TERMES DE RÉFÉRENCE

RECRUTEMENT D'UN CONSULTANT EN CYBERSÉCURITÉ POUR L'ÉVALUATION DES VULNÉRABILITÉS ET LES TESTS D'INTRUSION (VAPT) EN VUE DE LA CERTIFICATION ISO 27001:2022

Banque d'Investissement et de Développement de la CEDEAO (BIDC)

1. CONTEXTE ET JUSTIFICATION

1.1. À propos de la Banque d'Investissement et de Développement de la CEDEAO (BIDC)

La Banque d'investissement et de développement de la CEDEAO (BIDC) est une institution financière spécialisée de la Communauté économique des États de l'Afrique de l'Ouest (CEDEAO), dont le siège est situé à Lomé, au Togo. Créée en vue de la promotion du développement économique et de l'intégration régionale en Afrique de l'Ouest, la BIDC finance des projets de développement dans les quinze États membres de la CEDEAO, en appui aux initiatives des secteurs public et privé dans des domaines clés tels que les infrastructures, l'agriculture, l'industrie et l'énergie.

En sa qualité d'institution régionale de financement du développement, la BIDC évolue dans un environnement informatique complexe et dynamique qui prend en charge des transactions financières critiques, la gestion des données, la communication avec les parties prenantes ainsi que des systèmes opérationnels couvrant plusieurs juridictions au sein de la région CEDEAO.

1.2. Contexte stratégique et justification

Conformément à son plan directeur informatique (2025-2027) et à son engagement en faveur de l'excellence en matière de cybersécurité, la BIDC vise l'obtention de la certification ISO 27001:2022 afin de mettre en place un système de gestion de la sécurité de l'information (SGSI) robuste. Cette certification témoignera de l'engagement de la BIDC à protéger les données financières sensibles, à préserver la confiance des parties prenantes, à garantir la conformité réglementaire et à adopter les meilleures pratiques internationales en matière de sécurité de l'information.

La sophistication croissante des cybermenaces visant les institutions financières, en particulier dans les secteurs bancaires et du financement du développement, exige la mise en œuvre de mesures de sécurité proactives. L'évaluation des vulnérabilités et les tests d'intrusion (VAPT) constituent un élément essentiel de la conformité à la norme ISO 27001, en particulier au regard des dispositions A.8.8 (Gestion des vulnérabilités techniques) et A.12.6 (Gestion des vulnérabilités techniques) de la norme ISO 27001:2022.

1.3. Objet de la mission

La BIDC souhaite recruter un consultant qualifié et expérimenté en cybersécurité TIC qui mènera une évaluation complète des vulnérabilités et des tests d'intrusion (VAPT) sur l'ensemble de son infrastructure TIC, de ses applications, de ses réseaux et de ses systèmes. Cette évaluation permettra d'identifier les vulnérabilités de sécurité, d'apprécier l'efficacité des contrôles de sécurité existants et de formuler des recommandations concrètes pour renforcer la posture de cybersécurité de la BIDC en vue de la certification ISO 27001:2022.

2. OBJECTIFS DE LA MISSION

Les principaux objectifs de cette mission sont les suivants :

1. Aider la BIDC à définir le périmètre de la certification SGSI.
2. Aider la BIDC à élaborer une matrice RACI pour piloter le projet SGSI ISO 27001:2022.
3. Réaliser une évaluation complète des vulnérabilités de l'infrastructure TIC de la BIDC, couvrant notamment les réseaux, les serveurs, les bases de données, les applications, les terminaux (endpoints) et les environnements cloud.
4. Réaliser des tests d'intrusion à l'aide de méthodologies conformes aux normes du secteur afin de simuler des cyberattaques réelles et d'identifier les vulnérabilités exploitables.
5. Évaluer le niveau de sécurité des systèmes centraux, des applications financières et des systèmes métier critiques de la BIDC.
6. Évaluer la conformité aux exigences de la norme ISO 27001:2022, en particulier les contrôles relatifs à la gestion des vulnérabilités techniques (annexes A.8.8, A.12.6, A.14.2).

7. Identifier les failles de sécurité, les erreurs de configuration et les vulnérabilités susceptibles de compromettre la confidentialité, l'intégrité et la disponibilité des actifs informationnels de la BIDC.
8. Établir une hiérarchisation des vulnérabilités identifiées en fonction des risques, sur la base de leur gravité, de leur exploitabilité et de leur impact sur les activités de la Banque.
9. Fournir des rapports techniques et de synthèse contenant des conclusions détaillées, des évaluations des risques et des recommandations de remédiation.
10. Accompagner la Haute direction et les équipes techniques de la BIDC grâce au transfert de connaissances et aux conseils de remédiation.
11. Réaliser une évaluation de validation post- remédiation afin de vérifier l'efficacité des contrôles de sécurité mis en œuvre.
12. Fournir des recommandations conformes aux exigences de la certification ISO 27001:2022 et aux meilleures pratiques en matière de cybersécurité dans le secteur financier.

3. DÉLIMITATION

3.1. Portée de l'évaluation

La mission VAPT couvrira de manière exhaustive les domaines ci-après de l'environnement TIC de la BIDC :

3.1.1. Évaluation de l'infrastructure réseau

- Périmètre réseau externe (pare-feu, routeurs, commutateurs, systèmes de détection et de prévention d'intrusion, etc.).
- Segmentation du réseau interne et contrôles d'accès.
- Réseaux privés virtuels (VPN) et solutions d'accès à distance.
- Réseaux sans fil (sécurité Wi-Fi, réseaux invités, configurations des points d'accès, etc.).
- Systèmes de surveillance et de journalisation du réseau.
- Interconnexion entre agences et liaisons MPLS/WAN.
- Architecture réseau des centres de données.
- Dispositifs et configurations de sécurité réseau.

3.1.2. Évaluation des serveurs et des systèmes d'exploitation

- Environnements Windows Server (Active Directory, contrôleurs de domaine, serveurs de fichiers, etc.).
- Environnements de serveurs Linux/Unix.
- Serveurs de bases de données (SQL Server, Oracle, MySQL, PostgreSQL, etc.).
- Serveurs d'applications et plateformes middleware.
- Infrastructure de virtualisation (VMware, Hyper-V ou équivalent).
- Systèmes de sauvegarde et de reprise après sinistre.
- Serveurs de messagerie et de collaboration (Exchange, Office 365, etc.).
- Évaluation du renforcement de la sécurité du système d'exploitation et de la gestion des correctifs.

