LE PREMIER MINISTRE

REPUBLIQUE TOGOLAISE
Travail-Liberté-Patrie

ARRETE N° 2025-008 /PMRT
portant adoption du référentiel d'exigences des prestataires de services d'accompagnement et de conseil 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 référentiel d'exigences des prestataires de services d'accompagnement et de conseil 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

REFERENTIEL D'EXIGENCES

Prestataires de services d'Accompagnement et de Conseil en cybersécurité

Version du 31 JAN 2025

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 :

Adresse de l'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. Introduction

Ce référentiel d'exigences a été conçu pour encadrer les activités des entreprises qui offrent des services d'accompagnement et de conseil en cybersécurité aux Opérateurs de services essentiels (OSE). Son objectif principal est de garantir la qualité des prestations fournies, de renforcer la confiance des entreprises et institutions qui font appel à ces prestataires, et d'assurer que leurs pratiques respectent les standards internationaux en matière de cybersécurité, dans un contexte de risques croissants liés à la cybercriminalité.

2. Objectifs du référentiel

Le référentiel vise à :

- Fixer des critères clairs pour permettre aux prestataires d'obtenir un agrément officiel ;
- Encourager ces prestataires à améliorer continuellement leurs compétences techniques et organisationnelles ;
- Protéger efficacement les données et systèmes critiques des clients, en réduisant les risques de cyberattaques.

3. Exigences Clés

3.1. Exigences relatives au prestataire

- Le prestataire, qu'il soit une personne morale ou physique, doit démontrer sa capacité à fournir des services fiables, conformes aux standards internationaux ;
- Les prestataires doivent adhérer à un code d'éthique qui inclut la confidentialité des données, l'intégrité dans la prestation des services, et le respect des engagements contractuels ;
- Les prestataires doivent employer des consultants qualifiés et démontrer des compétences solides, validées par des certifications reconnues ;
- Ils doivent mettre en place des mesures strictes pour protéger les données sensibles des clients, notamment en sécurisant les systèmes utilisés pour exécuter les prestations.

3.2. Exigences relatives au déroulement des prestations

Le référentiel décrit des exigences spécifiques pour chaque type de prestation :

Sensibilisation en Cybersécurité

Les programmes de sensibilisation doivent être adaptés aux publics cibles et inclure des messages clairs sur les bonnes pratiques en cybersécurité.

Formation en Cybersécurité

- Formation non certifiante : vise à transmettre des compétences de base en cybersécurité.
- Formation certifiante : prépare les participants à obtenir des certifications reconnues.

Conseil en Cybersécurité

- Préparation : une convention de service doit être établie pour définir les attentes et les responsabilités des deux parties ;
- Exécution : inclut des activités spécifiques comme :
  - Gestion des risques des systèmes d'information ;
  - Sécurité des architectures ;
  - Continuité des activités et gestion des crises cyber.

4. Processus de qualification

Pour obtenir l'agrément, les prestataires doivent constituer un dossier qui prouve qu'ils répondent aux exigences définies dans le référentiel. Ce dossier inclut des informations sur leurs certifications, outils et méthodes de travail, ainsi qu'un engagement à respecter les règles du référentiel.

5. Évaluation

L'ANCy procède à une vérification approfondie des capacités des prestataires, notamment en réalisant un audit pour s'assurer qu'ils disposent des compétences techniques et organisationnelles nécessaires.

Une fois accordé, la qualification est valable pour une durée de trois ans. Pendant cette période, l'ANCy effectue des audits réguliers pour vérifier que les prestataires continuent de respecter les exigences du référentiel.

6. Mesures en cas de non-conformité

Si un prestataire ne respecte pas les exigences du référentiel, il peut faire l'objet de sanctions, notamment une suspension ou un retrait de son agrément. Avant cela, il peut lui être demandé de corriger les manquements identifiés dans un délai donné.

7. Conclusion

Ce référentiel représente un outil essentiel pour organiser et professionnaliser le secteur de la cybersécurité au Togo. En imposant des standards élevés, il contribue à bâtir un environnement numérique sûr, capable de résister aux menaces croissantes dans le cyberespace.

1.PRESENTATION GENERALE

1.1. AVANT-PROPOS

Afin de renforcer leur posture de sécurité et se préparer à faire face aux défis complexes liés à la cybersécurité, les entreprises et organisations peuvent solliciter un accompagnement et conseil dans les démarches de gestion des risques et la gestion des incidents associés par des Prestataires, afin de bénéficier de main d'œuvre et d'expertise souvent difficiles à réunir au sein même de leur organisation.

Cette approche proactive dans la protection des actifs numériques permet aux entreprises de se prémunir et d'assurer la pérennité de leurs activités.

1.2. OBJECTIF DU REFERENTIEL ET DOMAINE D'APPLICATION

Le présent document constitue le référentiel d'exigences applicables à un Prestataire de services d'accompagnement et de conseils en cybersécurité.

Il vise à établir un cadre permettant la qualification d'un Prestataire de service de conseils et d'accompagnement en cybersécurité. Il permet d'accompagner, d'une part les consultants dans la réalisation des missions de conseils et d'accompagnement en cybersécurité et permettre, d'autre part au Client final de la prestation, de disposer de garanties sur les compétences du Prestataire et de son personnel, sur la qualité des prestations fournies et sur la confiance que le Client final peut accorder au Prestataire.

Il a vocation à permettre la qualification de cette famille de Prestataires conformément à la règlementation en vigueur selon les modalités décrites dans le Modèle de qualification des Prestataires de service de confiance en cybersécurité.

1.3. DOCUMENTS DE REFERENCE

Le présent Référentiel s'inscrit dans un cadre légal et règlementaire plus global en vigueur au Togo, et applicable aux Prestataires de services de confiance en cybersécurité.

L'ensemble des textes découlant de ce cadre légal et règlementaire et susceptibles de s'appliquer aux Prestataires de services d'accompagnement et de conseils en cybersécurité ainsi qu'aux prestations d'accompagnement et de conseils, sont listés ci-dessous de manière non-exhaustive. Ils sont identifiés dans le Référentiel en tant que « Documents de référence ».

Le présent Référentiel s'applique en complément des Documents de référence dont il n'exclut pas l'application. Il n'exclut pas non plus l'application des règles générales imposées aux Prestataires en leur qualité de professionnels, et notamment leur devoir de conseil vis-à-vis des Clients finaux.

Le Référentiel peut être utilisé à titre de bonnes pratiques en dehors de tout contexte règlementaire.

