement accorder une dérogation à cette obligation d'hébergement, sous réserve que le prestataire concerné fournisse une justification crédible et documentée de son incapacité à satisfaire cette exigence. La demande de dérogation sera soumise à une évaluation rigoureuse avant approbation.

Le Prestataire de services de confiance devra donc s'engager à respecter ces exigences. Le formulaire contenant l'engagement doit être signé et joint au dossier de demande de qualification.

REF : Formulaire de demande de qualification

Le Prestataire doit protéger au minimum les informations sensibles relatives à la prestation, et notamment les preuves, les constats et les rapports.

3.1.2. Code d'éthique

Le Prestataire de services de confiance en cybersécurité doit se conformer à un code d'éthique (**REF Code d'éthique professionnel pour les Prestataires)**.

Une copie dudit code signée par tout le personnel technique est jointe au dossier de demande de qualification.

Ce code inclut par ailleurs les principes faisant référence à :

- La protection de la Nation, la société, et les Infrastructures ;
- L'indépendance, l'objectivité, la loyauté, la discrétion et l'impartialité ;
- Le secret professionnel et la confidentialité des informations ;
- Le professionnalisme ;
- Le respect de la législation et de la règlementation nationale en vigueur ainsi que des bonnes pratiques.

3.1.3. Ressources et compétences

3.1.3.1. Vérification du curriculum vitæ et de l'éthique

Dans le cas d'une personne morale, le Prestataire de services de confiance en cybersécurité est responsable au même titre que le personnel technique qu'il emploie et de la véracité des informations contenues dans leur CV.

Tout personnel technique doit signer une charte d'éthique lors de son engagement.

Le Prestataire de services de confiance en cybersécurité doit veiller au respect du code d'éthique par son personnel technique.

Dans le cas d'une personne physique, le Prestataire est responsable de la véracité des informations contenues dans son CV.

REF : Modèle de Cv

3.1.3.2. Mise à jour des compétences

Dans le cas d'une personne morale, il est de la responsabilité du Prestataire de services de confiance en cybersécurité d'établir un processus visant à maintenir continuellement les compétences de son personnel technique, en particulier dans les domaines où il est qualifié.

Ce processus est soumis à validation par le biais d'un plan de formation à inclure dans le dossier de demande de qualification.

3.1.3.3. Compétences du personnel technique

Dans le cas d'une personne morale, le Prestataire de services de confiance en cybersécurité doit garantir que tous les membres de son personnel technique affectés à une mission ou activité possèdent les compétences adéquates pour accomplir correctement les tâches liées à cette mission.

Il revient au Prestataire de services de confiance de constituer une équipe en fonction des services à fournir. Il doit également s'assurer d'avoir à sa disposition du personnel technique possédant les compétences nécessaires pour chaque prestation pour laquelle il est qualifié.

3.1.3.4. Solutions et procédures opérationnelles

Le Prestataire de services de confiance en cybersécurité est tenu de développer et exposer de manière détaillée ses solutions ainsi que les procédures opérationnelles qui seront mises en place dans le cadre de la fourniture du service.

3.2. EXIGENCES SPECIFIQUES RELATIVES AUX PERSONNES MORALES

3.2.1. Conditions administratives

Toute personne morale disposant d'une existence légale désirant exercer une activité de services de confiance en cybersécurité doit remplir les conditions suivantes :

- La carte d'identification fiscale doit mentionner « la sécurité des systèmes d'information et des réseaux » comme activité.
- Avoir une organisation interne comprenant à minima une direction technique ou équivalent.
- Ne pas être en état de faillite.
- Le représentant légal ainsi que le personnel technique relevant de la personne morale doivent jouir de leurs droits civils.

- Le représentant légal et le personnel technique relevant de la personne morale doivent être affiliés à la caisse nationale de sécurité sociale.
- Disposer d'un site sur le territoire togolais ou présenter une entrée en groupement avec un Prestataire résident sur le territoire togolais.

3.2.2. Conditions techniques

Les moyens techniques et matériels minimums nécessaires pour exercer une activité dans le domaine de la sécurité de l'information sont fixés comme suit :

- Détenir un manuel de procédures organisationnelles et techniques permettant d'assurer la qualité de la prestation et de protéger les informations et données qui seront récupérées et traitées contre les risques de dommages, de modifications ou autres pouvant survenir.
- Utiliser les outils et produits reconnus par l'ANCy pour mener les missions propres à chaque activité.

3.2.3. Conditions relatives aux personnels

Il est nécessaire de :

- Disposer de références d'activités similaires relevant du domaine de la prestation (Le nombre de missions minimal requis est identifié dans le référentiel d'exigence de la prestation objet de qualification).
- Disposer d'un personnel ayant les profils compatibles aux activités pour lesquelles le Prestataire demande la qualification.
- Disposer d'un nombre suffisant de personnels techniques par domaine où la qualification est demandée compte tenu du fait que la qualification peut être obtenue pour plusieurs prestations avec le même personnel, si le profil de ce dernier est conforme aux exigences des domaines de la prestation où le Prestataire de services de confiance le positionne.
- Dans le cas des prestations d'audit, de réponse, de détection et de maintenance sécurisée, le personnel technique doit être exclusivement togolais. Si le prestataire rapporte la preuve de l'impossibilité de remplir cette condition, l'ANCy peut de façon discrétionnaire accorder une dérogation.

- Le personnel technique doit avoir une expérience professionnelle (le nombre d'années d'expérience minimal requis est identifié dans le Référentiel d'exigences de la prestation objet de la qualification) dans l'activité de cybersécurité objet de la demande de qualification.
- Le personnel technique doit avoir exécuté des missions similaires à celles du domaine de la prestation (le nombre de missions minimal requis est identifié dans le Référentiel d'exigences de la prestation objet de qualification) durant les 2 dernières années.
- Le personnel technique doit être détenteur d'au moins un certificat professionnel dans le domaine de la sécurité de l'information.