3.1.3. Évaluation de la sécurité des applications

- Systèmes centraux et modules associés.
- Applications Internet et mobiles.
- Systèmes de traitement des paiements et infrastructure SWIFT.
- Applications de gestion financière et de comptabilité.
- Systèmes de ressources humaines et de paie.
- Systèmes de gestion documentaire et de flux de travail.
- Systèmes de gestion de la relation client (CRM).
- Portails Web et sites internet accessibles au grand public.
- API et services web (par exemple, REST, SOAP, GraphQL).
- Applications développées sur mesure et applications tierces.

3.1.4. Évaluation des services cloud et tiers

- Configurations de l'infrastructure cloud (par exemple, IaaS, PaaS, SaaS).
- Sécurité du stockage dans le cloud (chiffrement des données, contrôles d'accès).
- Configurations de la gestion des identités et des accès (IAM).
- Intégrations tierces et connexions avec les fournisseurs.
- Configurations de sécurité des fournisseurs de services cloud (par exemple, Microsoft 365, Azure AD, ITSM SysAid, etc.).

3.1.5. Évaluation des terminaux et de l'environnement utilisateur

- Configurations de sécurité des postes de travail et des ordinateurs portables.
- Systèmes de protection des terminaux (antivirus, solutions EDR).
- Gestion des appareils mobiles (MDM) et sécurité mobile.
- Gestion des accès privilégiés et comptes administratifs.
- Mécanismes d'authentification des utilisateurs et politiques de mots de passe.
- Mise en œuvre de l'authentification multifactorielle (MFA).

3.1.6. Évaluation de la sécurité physique et de l'ingénierie sociale

- Contrôles de sécurité physique et gestion des accès.
- Tests de vulnérabilité à l'ingénierie sociale (simulations de phishing).
- Sensibilisation à la sécurité et évaluation du comportement des utilisateurs.
- Évaluation de la vulnérabilité aux menaces internes.

3.2. Méthodologies et normes de test

Le consultant utilisera des méthodologies et des normes reconnues à l'échelle internationale, notamment, mais sans s'y limiter :

- Le top 10 et le guide de test de l'Open Web Application Security Project (OWASP).
- La norme OWASP de vérification de la sécurité des applications (ASVS).
- Le manuel de méthodologie de test de sécurité open source (OSSTMM).
- La norme d'exécution des tests d'intrusion (PTES).
- Le guide technique du NIST SP 800-115 pour les tests et l'évaluation de la sécurité de l'information.
- Les contrôles de l'annexe A de la norme ISO 27001:2022, en particulier A.8.8, A.12.6 et A.14.2.
- Les méthodologies de tests d'intrusion de la « SANS Institute ».
- Le système commun d'évaluation des vulnérabilités (CVSS) v3.1 ou version ultérieure pour l'évaluation des risques.

3.3. Types de tests

3.3.1. Évaluation des vulnérabilités

- Vérification du cadre de gouvernance interne pour la gestion des vulnérabilités.

- Analyse automatisée des vulnérabilités à l'aide d'outils conformes aux normes du secteur.
- Vérification et validation manuelles des vulnérabilités identifiées afin d'éliminer les faux positifs.
- Examen de la configuration et évaluation des normes de sécurité de base.
- Vérification de la conformité aux cadres de sécurité et aux meilleures pratiques.
- Identification des correctifs et mises à jour de sécurité manquants.
- Détection des configurations faibles et des identifiants par défaut.

3.3.2. Tests d'intrusion

Le consultant effectuera des tests d'intrusion en utilisant les approches suivantes :

3.3.2.1. Tests d'intrusion externes (boîte noire)

- Simulation d'un cyberattaquant externe n'ayant aucune connaissance préalable des systèmes.
- Tester les ressources exposées à Internet, les applications web et les services externes.
- Tenter de franchir les défenses périmétriques et d'obtenir un accès non autorisé.
- Exploitation des vulnérabilités identifiées pour démontrer leur impact réel.

3.3.2.2. Tests d'intrusion internes (boîte grise)

- Simulation d'un acteur interne malveillant ou d'un utilisateur interne compromis.
- Test de la segmentation du réseau interne et des contrôles de mouvement latéral.
- Test d'élévation des privilèges.
- Exploitation des applications et services internes.

3.3.2.3. Tests d'intrusion des applications Web

- Tests d'injection SQL, de Cross-Site Scripting (XSS) et de Cross-Site Request Forgery (CSRF).
- Tests d'authentification et de gestion des sessions.
- Évaluation des vulnérabilités de la logique métier.
- Tests de sécurité des API (authentification, autorisation, validation des entrées, etc.).

- Tests de référence directe d'objet non sécurisée (IDOR) et des contrôles d'accès.

3.3.2.4. Tests d'intrusion sur les réseaux sans fil

- Sécurité du chiffrement et de l'authentification Wi-Fi.
- Détection des points d'accès non autorisés.
- Évaluation de la segmentation des réseaux sans fil.
- Simulation d'attaques de type « man-in-the-middle ».

3.3.2.5. Tests d'ingénierie sociale

- Simulation d'une campagne de phishing ciblée.
- Évaluation du phishing (hameçonnage/phishing vocal), le cas échéant.
- Tests de contournement de la sécurité physique (avec autorisation préalable).

3.4. Tests d'intrusion axés sur les menaces (TLPT)

3.4.1. Objet

En plus de l'évaluation des vulnérabilités et des tests d'intrusion (VAPT) classiques, le consultant réalisera un exercice de test d'intrusion axé sur les menaces (TLPT) destiné à simuler des scénarios réalistes de cyberattaques, fondés sur le renseignement et les menaces, à l'encontre des activités métier critiques de la BIDC et de l'infrastructure qui les sous-tend.

La mission TLPT évaluera la capacité de la BIDC à :

- Prévenir les cyberattaques sophistiquées.
- Détecter rapidement les activités malveillantes.
- Réagir efficacement en cas d'incidents de sécurité.
- Contenir et surmonter les scénarios de menaces avancées.
- Renforcer sa résilience conformément aux contrôles opérationnels et de gestion des incidents de la norme ISO 27001:2022.