1.3.1. Publications de l'ISO

- La norme ISO 19011 :2018, qui fournit les principes théoriques de management d'un audit mais aussi les compétences attendues par les auditeurs et les responsables d'audits ;
- La norme ISO 22301 :2019, Sécurité et résilience, Systèmes de management de la continuité d'activité ;
- La norme ISO 27001 :2022, Sécurité de l'information, cybersécurité et protection de la vie privée ;
- La norme ISO 27002 :2022, Sécurité de l'information, cybersécurité et protection de la vie privée- Mesures de sécurité de l'information ;
- La norme ISO 27005 :2022, Sécurité de l'information, cybersécurité et protection de la vie privée- Préconisations pour la gestion des risques liés à la sécurité de l'information.

1.3.2. Textes législatifs et règlementaires

- La loi n° 2017-007 du 22 juin 2017 relative aux transactions électroniques en République togolaise ;
- 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°2018-062/PR du 21 mars 2018 portant réglementation des transactions et services électroniques au Togo ;
- L'arrêté n°016/MPEN/CAB du 17 décembre 2018 fixant les conditions de reconnaissance au Togo des certificats et signatures électroniques délivrés par des prestataires de services de confiance établis hors du territoire national ;
- La loi n°2019-014 du 29 octobre 2019 relative à la protection des données à caractère personnel ;
- La loi n°2020-009 du 10 septembre 2020 relative à l'identification biométrique des personnes physiques au Togo ;
- 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°2019-098/PR du 11 juillet 2019 portant création, attributions et organisation de la société CYBER DEFENSE AFRICA (CDA) ;
- 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 auprès de l'ANCy.

1.3.3. Documents de l'ANCy

- Décision ANCy portant liste des pays tiers de confiance ;
- Modèle de qualification des Prestataires de services de confiance en cybersécurité ;
- Déclaration de la politique de qualification.

1.3.4. Autres

- ITIL (*Information Technology Infrastructure Library*) ou « Bibliothèque pour l'infrastructure des technologies de l'information » : il s'agit d'un ensemble d'ouvrages recensant les bonnes pratiques (« *best practices* ») du management du système d'information.

1.4. IDENTIFICATION DU DOCUMENT ET DATE D'APPLICATION

Le présent document est dénommé « Référentiel d'exigences des Prestataires de services d'accompagnement et de conseils 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.

1.5. ACTIVITES D'ACCOMPAGNEMENT ET DE CONSEIL VISEES PAR LE REFERENTIEL

Une prestation de service d'accompagnement et de conseil en cybersécurité peut être associée à la réalisation de prestations complémentaires (audit, développement, intégration de produits de sécurité, supervision et détection, etc.) sans perdre le bénéfice de la qualification.

Le Prestataire peut demander la qualification pour tout ou partie des prestations ci-dessous :

❖ **Prestation de Sensibilisation en cybersécurité :**

La prestation de sensibilisation se réfère à la fourniture d'un service visant à accroître la conscience et la compréhension d'un sujet spécifique en sécurité de l'information. Les différentes activités liées à une prestation de sensibilisation sont :

- des présentations, ateliers,
- des campagnes de sensibilisation,
- ou autres activités visant à informer et éduquer le personnel du Client final sur les meilleures pratiques en sécurité de l'information.

❖ **Prestation de formation en cybersécurité :**

La prestation de formation en cybersécurité se réfère à l'ensemble des activités visant à doter les participants à la formation des connaissances et compétences nécessaires pour comprendre, prévenir, détecter et réagir aux menaces de cybersécurité.

La prestation de formation peut concerner des sujets généraux tels que la protection des données, la gestion des identités, les techniques d'attaque, la conformité réglementaire et l'utilisation d'outils de sécurité, ou encore il peut s'agir d'une formation personnalisée selon les besoins du Client final.

Dans le cas d'une formation certifiante (cas de l'ISO par exemple), l'objectif de la prestation est de préparer les participants à réussir un examen de certification ;

❖ **Prestation de Conseil en cybersécurité**

La prestation de conseil en cybersécurité se réfère à l'ensemble des services et des recommandations spécialisés fournis par les consultants en sécurité de l'information afin d'aider les organisations à identifier, évaluer et atténuer les risques liés à la sécurité des systèmes d'information. Les différentes activités liées à une prestation de conseil sont :

✓ *Activités de conseil en gestion des risques de cybersécurité*

L'activité de conseil en gestion des risques de sécurité des systèmes d'information implique de guider le Client final à travers les différentes phases visant à obtenir une évaluation précise des risques pesant sur son système d'information tout en élaborant un plan de traitement des risques correspondant. Ce soutien s'inscrit dans le contexte de la conception d'un nouveau système d'information, de l'évolution d'un système existant, ou de la révision d'un système déjà en place.

✓ *Activités de conseil en sécurité des architectures des systèmes d'information*

L'activité de conseil en sécurité des architectures des systèmes d'information consiste à accompagner le Client final dans la structuration des choix techniques et organisationnels de son système d'information. L'objectif est de l'assister dans la définition de modèles de référence détaillant les principes du modèle de sécurité globale. La prestation de conseil doit être réalisée en veillant à répondre aux exigences de sécurité spécifiques au système d'information visé et au contexte d'activité du Client final. Les recommandations formulées peuvent porter sur les architectures des systèmes d'information en tant que telles, ainsi que sur les configurations des éléments composant l'architecture (systèmes, réseaux, applications, etc.). Cet accompagnement peut intervenir dans le cadre de la conception d'un système d'information, de l'évolution d'un système existant, ou de l'examen d'un système d'information déjà en place.

✓ *Activités de conseil en continuité d'activités et gestion des cyber-crises*

L'activité de conseil en continuité d'activités et gestion des cyber-crises consiste à accompagner le Client final dans la structuration de son dispositif de continuité des activités pour intégrer les dimensions spécifiques des crises d'origine cyber, ainsi que pour préparer les équipes du Client final à acquérir des réflexes de réponse et de maintenir les opérations de manière proactive. Ce qui permet au Client final de définir sa gouvernance de gestion de crise et de détenir des politiques et leurs déclinaisons, des modèles et des outils pour rendre la réponse stratégique et opérationnelle concrète.

Les travaux peuvent porter sur des aspects organisationnels tels que la structuration d'équipes et de politiques, ou encore les techniques par la mise en place d'outils, ou de dispositifs opérationnels permettant de répondre aux enjeux de la continuité de l'activité. Cet accompagnement peut intervenir dans le cadre de la conception d'un dispositif de gestion de crise, de l'évolution d'un dispositif de gestion de crise existant ou sa revue.

