

TERMES DE RÉFÉRENCE

SÉLECTION D'UN CONSULTANT POUR LA RESTRUCTURATION DU SERVICE D'AUDIT INFORMATIQUE DE LA DIRECTION D'AUDIT INTERNE DE LA BANQUE DE LA RÉPUBLIQUE D'HAÏTI (BRH)

Intitulé de la mission	Sélection d'un consultant pour la restructuration du service d'audit informatique de la Direction d'Audit Interne de la Banque de la République d'Haïti (BRH)
Bénéficiaire(s)	Banque de la République d'Haïti (BRH)
Pays	Haïti
Lieu de travail	Présentiel (30% à Port-au-Prince et/ ou Cap-Haitien) et 70% distanciel Prise en charge par Expertise France dans le cadre de missions ou déplacements professionnels
Type de contrat	Contrat de prestation de service d'expertise individuelle (CPS EI)
Date de début souhaitée	15 Avril 2026
Durée de mise en œuvre	06 mois
Montant estimatif du marché	70,000.00 Euros

CONTEXTE DU PROJET

Le *State Building Contract II (SBC II)*, financé par l'Union européenne et mis en œuvre par Expertise France, vise à renforcer la résilience de l'État haïtien et à créer un environnement favorable à une croissance économique durable, inclusive et soutenue. Lancé en 2018, il s'inscrit dans un contexte marqué par une instabilité sociopolitique persistante et une insécurité généralisée, mais a su démontrer une capacité d'adaptation et produire des résultats tangibles, reconnus par les autorités haïtiennes et les partenaires techniques et financiers.

En juin 2024, au vu de ses résultats, une enveloppe a été accordée, élargissant le champ d'intervention du projet. Cette extension vise à consolider les acquis, intégrer de nouvelles activités et répondre aux besoins émergents identifiés par l'État haïtien. Elle traduit la confiance renouvelée de l'UE dans l'efficacité du dispositif et de sa volonté de renforcer son impact institutionnel et économique.

Le projet met désormais un accent particulier sur la coordination entre les niveaux central et local de l'administration publique, avec un focus sur deux secteurs clés : le fiscal et le douanier. Ces domaines sont essentiels à la mobilisation des ressources internes et à la sécurisation des recettes publiques. À travers ses appuis techniques, le SBC II soutient la stratégie nationale de mobilisation des recettes, tout en accompagnant le renforcement des capacités institutionnelles pour une croissance inclusive et durable.

Au-delà du volet financier, le SBC II agit comme un catalyseur de modernisation de l'administration publique. Il promeut la transparence, les bonnes pratiques de gouvernance et une meilleure articulation entre les institutions. Ces avancées renforcent l'efficacité de l'action publique et contribuent à restaurer la confiance entre l'État et ses partenaires.

En définitive, le SBC II constitue une étape clé dans la modernisation de l'État haïtien. En consolidant les institutions, en améliorant la mobilisation des ressources domestiques et en favorisant une gestion plus efficace des finances publiques, il contribue à la construction d'un contrat social renouvelé, fondé sur la responsabilité, la confiance et la recherche d'un avenir commun plus stable et prospère.

BENEFICIAIRE

La Banque de la République d'Haïti (BRH) gère des infrastructures critiques dans le cadre de ses missions qui consistent à assurer l'efficacité, le développement et l'intégrité du système de paiement, la stabilité du système financier et d'agir comme banquier, caissier et agent fiscal de l'État. En effet, au niveau de sa structure de gouvernance interne, la Direction d'Audit Interne à travers le Service d'audit informatique a pour rôle d'identifier les vulnérabilités liées aux systèmes d'information de la banque, d'évaluer les risques de cyberattaques et vérifier la résilience des systèmes face aux menaces. Consciente de l'importance de l'efficacité et de l'efficience de cette structure dans un contexte marqué par l'augmentation des menaces liées à la cybersécurité, Expertise France, dans le cadre du projet SBC II, lance un appel d'offres en vue de recruter un Consultant pour procéder à une restructuration du Service d'audit informatique de la BRH.