3.4.2. Délimitation du TLPT

Le TLPT ciblera les activités métier critiques et les actifs de grande valeur identifiés par la BIDC y compris, mais sans s'y limiter :

- Les systèmes centraux.

- Les systèmes de paiement et l'infrastructure SWIFT.
- Les plateformes de banque en ligne et mobile.
- Les systèmes de gestion des identités et des accès (IAM).
- Les environnements de gestion des accès privilégiés (PAM).
- L'infrastructure réseau et les systèmes de surveillance de la sécurité.
- Les services financiers hébergés dans le cloud.
- Active Directory et les services de domaine.

Le consultant concevra des scénarios de menaces en s'appuyant sur les renseignements pertinents relatifs aux menaces dans le secteur financier, y compris, mais sans s'y limiter :

- Campagnes de menaces persistantes avancées (APT).
- Scénarios d'attaques par ransomware (rançongiciel).
- Vol d'identifiants et prise de contrôle de comptes.
- Mouvements latéraux au sein des réseaux internes.
- Compromission de la chaîne d'approvisionnement.
- Simulation de menaces internes.
- Campagnes de phishing ciblées et ingénierie sociale.

3.4.3. Cadre méthodologique

Le TLPT doit être mené conformément à des méthodologies de simulation d'attaques reconnues à l'échelle internationale, notamment :

- La cartographie du cadre MITRE ATT&CK.
- L'élaboration de scénarios d'attaque fondés sur le renseignement.
- La modélisation de la chaîne d'attaque.
- Les recommandations du NIST SP 800-61 relatives à la gestion des incidents.
- Les contrôles de l'annexe A de la norme ISO 27001:2022 relatifs à la surveillance, à la journalisation et à la gestion des incidents.

Le TLPT doit être structuré selon les phases suivantes :

3.4.3.1. Phase 1 – Renseignements sur les menaces et élaboration de scénarios

- Collecte de renseignements sur les menaces spécifiques au secteur.
- Identification des acteurs malveillants pertinents.
- Cartographie des tactiques, techniques et procédures (TTP).

- Élaboration de scénarios d'attaque réalistes.
- Définition des règles d'engagement (RoE).
- Identification des actifs critiques (« joyaux de la couronne »).

3.4.3.2. Phase 2 – Exercice de la Red Team (simulation d'adversaire)

- Exécution d'attaques contrôlées et discrètes (selon autorisation).
- Tentatives d'accès initiales.
- Élévation des privilèges.
- Mouvement latéral.
- Mise en place d'une persistance.
- Simulation de commande et de contrôle.
- Simulation contrôlée d'exfiltration de données.
- Techniques de contournement des défenses.

3.4.3.3. Phase 3 - Évaluation de la détection et de la réponse

- Évaluation des capacités de surveillance et d'alerte.
- Analyse des délais de réponse aux incidents.
- Mesure du temps moyen de détection (MTTD).
- Mesure du temps moyen de réponse (MTTR).

3.4.3.4. Phase 4 - Évaluation de l'efficacité des contrôles et de la résilience

- Évaluation des contrôles préventifs, de détection et correctifs.
- Examen de la journalisation et de l'état de préparation en matière d'analyse forensique.
- Évaluation de la capacité de reprise.
- Identification des faiblesses systémiques.

L'ensemble des activités de test devra respecter strictement les règles d'engagement convenues et ne devra entraîner aucune perturbation incontrôlée des systèmes de production.

3.4.4. Règles d'engagement et mesures de sécurité

Avant le démarrage de la mission, le consultant devra :

- Obtenir une autorisation écrite officielle de la part de la BIDC.

- Définir des règles d'engagement détaillées.
- Mettre en place des procédures d'escalade et d'arrêt d'urgence.
- Identifier les systèmes protégés et les contraintes opérationnelles.
- Veiller à ce que l'exécution de la charge utile soit non destructrice, sauf autorisation expresse.
- Conserver un journal sécurisé de l'ensemble des activités de test.
- Les attaques par déni de service (DoS) ou les techniques destructrices doivent être menées en dehors de l'environnement de production.

3.5. Exclusions et contraintes

- Les tests seront réalisés durant des plages horaires convenues afin limiter les perturbations des activités de l'institution.
- Les tests de charge pourront faire l'objet d'une discussion distincte, si nécessaire.
- Les tests des systèmes de production devront être effectués conformément aux règles d'engagement et aux protocoles de sécurité convenus.
- Tout test destructif devra faire l'objet d'une approbation écrite expresse du département technologie et innovation de la BIDC.
- Les systèmes tiers ne relevant pas du contrôle direct de la BIDC pourront être exclus, sauf autorisation appropriée.

4. LIVRABLES ET EXIGENCES EN MATIÈRE DE RAPPORTS

4.1. Rapport de démarrage

Échéance : dans les 5 jours ouvrables suivant l'entrée en vigueur du contrat.

Contenu :

- Plan de travail détaillé et calendrier des tests.
- Documentation relative à la méthodologie et à l'approche retenue.
- Confirmation du périmètre et vérification de l'inventaire des actifs.
- Outils et techniques à mettre en œuvre.
- Stratégies d'atténuation des risques liés aux activités de test.
- Protocoles de communication et d'escalade.
- Composition de l'équipe de test et qualifications de ses membres.

4.2. Rapports d'avancement

Échéance : hebdomadaire pendant la phase active de test.

Contenu :

- Synthèse des activités réalisées.
- Conclusions préliminaires et vulnérabilités critiques découvertes.
- Difficultés rencontrées et mesures d'atténuation mises en œuvre.
- Activités à venir et respect du calendrier.

4.3. Projet de rapport technique VAPT

Échéance : dans les 15 jours ouvrables suivant la fin des tests.

Contenu :

- Résumé analytique avec évaluation globale de la posture de sécurité.
- Méthodologie détaillée et portée des tests.
- Inventaire complet des vulnérabilités relevées, assorti de précisions techniques.
- Classification des risques au moyen des scores CVSS et analyse de l'impact sur les activités.
- Documentation des éléments de preuve (captures d'écran, journaux, preuve de concept, etc.).
- Analyse de la chaîne d'attaque et scénarios d'exploitation.
- Recommandations détaillées de remédiation avec hiérarchisation.
- Analyse des écarts de conformité au regard des exigences de la norme ISO 27001:2022.
- Évaluation de l'efficacité des contrôles de sécurité.
- Annexes techniques et documentation à l'appui.