1.6. DEFINITIONS ET ACRONYMES

1.6.1. Client final

Partie qui sollicite ou commande la réalisation d'une prestation d'accompagnement et de conseil en cybersécurité.

1.6.2. Prestataire de service d'accompagnement et de conseil en cybersécurité qualifié

Prestataire qui dispose d'une qualification pour la réalisation des prestations d'accompagnement et de conseil en sécurité des systèmes d'information.

1.6.3. Responsable de prestation

Personne responsable de la prestation et de la constitution de l'équipe de consultants.

Dans le contexte d'un Prestataire personne physique, la personne responsable de prestation est directement la personne physique.

1.6.4. Consultant en cybersécurité

Personne liée contractuellement avec le Prestataire et qui intervient dans le cadre de la prestation pour prendre en charge tout ou partie des activités des services d'accompagnement et de conseil en cybersécurité. En fonction de la nature de ses services, on distingue :

- Un consultant en gestion des risques pour les activités de conseil en gestion des risques de cybersécurité,
- Un consultant en continuité d'activité et gestion des cyber-crises pour les activités de conseil en continuité d'activités et gestion des cyber-crises,
- Un consultant en sécurité des architectures des systèmes d'information pour la prestation de conseil en sécurité des architectures des systèmes d'information.

1.6.5. Formateur

Consultant disposant de compétences et de certifications pour assurer une formation. Dans le cas d'une formation certifiante, le formateur doit être agréé par un organisme de certification.

1.6.6. Équipe de consultant

Équipe intervenant lors de la prestation regroupant les consultants et le responsable de prestation.

1.6.7. Expert

Personne physique qualifiée ou non, sollicitée par le Prestataire, qui possède une ou plusieurs compétences spécifiques essentielles pour accomplir des tâches de la prestation.

1.6.8. Convention de service

Accord écrit entre un Client final et un Prestataire pour la réalisation d'une prestation de service d'accompagnement et de conseil en cybersécurité.

2. EXIGENCES RELATIVES AU PRESTATAIRE

2.1. EXIGENCES GENERALES

a) Le prestataire d'accompagnement et de conseil peut être (i) soit une entité ou une partie d'une entité, dotée de la personnalité morale ; (ii) soit une personne physique exerçant sous la forme d'un établissement, dans l'un ou l'autre cas, dûment enregistrée au RCCM (Registre du Commerce et du Crédit Mobilier) pour les besoins de l'activité d'accompagnement et de conseil.

b) Le prestataire d'accompagnement et de conseil doit pouvoir être tenu juridiquement responsable de toutes ses activités d'accompagnement et de conseil.

c) Le prestataire d'accompagnement et de conseil doit respecter la règlementation en vigueur au Togo y compris le Modèle de qualification des prestataires de services de confiance en cybersécurité et, le présent Référentiel ainsi que l'état de l'art.

d) Le Prestataire doit décrire l'organisation de son activité d'accompagnement et de conseil au bénéfice de chaque Client final et garantir que les informations qu'il fournit sont exactes.

e) Le prestataire d'accompagnement et de conseil a l'obligation de formaliser les activités qu'il réalise pour le compte du Client final dans le cadre d'une Convention de service avec le Client final écrite et signée avec celui-ci. Cette convention doit être conforme aux exigences du Référentiel et aux lois en vigueur au Togo.

f) Le Prestataire peut, après approbation du Client final, sous-traiter tout ou partie des activités requises par le Client final à un Prestataire de service d'accompagnement et de conseil en cybersécurité qualifié, sous réserve que ce dernier soit conforme et réponde aux exigences du référentiel d'exigences qui lui est applicable.

g) Le prestataire doit réaliser les prestations de service d'accompagnement et de conseil de manière loyale et impartiale. Il doit par ailleurs faire preuve de respect et de professionnalisme à l'égard du Client final, de son personnel et de ses infrastructures. A cet égard, le prestataire doit apporter une preuve suffisante que son organisation, ses moyens mis en œuvre pour délivrer la prestation, et les modalités de son fonctionnement, notamment financières, ne sont

pas susceptibles de compromettre son impartialité et la qualité de sa prestation à l'égard du Client final ou de provoquer des conflits d'intérêts.

h) Le prestataire d'accompagnement et de conseil doit s'assurer du consentement du Client final avant toute communication d'informations obtenues ou produites dans le cadre de la prestation. Plus spécifiquement en ce qui concerne les données à caractère personnel, le prestataire d'accompagnement et de conseil est tenu de procéder au traitement de ce type de données en observant strictement les exigences prévues par la loi togolaise n°2019-014 du 29 octobre 2019 relative à la protection des données à caractère personnel.

i) Le prestataire d'accompagnement et de conseil doit demander au Client final de lui communiquer les éventuelles exigences légales et réglementaires spécifiques auxquelles il est soumis et notamment celles liées à son secteur d'activité, s'y conformer, et le cas échéant accompagner le Client final dans la démarche de mise en œuvre de ces obligations si ce dernier lui en fait la demande et dans la mesure où la mobilisation du prestataire est nécessaire à ces fins.

j) Le prestataire d'accompagnement et de conseil doit informer le Client final lorsque ce dernier est tenu de déclarer un incident de sécurité à une instance gouvernementale (par exemple à l'ANCy dans le cadre de l'article 17 du décret n°2019-095/PR relatif aux opérateurs de services essentiels, aux infrastructures essentielles et aux obligations y afférentes) et doit l'accompagner dans cette démarche si ce dernier en fait la demande.

k) Le Prestataire doit disposer d'une convention avec une entité en charge du passage des examens de certification pour pouvoir délivrer des formations certifiantes en cybersécurité.

2.2. CODE D'ETHIQUE

Le prestataire d'accompagnement et de conseil en cybersécurité doit disposer d'un code d'éthique signé et/ou ratifié par chaque consultant/ formateur, et dont une copie doit être adressée à l'ANCy.

Le Code d'éthique inclut au minimum les exigences ci-après :

- Les prestations sont réalisées avec loyauté, discrétion, impartialité et indépendance ;
- Les consultants/ formateurs ne recourent qu'aux méthodes, outils et techniques validés par le Prestataire ;
- Les consultants/ formateurs s'engagent à ne pas divulguer d'informations à un tiers, même anonymisées et décontextualisées, obtenues ou générées dans le cadre de la prestation, sauf autorisation formelle écrite et préalable du Client final.

