RÉPUBLIQUE DU BURUNDI
MINISTERE DES FINANCES, DU BUDGET ET DE L'ECONOMIE NUMERIQUE
PROJET D'APPUI AUX FONDATIONS DE L'ECONOMIE NUMERIQUE AU BURUNDI « PAFEN »

Intitulé du projet	**PROJET D'APPUI AUX FONDATIONS DE L'ECONOMIE NUMERIQUE AU BURUNDI « PAFEN »**
SUR FINANCEMENT IDA :	**E0930-BI/E2820-BI**
N° du Projet :	**P176396/P180987**

TERMES DES REFERENCES

Recrutement d'un cabinet pour assurer la formation et la certification des techniciens du MFBEN, du SETIC et de l'OBR sur le Hacking Forensic Investigation

FORMATION HACKING FORENSIC INVESTIGATOR

PROJET D'APPUI AUX FONDATIONS DE L'ECONOMIE NUMERIQUE AU BURUNDI PAFEN

Novembre 2026

Official Use On

Titre : ***Termes de référence pour le Recrutement d'un cabinet pour assurer le renforcement des capacités en matière de gouvernance, d'utilisation et de gestion des technologies de l'information pour les cadres du Ministère des Finances, du Budget et de l'Economie Numérique, du Secretariat Exécutif des technologies de l'Information et l'Office Burundais des Recettes- OBR.***

Ministère	Ministère des finances, du budget et de l'économie numérique
Projet	Projet d'Appui aux Fondations de l'Economie Numérique
Activité 2.4.1.13d	MFBEN - DSI - AT CABINET- Recrutement d'un consultant pour la formation et la certification des techniciens du MFBEN, SETIC et de l'OBR sur le Hacking Forensic Investigation
Bénéficiaire	MFBEN, SETIC et OBR

I. INTRODUCTION

Le Gouvernement du Burundi a reçu un financement de la Banque Mondiale pour la mise en place du Projet d'Appui aux Fondations de l'Economie Numérique du Burundi (PAFEN) en sigle « le Projet », et financer ses activités. Il est prévu qu'une partie des ressources de ce financement soit utilisée pour financer le **Renforcement des capacités en matière de gouvernance, d'utilisation et de gestion des technologies de l'information » pour le compte du Ministère des Finances, du Budget et de l'Economie Numérique, du Secrétariat Exécutif des Technologies de l'Information et de l'Office Burundais des Recettes-OBR.**

II. CONTEXTE ET JUSTIFICATION

1. Objectif et Description du Projet PAFEN

L'objectif du PAFEN est d'accroître l'accès à l'Internet haut débit, en particulier pour les communautés mal desservies, et améliorer la capacité du gouvernement à gérer les ressources plus efficacement et fournir des services publics par voie numérique.

Les activités du projet viseront à accroître l'adoption du numérique en élargissant la couverture du réseau et la base existante de consommateurs de services numériques par le biais d'initiatives qui stimulent l'investissement dans des infrastructures à large bande durables et intelligentes sur le plan climatique et

Official Use On

catalysent la demande croissante de services électroniques par le biais de programmes d'accès numérique.8082018

Les Composantes du Projet

Le Projet comprend 4 composantes ci-après :

- **Composante 1** : Accès et inclusion numériques
  - Sous-composante 1.1 : Environnement favorable au développement du marché du haut débit et à l'accès numérique ;
  - Sous -composante 1.2 : Accès à la connectivité locale
  - Sous -composante 1.3 : Facilitateurs d'accès local et d'inclusion numérique

- **Composante 2** : Facilitateurs de la prestation de services publics numériques
  - Sous-composante 2.1 : Cadres institutionnels, juridiques, de gouvernance et technologiques pour les services en ligne
  - Sous -composante 2.2 : Infrastructure et plates-formes gouvernementales numériques partagées et capacités de l'administration publique
  - Sous -composante 2.3 : Numérisation de certains services et de cas d'utilisation phares
  - Sous -composante 2.4 : Modernisation des principaux processus de GFP

Composante 3 : Coordination institutionnelle et gestion du projet.