4.4. Rapport de synthèse

Échéance : Parallèlement au projet de rapport technique.

Contenu :

- Aperçu général des conclusions de l'évaluation de sécurité.
- Synthèse des risques et des principales vulnérabilités nécessitant une attention immédiate.
- Analyse de l'impact des risques identifiés sur les activités de l'institution.

- Recommandations pour la résolution des problèmes et la mise en place de mesures correctives.
- Recommandations stratégiques à l'intention de la Haute direction.
- État d'avancement de la conformité en vue de la certification ISO 27001:2022.
- Représentations visuelles (graphiques, diagrammes, cartes thermiques, etc.).
- Formulation dans un langage non technique adapté au Conseil d'administration et à la Haute direction.

4.5. Rapport final VAPT

Échéance : dans les 10 jours ouvrables suivant la réception des observations sur le projet de rapport.

Contenu :

- Prise en compte des observations et précisions de la BIDC.
- Conclusions et recommandations affinées.
- Actualisation de l'évaluation des risques sur la base d'informations complémentaires.
- Rapports techniques et exécutifs finaux complets.

4.6. Rapport de validation des mesures de remédiation

Échéance : dans les 10 jours ouvrables suivant la fin des tests post-remédiation (généralement 60 à 90 jours après la soumission du rapport final).

Contenu :

- Vérification des mesures de remédiation mises en œuvre.
- Nouveaux tests des vulnérabilités précédemment identifiées.
- Évaluation des risques résiduels.
- Confirmation de l'efficacité des contrôles de sécurité.
- Mise à jour de l'état de conformité.
- Recommandations en vue de l'amélioration continue.

4.7. Livrables des tests d'intrusion axés sur les menaces (TLPT)

Les livrables ci-après devront être produits dans le cadre de la mission TLPT et viendront compléter les livrables VAPT standard définis dans le présent chapitre.

4.7.1. Rapport de renseignement sur les menaces et de conception de scénarios TLPT

Échéance : dans les 10 jours ouvrables suivant l'achèvement de la phase de renseignements sur les menaces et de conception de scénarios.

Contenu :

- Aperçu du paysage des menaces pertinent pour les institutions de financement du développement et les environnements bancaires régionaux.
- Identification des acteurs malveillants, de leurs capacités et de leurs motivations.
- Cartographie des tactiques, techniques et procédures (TTP) identifiées par rapport au cadre MITRE ATT&CK.
- Définition des scénarios d'attaque définis avec justification à l'appui.
- Hypothèse d'exposition au risque pour les services opérationnels critiques de la BIDC.
- Identification et hiérarchisation des actifs de grande valeur (« joyaux de la couronne »).

4.7.2. Rapport technique de la Red Team TLPT

Échéance : dans les 15 jours ouvrables suivant la fin de l'exercice de la Red Team.

Contenu :

- Résumé des résultats de l'attaque.
- Description détaillée de l'attaque structurée à l'aide de l'analyse Kill Chain.
- Vecteurs d'accès initiaux exploités.
- Techniques d'élévation des privilèges et chemins de mouvement latéral.
- Mécanismes de persistance identifiés.
- Résultats de la simulation d'exfiltration de données.
- Techniques de contournement des défenses et de contournement des contrôles.
- Preuves techniques (captures d'écran, journaux, artefacts de preuve de concept).
- Évaluation de la gravité des risques alignée en lien avec l'analyse d'impact sur l'activité de l'institution.
- Cartographie des techniques exploitées par rapport aux contrôles pertinents de la norme ISO 27001:2022.

4.7.3. Rapport sur l'efficacité de la détection et de la réponse

Échéance : Parallèlement au rapport technique de la Red Team TLPT.

Contenu :

- Analyse de la génération et de la qualité des alertes.
- Identification des lacunes en matière de capacités de détection.
- Examen de l'escalade des incidents et de la communication.
- Mesure du temps moyen de détection (MTTD).
- Mesure du temps moyen de réponse (MTTR).
- Évaluation de l'efficacité de la surveillance et de la journalisation.
- Recommandations en vue de l'amélioration de l'ingénierie de détection et de la surveillance.
- Observations relatives à la maturité de la réponse aux incidents.

4.7.4. Note d'information TLPT

Échéance : Soumis en même temps que les rapports finaux TLPT.

Format : présentation destinée au Conseil d'administration avec un document de synthèse.

Contenu :

- Évaluation globale de la cyber-résilience et du niveau de maturité.
- Analyse de l'impact de scénarios d'attaques simulées sur les activités de l'institution.
- Identification des faiblesses systémiques critiques.
- Lacunes stratégiques en matière de maturité de la cybersécurité.
- Recommandations pour la hiérarchisation des investissements.
- Analyse de la conformité aux exigences de la norme ISO 27001:2022 et aux contrôles de l'annexe A.
- Priorités de remédiation de haut niveau et considérations en matière de gouvernance.

La présentation devra être adaptée à la Haute direction ainsi qu'aux parties prenantes au niveau du Conseil d'administration.

4.7.5. Feuille de route pour la remédiation et l'amélioration

Échéance : fournie en même temps que le rapport technique final TLPT.

Contenu :

- Plan de remédiation hiérarchisé (mesures à court, moyen et long terme).
- Recommandations d'amélioration de l'architecture défensive.
- Plan d'amélioration de la surveillance et de la journalisation.
- Feuille de route de maturité en matière de réponse aux incidents.
- Recommandations pour l'amélioration de la gouvernance et des politiques.
- Alignement sur l'amélioration continue au regard de la norme ISO 27001:2022.

4.7.6. Rapport de validation TLPT post-remédiation

Échéance : dans les 10 jours ouvrables suivant la fin des tests de validation post-remédiation (généralement 60 à 90 jours après la soumission du rapport TLPT final).

Contenu :

- Nouveau test des chemins d'attaque précédemment exploités.
- Vérification de l'amélioration des capacités de détection et de réponse.
- Évaluation de l'exposition au risque résiduel.
- Mise à jour de l'évaluation de la résilience.
- Confirmation de l'efficacité des contrôles.
- Recommandations pour des améliorations complémentaires, le cas échéant.

4.8. Transfert de connaissances et présentation

Échéance : dès la soumission du rapport final et du rapport de validation.