- Les consultants / formateurs en leur qualité de professionnels, s'engagent à respecter les Documents de Référence, l'état de l'art, et toutes les bonnes pratiques liées à la prestation.

2.3. GESTION DES RESSOURCES ET DES COMPETENCES

2.3.1. Le Prestataire est une personne morale

a. Le Prestataire doit employer au minimum deux (02) consultants par prestation de service. Le non-respect de cette condition sur une période au moins égale à six (06) mois constitue pour l'ANCy un motif de suspension de la qualification du prestataire de service d'accompagnement et de conseil en cybersécurité.
b. La relation entre le prestataire d'accompagnement et de conseil en cybersécurité et chaque consultant/formateur doit être encadrée par un contrat signé.
c. Il doit désigner un responsable de prestation pour chaque prestation et éventuellement des sous-traitants pour assurer les activités pour lesquelles il a établi des conventions de service avec le Client final.
d. Le Prestataire doit s'assurer, pour chaque activité de la prestation, que les consultants désignés pour réaliser les activités de la prestation ont les qualités et les compétences requises.
e. Au moment du recrutement, le prestataire doit procéder à une vérification, des formations, compétences et références professionnelles des consultants/ formateurs, et de la véracité de leur curriculum vitae. Il doit par ailleurs s'assurer par tous moyens, que les consultants en cours de recrutement ne font pas l'objet d'une mesure ou d'une sanction incompatible avec l'exercice de leurs fonctions.
f. Le Prestataire doit s'assurer de la compétence de ses ressources et du maintien de cette compétence, à travers un processus de formation continue et une veille technologique. La formation continue du Prestataire et de son personnel peut prendre plusieurs formes notamment des modules d'auto-formation, des séminaires internes, ou des séminaires assurés par le CERT.tg ou par l'ANCy. Le Prestataire doit à tout moment, être en mesure de documenter son plan de formation continue à l'ANCy sur simple demande de celle-ci.
g. Le Prestataire doit mettre à disposition de son personnel les guides de bonnes pratiques et normes nécessaires aux activités de la prestation concernée.
h. Le Prestataire est responsable des méthodologies, outils (logiciels ou matériels) et techniques utilisées par ses consultants et de leur bonne utilisation (précautions d'usage, maîtrise de la configuration...).

l) Le Prestataire peut faire intervenir un expert pour la réalisation de certaines activités de la prestation au motif que certaines compétences spécifiques nécessaires ne sont couvertes par son équipe de consultants sous réserve que :

- il existe un cadre contractuel entre le Prestataire et l'expert ;
- le recours à un expert est accepté par écrit par le Client final ;
- L'expert est dûment encadré par le responsable de prestation.

i. Le Prestataire doit justifier au travers de son recrutement, qu'il dispose des compétences techniques, théoriques et pratiques nécessaires pour mener des activités d'accompagnement et de conseils couvertes par la qualification obtenue.

j. Plus spécifiquement, le prestataire d'accompagnement et de conseil doit disposer des compétences suivantes :

COMPETENCES TECHNIQUES	
RESEAU ET ARCHITECTURE	▪ Protocoles réseau et infrastructures ▪ Protocoles applicatifs et service d'infrastructure ▪ Configuration sécurisée des équipements réseau ▪ Réseaux télécoms ▪ Technologies WIFI, voix sur Ip
SYSTEMES D'EXPLOITATION (ENVIRONNEMENT ET DURCISSEMENT)	▪ Architectures Microsoft ▪ Systèmes UNIX/Linux ▪ Solution de virtualisation
COUCHE APPLICATIVE	▪ Méthodes d'intrusion (Black, Grey et white Box) ▪ Guides et principes de développement sécurisé ▪ Applications de type client/serveur ▪ Langages de programmation dans le cadre d'audits de code source ▪ Mécanismes cryptographiques ▪ Infrastructure applicative (serveurs web serveurs d'application, systèmes de gestion de bases de données)
ÉQUIPEMENTS ET LOGICIELS DE SECURITE	▪ Firewall ▪ Système de sauvegarde ▪ Système de stockage mutualisé ▪ Serveurs de proxy ▪ IDS/IPS

Compétences organisationnelles et physiques	
CADRE NORMATIF	▪ Norme ISO/IEC 27001 et ISO 27002 ▪ Norme ISO 27005 ▪ Norme ISO 22301 ▪ Les textes réglementaires relatifs à la sécurité des systèmes d'information,
GESTION DES RISQUES	▪ Méthodes de gestion des risques (EBIOS, etc.) ▪ Politique de sécurité des systèmes d'information ▪ Fonctions de responsabilités en sécurité des systèmes d'information ▪ Sécurité liée aux ressources humaines ▪ Gestion de l'exploitation et de l'administration du système d'information ▪ Contrôle d'accès logique au système d'information ▪ Développement et maintenance des applications ▪ Gestion des incidents liés à la sécurité de l'information ; ▪ Gestion de crise d'origine cyber ; ▪ Gestion du plan de continuité de l'activité ▪ Sécurité physique ▪ Protection des données
Méthodes liées à l'audit	▪ Conduite d'entretien ▪ Visite sur site ▪ Revue documentaire
Formation et sensibilisation	▪ Formations certifiantes ▪ Cyber exercices ▪ Ateliers pratiques ▪ Formations personnalisées
REFERENTIEL	
REFERENTIELS TECHNIQUES	▪ Référentiel d'exigences des Prestataires d'accompagnement et de conseils ▪ Référentiel d'exigences des Prestataires d'audit

	▪ Règles de cybersécurité en République togolaise, Annexe de l'arrêté N°2022-040 /PMRT portant adoption des règles de cybersécurité en République togolaise