3.2.4. Documents demandés

Toute personne morale doit fournir les documents suivants :

- Une demande adressée au directeur général de l'ANCy ;
- Le Formulaire de demande de qualification dûment rempli **REF : Formulaire de demande de qualification ;**
- Une (01) photo d'identité du représentant légal de la société se présentant comme Candidat à la qualification ;
- Un plan de localisation de l'entreprise ;
- Une copie des statuts de la société ;
- Un organigramme de l'entreprise ;
- Une copie de l'attestation d'inscription au Registre du Commerce et du Crédit Mobilier (RCCM) ;
- Une copie de la pièce d'identité des dirigeants et/ou du représentant légal de la société ;
- Une copie de la carte d'adhésion à la Caisse Nationale de Sécurité Sociale du représentant légal de la société ;
- Une copie des cartes d'identité nationale du personnel technique ;
- Une copie des cartes d'adhésion à la caisse nationale de la sécurité sociale du personnel technique ;
- Le bulletin N°3 du casier judiciaire datant de moins de trois mois des dirigeants et/ou du représentant légal de la société et du personnel technique ;
- Une clé publique issue d'une autorité de certification électronique de confiance, s'il en existe ;
- Le code d'éthique signé REF **: Code d'éthique professionnel pour les Prestataires** ;

- Les CVs du personnel technique dûment remplis et signés **REF : Modèle de CV ;**
- Une copie des diplômes universitaires du personnel technique prouvant le niveau scientifique requis ;
- Une copie des certificats professionnels du personnel technique dans le domaine de la sécurité informatique reconnus par l'ANCy ;
- Les documents justifiant l'expérience professionnelle du personnel technique dans l'activité de cybersécurité objet de la demande de qualification ;
- Chaque attestation d'expérience du personnel technique doit être accompagnée de l'attestation d'expérience dûment remplie **REF : Attestation d'expérience ;**
- Toute preuve d'exécution des projets de sécurité réalisés à savoir les références de la société (attestation de la bonne exécution, Procès-verbaux, etc..) et dans l'activité de cybersécurité objet de la demande de qualification ;
- Une copie du manuel de procédures organisationnelles et techniques pour assurer la qualité de la prestation et pour protéger les données reçues et traitées contre le risque de dommages, de modifications ou d'autres risques pouvant survenir ;
- La liste des outils et produits reconnus par l'ANCy pour mener les missions propres à chaque activité. **REF : liste des outils et produits.**

3.3. EXIGENCES SPECIFIQUES RELATIVES AUX PERSONNES PHYSIQUES

3.3.1. Conditions administratives

Toute personne physique désirant exercer une activité de services de confiance en cybersécurité doit remplir les conditions suivantes :

- Jouir de ses droits civils ;
- La carte d'identification fiscale doit mentionner « la sécurité des systèmes d'information et des réseaux » comme activité ;
- Être titulaire au moins d'une licence en informatique ou en télécommunications ou d'un diplôme équivalent ;
- Être détenteur d'un certificat professionnel dans le domaine de la sécurité de l'information ;

- Disposer d'une expérience professionnelle dans l'activité de cybersécurité objet de la demande de qualification (le nombre d'années d'expérience minimal requis est identifié dans le Référentiel d'exigences de la prestation objet de qualification) ;
- Avoir exécuté des missions similaires à celles de l'activité objet de qualification durant les trois (03) dernières années. (Le nombre de missions minimal requis est identifié dans le Référentiel d'exigences de la prestation objet de qualification) ;
- Être affilié à la Caisse Nationale de Sécurité Sociale ;
- Ne faire l'objet d'aucune condamnation judiciaire ;

3.3.2. Conditions techniques

Les moyens techniques et matériels minimums nécessaires pour exercer une activité dans le domaine de la sécurité de l'information sont fixés comme suit :

- Détenir un manuel de procédures organisationnelles et techniques permettant d'assurer la qualité de la prestation et de protéger les informations et données qui seront récupérées et traitées contre les risques de dommages, de modifications ou autres risques pouvant survenir.
- Utiliser les outils et produits reconnus par l'ANCy pour mener les missions propres à chaque activité, (**REF : Liste des outils et produits**).

3.3.3. Documents demandés

Toute personne physique doit fournir les documents suivants :

- Une demande adressée au directeur général de l'ANCy ;
- Le Formulaire de demande de qualification dûment rempli **REF : Formulaire de demande de qualification** ;
- Une photo d'identité du Candidat à la qualification ;
- Une copie de la carte d'adhésion à la Caisse Nationale de Sécurité Sociale ;
- Une copie de la carte d'identité nationale ;
- Le bulletin N°3 du casier judiciaire datant de moins de trois mois ;
- Une clé publique issue d'une autorité de certification électronique de confiance, s'il en existe ;
- Une copie de la carte d'identification fiscale ;

- Le code d'éthique signé **REF : Code d'éthique professionnel pour les Prestataires** ;
- Un CV dûment rempli et signé **REF : Modèle de Cv ;**
- Une copie du diplôme universitaire prouvant le niveau scientifique requis ;
- Une copie des certificats professionnels dans le domaine de la sécurité informatique reconnus par l'ANCy ;
- Les documents justifiant l'expérience professionnelle minimale de trois (3) années dans l'activité de cybersécurité objet de la demande de qualification ;
- Une attestation d'expérience dûment remplie **REF : Attestation d'expérience ;**
- Toute preuve d'exécution des projets de sécurité réalisés (attestation de la bonne exécution, Procès-verbaux, etc..), et dans l'activité de cybersécurité objet de la demande de qualification ;
- Une copie du manuel de procédures organisationnelles et techniques pour assurer la qualité de la prestation et pour protéger les données reçues et traitées contre le risque de dommages, de modifications ou d'autres risques pouvant survenir ;
- La liste des outils et produits reconnus par l'ANCy pour mener les missions propres à chaque activité. **REF : liste des outils et produits.**

3.4. EXIGENCES SPECIFIQUES PAR TYPE DE PRESTATION

Les Référentiels établissent des exigences et des recommandations spécifiques pour les Prestataires de services de confiance en cybersécurité par type de prestation.

La qualification d'un Prestataire est effectuée en suivant le processus de qualification, qui atteste que le Prestataire est en conformité avec les exigences définies dans les Référentiels.

Les exigences spécifiques doivent être respectées par les Prestataires de services de confiance pour obtenir la qualification.

La liste suivante des Référentiels des exigences par type de prestations est publiée sur le site web de l'ANCy et comprend :

- Le Référentiel d'exigences pour les Prestataires d'audit de la sécurité des systèmes d'information.
- Le Référentiel d'exigences pour les Prestataires de détection des incidents de sécurité ;
- Le Référentiel d'exigences pour les Prestataires de réponse aux incidents de sécurité ;

- Le Référentiel d'exigences pour les Prestataires d'intégration, administration et de maintenance sécurisées ;
- Le Référentiel d'exigences des Prestataires de services d'accompagnement et de conseil en cybersécurité.

ANNEXES

REF : Déclaration de la politique de qualification de l'ANCy

REF : Formulaire de demande de qualification

REF : Formulaire de demande de reconnaissance de qualification

REF : Modèle de Cv

REF : Attestation d'expérience

REF : Liste des outils et produits

REF : Code d'éthique professionnel pour les Prestataires

DECLARATION DE POLITIQUE DE QUALIFICATION DES PRESTATAIRES DE SERVICE DE CONFIANCE EN CYBERSÉCURITÉ

Le système de qualification des prestataires de services de confiance en cybersécurité au Togo a été créé dans le cadre de la politique nationale qui vise à développer l'infrastructure de sécurité et soutenir la compétitivité des entreprises togolaises au niveau du marché national et international.