Composante 4 : Composante de réponse d'urgence

Le PAFEN soutiendra une série de réformes visant à rapprocher les services des citoyens et à améliorer l'efficacité et la transparence du secteur public. De plus, le projet vise à soutenir l'utilisation des technologies numériques et des données pour faciliter la prise de décisions politiques et promouvoir les investissements. Le projet est mis en œuvre par une Unité de Gestion du Projet (UGP) mise en place au Secrétariat Exécutif des Technologies de l'Information et de la Communication (SETIC).

2. Justification de la Mission

Le Ministère des Finances, du Budget et de l'Économie Numérique (MFBEN), le Secrétariat Exécutif des Technologies de l'Information et de la Communication (SETIC) et l'Office Burundais des Recettes (OBR) ont engagé depuis plusieurs années un processus de modernisation et de sécurisation de leurs systèmes d'information afin de soutenir les réformes des finances publiques et de renforcer l'efficacité de l'administration dans la gestion des dépenses et des recettes publiques.

Pour ce qui est du Secrétariat Exécutif de l'Information, il entre autres rôles :

- Piloter la politique nationale des TIC ;
- Accompagner la transformation numérique de l'État ;
- Définir des normes et standards TIC ;

- Assurer l'hébergement et l'exploitation des infrastructures numériques ;
- Renforcer la cybersécurité.

Dans cette dynamique, la maîtrise des risques liés à la cybersécurité et la capacité à réagir efficacement face aux incidents informatiques constituent des enjeux stratégiques majeurs. En effet, la multiplication des menaces et des attaques informatiques met en évidence la nécessité de disposer de ressources humaines qualifiées, capables d'assurer la détection, l'investigation et la réponse aux incidents de sécurité.

La présente mission s'inscrit précisément dans le cadre de la mise en œuvre du PTBA 2026-2027, elle relève de l'activité intitulée activité 2.4.1.13d « MFBEN - DSI - AT CABINET- Recrutement d'un consultant pour la formation et la certification des techniciens de la DSI, SETIC et de l'OBR sur le Hacking Forensic Investigation ».

Dans cette optique, la formation en Hacking Forensic Investigator (CHFI) vient renforcer la résilience et la maturité en cybersécurité du MFBEN, du SETIC et de l'OBR, en dotant leurs équipes de compétences avancées pour mener des investigations numériques, collecter et analyser des preuves et protéger les infrastructures critiques contre les menaces cybernétiques.

III. OBJECTIFS DE LA MISSION

1. Objectif global

L'objectif global de la mission est de recruter un cabinet de formation spécialisé et accrédité pour dispenser une formation certifiante en Hacking Forensic Investigator (CHFI) au profit du personnel de la Direction Générale de l'Économie Numérique (DGEN) du Ministère des Finances, du Budget et de l'Économie Numérique (MFBEN), du Secrétariat Exécutif des Technologies de l'Information ainsi que du personnel de la Direction des Technologies de l'Information (DTI) et du Commissariat des Taxes Internes de l'Office Burundais des Recettes (OBR). Le cabinet devra être accrédité par l'EC-Council ou autorisé par un organisme reconnu par celui-ci à dispenser la formation et à préparer les candidats à la certification Certified Hacking Forensic Investigator (CHFI), afin de garantir la conformité du contenu, des outils pédagogiques et des méthodes de formation aux standards internationaux.

Cette mission vise à renforcer les capacités techniques et opérationnelles des participants dans les domaines de la cybersécurité, de l'investigation numérique et de l'analyse forensique. Elle permettra aux bénéficiaires d'acquérir les compétences nécessaires pour collecter, préserver et analyser les preuves numériques, identifier les traces d'activités malveillantes et contribuer efficacement à la détection, l'investigation et la réponse aux incidents de sécurité, en vue de renforcer la protection et la résilience des systèmes d'information du MFBEN et de l'OBR.

Official Use On

2. *Objectifs spécifiques*

Afin d'atteindre les résultats attendus de cette formation en Hacking Forensic Investigator, les participants devront développer des compétences pratiques et théoriques précises. Plus particulièrement, la formation vise à :

- Former les participants au cadre l'égal, éthique et procédural de l'investigation numérique, appliqué au contexte institutionnel et juridique du Burundi
- Comprendre le cadre légal et éthique du forensic.
- Collecter et conserver des preuves numériques.
- Créer et analyser des images forensiques.
- Retrouver et examiner des données supprimées.
- Analyser la mémoire vive et les systèmes de fichiers.
- Investiguer les activités réseau et les journaux.
- Détecter et analyser des malwares.
- Rédiger des rapports d'enquête exploitables.
- Préparer les participants au passage et à la réussite de l'examen officiel CHFI (ECHO 312-49), et organiser le passage de cet examen.