2.3.2. Le Prestataire est une personne physique

a. Le Prestataire de service d'accompagnement et de conseils, agit directement en tant que représentant dans le contexte de la prestation d'accompagnement et de conseil.
b. Le prestataire de service d'accompagnement et de conseil doit s'assurer du maintien à jour de ses compétences à travers un processus de formation continue et une veille technologique. A cet égard, le prestataire a l'obligation de suivre au minimum une (01) formation chaque année dans le domaine de la sécurité des systèmes d'information. La formation continue du Prestataire de service d'accompagnement et de conseils peut prendre plusieurs formes notamment des modules d'auto-formation, des séminaires internes, ou des séminaires assurés par le CERT.tg ou par l'ANCy. Le Prestataire de service d'accompagnement et de conseils doit à tout moment être en mesure de documenter son plan de formation continue à l'ANCy sur simple demande de celle-ci.
c. Le Prestataire doit disposer de contrats de travail d'une durée d'un (01) an, renouvelable ou à durée indéterminée, ou un partenariat avec des consultants pour chaque prestation.
d. Le prestataire doit disposer de guides de bonnes pratiques et des normes nécessaires aux activités de cybersécurité. Il doit par ailleurs s'assurer qu'il est suffisamment sensibilisé à la règlementation en vigueur au Togo et applicable à ses missions.
e. Le prestataire est responsable des méthodes, outils (logiciels ou matériels) et techniques qu'il utilise et de leur bonne utilisation (précautions d'usage, maîtrise de la configuration...). Il doit par ailleurs s'assurer de la mise à jour continue de ces méthodes, outils et techniques, ainsi que de leur pertinence à pouvoir répondre aux besoins des activités menées.
f. Le prestataire doit justifier qu'il dispose des compétences techniques, théoriques et pratiques nécessaires pour mener toutes les prestations d'accompagnement et de conseils, ou bien une partie des prestations couvertes par la qualification obtenue.
g. Le Prestataire doit disposer des compétences mentionnées dans le tableau du point 2.3.1.

2.4. PROTECTION DE L'INFORMATION DU PRESTATAIRE

Le Prestataire doit avoir réalisé une évaluation des risques pour son système d'information en utilisant la méthode EBIOS_RM ou autres.

Le Prestataire doit préserver la confidentialité des informations et supports relatifs à la prestation selon leur niveau de sensibilité.

Les informations relatives à la prestation traités au niveau du système d'information du Prestataire doivent être protégés au minimum au niveau Diffusion Restreinte.

Le système d'information que le prestataire de service d'accompagnement et de conseil utilise pour le traitement de ces informations doit respecter les normes internationales et les bonnes pratiques relatives aux mesures de protection des systèmes d'information traitant d'informations sensibles non classifiées de défense de niveau Diffusion Restreinte.

2.5. EXIGENCES RELATIVES AU PERSONNEL

Le Prestataire doit définir un (01) profil par activités des consultants, les responsabilités à assumer, ainsi que les connaissances et compétences requises, pour chaque catégorie de service :

2.5.1. Consultant en gestion des risques

Éducation
Minimum Niveau Bac +3 et plus en technologie des systèmes d'information et de communication ou équivalent
Formation
Formation en opérations de cybersécurité
Expérience
Minimum 03 années d'expérience dans le domaine de la sécurité des systèmes d'information dont 02 années d'expérience dans le domaine de la gestion des risques
Principales missions
- Élaboration d'un état des lieux réaliste et pertinent du niveau de sécurité d'un système d'information - Analyse et traitement des risques - Réalisation d'un plan de traitement des risques de l'architecture pertinent par rapport à l'étude de l'existant - Élaboration des recommandations produites et leurs finalités

Les connaissances, compétences et aptitudes
▪ Connaissances transverses de la réglementation ▪ Connaissances transverses en sécurité des systèmes d'information : Analyse des risques et politiques de sécurité des systèmes d'information, gestion de l'exploitation et de l'administration des systèmes d'information, gestion de la sécurité des systèmes d'information ▪ Connaissances en architectures sécurisées des systèmes d'information ▪ Connaissances en préparation à la gestion de crise d'origine cyber ▪ Maitrise des méthodes de gestion des risques ▪ Maitrise des normes et méthodologies relatives à la sécurité de l'information, Normes ISO/IEC 2700x, EBIOS, NIST, Cobit, Mehari, GDPR, etc.

2.5.2. Consultant en sécurité des architectures des systèmes d'information

Éducation
Minimum Niveau Bac +3 et plus en technologie des systèmes d'information et de communication ou équivalent
Formation
Formation en opérations de cybersécurité
Expérience
Minimum 03 années d'expérience dans le domaine des technologies des systèmes d'information et de communication Dont 02 années d'expérience dans le domaine de la gestion des risques et 01 année d'expérience dans la sécurité des architectures des systèmes d'information
Principales missions
- Réaliser un état des lieux réaliste et pertinent du niveau de sécurité d'un système d'information - Analyse des cyber- risques - Élaboration de politiques et procédures de sécurité

- Élaborations de plans de gestion des incidents, - Conformité aux normes et cadres réglementaires - Optimisation des processus de sécurité - Élaborer les recommandations produites et leurs finalités
Les connaissances, compétences et aptitudes
↳ Connaissances transverses de la réglementation ↳ Connaissances transverses en sécurité des systèmes d'information : Analyse des risques et politiques de sécurité des systèmes d'information, gestion de l'exploitation et de l'administration des systèmes d'information, gestion de la sécurité des systèmes d'information ↳ Maitrise des normes et méthodologies relatives à la sécurité de l'information, Normes ISO/IEC 2700x, EBIOS, NIST, Cobit, Mehari, GDPR, etc... ↳ Connaissances en préparation à la gestion de crise d'origine cyber ↳ Maîtrise des concepts d'administration sécurisée ↳ Maîtrise des concepts et protocoles réseaux ↳ Maîtrise des concepts système et des principaux systèmes d'exploitation ↳ Maîtrise des concepts d'administration sécurisée ↳ Maîtrise des concepts d'architectures applicatives ↳ Maîtrise des concepts de gestion des accès et de la protection des données ↳ Maîtrise des principaux modèles de sécurité et des principes de défense en profondeur

2.5.3. Consultant en continuité des activités et gestion des cyber-crises

Éducation
Minimum Niveau Bac +3 et plus en technologie des systèmes d'information et de communication ou équivalent
Formation
Formation en opérations de cybersécurité
Expérience
Minimum 03 années d'expérience dans le domaine de la sécurité des systèmes d'information Dont