Contenu :

- Présentation détaillée des conclusions aux équipes techniques et à la Haute direction de la BIDC.
- Séances interactives de questions-réponses.
- Atelier sur les recommandations de remédiation et les meilleures pratiques.
- Recommandations en matière de sensibilisation à la sécurité.
- Documentation des enseignements tirés.

5. COMPÉTENCES ET EXIGENCES REQUISES POUR LES CONSULTANTS

5.1. Qualifications obligatoires

Le cabinet de conseil ou le consultant individuel devra justifier des qualifications suivantes :

5.1.1. Exigences organisationnelles

- Être dûment enregistré et exercer légalement dans son pays d'implantation.
- Justifier d'au moins 7 années d'expérience dans la prestation de services de cybersécurité, de tests d'intrusion et de tests d'intrusion axés sur les menaces (TLPT).
- Démontrer une expérience avérée dans la réalisation de tests VAPT au profit d'institutions financières, de banques ou d'institutions de financement du développement.
- Justifier d'une participation avérée à un minimum de quatre (4) environnements de systèmes financiers de taille moyenne à importante, notamment dans les domaines de l'architecture de sécurité, de l'assurance ou la protection de plateformes critiques.
- Être certifié ISO 27001 (gestion de la sécurité de l'information) et ISO 22301 (gestion de la continuité des activités).
- Disposer d'une expérience dans l'accompagnement de projets de certification ISO 27001.
- Disposer d'une assurance responsabilité civile professionnelle en cours de validité couvrant les services de conseil en cybersécurité.
- Respecter les normes éthiques et les codes de conduite professionnels.

5.1.2. Qualifications de l'équipe technique

L'équipe technique proposée devra être composée de professionnels titulaires des certifications ci-après (exigences minimales pour chaque profil) :

5.1.2.1. Responsable des tests d'intrusion/consultant en sécurité

- Être un professionnel certifié en sécurité offensive (OSCP- Offensive Security Certified Professional), ou
- Être un hacker éthique certifié (CEH- Certified Ethical Hacker) - EC-Council, ou
- Être un testeur d'intrusion GIAC (GPEN- GIAC Penetration Tester), ou
- Être un ingénieur certifié en tests d'intrusion (CPTE).

- Disposer d'au moins 5 années d'expérience pratique en tests d'intrusion.

5.1.2.2. Spécialiste ISO 27001 :

- Détenir une certification d'auditeur principal ou de responsable de la mise en œuvre ISO 27001.
- Disposer d'au moins 5 années d'expérience en mise en œuvre et en audit de la norme ISO 27001.
- Justifier d'une expérience en matière de conformité dans le secteur financier.

5.1.2.3. Spécialiste en sécurité des applications web :

- Être un expert en sécurité Web offensive (OSWE- Offensive Security Web Expert), ou
- Être un testeur d'intrusion d'applications Web GIAC (GWAPT- GIAC Web Application Penetration Tester), ou
- Être un testeur certifié en sécurité des applications Web (équivalent).
- Disposer d'une expérience avérée dans les tests de sécurité des applications bancaires

5.1.2.4. Spécialiste en sécurité des réseaux :

- Être un Professionnel certifié Cisco en réseaux (CCNP- Cisco Certified Network Professional) Securité, ou
- Être un analyste en intrusion certifié GIAC (GCIA- GIAC Certified Intrusion Analyst), ou
- Disposer d'une certification CompTIA Security+ avec spécialisation en sécurité réseau.
- Disposer d'au moins 4 années d'expérience en sécurité réseau.

5.1.3. Certifications supplémentaires souhaitées

- Professionnel certifié en sécurité des systèmes d'information (CISSP- Certified Information Systems Security Professional)

- Responsable certifié en sécurité de l'information (CISM- Certified Information Security Manager).
- GIAC Security Essentials (GSEC).
- Professionnel certifié en sécurité du cloud (CCSP- Certified Cloud Security Professional).
- Professionnel du secteur des cartes de paiement (PCIP- Payment Card Industry Professional).
- Expert certifié en sécurité offensive (OSCE- Offensive Security Certified Expert).
- Auditeur certifié en systèmes d'information (CISA- Certified Information Systems Auditor).

5.2. Exigences relatives à l'expérience

- Avoir mené à bien au moins 5 projets VAPT et TLPT pour des institutions financières, des banques ou des organisations similaires.
- Avoir mené à bien au moins 3 projets d'accompagnement à la certification ISO 27001.
- Disposer d'une expérience avérée dans le secteur bancaire africain ou ouest-africain (vivement souhaitée).
- Disposer d'une expérience en matière d'évaluation de la sécurité des systèmes bancaires de base (vivement souhaitée).
- Avoir une Connaissance des exigences réglementaires régionales (réglementations de la BCEAO, des banques centrales des pays de la CEDEAO, etc.).
- Disposer d'une expérience avérée dans la conduite de VAPT dans des environnements multilingues et multiculturels.

5.3. Compétences techniques

- Maîtrise des outils de référence en matière d'évaluation des vulnérabilités, des tests d'intrusion et des tests de performance (TLPT).
- Expertise en techniques de scan automatisé et de tests manuels.
- Capacité à développer des exploits et des scripts de test personnalisés.
- Expérience des pratiques de codage sécurisé et de la sécurité des applications.

- Connaissance des cadres et des réglementations en matière de cybersécurité dans le secteur financier.
- Compréhension de la sécurité des machines virtuelles et du cloud (notamment, AWS, Azure, Google Cloud, etc.).
- Capacité à mener des évaluations avec un impact minimal sur les activités quotidiennes de l'institution.

5.4. Exigences linguistiques

- Maîtrise de l'anglais (obligatoire).
- Maîtrise du français (obligatoire dans le contexte de la CEDEAO/BIDC).
- L'ensemble des livrables devra être fourni en anglais et en français.