Cet objectif peut être assuré par le biais du processus de qualification par l'ANCy, qui traduit l'aptitude des entités à fournir des services de confiance en cybersécurité de qualité.

L'objectif principal de la qualification est de garantir l'efficacité et l'efficience technique des prestataires offrant des services de confiance en cybersécurité, ce qui contribue à développer la confiance dans l'économie numérique, en se fondant sur des audits de conformité.

La qualification par l'ANCy vise ainsi à mettre à la disposition de l'administration, des organismes de services essentiels, et toutes autres personnes, des produits et services répondant à leurs besoins en matière de sécurité des systèmes d'information.

La Direction Générale de l'ANCy s'engage à fournir et mettre en 'œuvre les moyens nécessaires afin de garantir la conformité du système de qualification togolais à la réglementation nationale et aux normes internationales en vigueur.

La Direction Générale de l'ANCy s'engage à ce que les procédures qui composent le système de qualification mis en place soient appliquées de manière non discriminatoire et qu'elles garantissent l'impartialité, la confidentialité, l'objectivité et la transparence à tous les niveaux dans le but d'instaurer la confiance nécessaire envers la qualité des services fournis par les prestataires de services de confiance en cybersécurité qualifiés par l'ANCy.

L'ANCy dispose des pouvoirs prévus par la législation togolaise et qui garantissent son indépendance dans le mécanisme de prise de décision.

La Direction Générale de l'ANCy répond de la politique de qualification togolaise ainsi que des décisions prises dans ce domaine.

Considérant que les personnes impliquées dans le processus de qualification constituent un facteur important de la reconnaissance du système de qualification togolais, la Direction Générale de l'ANCy s'engage à veiller à la compétence et à l'objectivité de ces personnes, leur formation, ainsi qu'au suivi de leurs prestations de façon périodique. Le maintien et le développement de la compétence du personnel impliqué dans le système de qualification est en effet garant du niveau de performance des prestataires de services de confiance qualifiés.

La Direction Générale de l'ANCy s'engage à déployer les moyens nécessaires pour fournir des prestations de haute qualité permettant de répondre aux attentes et aux besoins de toutes les parties prenantes. Elle veille au maintien d'une communication suffisante pour assurer une bonne identification de ces besoins, et accorde la plus grande importance au développement de nouvelles activités dans les meilleurs conditions et délais.

La Direction Générale de l'ANCy s'assure, avec l'engagement de tout le personnel de l'ANCy, du respect à tous les niveaux de la mise en œuvre et de la consolidation des politiques et objectifs mis en place, et en particulier de la politique de qualification. Les objectifs généraux permettant la mise en œuvre de cette politique sont traduits en plans d'actions, et sont revus et améliorés périodiquement.

Les résultats des revues de direction, des audits internes, l'examen des plaintes et appels, et de toutes autres informations reçues, sont indispensables pour la revue de l'efficacité et du bon fonctionnement du système de management de la qualification de l'ANCy.

La Direction Générale de l'ANCy veille à établir des procédures documentaires et correctives nécessaires, ainsi qu'à développer des mécanismes d'amélioration continue dans toutes les phases de gestion du système de qualification au sein de l'ANCy.

Dans le cadre du respect des principes de bonne gouvernance, de transparence et d'impartialité, la Direction Générale de l'ANCy veille à assurer un suivi permanent des activités de qualification à tous les niveaux et auprès des différents intervenants.

Date / Signature

FORMULAIRE DE DEMANDE DE QUALIFICATION DES PRESTATAIRES DE SERVICES DE CONFIANCE EN CYBERSECURITE

I. Demandeur personne morale

1. Fiche contact

Entité	
Dénomination sociale	
N° RCCM ou équivalent	
Adresse postale du siège social	
Courrier électronique	
Téléphone	
Représentant légal	
Nom &Prénom	
Fonction	
Adresse postale	
Pays	
Courrier électronique	
Téléphone	
Représentant du projet de qualification	
Nom &Prénom	
Fonction	
Adresse postale	
Courrier électronique	
Téléphone	
Contact opérationnel en cas d'incident	
Nom &Prénom	
Fonction	
Adresse postale	
Courrier électronique	
Téléphone	

2. Fiche service (s)

Famille de services susceptibles d'être qualifiés	Services sollicités au titre de la demande qualification (à cocher)
Prestataire de services d'audit de la sécurité des systèmes d'information	
Prestataire de services de détection des incidents de sécurité	
Prestataire de services de réponse aux incidents de sécurité	
Prestataire de services d'intégration, administration et de maintenance sécurisées	
Prestataire de service d'accompagnement et de conseils en cybersécurité	

3. Présentation générale de la société

La présentation devra inclure les activités / métiers, la gamme de produits utilisés dans le cadre de la prestation du service de sécurité des systèmes d'information, la gamme de services relatifs à la sécurité des systèmes d'information, l'organisation et l'organigramme, les implantations géographiques, l'effectif, la répartition du capital et le chiffre d'affaires, et toute autre information pertinente.

4. Présentation générale du service

La présentation du service doit être impartiale, neutre et exempte de tout langage promotionnel. Elle devra faire référence à la liste des services et produits, aux fonctions de sécurité, aux performances et caractéristiques, l'architecture matérielle et/ou logicielle, le cadre de déploiement de cette architecture.
Le service dispose-t-il de certification (s)(ISO 27001, ISO 22301, ou autres) ?