IV. RÉSULTATS ATTENDUS

À l'issue de la formation, les résultats attendus sont les suivants :

- 5 personnes (2 du MFBEN, 2 de l'OBR et 1 du SETIC) sont formées sur le module Hacking Forensic Investigator.
- Les participants acquièrent des compétences pratiques en investigation numérique et en analyse forensique.
- Les bénéficiaires sont capables d'appliquer les méthodes et outils appris dans leur cadre professionnel.
- Les participants sont capables à produire des rapports forensiques recevables dans le cadre des procédures judiciaires burundaises.

V. SESSIONS DE FORMATION

Session	Langue	Lieu	Durée/session (jours)
1	Français	Au Burundi	5

Official Use On

NB. La formation sur la matière durera 5 jours. Cette durée est exclusive de la préparation à l'examen de certification et la certification elle-même. Ces deux dernières activités s'étendront sur une durée à convenir avec le bénéficiaire sans dépasser huit semaines.

A l'issue de la session, les formés devront :

(a) Avoir une compétences techniques et stratégiques essentielles ;
(b) Acquérir des connaissances innovatrices et adaptées aux meilleures pratiques modernes dans les domaines définis dans les présents termes de référence.

VI. CONTENU ESSENTIEL DU MODULE

- Définir et comprendre le cadre juridique et règlementaire applicable en matière de répression de piratage informatique au Burundi
- Comprendre ce que représente l'investigation numérique ;
- Connaître les techniques de récupération de fichiers supprimés et de décryptage de mots de passe ;
- Agir en tant que premier intervenant lors d'une attaque informatique ;
- Sécuriser et analyser la surface d'une zone d'attaque ;
- Mener des enquêtes préparatoires ;
- Identifier les traces numériques laissées par des attaquants et rassembler des preuves suffisantes pour engager une action en justice ;
- Rédiger des rapports d'enquête complets ;
- Collecter et stocker en toute sécurité des preuves numériques ;
- Faire passer l'examen de certification ECHO 312-49 pour la certification CHFI du EC-Council.

VII. LIVRABLES

Le cabinet devra produire les livrables suivants :

(a) Les livrables attendus seront produits en français en word et en PDF et sont les suivants : Pour la phase formation, le consultant produira un rapport pour chaque description des taches et un rapport final à la fin de chaque formation au plus tard quinze (15) jours après le dernier jour de la formation ;
(b) Tous les rapports seront livrés en 3 exemplaires et sur support électronique ou papier ;
(c) Les supports de cours à tous les participants au cours des différentes sessions de formation ;
(d) Le consultant devra produire et livrer des certificats de participation pour tous les participants ;

Official Use On

(e) Le consultant devra aussi livrer les certificats de ceux qui ont passé avec succès les examens de certification et validés par les organismes habilités à le faire. L'authentification des certificats se fera à travers le site de l'organisme habilité ou par tout autre moyen reconnu par le bénéficiaire.

VIII. PROFIL ET QUALIFICATIONS

1. Qualifications du Cabinet

La présente mission sera exécutée par un cabinet de formation agréé et reconnu au niveau international pour son expertise dans le domaine du forensic numérique et de la cybersécurité.
Le cabinet devra répondre aux exigences suivantes :

1. Justifier d'au moins dix (10) ans d'expérience dans la conduite de formations certifiantes en cybersécurité ;
2. Disposer d'au moins cinq (5) références pertinentes démontrant la réalisation de missions similaires dans le domaine de la formation professionnelle en sécurité de l'information ou en investigation numérique au cours des trois (3) dernières années ;
3. Fournir des preuves d'accréditation officielles (contrats, certificats, lettres de partenariat, etc.) émises par l'EC-Council ou tout autre organisme reconnu, attestant que le cabinet est habilité à dispenser la formation et à faire passer la certification CHFI (Certified Hacking Forensic Investigator) ;
4. Fournir un lien vers son site Internet officiel, permettant de vérifier ses activités, ses références et son statut institutionnel.

