DEMANDE DE MANIFESTATIONS D'INTÉRÊT

(SERVICES DE CONSULTANTS)

SÉLECTION DE FIRMES/CABINETS

Pays : République du Burundi
N° du Projet : P176396/P180987
DON IDA N° E0930-BI/E2820-BI

RECRUTEMENT D'UN CONSULTANT POUR RÉALISER UN PLAN DE MISE EN ŒUVRE DU CIRT (COMPUTER INCIDENT REPONSE TEAM)

Réf. STEP: BI-PAFEN-PIU-1.1.3.13-CS-CQS

Le Gouvernement de la République du Burundi a obtenu de l'Association Internationale de Développement (IDA) un Don d'un montant équivalant à 92 000 000 USD pour le financement du Projet d'Appui aux Fondations de l'Economie Numérique (PAFEN) dont l'Objectif de Développement (ODP) 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.

Il a l'intention d'utiliser une partie de ce financement pour effectuer des paiements prévus au titre du contrat des services d'un **« Cabinet chargé de réaliser un plan de mise en œuvre du CIRT (Computer Incident Response Team)»**.

Le Gouvernement du Burundi recherche les services d'une entreprise qualifiée pour mener une évaluation de l'état des lieux des capacités de réponse aux incidents et élaborer un plan de création du CIRT National (« le Plan »). Le Plan reflétera les besoins, les exigences et les objectifs du pays et détaillera les services que le CIRT national devrait fournir, son public cible et les ressources nécessaires. Le Plan devrait également inclure une feuille de route pour l'établissement d'un CIRT national, ainsi que des documents d'appel d'offres pertinents. Le Consultant incorporera des Bonnes Pratiques largement acceptées pour permettre au CIRT national établi grâce au Plan de participer à des initiatives et forums de coopération internationale (par exemple, FIRST).

La mission du bureau se déroulera sur une durée estimée à vingt-deux (22) semaines.

Les Termes de Références (TDRs) détaillés de la mission peuvent être obtenus à l'adresse indiquée ci-dessous.

Le PAFEN invite pour le moment les Cabinets éligibles (« Consultants ») à manifester leur intérêt à fournir les services décrits ci-dessus. Les Consultants intéressés doivent fournir les informations démontrant qu'ils

possèdent les qualifications requises et une expérience pertinente pour l'exécution des Services (brève présentation de leurs cabinets, références concernant l'exécution de contrats analogues, expérience dans des conditions semblables, copies des contrats déjà réalisés, etc.).

Les missions similaires réalisées doivent être accompagnées des preuves de réalisation.

PROFIL DU CABINET

Le consultant sélectionné devra démontrer :

- De solides compétences et une expérience en cybersécurité et en technologies de l'information et de la communication (TIC), notamment dans les domaines suivants : réponse aux incidents, renseignement sur les menaces cybernétiques, cybercriminalité, avec au moins 5 ans d'expérience pertinente.
- Au moins 3 références de projet au cours des 5 dernières années dans l'intégration et la personnalisation d'outils CSIRT/CERT/CIRT/SOC ; le développement de politiques et de procédures liées aux opérations CSIRT/CERT/CIRT/SOC (flux de travail opérationnels, SOP, processus de gestion des incidents, cadres de gestion des niveaux de service, entre autres) ; la mise en place d'outils de centre opérationnel de cybersécurité ; la configuration de leurres informatiques et l'intégration de flux externes, la mise en place de solutions de criminalistique numérique ; ou similaires
- Une connaissance approfondie des politiques, stratégies et opérations en matière de cybersécurité dans un contexte gouvernemental.
- Une compréhension des cadres, méthodologies et meilleures pratiques en matière de cybersécurité.
- Une expérience préalable de travail avec le secteur public est préférable.
- Une expérience dans un contexte de pays en développement est considérée comme un avantage.

Le consultant doit proposer une équipe de base comprenant au minimum (1) Chef d'équipe, (2) Spécialistes de la réponse aux incidents, (1) Spécialiste en gouvernance et gestion des risques en cybersécurité, (1) Expert Juridique, ainsi que tout personnel de soutien supplémentaire jugé nécessaire pour mener à bien la mission. Tous les membres de l'équipe doivent être parfaitement francophones et anglophones.

Le consultant doit fournir un plan de dotation en personnel avec les noms, les rôles et les CV des membres de l'équipe de base du projet dans le cadre de la proposition.

Position clé	Expérience	Qualifications
(1) Chef d'équipe, ou équivalent	Minimum 7 ans d'expérience en gestion de programmes ou de projets de cybersécurité, en particulier en réponse aux incidents, en renseignement sur les menaces cybernétiques et en criminalistique numérique.	• Expérience avérée dans la gestion et la mise en œuvre de projets liés aux CIRT/CERT/CSIRT/SOC dans des pays en développement serait un avantage. • Certifications pertinentes telles que CISSP, CISM ou GCIH, ainsi qu'une certification d'auditeur SOC reconnue internationalement. • Master en informatique, cybersécurité, sciences/technologie et/ou autres domaines pertinents.