5. Localisation (uniquement pour personne morale)

Localisation des systèmes d'information impliqués dans l'administration, l'exploitation, la maintenance ou le support du service.	
Togo	

Autres	

6. Support

Est-ce que le service dispose d'un centre d'assistance capable de traiter les questions les plus courantes posées par les utilisateurs du service ? Oui ☐ Non ☐ SI Oui	
Contact du responsable du centre	
Courrier électronique du centre	
Téléphone du centre	
Description du centre : Système de Gestion des Tickets, Outils de Support à Distance, Outils de Reporting et d'Analyse, Accords de Niveau de Service (SLA)	

7. Formation

Plan de formation des 2 dernières années du personnel selon le type de service Années	Intitulé de la formation	Nom prénom Personnel technique Bénéficiaire	Qualité	Formation certifiante (certificate number)

8. Centre de formation

Le service bénéficie-t-il d'un centre de formation ? Oui ☐ Non ☐ Si Oui	
Contact du responsable du centre	
Adresse	
Courrier électronique	
Site web (*optionnel)	
Téléphone	
Contact	
Le centre dispose-t-il d'un agrément ? Oui ☐ Non ☐ Si Oui	
Référence d'agrément	

9. Cryptologie

Le service bénéficie-t-il de mécanismes de cryptologie ?	
NON	
OUI	

(Précisez l'ensemble des mécanismes cryptographiques)	

10. Compétences et références

Prestataire d'audit de la sécurité des systèmes d'information	
Nombre de prestations réalisées au cours des 24 derniers mois	
Nombre de prestations réalisées depuis le début de l'exercice en cours	
Nombre du personnel	
Nombre du personnel disposant de certification en sécurité de l'information	
Prestataire de détection des incidents de sécurité (*personne morale)	
Nombre de prestations réalisées au cours des 24 derniers mois	
Nombre de prestations réalisées depuis le début de l'exercice en cours	
Nombre du personnel	
Personnel disposant de certification en sécurité de l'information	
Prestataire de réponse aux incidents de sécurité (*personne morale)	
Nombre de prestations réalisées au cours des 24 derniers mois	
Nombre de prestations réalisées depuis le début de l'exercice en cours	
Nombre du personnel	
Personnel disposant de certification en sécurité de l'information	
Prestataire d'intégration, d'administration et de maintenance sécurisées (*personne morale	
Nombre de prestations réalisées au cours des 24 derniers mois	
Nombre de prestations réalisées depuis le début de l'exercice en cours	
Nombre du personnel	
Personnel disposant de certification en sécurité de l'information	
Prestataire de service d'accompagnement et de conseil en cybersécurité	
Nombre de prestations réalisées au cours des 24 derniers mois	
Nombre de prestations réalisées depuis le début de l'exercice en cours	
Nombre du personnel	
Personnel disposant de certification en sécurité de l'information	

11. Manuel des procédures opérationnelles

Ce manuel permet d'assurer la qualité de la prestation et de protéger les données reçues et traitées contre le risque de dommages, de modifications ou d'autres risques pouvant survenir.
Joindre le document en décrivant les données ci-dessous : 1. Date d'Élaboration : La date à laquelle le document a été initialement créé. 2. Auteur : La personne ou l'entité responsable de la création du document. 3. Statut : Indique si le document est en cours de rédaction, en révision, approuvé, etc. 4. Historique des Révisions : Une liste des modifications apportées au document, y compris les dates de révision et une brève description des changements effectués. 5. Résumé : Une brève description du contenu et des objectifs du document.

II. Demandeur personne physique

1. Fiche contact

Prestataire physique	
Nom et prénom	
Nationalité	
Adresse	
Carte d'identité nationale	
N° Adhésion à la caisse nationale de la sécurité sociale	
Identifiant fiscal	
Email	
Site web (*optionnel)	

2. Fiche service (s)

Famille de services susceptibles d'être qualifiés	Services sollicités au titre de la demande qualification (à cocher)
Prestataire de services d'audit de la sécurité des systèmes d'information	
Prestataire de service d'accompagnement et de conseils en cybersécurité	

3. Présentation générale

La présentation du service doit être impartiale, neutre et exempte de tout langage promotionnel. Cette présentation fera référence à l'expertise du prestataire, ses compétences et ses connaissances.

4. Formation

Plan de formation des 2 dernières années du personnel selon le type de service				
Années	Intitulé de la formation	Personnel technique Bénéficiaire	Qualité	Formation certifiante (certificate number)

5. Centre de formation

Le service bénéficie-t-il d'un centre de formation ? Oui ☐ Non ☐ Si oui	
Contact	
Adresse	
Courrier électronique	
Site web (*optionnel)	
Téléphone	

Contact	

6. Cryptologie

Le service bénéficie-t-il de mécanismes de cryptologie ?	
NON	
OUI (Précisez l'ensemble des mécanismes cryptographiques)	

7. Compétences et références

Prestataire d'audit de la sécurité des systèmes d'information	
Nombre de prestations réalisées au cours des 24 derniers mois	
Nombre de prestations réalisées depuis le début de l'exercice en cours	
Nombre du personnel	
Personnel disposant de certification en sécurité de l'information	
Prestataire de détection des incidents de sécurité (*personne morale)	
Nombre de prestations réalisées au cours des 24 derniers mois	
Nombre de prestations réalisées depuis le début de l'exercice en cours	
Nombre du personnel	
Personnel disposant de certification en sécurité de l'information	
Prestataire de réponse aux incidents de sécurité (*personne morale)	
Nombre de prestations réalisées au cours des 24 derniers mois	
Nombre de prestations réalisées depuis le début de l'exercice en cours	
Nombre du personnel	
Personnel disposant de certification en sécurité de l'information	
Prestataire d'administration et de maintenance sécurisées (*personne morale)	
Nombre de prestations réalisées au cours des 24 derniers mois	
Nombre de prestations réalisées depuis le début de l'exercice en cours	
Nombre du personnel	
Personnel disposant de certification en sécurité de l'information	
Prestataire de service d'accompagnement et de conseil en cybersécurité	
Nombre de prestations réalisées au cours des 24 derniers mois	
Nombre de prestations réalisées depuis le début de l'exercice en cours	
Nombre du personnel	

Pièces à joindre demandeur personne morale

Documents administratifs	Demande adressée au directeur général de l'ANCy
	(01) photo d'identité du représentant légal de la société
	Un plan de localisation de l'entreprise
	Une copie des statuts de la société
	Un organigramme de l'entreprise
	Une copie de l'attestation d'inscription au Registre du Commerce et du Crédit Mobilier (RCCM)
	Une copie de la pièce d'identité des dirigeants et/ou du représentant légal de la société
	Une copie de la carte d'adhésion à la caisse nationale de la sécurité sociale du représentant légal de la société
	Une copie des cartes d'identité nationale du personnel technique
	Une copie des cartes d'adhésion à la caisse nationale de la sécurité sociale du personnel technique
	Le bulletin N°3 du casier judicaire datant de moins de trois mois des dirigeants et/ou du représentant légal d²e la société et du personnel technique
	Une clé publique issue d'une autorité de certification électronique de confiance, s'il en existe.
	Le code d'éthique signé par le représentant légal
	Une déclaration sur l'honneur signée **Déclaration sur l'honneur**
Personnel	Liste et curriculum vitae du personnel selon le type de service * : **Modèle de Cv**
	Liste des diplômes et certifications du personnel technique
	Liste des formations et copies des certificats professionnels du personnel technique
Références	Liste des Références clients (Pv de réception, contrat, attestation de bonne fin d'exécution)
	Copies des attestations de bonne fin d'exécution relatives à la prestation devant préciser la nature et la date de réalisation durant les 3 dernières années
	Preuve de partenariat en vigueur avec l'éditeur des solutions proposées s'il en existe
	La liste des outils et produits **liste des outils et produits**

Personnel disposant de certification en sécurité de l'information	

8. Manuel des procédures opérationnelles

Ce manuel permet d'assurer la qualité de la prestation et de protéger les données reçues et traitées contre le risque de dommages, de modifications ou d'autres risques pouvant survenir.
Joindre le document en décrivant les données ci-dessous : 1. Date d'Élaboration : La date à laquelle le document a été initialement créé. 2. Auteur : La personne ou l'entité responsable de la création du document. 3. Statut : Indique si le document est en cours de rédaction, en révision, approuvé, etc. 4. Historique des Révisions : Une liste des modifications apportées au document, y compris les dates de révision et une brève description des changements effectués. 5. Résumé : Une brève description du contenu et des objectifs du document.