6. DURÉE ET CALENDRIER

6.1. Durée du contrat

La durée totale de la mission de conseil sera d'environ **100 jours calendaires** à compter de la date de signature du contrat, selon le calendrier indicatif suivant :

Phase	Activité	Durée
Phase 1	• Signature du contrat et mobilisation	Jours 1 à 5
Phase 2	• Réunion de démarrage et planification	Jours 5 à 10
Phase 3	• Évaluation des vulnérabilités	Jours 10 à 25
Phase 4	• Tests d'intrusion (externes et internes) et TLPT	Jours 25 à 60
Phase 5	• Analyse et élaboration du rapport	Jours 60 à 75
Phase 6	• Soumission et examen du projet de rapport	Jours 75 à 85
Phase 7	• Soumission du rapport final	Jours 85 à 90
Phase 8	• Présentation et transfert de connaissances	Jours 90 à 100
Phase 9	• Validation post-remédiation (après 60 à 90 jours)	Selon le calendrier prévu

Tableau 1 : Calendrier indicatif du projet.

6.2. Lieu d'exécution

- Une présence sur site au siège de la BIDC à Lomé, au Togo, est requise pour :

- ∞ Les réunions de démarrage et le lancement du projet.
- ∞ Les tests de sécurité physique et du réseau interne.
- ∞ La présentation finale et les sessions de transfert de connaissances.

- Le travail à distance est acceptable pour :
  - ∞ Les tests d'intrusion externes.
  - ∞ La préparation et l'analyse des rapports.
  - ∞ Les rapports d'avancement et la coordination.
- Estimation de la présence sur site : 15 à 20 jours ouvrables répartis sur les différentes phases du projet.

7. RESPONSABILITÉS DE LA BIDC

La BIDC fournira le soutien suivant afin de faciliter la bonne exécution du projet :

- Désignation d'un point focal du projet et d'un interlocuteur technique.
- Accès aux infrastructures, aux systèmes et à la documentation TIC nécessaires.
- Mise à disposition des identifiants de test et des droits d'accès requis.
- Fourniture des schémas réseau, de la documentation d'architecture des systèmes et de l'inventaire des actifs.
- Communication de la liste des VLAN.
- Coordination avec les départements concernés et les administrateurs systèmes.
- Mise à disposition d'un espace de travail et de salles de réunion lors des visites sur site.
- Examen et retour d'informations en temps opportun sur les livrables.
- Coordination avec les prestataires tiers, le cas échéant.
- Délivrance des lettres d'autorisation et des documents juridiques nécessaires aux activités de tests d'intrusion.

8. CONFIDENTIALITÉ ET PROTECTION DES DONNÉES

- Le consultant devra signer un accord de confidentialité (NDA) complet avant le démarrage des travaux.
- L'ensemble des informations, données et conclusions devra être traité de manière strictement confidentielle.

- Le consultant ne devra divulguer aucune information relative à la BIDC à des tiers sans un consentement écrit explicite.
- L'ensemble des données, rapports et documents de test devra être détruit de manière sécurisée ou restitué à la BIDC à l'issue du projet.
- Le consultant devra se conformer aux lois et réglementations applicables en matière de protection des données et de confidentialité.
- La BIDC conserve l'intégralité des droits de propriété intellectuelle sur les livrables et les conclusions.
- Le consultant devra mettre en œuvre les mesures de sécurité appropriées pour protéger les données de la BIDC pendant toute la durée de la mission.
- Le consultant devra respecter des protocoles de stockage sécurisé pendant toute la durée de la mission.
- Le consultant devra suivre des procédures certifiées de destruction des données à la fin de la mission.
- Le consultant devra s'aligner sur les principes de restriction concernant l'utilisation des outils cloud (afin de prévenir toute fuite potentielle de données).

9. CRITÈRES D'ÉVALUATION

Les offres seront évaluées selon une méthodologie **de sélection basée sur la qualité et le coût (QCBS)** avec la répartition suivante :

- Qualité technique : 70 %
- Offre financière : 30 %

9.1. Critères d'évaluation technique (70 points)

Critères	Nombre maximal de points
Qualifications et expérience du consultant	20
Profil de l'organisation et expérience avérée	(8)
Certifications et accréditations pertinentes	(7)
Expérience dans le secteur financier	(5)
Méthodologie et approche proposées	25
Exhaustivité de la méthodologie	(10)
Stratégie d'alignement sur la norme ISO 27001	(8)

Atténuation des risques et protocoles de sécurité	(7)
Composition et expertise de l'équipe technique	15
Qualifications et expérience du chef d'équipe	(6)
Certifications et expertise des membres de l'équipe	(6)
Qualifications des spécialistes ISO 27001	(3)
Compréhension de la mission et du plan de travail	10
Compréhension de la portée et de la couverture	(5)
Réalisme en termes d'échéance et de gestion de projet	(5)
NOTE TECHNIQUE TOTALE	**70**

- **REMARQUE :**
  - Note technique minimale : 49 points (70 % de la note technique).

Tableau 2 : Matrice de notation de l'évaluation technique.

9.2. Évaluation financière (30 points)

Les offres financières seront évaluées selon la formule suivante :

$$\text{Note financière} = \left(\frac{\text{Prix le plus bas proposé}}{\text{Prix de l'offre}}\right) \times 30$$

9.3. Note finale combinée

$$\text{Note finale} = \text{Note technique} + \text{Note financière}.$$

Le consultant ayant obtenu la note combinée la plus élevée sera sélectionné pour la négociation du contrat.

10. EXIGENCES RELATIVES À LA SOUMISSION

10.1. Offre technique

L'offre technique doit comprendre :

1. Une lettre de soumission d'appel d'offres et un résumé analytique.
2. Le profil de l'entreprise et les documents d'immatriculation.
3. Une compréhension détaillée de la mission et des objectifs.
4. La méthodologie et l'approche proposées.
5. Un plan de travail détaillé et un calendrier d'exécution.

6. La composition de l'équipe, accompagnée des CV et certifications.
7. Des preuves de missions similaires réalisées par le passé (au moins 5 projets).
8. Les coordonnées d'au moins 3 références professionnelles.
9. Les outils et technologies à utiliser.
10. Les procédures d'assurance qualité et de validation.
11. Les stratégies de gestion et d'atténuation des risques.

10.2. Offre financière

L'offre financière doit être soumise séparément et inclure :

1. Le montant forfaitaire total en dollars américains (USD).
2. La répartition détaillée des coûts :
    - Honoraires professionnels par membre de l'équipe.
    - Frais de déplacement et d'hébergement.
    - Outils et licences logicielles (le cas échéant).
    - Rédaction des rapports et documentation.
    - Frais de validation post-remédiation.
    - Toute autre dépense prévue.
3. Le calendrier de paiement lié aux livrables.
4. La durée de validité de l'offre (minimum 90 jours).
5. Les informations relatives à la conformité fiscale et réglementaire.