Position clé	Expérience	Qualifications
(2) Spécialiste en réponse aux incidents	Au moins 5 ans d'expérience en réponse aux incidents de cybersécurité, avec un accent sur l'établissement et la gestion des CIRT.	• Connaissance approfondie des cadres et méthodologies de réponse aux incidents et d'établissement des CIRT, tels que le cadre de services FIRST, NIST SP 800-61, ISO/IEC 27035, lignes directrices de manipulation d'incidents SANS, et leur application à la construction et à l'exploitation de CIRT efficaces. • Capacité avérée à concevoir et mettre en œuvre des politiques, des procédures et des flux de travail de réponse aux incidents, ainsi qu'à former et encadrer les membres du CIRT sur les meilleures pratiques en matière de réponse aux incidents. • Certifications pertinentes, telles que Certified Information Systems Security Professional (CISSP), GIAC Certified Incident Handler (GCIH) ou EC-Council Certified Incident Handler (ECIH). • Master en cybersécurité/sécurité de l'information, administration des affaires/administration publique, économie, études de développement, commerce, sciences/technologie ou autres domaines pertinents.
(1) Spécialiste en gouvernance et gestion des risques	Au moins 5 ans d'expérience en gestion des risques et CIIP, de préférence au niveau national.	• Connaissance approfondie des cadres de gestion des risques et de la CIIP, tels que NIST SP 800-53, ISO/IEC 27001 ou CIP-014-1, et leur application aux processus de protection des CII. • Certifications pertinentes, telles que Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM) ou Certified Critical Infrastructure Protection Professional (CCIPP). • Master en cybersécurité/sécurité de l'information, administration des affaires/administration publique, économie, études de développement, commerce, sciences/technologie ou autres domaines pertinents.
(1) Expert Juridique	Au moins 5 ans d'expérience dans la fourniture de services de conseil juridique et politique dans le domaine de la cybersécurité.	• Solide compréhension des lois, règlements et normes de l'industrie régissant le partage d'informations et la cybersécurité. - Expérience dans la rédaction et la négociation d'accords juridiques, de contrats et de politiques liés au partage d'informations et à la cybersécurité • Une maîtrise en droit d'une école de droit accréditée, avec une spécialisation en droit de la cybersécurité ou dans des domaines connexes, est préférable

L'attention des consultants intéressés est attirée sur la section III, paragraphes, 3.14, 3.16 et 3.17 du « Règlement de Passation des Marchés pour les Emprunteurs sollicitant le Financement de Projets d'Investissement (FPI) datant de septembre 2023 ». En outre, veuillez-vous référer aux informations spécifiques sur les conflits d'intérêts liés à cette mission.

Les consultants peuvent s'associer à d'autres firmes pour améliorer leurs qualifications, mais doivent indiquer clairement si l'association prend la forme d'un groupement et/ou d'un sous-traitant. Dans le cas d'un groupement,

tous les partenaires de la coentreprise seront conjointement et solidairement responsables de l'intégralité du contrat, s'ils sont sélectionnés.

Le bureau de consultants sera sélectionné selon la méthode de Sélection Fondée sur les Qualifications du consultant (SQC), conformément au Règlement de Passation des Marchés pour les Emprunteurs sollicitant le financement de Projets d'Investissement (FPI), édition de Septembre 2023 et conformément aux critères exigés au regard des termes de référence.

Les Consultants intéressés peuvent obtenir des informations supplémentaires à l'adresse ci-dessous du Lundi au Jeudi de *8 heures 12 heures et de 14 heures à 17 heures et les Vendredi de 8h à 14 heures (heures locales).*

Les manifestations d'intérêt doivent être livrées par écrit à l'adresse ci-dessous (en personne, ou par courrier, ou par e-mail) avant le **27/8/2024 au plus tard à 16 heures** *avec mention :*

« REPONSE A L'AVIS DE SOLLICITATION DE MANIFESTATIONS D'INTERET N° BI-PAFEN-PIU-1.1.3.13-CS-CQS POUR LE RECRUTEMENT D'UN CONSULTANT POUR RÉALISER UN PLAN DE MISE EN ŒUVRE DU CIRT (COMPUTER INCIDENT REPONSE TEAM) »

Attn: Monsieur le Coordonnateur du PAFEN

Boulevard Ndadaye Melchior, Building Orée du Golf, 4ème étage
E-mail: info@pafen.gov.bi avec copies obligatoires à bienvenu.irakoze@pafen.gov.bi , sitou.lawson@pafen.gov.bi , gaspard.mvukiye@pafen.gov.bi et pierre.ndamama@pafen.gov.bi

Pour autorisation de publication

Bienvenu IRAKOZE

Coordonnateur du PAFEN