Pièces à joindre demandeur personne physique

Documents administratifs & Personnel	Une photo d'identité du prestataire
	Une demande adressée au directeur général de l'ANCy
	Une copie de la carte d'adhésion à la caisse nationale de la sécurité sociale.
	Une copie de la carte d'identité nationale
	Le bulletin N°3 du casier judiciaire datant de moins de trois mois.
	Une clé publique issue d'une autorité de certification électronique de confiance, s'il en existe.
	Une copie de la carte d'identification fiscale
	Le code d'éthique signé
	Une déclaration sur l'honneur signée **Déclaration sur l'honneur**
	Un cv dûment rempli et signé Modèle **de Cv**
	Une copie du diplôme universitaire prouvant le niveau scientifique requis.
	Une copie des certificats professionnels dans le domaine de la sécurité informatique reconnus par l'ANCy.
	Les documents justifiant l'expérience professionnelle minimale de (3) années dans l'activité de cybersécurité objet de la demande de qualification.
	Une attestation d'expérience dûment remplie **Attestation d'expérience.**
	Toute preuve d'exécution des projets de sécurité réalisés (attestation de la bonne exécution, PVs, ...) et dans l'activité de cybersécurité objet de la demande de qualification.

ENGAGEMENT DU PRESTATAIRE

[Si demandeur personne morale]

La société dénommée .....

Ayant son siège social à .....

Représentée par ..... en sa qualité de .....

Ou

[Si demandeur personne physique]

Je soussigné(e) Madame/Monsieur.....

Domicilié à .....

Reconnais avoir été informé(e) :

Du caractère obligatoire du présent formulaire, dont l'absence rend irrecevable la demande et le dossier de qualification.

Que les informations recueillies font l'objet d'un traitement informatique destiné à la gestion de la qualification des services, et que je dispose des droits conférés par la législation en vigueur sur la protection des données personnelles relativement aux données à caractère personnel recueillies dans le cadre de la qualification.

M'engage à respecter et à faire respecter par les personnes sous ma responsabilité :

Toutes les obligations prévues par la législation togolaise et les bonnes pratiques, dans le cadre du processus de qualification des services de confiance de cybersécurité.

Les exigences prévues par le Modèle de qualification des prestataires de services de confiance de cybersécurité ainsi que les Référentiels en vigueur applicables aux différents services de confiance de cybersécurité.

L'ensemble des critères de confiance ayant permis l'obtention de la qualification par l'ANCy, et par conséquent, à informer l'ANCy de toute modification qui surviendrait dans l'environnement du service qualifié, ou tout changement des circonstances de droit ou de fait dans lesquelles la qualification aurait été obtenue, notamment tout changement de contrôle direct ou indirect, de structure juridique, d'organisation, de locaux, toute cessation d'activité etc.

Toutes conditions et réserves qui seraient fixées par la décision de qualification, et reconnait qu'en cas de manquement l'ANCy pourrait procéder à la suspension ou au retrait immédiat de la qualification.

En conséquence j'autorise à tout moment, l'ANCy à contrôler ou faire contrôler par un centre d'évaluation le respect des présents engagements.

M'engage par ailleurs :

À tout mettre en œuvre pour assurer la protection et la sécurité des informations collectées dans le cadre des prestations de services de confiance fournies, et à répondre de ma responsabilité sur les plans civil et/ou pénal, pour tout acte ou défaillance entrainant un préjudice ou une infraction.

À mettre immédiatement à la disposition de l'ANCy sur sa simple demande dans le cadre de sa mission de coordination de l'action gouvernementale en matière de défense des systèmes d'information, les noms des autorités administratives et opérateurs de services essentiels utilisateurs du service dont j'aurai connaissance, ou toute autre information pertinente sollicitée. Par ailleurs, je garantis à l'ANCy et aux centres d'évaluation le cas échéant, l'accès aux éléments techniques, aux locaux, à la documentation, aux ressources et aux personnels nécessaires, dans le cadre du traitement de la demande de qualification ou du suivi de la qualification.

À procéder à la déclaration de tout incident affectant mon système d'information et/ou susceptible d'impacter les systèmes d'informations des Clients finaux, dans les délais et selon les formes et modalités prévues par la législation en vigueur.

A assurer une veille de la sécurité du service qualifié afin d'identifier au plus tôt toute vulnérabilité relative au service qualifié, et informer sans délai et par écrit l'ANCy et l'ensemble des utilisateurs du service qualifié, de tout arrêt de cette veille sécurité.

Date / Signature / Cachet :

DECLARATION SUR L'HONNEUR

Je soussigné(e) Madame/Monsieur.....,

[1]*Agissant en qualité de ..... de la société .....

Déclare sur l'honneur avoir pris connaissance et avoir été clairement informé(e) du processus de qualification des services de confiance par l'ANCy, notamment les différentes étapes du processus ainsi que les obligations à respecter.

Je déclare par ailleurs et certifie l'exactitude et la complétude des informations fournies dans le dossier de demande de qualification ainsi que toutes les pièces y jointes.

En conséquence, j'admets et reconnais avoir été informé que toute fraude ou fausse déclaration constitue un motif de décision d'interruption du processus de qualification ou de refus de qualification par l'ANCy.

Conformément aux engagements pris dans le Formulaire de demande de qualification, je m'engage à informer immédiatement l'ANCy pendant le traitement de ma demande ainsi qu'après l'obtention de la qualification sollicitée, de toute modification des informations ainsi communiquées.