10.3. Pièces justificatives

1. Certificat d'immatriculation de l'entreprise.
2. Quitus fiscal ou attestation de régularité fiscale.
3. Attestation d'assurance de la responsabilité civile professionnelle.
4. Certifications professionnelles (ex : OSCP, CEH, auditeur principal ISO 27001, etc.).
5. Profil de l'entreprise et brochures.
6. Documentation relative au système de gestion de la qualité (le cas échéant).
7. Déclarations relatives à la lutte contre la corruption et à l'éthique professionnelle.

11. MODALITÉS DE SOUMISSION

Date limite de soumission :	28 mai 2026, à 10 h 00 GMT
Mode de soumission :	• Soumission électronique par courriel et dépôt d'une version papier.
Soumission électronique :	• ichabimougnan@bidc-ebid.org/secretariatdasg@bidc-ebid.org
Soumission de la version papier :	• Banque d'investissement et de développement de la CEDEAO
	• Division des services généraux.
	• 128, boulevard du 13 janvier.
	• BP 2704, Lomé, Togo.
Format de l'offre :	• Offre technique (sous pli fermé séparé).
	• Offre financière (sous pli fermé séparé).
	• Documents rédigés en anglais et en français.
Demandes de clarification :	• À soumettre au plus tard le 21 mai 2026.
	• Par courriel : ichabimougnan@bidc-ebid.org/secretariatdasg@bidc-ebid.org
Attribution prévue du marché :	• Juillet 2026.
Début du projet :	• Juillet 2026.

Tableau 3 : Modalités de soumission.

12. MODALITÉS DE PAIEMENT LIÉES AUX LIVRABLES

Les paiements seront effectués en dollars américains (USD) selon le calendrier suivant :

Livrable/Étape	Pourcentage du montant total
À la signature du contrat (avance de mobilisation)	50%
Soumission et approbation du rapport de démarrage	0%
Achèvement de l'évaluation des vulnérabilités et des tests d'intrusion	0%
Soumission et approbation du projet de rapport VAPT	0 %
Soumission et validation du rapport final VAPT	30 %

Achèvement de la présentation et du transfert de connaissances	0%
Achèvement du rapport de validation post- remédiation	20%
TOTAL	**100 %**

Tableau 4 : Calendrier de paiement.

Tous les paiements seront subordonnés au/à :

- L'achèvement satisfaisant et à l'approbation des livrables.
- La présentation de factures fiscales valides.
- Respect des obligations contractuelles.
- La retenue à la source applicables conformément à la réglementation fiscale togolaise.

13. CONDITIONS GÉNÉRALES

13.1 Conformité et normes éthiques

- Se conformer aux politiques et procédures de passation de marchés de la BIDC.
- Tolérance zéro à l'égard de la fraude, de la corruption et des pratiques contraires à l'éthique.
- Respect des codes de conduite professionnels et des normes du secteur.
- Respect des lois et réglementations en vigueur au Togo et dans la région de la CEDEAO.

13.2 Conflit d'intérêts

- Le consultant devra déclarer tout conflit d'intérêts potentiel.
- Il ne pourra pas participer aux travaux ultérieurs de mise en œuvre ou de remédiation découlant de la présente mission (délai de réflexion de 12 mois).
- L'indépendance et l'objectivité doivent être préservées tout au long de la mission.

13.3 Propriété intellectuelle

- Tous les rapports, conclusions et livrables deviennent la propriété exclusive de la BIDC.

- La BIDC se réserve le droit de publier ou de partager les conclusions selon qu'elle jugera approprié.
- Le consultant pourra faire référence au projet dans son portefeuille, sous réserve d'une autorisation écrite préalable (sans divulgation d'informations confidentielles).

13.4 Assurance et responsabilité

- Le consultant doit souscrire une assurance responsabilité civile professionnelle adéquate.
- La couverture minimale doit être de 50 000 USD pour la responsabilité civile professionnelle.
- Le consultant est responsable de tout dommage résultant d'une négligence ou du non-respect des protocoles convenus.

13.5 Résiliation du contrat

La BIDC se réserve le droit de résilier le contrat dans les cas suivants :

- Violation des obligations de confidentialité ou de protection des données.
- Non-respect des délais convenus pour la livraison des prestations convenues.
- Qualité du travail jugée insuffisante de l'avis de la BIDC.
- Violation des normes éthiques ou de déontologie professionnelle.
- Cas de force majeure indépendants de la volonté des deux parties.

14. COORDONNÉES

Pour toute information complémentaire ou demande de clarification relative aux présents termes de référence, veuillez contacter :

Banque d'investissement et de développement de la CEDEAO (BIDC)

Division des services généraux ;

Adresse : 128 Boulevard du 13 Janvier BP 2704, Lomé, Togo.

E-mail : ICHABIMOUGNAN@bidc-ebid.org/secretariatdasg@bidc-ebid.org

Site web : www.bidc-ebid.org.

À l'attention du président du comité de la passation des marchés.

15. CONTENU DES OFFRES TECHNIQUES ET FINANCIÈRES

L'OFFRE TECHNIQUE NE DOIT CONTENIR AUCUNE INFORMATION FINANCIÈRE, SOUS PEINE DE REJET DE L'OFFRE.

A. OFFRE FINANCIÈRE

L'offre financière, exprimée en Dollars américains hors taxes, devra être ventilée comme suit :

- **Montant forfaitaire :**
  - Honoraires (détail par expert).
- **Frais remboursables :**
  - indemnités journalières (hébergement et restauration) ;
  - billets d'avion ;
  - transport local ;
  - dépenses diverses (communication, administration et préparation des rapports, etc.).

Les coûts de toutes les activités et prestations décrites dans l'offre technique doivent être indiqués séparément. Il est entendu que les activités et prestations décrites dans l'offre technique pour lesquelles aucun coût n'est indiqué sont réputées incluses dans les coûts des autres activités et prestations. Lorsque la mission comporte plusieurs phases, étapes ou activités, le coût de chacune d'elles doit être clairement précisé dans l'offre financière.