2. Qualifications des Consultants/Formateurs

Le cabinet devra mobiliser des formateurs accrédités et expérimentés, capables d'assurer un transfert de compétences pratique et de haut niveau aux bénéficiaires.

Les formateurs proposés devront répondre aux critères suivants :

1. Un Expert formateur en cybersécurité

- Être titulaires de la certification EC-Council Certified Hacking Forensic Investigator (CHFI) en cours de validité ;

Official Use On

- Justifier d'une expérience pratique confirmée en investigation numérique, couvrant notamment la collecte, l'analyse et la préservation de preuves numériques, ainsi que la gestion d'incidents de cybersécurité ;
- Avoir animé au moins deux (2) formations ou ateliers certifiants dans le domaine du Hacking Forensic Investigator ou dans un domaine connexe (Digital Forensics, Cybercrime Investigation, Incident Response) ;
- Avoir une expérience avérée dans la formation d'équipes techniques au sein d'administrations publiques, d'entreprises ou d'institutions financières ;
- Maîtriser le français, à l'oral comme à l'écrit, pour assurer une communication fluide et un transfert efficace des connaissances ;
- Fournir les preuves de certification et d'accréditation au moins deux (2) semaines avant le démarrage de la formation.

2. Un Expert juridique local

- Expérience professionnelle : Minimum 5 à 7 ans d'expérience pratique (Avocat spécialisé, Magistrat, Consultant en cybersécurité, ou Cadre technique d'une autorité de régulation au Burundi).
- ayant animé au moins deux(2) formations ou atéliers sur le cadre légal,éthique et procédural de l'investigation numérique ,appliqué au contexte institutionnel et juridique du Burundi.
- Avoir une Maîtrise du cadre légal du domaine numérique : Connaissance approfondie de la loi burundaise n°1/12 du 12 mai 2020 portant code de l'offre de cybersécurité et de la lutte contre la cybercriminalité.
- Connaissance des procédures pénales : Maîtrise du Code de procédure pénale burundais, spécifiquement sur la qualification des faits, la légalité des saisies et la force probante des preuves électroniques devant les cours et tribunaux du Burundi.
- Ancrage institutionnel : Compréhension du rôle des acteurs clés comme le Ministère en charge des TIC, l'ARCT (Agence de Régulation des Technologies de l'Information et de la Communication), la Police Judiciaire (BPE) et le Parquet.
- Protection des données : Maîtrise des principes de respect de la vie privée, de la préservation de la confidentialité et des secrets professionnels applicables au Burundi.

Official Use On

IX DUREE ET LIEU DE FORMATION

La durée globale de la mission (formation, préparation à l'examen de certification puis passation de l'examen) sera négociée entre l'Acheteur et le fournisseur mais devra s'étendre sur une période ne dépassant pas 8 semaines, à compter de la date de mise en œuvre du contrat.

Les dates d'exécutions des différentes formations seront convenues de commun accord avec les bénéficiaires.
La formation se déroulera au Burundi, dans le lieu qui sera déterminé d'un commun accord entre le client et le cabinet retenu.
La logistique liée aux sessions de formation sera prise en charge par le PAFEN.

X SUPERVISION DE LA FORMATION

La supervision de la formation sera assurée une commission technique de suivi (CTS) ad hoc mise en place par le coordonnateur du PAFEN.

L'unité de gestion du projet (UGP) du PAFEN assurera la gestion administrative, fournira des services d'appui administratif et logistique ainsi que la réception et l'approbation des factures devant donner lieu à un paiement après acceptation des livrables y afférents par le CTS. Le CTS est responsable de la coordination des activités relevant du Contrat, de l'acceptation et de l'approbation des rapports et autres produits au nom du Client. Le cabinet de conseil est tenu de mener à bien la mission en consultant les parties prenantes, ce qui doit être documenté.

XI METHODE DE SELECTION DU BUREAU

« Le Consultant » sera sélectionné selon la méthode de **Sélection fondée sur les Qualifications du Consultants (SQC)**, conformément au Règlement de Passation des Marchés pour les Emprunteurs sollicitant le financement de Projets d'Investissement (FPI) de la Banque mondiale, édition de Septembre 2023 et conformément aux critères exigés au regard des présents termes de référence ».

Official Use On