02 années d'expérience dans le domaine de continuité des activités et gestion des crises cyber
Principales missions
- Réaliser un état des lieux réaliste et pertinent du niveau de sécurité d'un système d'information - Analyse et traitement des risques - Élaboration de plans de Continuité en cybersécurité - Gestion des cyber-incidents - Évaluation des cyber- risques - Conformité aux normes et cadres réglementaires - Optimisation des processus de sécurité - Elaborer les recommandations produites et leurs finalités
Les connaissances, compétences et aptitudes
↓ Connaissances transverses de la réglementation ↓ Connaissances transverses en sécurité des systèmes d'information : Analyse des risques et politiques de sécurité des systèmes d'information, gestion de l'exploitation et de l'administration des systèmes d'information, gestion de la sécurité des systèmes d'information ↓ Maitrise des normes et méthodologies relatives à la sécurité de l'information, Normes ISO/IEC 2700x, EBIOS, NIST, Cobit, Mehari, GDPR, etc... ↓ Connaissances en architectures sécurisées des systèmes d'information ↓ Connaissances en préparation à la gestion de crise d'origine cyber ↓ Maîtrise des concepts de continuité d'activité et de reprise d'activité et des recommandations de la norme ISO22301

2.5.4. Responsable de prestation

Education
Minimum Niveau Bac +5 et plus en technologie des systèmes d'information et de communication ou équivalent
Formation
Formation en opérations de cybersécurité
Expérience

Minimum 05 années d'expérience dans le domaine de la sécurité des systèmes d'information et de communication
Principales missions
• Assurer la définition, le pilotage et le contrôle des activités des consultants • Permettre en œuvre les moyens adaptés aux objectifs de la prestation • Maintenir à jour un état de la progression de la prestation et présenter l'information utile au Client final • Contrôler la qualité
Les connaissances, compétences et aptitudes
➢ Connaissances transverses de la réglementation ➢ Connaissances transverses en sécurité des systèmes d'information : Analyse des risques et politiques de sécurité des systèmes d'information, gestion de l'exploitation et de l'administration des systèmes d'information, gestion de la sécurité des systèmes d'information ➢ Maitrise des normes et méthodologies relatives à la sécurité de l'information, Normes ISO/IEC 2700x, EBIOS, NIST, Cobit, Mehari, GDPR, etc... ➢ Maitrise des concepts d'architectures sécurisées des systèmes d'information ➢ Maitrise de la continuité d'activité et de gestion de cyber crises ➢ Maitrise de la préparation à la gestion de crise d'origine cyber ➢ Capacité rédactionnelle ➢ Capacité de conseils et recommandations pour différents acteurs

2.5.5. Formateur

Education
Min Niveau Bac +5 et plus en technologie des systèmes d'information et de communication ou équivalent
Formation
Formation en opérations de cybersécurité
Expérience
• Minimum 05 années d'expérience dans le domaine de la sécurité des systèmes d'information et de communication

• Certifications en sécurité de l'information (ISO 2700X, CISSP, CEH, etc.)
Missions
• Élaborer le plan de formation • Préparation des outils de la formation • Assurer la formation et l'évaluation des participants
Les connaissances, compétences et aptitudes
➢ Expertise technique approfondie avec des compétences pédagogiques. ➢ Élaboration de scénarios de formation pratiques et des exercices en temps réel pour renforcer les compétences des participants (cyber exercice, etc.). ➢ Revue régulière et efficace des programmes de formation. ➢ Capacité à fournir des conseils et des orientations aux participants pour renforcer leur compréhension des concepts de cybersécurité. ➢ Veille technologique.

3. EXIGENCES RELATIVES AU DEROULEMENT D'UNE PRESTATION : SPECIFIQUES PAR TYPE

Les exigences auxquelles doivent se conformer les Prestataires d'accompagnement et de conseil sont définis par type de prestation :

3.1. PRESTATION DE SENSIBILISATION EN CYBERSECURITE

- Le Prestataire doit établir une convention de service avec le Client final avant l'exécution de la prestation.
- Le Prestataire doit désigner un ou plusieurs consultants dont les compétences et l'expertise répondent aux besoins particuliers de chaque prestation. Le Prestataire choisit l'un des trois profils présentés dans le Point 5 du chapitre 2.
- Le consultant doit fournir des informations précises, à jour et adaptées aux besoins spécifiques de chaque Client final.
- Le consultant doit être capable de personnaliser les programmes de sensibilisation pour répondre aux besoins spécifiques de chaque Client final.
- Le Prestataire doit disposer d'un ensemble de mécanismes permettant d'évaluer l'impact des programmes de sensibilisation, que ce soit par des évaluations de connaissances, des simulations d'attaque, ou autres méthodes dont il dispose.
- Le consultant doit maintenir les programmes de sensibilisation à jour en fonction des évolutions du paysage de la cybersécurité.
- Le Prestataire doit garantir la confidentialité des informations sensibles du Client final traitées pendant la sensibilisation.
- Le consultant doit fournir une documentation claire sur les sujets abordés, ainsi que des rapports sur l'efficacité des programmes de sensibilisation au profit du Client final et de son personnel bénéficiaire des activités de sensibilisation.

3.2. PRESTATION DE FORMATION EN CYBERSECURITE

3.2.1. Formation non certifiante

- Le Prestataire doit établir une convention de service avec le Client final avant l'exécution de la prestation.
- Le Prestataire doit désigner un formateur qui élabore le programme de formation, y compris les sujets à couvrir, les activités pratiques, les exercices, et les éventuelles évaluations.

- Le formateur doit adapter la formation en fonction du niveau d'expérience des participants et de tout contexte spécifique à leur environnement professionnel.
- Le formateur doit procéder à la préparation des supports de formation, y compris des présentations, des documents, des démonstrations, des exercices pratiques.
- Le formateur doit savoir stimuler les échanges, inciter aux questionnements, et favoriser une participation active des participants.
- Le formateur doit disposer d'un ensemble de mécanismes permettant d'évaluer les séances de formation et délivrer des certificats aux participants.
- Le formateur doit fournir une documentation claire sur les sujets abordés, ainsi que des rapports sur l'efficacité de la formation au profit du Client final et de son personnel bénéficiaire de la formation.

3.2.2. Formation certifiante

- Le Prestataire doit disposer de formateurs agréés par les organismes de certification.
- Pour les certifications qui requiert un centre d'examen, le Prestataire doit disposer d'une convention avec un centre d'examen disposant de l'infrastructure technologique nécessaire permettant aux candidats de passer des examens de certification dans un environnement sécurisé et contrôlé de type Person VUE.
- Il est recommandé que le Prestataire dispose de partenariat avec des entités de Certification
- Le formateur agréé doit se conformer au programme de la formation issu de l'organisme de certification.

3.3. PRESTATION DE CONSEIL EN CYBERSECURITE

Les exigences auxquelles doivent se conformer les Prestataires sont regroupées dans les différentes étapes du déroulement d'une prestation de conseil :

- Établissement de la convention de service ;
- Préparation et déclenchement de la prestation ;
- Exécution des travaux ;
- Élaboration du rapport de la prestation ;
- Conclusion de la prestation.