Date / Signature / Cachet :

[1] ***Si demandeur personne morale**

FORMULAIRE DE DEMANDE DE RECONNAISSANE DES PRESTATAIRES DE SERVICES DE CONFIANCE EN CYBERSECURITE QUALIFIES DANS UN PAYS ETRANGER

I. Demandeur personne morale

1. Fiche contact

Entité	
Dénomination sociale	
N° RCCM ou équivalent	
Adresse postale du siège social	
Pays	
Courrier électronique	
Téléphone	
Site web (***optionnel)**	
Représentant légal	
Nom &Prénom	
Fonction	
Adresse postale	
Pays	
Nationalité	
Courrier électronique	
Téléphone	
Représentant du projet de qualification	
Nom &Prénom	
Fonction	
Adresse postale	
Pays	
Nationalité	
Courrier électronique	
Téléphone	
Contact opérationnel en cas d'incident	
Nom &Prénom	
Fonction	
Adresse postale	
Pays	
Courrier électronique	
Téléphone	

2. Fiche service (s)

Famille de services susceptibles d'être qualifiés	Services sollicités au titre de la demande qualification (à cocher)
Prestataire de services d'audit de la sécurité des systèmes d'information ou équivalent	
Prestataire de services de détection des incidents de sécurité ou équivalent	
Prestataire de services de réponse aux incidents de sécurité ou équivalent	
Prestataire de services d'intégration, administration et de maintenance sécurisées ou équivalent	
Prestataire de service d'accompagnement et de conseils en cybersécurité ou équivalent	

3. Présentation générale de la société

La présentation devra inclure les activités / métiers, la gamme de produits utilisés dans le cadre de la prestation du service de sécurité des systèmes d'information, la gamme de services relatifs à la sécurité des systèmes d'information, l'organisation et l'organigramme, les implantations géographiques, l'effectif, la répartition du capital et le chiffre d'affaires, et toute autre information pertinente.

4. Présentation générale du service

La présentation du service doit être impartiale, neutre et exempte de tout langage promotionnel. Elle devra faire référence à la liste des services et produits, aux fonctions de sécurité, aux performances et caractéristiques, l'architecture matérielle et/ou logicielle, le cadre de déploiement de cette architecture.
Le service dispose-t-il de certification (s)(ISO 27001, ISO 22301) ?

5. Localisation (*personne morale)

Localisation des systèmes d'information impliqués dans l'administration, l'exploitation, la maintenance ou le support du service	
Pays étranger	
Autres	

6. Support (*personne morale)

Est-ce que le service dispose d'un centre d'assistance capable de traiter les questions les plus courantes posées par les utilisateurs du service ? Oui ☐ Non ☐ SI Oui	
Contact	
Courrier électronique	
Téléphone	
Description du centre : Système de Gestion des Tickets, Outils de Support à Distance, Outils de Reporting et d'Analyse, Accords de Niveau de Service (SLA)	

7. Formation (*personne morale)

Plan de formation des 2 dernières années du personnel selon le type de service				
Années	Intitulé de la formation	Personnel technique Bénéficiaire	Qualité	Formation certifiante (certificate number)

8. Centre de formation

Le service bénéficie-t-il d'un centre de formation ? Oui ☐ Non ☐ Si Oui	
Contact	
Adresse	
Courrier électronique	
Site web (*optionnel)	
Téléphone	

9. Cryptologie

Le service bénéficie-t-il de mécanismes de cryptologie ?	
NON	
OUI (Précisez l'ensemble des mécanismes cryptographiques)	

10. Compétences et références

Prestataire d'audit de la sécurité des systèmes d'information	
Nombre de prestations réalisées au cours des 24 derniers mois	
Nombre de prestations réalisées depuis le début de l'exercice en cours	
Nombre du personnel	
Personnel disposant de certification en sécurité de l'information	
Prestataire de détection des incidents de sécurité (*personne morale)	
Nombre de prestations réalisées au cours des 24 derniers mois	
Nombre de prestations réalisées depuis le début de l'exercice en cours	
Nombre du personnel	
Personnel disposant de certification en sécurité de l'information	
Prestataire de réponse aux incidents de sécurité (*personne morale)	
Nombre de prestations réalisées au cours des 24 derniers mois	
Nombre de prestations réalisées depuis le début de l'exercice en cours	
Nombre du personnel	
Personnel disposant de certification en sécurité de l'information	

Prestataire d'administration et de maintenance sécurisées (*personne morale)	
Nombre de prestations réalisées au cours des 24 derniers mois	
Nombre de prestations réalisées depuis le début de l'exercice en cours	
Nombre du personnel	
Personnel disposant de certification en sécurité de l'information	
Prestataire de service d'accompagnement et de conseil en cybersécurité	
Nombre de prestations réalisées au cours des 24 derniers mois	
Nombre de prestations réalisées depuis le début de l'exercice en cours	
Nombre du personnel	
Personnel disposant de certification en sécurité de l'information	

11. Manuel des procédures opérationnelles

Ce manuel permet d'assurer la qualité de la prestation et de protéger les données reçues et traitées contre le risque de dommages, de modifications ou d'autres risques pouvant survenir.
Joindre le document en décrivant les données ci-dessous : 6. Date d'Élaboration : La date à laquelle le document a été initialement créé. 7. Auteur : La personne ou l'entité responsable de la création du document. 8. Statut : Indique si le document est en cours de rédaction, en révision, approuvé, etc. 9. Historique des Révisions : Une liste des modifications apportées au document, y compris les dates de révision et une brève description des changements effectués. 10. Résumé : Une brève description du contenu et des objectifs du document.

12. Centre d'évaluation ou organisme ayant délivré la qualification

Centre d'évaluation /entité ayant délivré la qualification	
Dénomination	
Adresse postale du siège social	
Pays	
Téléphone	
Courrier Électronique	
Téléphone	
Site web (***optionnel)**	

Responsable de qualification du centre d'évaluation ou de l'organisme ayant délivré la qualification	
Nom &Prénom	
Adresse postale	
Pays	
Nationalité	
Courrier électronique	
Téléphone	

13. Qualification obtenue

Qualification	
Date d'octroi	
Date de dernière supervision	
Date de fin de qualification	
Pays	
Prestations Objet de qualification	
Décrire la méthodologie d'évaluation déployée ayant conduit à la qualification	

II. Demandeur personne physique

1. Fiche contact

Prestataire physique	
Nom et prénom	
Nationalité	
Adresse	
Pays	
Carte d'identité nationale ou équivalent	
N° Adhésion à la caisse nationale de la sécurité sociale ou équivalent	
Identifiant fiscal ou équivalent	
Courrier électronique	
Téléphone	
Site web (*optionnel)	

2. Fiche service (s)

Famille de services susceptibles d'être qualifiés	Services sollicités au titre de la demande qualification (à cocher)
Prestataire de services d'audit de la sécurité des systèmes d'information	
Prestataire de service d'accompagnement et de conseils en cybersécurité	

3. Présentation générale de la société

La présentation devra inclure les activités / métiers, la gamme de produits utilisés dans le cadre de la prestation du service de sécurité des systèmes d'information, la gamme de services relatifs à la sécurité des systèmes d'information, l'organisation et l'organigramme, les implantations géographiques, l'effectif, la répartition du capital et le chiffre d'affaires, et toute autre information pertinente.