OBJECTIF DU MANDAT

L'objectif de ce mandat est de renforcer durablement la fonction d'audit informatique de la BRH conformément aux standards internationaux et aux bonnes pratiques des banques centrales.

Il comprend :

- Procéder à une réévaluation complète de l'organisation du Service d'Audit des Systèmes d'Information (SASI) de la Direction d'Audit Interne (DAINT) afin de le renforcer et le doter d'un niveau standard, accompagné d'un manuel de procédures pour la réalisation des missions d'audit ;
- Élaborer une cartographie des risques informatiques de la BRH, accompagnée d'un plan d'audit triennal basé sur les risques identifiés ;
- Mettre en place un programme structuré de formation, et de coaching pour renforcer les capacités des cadres du SASI , notamment dans les domaines de la cybersécurité, de

l'intelligence artificielle et de l'audit assisté par la technologie, assurant un transfert effectif de compétences ;

- Évaluer le niveau de maturité de la fonction d'audit selon les référentiels internationaux COBIT, IIA et NIST, afin d'identifier les écarts et proposer une trajectoire d'amélioration progressive ;
- Définir un modèle opérationnel cible (Target Operating Model) précisant la structure, les rôles et responsabilités, les processus, les outils et le reporting ;
- Élaborer une feuille de route opérationnelle détaillant la mise en œuvre progressive des recommandations.

PORTÉE DU MANDAT

Le Consultant devra faire un examen suffisamment approfondi de l'environnement informatique de la banque afin d'identifier les vulnérabilités, d'évaluer les risques et de proposer les mesures correctives nécessaires.

L'analyse comprendra :

- L'évaluation de la gouvernance et de l'organisation de la fonction d'audit informatique ;
- L'analyse des méthodologies et pratiques d'audit actuellement utilisées ;
- L'évaluation des contrôles généraux informatiques (ITGC), incluant la gestion des accès, des changements, des incidents, les sauvegardes, la sécurité réseau et la gestion des vulnérabilités ;
- L'analyse de la cyber résilience et des dispositifs de continuité d'activité ;
- L'examen de la sécurisation des systèmes financiers critiques et des infrastructures supportant les opérations de paiement ;
- L'identification des risques liés aux technologies émergentes, telles que l'intelligence artificielle et l'automatisation ;
- L'évaluation de la coordination entre le SASI, la Direction des Systèmes d'Information, les fonctions de gestion des risques et de sécurité informatique.

Par ailleurs, le Consultant sera autorisé (e) à visiter toutes les installations de la BRH à Port-au-Prince, au Cap-Haïtien et la ville des Cayes afin d'obtenir toutes les informations qui seront jugées pertinentes pour atteindre ses objectifs. Le Consultant se référera à la Direction d'Audit de la BRH qui jouera le rôle d'interlocuteur privilégié dans le cadre de cette mission.

INFORMATIONS À FOURNIR PAR LA BRH

La BRH mettra à la disposition du Consultant tous les documents et rapports qui seront sollicités pour permettre la réalisation du mandat.

Méthodologie et transfert de compétences

Le consultant proposera une méthodologie structurée incluant :

- Revue documentaire et analyse institutionnelle ;

- Entretiens avec les parties prenantes clés (Direction Générale, DSI, Audit interne, Gestion des risques, Sécurité informatique) ;
- Évaluation de maturité des processus d’audit informatique selon standards internationaux ;
- Benchmark des pratiques des banques centrales et institutions financières internationales ;
- Validation progressive des résultats avec la Direction d’Audit Interne.

Le transfert de compétences sera assuré par :

- Ateliers pratiques ;
- Sessions de coaching ;
- Documentation méthodologique développée pour la mission.

Gouvernance, suivi et gestion des risques

Un comité de suivi, composé de représentants de la Direction d’Audit Interne, de la DSI et d’Expertise France, supervisera la mission.

Le comité assurera :

- la validation des livrables intermédiaires ;
- l’identification des contraintes éventuelles ;
- l’ajustement du plan de travail si nécessaire.

Le consultant identifiera également les risques pouvant affecter la réalisation de la mission (contraintes sécuritaires, disponibilité des parties prenantes, accès aux infrastructures) et proposera des mesures d’atténuation.