3.3.1. Convention de service

- La convention de service établie entre le Prestataire et le Client final doit contenir ou faire référence aux éléments suivants :
    - Le Prestataire et le Client final peuvent préciser les modalités de partage des responsabilités au sein de la convention de service.
    - Le Prestataire peut sous-traiter tout ou partie des activités à un autre Prestataire qualifié conformément aux exigences du référentiel qui lui sont applicables sous réserve que :
        - Il existe une convention ou un cadre contractuel documenté entre le Prestataire et le sous-traitant ;
        - Le recours à la sous-traitance est validé par le Client final de la prestation de conseil.

3.3.2. Préparation et déclenchement de la prestation

- Le Prestataire désigne un responsable de prestation qui doit constituer une équipe de consultants.
- Le responsable de prestation peut, s'il dispose des compétences suffisantes, réaliser la prestation lui-même et seul.
- Le Prestataire doit élaborer un plan de cadrage qui fait références aux éléments suivants :
    - Le périmètre, les objectifs et les activités de la prestation (jalons, livrables, objectifs, méthodologies etc.) ;
    - Les rôles et les responsabilités des différents intervenants dans les activités de la prestation ;
    - La responsabilité du Prestataire ;
    - La responsabilité du Client final ;
    - La liste des prérequis ;
    - Les détails logistiques nécessaires au déroulement de la mission (moyens matériels, humains, techniques) ;
    - Les différents livrables, les destinataires ainsi que leurs modalités de restitution ;
    - Les modalités de conservation, de restitution ou de destruction en fin de mission, des traces et des informations ou documents relatifs au système d'information cible obtenues par le Prestataire ;
    - Les éventuelles exigences légales et réglementaires spécifiques auxquelles est soumis le Client final ;

- En fonction du type de prestation, l'équipe de consultants doit obtenir, au préalable, toute la documentation existante (politique de sécurité, analyse de risques, procédures d'exploitation de la sécurité, cartographie du système d'information, schémas d'architecture, rapports d'audit réalisés, etc.), relative au périmètre dans l'objectif d'acquérir une compréhension suffisante du système d'information cible ;
- L'équipe doit le cas échéant, demander au Client final des compléments d'informations par rapport aux documents déjà transmis lors de l'élaboration de la proposition de service ou la réponse technique répondant à la demande du Client final ;

La prestation ne doit débuter qu'après une réunion formelle au cours de laquelle les représentants habilités du Prestataire et ceux du Client final confirment leur accord sur l'ensemble des modalités de la prestation.

3.3.3. Exécution des travaux

Le Prestataire doit réaliser sa prestation dans le respect des personnels et des infrastructures du Client final.

3.3.3.1. Exécution des activités de conseil en gestion des risques de sécurité des systèmes d'information

- Le Prestataire doit proposer au Client final une méthode d'analyse de risques éprouvée, maintenue, pérenne et respectant la norme ISO 27005.
- Le Prestataire doit préconiser auprès du Client final l'utilisation de la méthode EBIOS_RM ou autres, lors de l'assistance à l'analyse des risques d'un système d'information.
- L'équipe de consultants doit procéder à une étude de l'existant à travers une revue documentaire et des entrevues avec les acteurs impliqués afin de comprendre les besoins spécifiques de Client final en matière de sécurité de l'information et aligner les objectifs de sécurité sur les objectifs métier de l'organisation.
- Le Prestataire et le Client final doivent parvenir à un consensus concernant les échelles et les métriques qui seront utilisées dans le cadre de la prestation.
- L'équipe de consultants doit procéder à des réunions de validation intermédiaire à chaque étape de l'analyse des risques.
- L'équipe de consultants doit fournir au Client final un plan de traitement des risques préconisé, hiérarchisant la liste des mesures de sécurité pour les risques réduits.

- L'équipe de consultants doit fournir au Client final la cartographie des risques avant et après traitement par les mesures préconisées ainsi que la cartographie des risques résiduels après traitement par les mesures de sécurité préconisées.
- L'équipe de consultants doit expliquer au Client final les points forts, les limites des différentes mesures de risques et les incertitudes qui entourent les estimations du risque.
- Le Prestataire doit rappeler la nécessité de mise en œuvre par le Client final d'un processus de gestion des risques résiduels.
- L'équipe de consultants peut présenter des recommandations générales non associées à des risques et destinées à conseiller le Client final sur des actions complémentaires qui seraient pertinentes pour améliorer la sécurité du système d'information.

3.3.3.2. Exécution des activités de conseil en sécurité des architectures et management des systèmes d'information

- L'équipe de consultants doit procéder à une étude de l'existant à travers une revue documentaire et des entrevues avec les acteurs impliqués afin de comprendre les besoins spécifiques de Client final en matière de sécurité de l'information et aligner les objectifs de sécurité sur les objectifs métier de l'organisation.
- Le responsable de prestation peut juger nécessaire de réaliser un audit de sécurité des architectures du système d'information existant. L'équipe de consultants peut le réaliser par elle-même, si le Prestataire est qualifié comme étant un Prestataire d'audit des systèmes d'information. Dans le cas contraire, il peut recourir à un Prestataire qualifié.
- L'équipe de consultants doit procéder à une analyse des écarts.
- L'équipe de consultants doit, en fonction des résultats de l'analyse des écarts, déterminer les exigences spécifiques au système d'information du Client final.
- L'équipe de consultants doit s'assurer que les exigences sont en conformité avec les normes de sécurité et les réglementations applicables.
- L'équipe de consultants doit proposer au Client final des recommandations adaptées à son contexte, prenant en compte les nouvelles menaces et les avancées technologiques ;
- L'équipe de consultants doit proposer au Client final des recommandations basées sur des standards éprouvés, maintenus, pérennes, respectant les principes des textes et guides de bonnes pratiques reconnus comme conformes aux normes existantes en matière d'architecture des systèmes d'information sécurisés.
- Les recommandations peuvent concerner entres autres :
    - Le durcissement de l'architecture actuelle du Client final.

• L'intégration des principes de conception robustes, des technologies, solutions et bonnes pratiques pour renforcer la sécurité.

• L'implémentation des systèmes de management de la sécurité de l'information et l'élaboration des différentes procédures de sécurité alignées sur les meilleures pratiques et les normes de sécurité.