4. Formation

Plan de formation des 2 dernières années du personnel selon le type de service				
Années	Intitulé de la formation	Personnel technique Bénéficiaire	Qualité	Formation certifiante (certificate number)

5. Centre de formation

Le service bénéficie-t-il d'un centre de formation ? Oui ☐ Non ☐ Si Oui	
Contact	
Adresse	
Courrier électronique	
Site web (*optionnel)	
Téléphone	
Contact	

6. Cryptologie

Le service bénéficie-t-il de mécanismes de cryptologie ? Oui ☐ Non ☐	
NON	
OUI (Précisez l'ensemble des mécanismes cryptographiques)	

7. Compétences et références

Prestataire d'audit de la sécurité des systèmes d'information	
Nombre de prestations réalisées au cours des 24 derniers mois	
Nombre de prestations réalisées depuis le début de l'exercice en cours	
Nombre du personnel	
Personnel disposant de certification en sécurité de l'information	
Prestataire de détection des incidents de sécurité (*personne morale)	
Nombre de prestations réalisées au cours des 24 derniers mois	
Nombre de prestations réalisées depuis le début de l'exercice en cours	
Nombre du personnel	
Personnel disposant de certification en sécurité de l'information	
Prestataire de réponse aux incidents de sécurité (*personne morale)	
Nombre de prestations réalisées au cours des 12 derniers mois	
Nombre de prestations réalisées depuis le début de l'exercice en cours	
Nombre du personnel	
Personnel disposant de certification en sécurité de l'information	

Prestataire d'administration et de maintenance sécurisées (*personne morale)	
Nombre de prestations réalisées au cours des 24 derniers mois	
Nombre de prestations réalisées depuis le début de l'exercice en cours	
Nombre du personnel	
Personnel disposant de certification en sécurité de l'information	
Prestataire de service d'accompagnement et de conseil en cybersécurité	
Nombre de prestations réalisées au cours des 24 derniers mois	
Nombre de prestations réalisées depuis le début de l'exercice en cours	
Nombre du personnel	
Personnel disposant de certification en sécurité de l'information	

8. Manuel des procédures opérationnelles

Ce manuel permet d'assurer la qualité de la prestation et de protéger les données reçues et traitées contre le risque de dommages, de modifications ou d'autres risques pouvant survenir.

9. Centre d'évaluation ou organisme ayant délivré la qualification

Centre d'évaluation /entité ayant délivré la qualification	
Dénomination	
Adresse postale du siège social	
Pays	
Téléphone	
Courrier Électronique	
Téléphone	
Site web (***optionnel**)	
Responsable de qualification du centre d'évaluation ou de l'organisme ayant délivré la qualification	
Nom & Prénom	

Adresse postale	
Pays	
Nationalité	
Courrier électronique	
Téléphone	

10. Qualification obtenue

Qualification	
Date d'octroi	
Date de dernière supervision	
Date de fin de qualification	
Pays	
Prestations Objet de qualification	
Décrire la méthodologie d'évaluation déployée ayant conduit à la qualification	

Pièces à joindre

I. Demandeur personne morale

Documents administratifs	Demande adressée au directeur général de l'ANCy
	Une photo d'identité du représentant légal de la société.
	Un plan de localisation de l'entreprise.
	Une copie des statuts de la société.
	Un organigramme de l'entreprise.
	Une copie de l'attestation d'inscription au Registre du Commerce et du Crédit Mobilier (RCCM) ou équivalent.
	Une copie de la pièce d'identité des dirigeants et/ou du représentant légal de la société ou équivalent.
	Une copie de la carte d'adhésion à la caisse nationale de la sécurité sociale du représentant légal de la société ou équivalent.
	Une copie des cartes d'identité nationale du personnel technique ou équivalent.
	Une copie des cartes d'adhésion à la caisse nationale de la sécurité sociale du personnel technique ou équivalent.
	Le bulletin N°3 du casier judiciaire datant de moins de trois mois des dirigeants et/ou du représentant légal de la société et du personnel technique.
	Une clé publique issue d'une autorité de certification électronique de confiance, s'il en existe.
	Le code d'éthique signé.
	Une preuve de qualification obtenue auprès d'un organisme officiel ou un centre d'évaluation agrée dans un pays tiers.
Personnel	Liste et curriculum vitae du personnel selon le type de service **Modèle de CV**
	Liste des diplômes et certifications.
	Liste des formation et copies des certificats professionnels.
Références	Liste des Références.
	Copies des attestations de bonne fin d'exécution relatives à la prestation devant préciser la nature et la date de réalisation durant les 3 dernières années.
	Preuve de partenariat en vigueur avec l'éditeur des solutions proposées s'il en existe.
	La liste des outils et produits **liste des outils et produits**

II. Demandeur personne physique

Documents administratifs & Personnel	Une photo d'identité du prestataire.
	Une demande adressée au directeur général de l'ANCy.
	Une copie de la carte d'adhésion à la caisse nationale de la sécurité sociale ou équivalent.
	Une copie de la carte d'identité nationale ou équivalent.
	Le bulletin N°3 du casier judiciaire datant de moins de trois mois.
	Une clé publique issue d'une autorité de certification électronique de confiance, s'il en existe.
	Une copie de la carte d'identification fiscale ou équivalent
	Le code d'éthique signé.
	Un cv dûment rempli et signé Modèle **de CV.**
	Une copie du diplôme universitaire prouvant le niveau scientifique requis.
	Une copie des certificats professionnels dans le domaine de la sécurité informatique reconnus par l'agence nationale de la sécurité informatique.
	Les documents justifiant l'expérience professionnelle minimale de (3) années dans l'activité de cybersécurité objet de la demande de qualification.
	Une attestation d'expérience dûment remplie **Attestation d'expérience**
	Toute preuve d'exécution des projets de sécurité réalisés (attestation de la bonne exécution, PVs, ...) et dans l'activité de cybersécurité objet de la demande de qualification.

ENGAGEMENT DU PRESTATAIRE ETRANGER

[Si demandeur personne morale]

La société dénommée .....

Ayant son siège social à .....

Représentée par ..... en sa qualité de .....

Ou

[Si demandeur personne physique]

Je soussigné(e) Madame/Monsieur.....

Domicilié à .....