LIVRABLES ATTENDUS

Livrables	Date de livraison
-----------	-------------------

1. Rapport d'évaluation détaillé de la structure existante et la proposition d'une nouvelle structure organisationnelle pour la fonction d'audit informatique, incluant l'évaluation de maturité du SASI, l'analyse des contrôles généraux informatiques (ITGC), la cyber résilience et la continuité d'activité, ainsi que l'évaluation des systèmes financiers critiques et infrastructures de paiement.	Mois 01
2. Un manuel de procédures pour la réalisation des missions d'audit aligné avec les normes internationales (IIA, COBIT, ISO, etc.), intégrant méthodologies, outils, bonnes pratiques et recommandations pour la conduite des audits assistés par la technologie.	Mois 2 et 3
3. Une cartographie complète des risques informatiques de la banque, intégrant les risques liés aux technologies émergentes (IA, automatisation), la gouvernance des données et les risques de sécurité, accompagnée du plan d'audit sur trois (3) ans au moins correspondant et des priorités de traitement.	Mois 3 et 4
4. Plan de formation et sessions de coaching pour le personnel du SASI, couvrant cybersécurité, intelligence artificielle, audit assisté par la technologie, bonnes pratiques internationales et certifications pertinentes (CISA, CISSP, ISO 27001, etc.)	Mois 4 et 6
5. Feuille de route opérationnelle pour la mise en œuvre des recommandations, détaillant la priorisation des actions, les ressources nécessaires, le calendrier prévisionnel et les indicateurs de performance	Mois 4 et 6

PROFIL RECHERCHÉ

Le Consultant doit impérativement posséder les expériences et compétences suivantes

- Détenir au moins un Master dans le domaine ;
- Jouir d'une bonne réputation professionnelle ;
- Être un expert de référence en matière d'audit informatique et avoir au moins cinq années d'expérience consécutives dans le domaine ;
- Avoir de l'expérience en restructuration de fonctions d'audit particulièrement dans le secteur bancaire. L'expérience dans les banques centrales serait un atout;
- Maîtriser les référentiels internationaux (ISO 27001, COBIT, ITIL, NIST, les normes ISACA et de l'IIA, etc.);
- Détenir des certifications reconnues dans les standards pertinents (CISA, CBCM, CISSP, PCI-DSS, ISO 27001, etc.);
- Expertise dans l'analyse des risques et l'évaluation de la sécurité des infrastructures complexes ;
- Sensibilité à la sécurité et respect strict de la confidentialité des informations traitées ;
- Capacité à travailler en contexte multi-sites et à coordonner avec des partenaires internationaux ;
- Expérience en gestion de projets d'audit IT et suivi opérationnel des recommandations ;
- Avoir une excellente maîtrise du français oral et écrit.

DOSSIER DE CANDIDATURE

A soumettre dans un seul fichier :

- Une proposition technique présentant sa compréhension de la mission, décrivant sa méthodologie de travail et un calendrier prévisionnel
- CV du consultant ou de l'équipe de consultants
- Un relevé d'expérience du consultant
- Une proposition financière forfaitaire, incluant l'ensemble de la prestation ainsi que tous les frais y afférents

CRITERES DE SELECTION

- La présentation du dossier de candidature en **SEUL DOCUMENT** ne dépassant pas 40 pages - **10 points** ;
- La qualité de l'offre technique et de la cohérence de la méthodologie proposée - **30 points** ;
- Le CV du candidat détaillant ses expériences dans le domaine - **30 points** ;
- 3 références - **10 points** ;
- L'offre financière en USD ou EUR – **20 points**

DÉLAI ET DURÉE

Les livrables devront être soumis de manière progressive selon le calendrier de mise en œuvre de la prestation. L'ensemble des livrables doivent être soumis dans un délai maximal de six (6) mois à partir de la date de la signature du contrat.

CONFIDENTIALITÉ

Le Consultant s'engage à tenir confidentiels, tant pendant la durée du mandat et après son expiration, tous documents et informations, de quelque nature qu'ils soient, auxquels il ou elle aurait pu avoir accès ou aurait eu connaissance.