- Selon les types d'activités réalisées au cours de la prestation, les recommandations peuvent être regroupées par thématiques de sécurité. Ces thématiques sont à adapter en fonction du périmètre et des objectifs de la prestation. Les thématiques de sécurité de systèmes d'information, peuvent inclure :
  - La politique de sécurité des systèmes d'informations ;
  - Les procédures de sécurité ;
  - La continuité des activités : plan de continuité d'activité (PCA), plan de reprise d'activité (PRA).
- Le Prestataire doit proposer au Client final un ou plusieurs scénarios adaptés à son contexte, permettant d'atteindre les objectifs de sécurité, avec des indicateurs de priorité et recommandations de mise en œuvre pour chacune d'entre elles.
- Une liste des écarts et vulnérabilités résiduels pour chaque scénario, si l'atteinte des objectifs de sécurité est jugée impossible par le Prestataire, à la suite de l'analyse.
- Une synthèse à l'attention de la direction du Client final, reprenant les axes principaux de l'analyse, un résumé des différents scénarios proposés, les écarts et vulnérabilités résiduels les plus critiques pour chacun d'entre eux, et les impacts pour le Client final.
- Le Prestataire doit veiller à organiser des points de suivi réguliers avec le Client final pour discuter de l'état d'avancement et des constats et des premières conclusions de la prestation.
- Le responsable de prestation doit tenir informé le Client final des risques et vulnérabilités majeures et critiques constatés. Il doit, et dans la mesure du possible, lui proposer des recommandations immédiates.

3.3.3.3. Exécution des activités de conseil en continuité d'activité des systèmes d'information et gestion des crises cyber

- Le Prestataire doit proposer au Client final une méthodologie de continuité des activités éprouvée, maintenue, pérenne et respectant la norme ISO 22301.
- Le Prestataire doit préconiser auprès du Client final l'utilisation de la méthode EBIOS_RM ou autres, lors de l'assistance à l'analyse des risques d'un système d'information.

- L'équipe de consultants doit réaliser une étude de l'existant à travers une revue documentaire et des entrevues avec les acteurs impliqués pour effectuer une analyse des risques et impacts ou procéder à sa revue.
- L'équipe de consultants doit élaborer une stratégie de continuité des activités et procéder à définir les différents objectifs de continuité d'activité, les stratégies de continuité pour chaque activité critique ainsi que les ressources nécessaires à la mise en œuvre de ces stratégies.
- L'équipe de consultants doit procéder au développement des plans de continuité d'activité détaillé pour chaque scénario de perturbation identifié.
- L'équipe de consultants doit inclure des procédures claires pour la gestion de crise et la reprise des activités et assigner des responsabilités spécifiques à chaque membre du personnel du Client final.
- L'équipe de consultants doit mettre en œuvre et intégrer la continuité d'activité dans les processus organisationnels existants en termes de solutions techniques et de coordination entre les différentes équipes et services.
- L'équipe de consultants doit procéder à la planification et l'exécution des exercices de simulations de crises et sensibiliser les parties prenantes sur les plans de continuité au sein d'une organisation. Le Prestataire doit veiller à impliquer les parties prenantes clés dans ces exercices.
- L'équipe de consultants doit mettre en place un système d'évaluation et d'amélioration continue permettant de mettre à jour les plans en fonction des changements organisationnels du Client final.
- L'équipe de consultants doit documenter toutes les activités liées à la continuité d'activité et établir des canaux de communication clairs pendant les crises.
- L'équipe de consultants doit procéder à des réunions de validation intermédiaire à chaque étape.
- Le Prestataire doit fournir au Client final un rapport d'audit évaluant le niveau de maturité du dispositif de continuité d'activité face à la menace d'origine existante en fonction des incidents passés, si existants.
- Le Prestataire doit fournir au Client final un bilan d'impact d'activité (BIA) précisant le besoin de continuité cyber et la stratégie de continuité.
- Le Prestataire doit fournir au Client final un plan de continuité d'activité (PCA) cyber ainsi qu'un plan de reprise d'activité (PRA), un ensemble de procédures pour outiller la continuité d'activité, prenant en compte les besoins établis par le BIA ainsi que les scénarios cyber redoutés.

- Le Prestataire doit fournir au Client final un document décrivant la stratégie de vérification, d'audit et de retour sur expériences réelles des capacités opérationnelles garantissant un niveau adapté de continuité d'activité face à la menace d'origine cyber.
- Le Prestataire doit fournir au Client final un plan de formation ainsi que des supports de sensibilisation.

3.3.4. Élaboration du rapport de la prestation

- L'équipe de consultant doit, pour toute prestation, élaborer un rapport de prestation et le transmettre au Client final.
- Le rapport de prestation précise les activités d'accompagnement et de conseil en cybersécurité réalisées.
- Le rapport doit contenir en particulier une synthèse compréhensible par des non experts, qui précise :
  - le périmètre et les objectifs de la prestation ;
  - la documentation ;
  - le contexte et l'analyse de la menace actuelle ;
  - la cartographie du système d'information cible ;
  - les différentes étapes de la prestation ;
  - Les normes, méthodologies utilisées ;
  - les différentes activités réalisées ;
  - la synthèse globale de la prestation.
- Le rapport de prestation doit mentionner les noms, coordonnées et fonctions des responsables de prestation, consultant et, le cas échéant experts, qui ont réalisé la prestation.
- Le rapport doit mettre en évidence, pour chaque prestation une analyse des écarts par rapport aux bonnes pratiques.
- Le rapport doit permettre d'évaluer les risques résiduels après l'implémentation des mesures correctives proposées.
- Le rapport doit contenir un plan d'action.
- Le rapport de prestation doit identifier l'ensemble des documents sur lesquels s'appuie la prestation.

3.4. CONCLUSION DE LA PRESTATION

- Il est recommandé qu'une réunion de clôture de la prestation soit organisée avec le Prestataire et le Client final suite à la livraison du rapport de la prestation.

- Cette réunion permet d'expliquer les recommandations complexes et, éventuellement, de proposer d'autres consignes.
- Un procès-verbal est élaboré dans ce sens afin de clôturer la mission, mentionnant aussi que toutes les traces, et informations relatives au système d'information du Client final traités par le Prestataire ont été restitués au Client final ou, sur sa demande, détruites conformément à la convention de service.
- La prestation est considérée comme terminée lorsque toutes les actions planifiées ont été exécutées et que le Client final a reçu et validé la conformité du rapport de la prestation par rapport aux objectifs stipulés dans la convention de service.