L'original et la copie de l'offre technique devront être placés dans une enveloppe cachetée portant clairement la mention :

« OFFRE TECHNIQUE – RECRUTEMENT D'UN CABINET DE CONSEIL POUR LA RÉALISATION DE L'ÉVALUATION DES EMPLOIS, DU BENCHMARKING DES RÉMUNÉRATIONS, DE L'HARMONISATION DE LA STRUCTURE DES GRADES ET DE L'ÉLABORATION D'UN CADRE DE GESTION DES CARRIÈRES POUR LA BANQUE D'INVESTISSEMENT ET DE DÉVELOPPEMENT DE LA CEDEAO (BIDC) »

ainsi que le nom et l'adresse du Consultant, avec la mention :

« À N'OUVRIR QU'AU MOMENT DE LA SÉANCE D'OUVERTURE DES OFFRES TECHNIQUES ».

De même, l'original et la copie de l'offre financière devront être placés dans une enveloppe cachetée portant clairement la mention :

« OFFRE FINANCIÈRE – RECRUTEMENT D'UN CABINET DE CONSEIL POUR LA RÉALISATION DE L'ÉVALUATION DES EMPLOIS, DU BENCHMARKING DES RÉMUNÉRATIONS, DE L'HARMONISATION DE LA STRUCTURE DES GRADES ET DE L'ÉLABORATION D'UN CADRE DE GESTION DES CARRIÈRES POUR LA BANQUE D'INVESTISSEMENT ET DE DÉVELOPPEMENT DE LA CEDEAO (BIDC) »

ainsi que le nom et l'adresse du Consultant, avec la mention :

« NE PAS OUVRIR EN MÊME TEMPS QUE L'OFFRE TECHNIQUE ».

Ces deux enveloppes cachetées contenant respectivement l'offre technique et l'offre financière devront être placées dans une troisième enveloppe cachetée. Cette enveloppe extérieure devra porter l'adresse de soumission des offres ainsi que la mention suivante :

« À N'OUVRIR QU'AU MOMENT DE LA SÉANCE D'OUVERTURE DES OFFRES TECHNIQUES ».

TOUTE OFFRE FINANCIÈRE NON PRÉSENTÉE DANS UNE ENVELOPPE DISTINCTE PORTANT LES INDICATIONS CI-DESSUS SERA AUTOMATIQUEMENT REJETÉE.

Les offres technique et financière devront être soumises chacune en deux (02) exemplaires, dont un (01) original et une (01) copie portant clairement cette mention. En cas de divergence, l'original fera foi. En outre, le Consultant devra joindre un CD ou une clé USB contenant les versions électronique de ses offres technique et financière.

Toutes les pages de la proposition devront être paraphées par un représentant dûment habilité du Consultant. Dans le cas d'un groupement, la proposition devra être signée par tous les membres du groupement afin de garantir son caractère juridiquement contraignant à leur égard, ou par un représentant dûment mandaté à cet effet, muni d'une procuration signée par tous les représentants autorisés du groupement.

16. CRITÈRES D'ÉVALUATION DES OFFRES

L'évaluation des offres, assurée par un Comité, se déroulera en deux étapes.

Dans un premier temps, le Comité procédera à l'évaluation des offres techniques sur la base des critères et sous-critères suivants :

a. Qualifications générales du soumissionnaire pour la mission : **10 points** ;

b. Conformité du plan de travail et de l'approche technique avec les termes de référence (TDR) : **30 points** ;

c. Sous-critères :

- approche technique et méthodologie : **20 points** ;
- plan de travail détaillé : **10 points** ;
- expériences similaires (au moins 4) : **20 points** ;

d. Qualifications et compétences du personnel clé affecté à la mission : **40 points**.

Total : 100 points

Dans un second temps, les offres financières seront analysées. Seules les offres financières des soumissionnaires ayant obtenu une note technique égale ou supérieure à 80 points seront ouvertes et soumises à l'évaluation financière. Les offres financières seront évaluées hors taxes.

L'offre financière la moins-disante recevra la note financière maximale (Sf) de 100 points. La note financière (Sf) des autres offres sera calculée selon la formule suivante :

Sf=100×FmFSf = 100 \times \frac{Fm}{F}Sf=100×FFm

où :

- **Fm** représente le montant de l'offre financière la moins-disante ;
- **F** représente le montant de l'offre financière considérée.

Le classement final des propositions sera effectué sur la base d'une pondération des notes technique et financière :

- Offre technique : **80 %** ;
- Offre financière : **20 %**.

Le Consultant ayant obtenu la note combinée la plus élevée sera invité à des négociations en vue de l'attribution du contrat.

Les offres devront demeurer valides pendant une période de quatre-vingt-dix (90) jours à compter de la date limite de soumission des offres, y compris en cas de prorogation éventuelle. Durant cette période, le Consultant devra maintenir inchangée sa proposition initiale, notamment le personnel clé proposé, les taux appliqués ainsi que les montants totaux proposés.

17. DATE ET LIEU DE SOUMISSION DES OFFRES

Les offres rédigées en français ou en anglais devront être déposées à l'adresse suivante :

Secrétariat du Directeur de l'Administration et des Services Généraux
Banque d'Investissement et de Développement de la CEDEAO (BIDC)
128, Boulevard du 13 Janvier
B.P. 2704 Lomé – Togo
Tél. : (228) 22 21 68 64

Au plus tard le **28 mai 2026 à 10h00**. L'ouverture des offres est prévue idéalement le même jour à **10h30**, si possible.

Aucune offre ne devra être transmise par courrier électronique. Toute offre reçue après la date et l'heure limites ne sera pas évaluée.

Pour toute information relative aux présents termes de référence, veuillez adresser un courriel à :
ichabimougnan@bidc-ebid.org / secretariatdasg@bidc-ebid.org.

16. ANNEXES

Annexe A : Modèle d'inventaire des actifs

À fournir aux consultants présélectionnés

Annexe B : Schémas d'architecture réseau

À fournir à la signature du contrat

Annexe C : Modèle d'accord de confidentialité

À signer avant le démarrage des travaux

Annexe D : Liste de contrôle de conformité à la norme ISO 27001:2022

À utiliser pour l'analyse des écarts

Annexe E : Matrice de classification des vulnérabilités

Cadre d'évaluation et de hiérarchisation des risques.

Annexe F : Politiques de sécurité informatique de la BIDC

Extraits pertinents à communiquer au consultant retenu.