1. Reconnais avoir été informé(e) :
   - Du caractère obligatoire du présent formulaire, dont l'absence rend irrecevable la demande et le dossier de reconnaissance.
   - Que les informations recueillies font l'objet d'un traitement informatique destiné à la gestion de la qualification des services, et que je dispose des droits conférés par la législation en vigueur sur la protection des données personnelles relativement aux données à caractère personnel recueillies dans le cadre de la reconnaissance de la qualification.
2. M'engage à respecter et à faire respecter par les personnes sous ma responsabilité :
   - Toutes les obligations prévues par la législation togolaise et les bonnes pratiques, dans le cadre du processus de qualification des services de confiance de cybersécurité y compris en matière de reconnaissance des qualifications obtenues à l'étranger.
   - Les exigences prévues par le Modèle de qualification des prestataires de services de confiance de cybersécurité ainsi que les Référentiels en vigueur applicables aux différents services de confiance de cybersécurité.
   - L'ensemble des critères de confiance ayant permis l'obtention de la reconnaissance de qualification par l'ANCy, et par conséquent, à informer l'ANCy de toute modification qui surviendrait dans l'environnement du service qualifié, ou tout changement des circonstances de droit ou de fait dans lesquelles la reconnaissance de qualification aurait été obtenue,

notamment tout changement de contrôle direct ou indirect, de structure juridique, d'organisation, de locaux, toute cessation d'activité etc.

- Toutes conditions et réserves qui seraient fixées par la décision de reconnaissance de qualification, et reconnait qu'en cas de manquement l'ANCy pourrait procéder à la suspension ou au retrait immédiat de la reconnaissance de qualification.

En conséquence, autorise à tout moment, l'ANCy à contrôler ou faire contrôler par un centre d'évaluation le respect des présents engagements.

3. M'engage par ailleurs :
   - À tout mettre en œuvre pour assurer la protection et la sécurité des informations collectées dans le cadre des prestations de services de confiance fournies, et à répondre de ma responsabilité sur les plans civil et/ou pénal, pour tout acte ou défaillance entrainant un préjudice ou une infraction.
   - À mettre immédiatement à la disposition de l'ANCy sur sa simple demande dans le cadre de sa mission de coordination de l'action gouvernementale en matière de défense des systèmes d'information, les noms des autorités administratives et opérateurs de services essentiels utilisateurs du service dont j'aurai connaissance, ou toute autre information pertinente sollicitée. Par ailleurs, je garantis à l'ANCy et aux centres d'évaluation le cas échéant, l'accès aux éléments techniques, aux locaux, à la documentation, aux ressources et aux personnels nécessaires, dans le cadre du traitement de la demande de reconnaissance ou du suivi de la qualification.
   - À procéder à la déclaration de tout incident susceptible d'impacter les systèmes d'informations dans les délais et selon les formes et modalités prévus par la législation en vigueur.
   - A assurer une veille de la sécurité du service qualifié afin d'identifier au plus tôt toute vulnérabilité relative au service qualifié, et informer sans délai et par écrit l'ANCy et l'ensemble des utilisateurs du service qualifié, de tout arrêt de cette veille sécurité.

Date / Signature / Cachet :

DECLARATION SUR L'HONNEUR

Je soussigné(e) Madame/Monsieur.....,

2*Agissant en qualité de ..... de la société .....

Disposant d'une qualification en service de .....

Délivrée à ..... Par ..... En date du .....

Déclare, sur l'honneur, avoir pris connaissance et avoir été clairement informé(e) du processus de qualification des services de confiance par l'ANCy, notamment les différentes étapes du processus ainsi que les obligations à respecter.

Je déclare par ailleurs et certifie l'exactitude et la complétude des informations fournies dans le dossier de demande de reconnaissance de qualification ainsi que toutes les pièces y jointes.

En conséquence, j'admets et reconnais avoir été informé que toute fraude ou fausse déclaration constitue un motif de décision d'interruption du processus de reconnaissance de qualification ou de refus de reconnaissance de qualification par l'ANCy.

Conformément aux engagements pris dans le Formulaire de demande de reconnaissance, je m'engage à informer immédiatement l'ANCy pendant le traitement de ma demande ainsi qu'après l'obtention de la reconnaissance de qualification sollicitée, de toute modification des informations ainsi communiquée.

Date / Signature / Cachet :

[2] ***Si demandeur personne morale**

1 MODELE DE CV

Renseignements généraux :

- Nom & prénom : .....
- Profil : ....
- Nationalité : .....
- CNI / Passeport N° ..... délivrée le ..... À ....
- Adresse : .....
- Tél. : .....
- E-mail : .....
- Site Web (optionnel) : .....

Diplômes universitaires :

Diplôme	Institution	Spécialité / Année	Références de la pièce justificative*

[Joindre les diplômes universitaires et Indiquer la référence du dossier renfermant ces pièces justificatives dans la colonne appropriée]

Cycles de Formations :

Formation / Certification	Institut / Organisme ayant délivré la certification	Promotion / Année	Références de la pièce justificative*

[Joindre l'attestation de réussite ou le certificat de réussite pour chaque cycle de formation mentionné dans le tableau ci-dessus et Indiquer la référence du dossier renfermant ces pièces justificatives dans la colonne appropriée]

Cursus professionnel :

Organisme	Type de recrutement (Contractuel, ...)	Fonctions exercées	Durée		Numéro de la pièce justificative*
			Du	Au	

[Joindre l'attestation de travail et les pièces justificatives de chaque expérience professionnelle mentionnée dans le tableau ci-dessus et Indiquer la référence du dossier renfermant ces pièces justificatives dans la colonne appropriée]

Date / Signature / Cachet :

2 ATTESTATION D'EXPERIENCE

Je soussigné(e) Madame/Monsieur.....,

Agissant en qualité de .....

De la société .....

Atteste par la présente, que Madame / Monsieur..... a acquis une expérience en sécurité informatique durant son activité professionnelle au sein de notre organisme, en assurant les missions suivantes :

Mission réalisée	Période		Taux d'occupation	
	De	À	A plein temps	A temps partiel (indiquer pourcentage)

Observations (Optionnel) :

.....

.....

Date / Signature / Cachet :

3 LISTE DES OUTILS ET PRODUITS

Outil	Version utilisée	Licence	Fonctionnalités	Activités de la prestation

NB : Les critères exigés pour les outils sont :

Pour les produits Commerciaux :

- Avoir une licence valide permettant leur usage correct pour de telles missions avec présentation d'une copie de la licence originale et nominative ;
- Avoir une version récente.

Pour les outils disponibles dans le domaine du logiciel libre ou gratuits :

- Avoir une communauté active ;
- Avoir une source officielle ;
- Avoir une version récente.

Date / Signature / Cachet :