BCEAO
BANQUE CENTRALE DES ETATS DE L'AFRIQUE DE L'OUEST

Direction Générale de la Comptabilité et des Systèmes d'Information

Direction des Infrastructures Informatiques et des Réseaux

Avis N° 1 – Réponses aux demandes de compléments d'informations sur le dossier d'appel d'offres n° DP/Z00/DBA/0139/2025 – Plan de réponse aux incidents de cybersécurité

Prorogation de la date de dépôt des offres

La date de dépôt initialement fixée au 27 novembre 2025 est prorogée au **12 décembre 2025 à 12h TU.**

Questions : 1er Lot

1. Périmètre organisationnel de la mission

Question 1 : Pourriez-vous préciser si la mission porte uniquement sur le Siège ou si elle englobe également certaines ou l'ensemble des Directions Nationales, le SGCB, le CTF ou d'autres entités de l'Union ?

Question 2 : Est ce que le périmètre de l'intervention couvre l'ensemble des 8 pays couverts par la BCEAO ?

Question 3 : Le périmètre concerne-t-il SI interne, filiales, prestataires, fournisseurs ?

Réponse : Le périmètre de la mission englobe l'ensemble des structures et sites de la Banque. Toutefois, le soumissionnaire est invité à faire des propositions.

2. Format et volumétrie des formations

Question 1 : Pour la "formation des équipes", pourriez-vous indiquer :

- le nombre approximatif de participants,
- les profils concernés (équipes techniques, SOC, métiers, management),
- le format attendu (présentiel uniquement ou possibilité de sessions en ligne).

Question 2 : Pouvez-vous préciser quelles catégories d'équipes sont concernées par la formation et la sensibilisation (équipes techniques, SOC, direction, métiers, etc.) ?

Question 3 : Avez-vous des attentes particulières concernant le format des formations (présentiel sur site BCEAO, distanciel…) ?

Question 4 : Combien de personnes seront-elles formées sur le nouveau plan de réponse aux incidents ? De quelles populations s'agit-il ? (Analystes de sécurité, Techniciens informatiques ...)

Réponse : Le nombre approximatif des participants est d'une trentaine avec des profils principalement techniques, SOC et gestion des risques de sécurité des systèmes

d'Information. Le soumissionnaire est invité à proposer le format qu'il juge adéquat au regard du contenu proposé.

3. Ateliers et exercices de simulation

Question 1 : Pour une estimation précise, pouvons-nous connaître :

- le nombre d'ateliers attendus,
- le type d'exercices souhaités (Tabletop, simulations techniques, exercices de crise),
- le nombre de scénarios à développer.

Question 2 : Combien de scénarios de simulation d'incident sont-ils attendus ? Souhaitez-vous des exercices en mode table-top, ou des simulations techniques réelles ?

Réponse : Le soumissionnaire devra préciser dans son offre les propositions qu'il juge adéquates pour chacun des points cités, au regard du contexte et du périmètre de la mission.

4. Niveau de détail des livrables

Question : Confirmez-vous l'attente d'un Plan de Réponse aux Incidents unique, ou souhaitez-vous également des playbooks détaillés par typologie d'incident (ex. ransomware, phishing, compromission AD, incident monétique, SWIFT, e-banking, etc.)

Réponse : Le soumissionnaire est invité à inclure dans son offre, les propositions jugées adéquates

5. Environnement technique et documentation disponible

Question : Dans le cadre de l'audit de maturité, quels types de documents ou outils seront mis à disposition (SIEM, EDR, ticketing/ITSM, politiques existantes, logs, inventaires…) ?

Réponse : Tous les documents et outils sollicités et disponibles seront communiqués durant cette phase.

6. Modalités de présence sur site

Question : Pourriez-vous préciser le niveau de présence physique requis à Dakar et si certaines phases (entretiens, ateliers, suivi) peuvent être menées en distanciel ?

Réponse : Le niveau de présence physique est laissé à l'appréciation du soumissionnaire qui devra toutefois justifier ses choix pour les travaux menés en distanciel.

Questions : 2ème Lot

Question : Disposez vous déjà d'un SOC

Réponse : Oui

Question : we ask for you to provide detailed requirements regarding the scope of work required

Réponse : The scope of work covers all sites of the Organization. The requirements are specified in the specifications document. Please note that the bids must be in French and that the working language is French.

Question : Quelles sont les équipes de la BCEAO impliquées dans la gestion des incidents ? Quelle est la localisation géographique de chaque équipe ?

Réponse : Toutes les équipes en charge des réseaux, des systèmes, du helpdesk, de la cybersécurité, de la gestion des risques, et le RSSI.

Question : Quelle est la documentation existante en matière de gestion des incidents ? Si oui, serait-il possible d'avoir plus de détails sur les procédures existantes ?

Réponse : L'existant sera fourni au prestataire qui sera retenu.

Question : Quels sont les outils utilisés dans le cadre de la détection et de la réponse aux incidents (SIEM, EDR...) ?

Réponse : L'existant sera fourni au prestataire qui sera retenu.

Questions : 3ème Lot

Question : Pouvez-vous confirmer si une analyse de risques relative à la cybersécurité ou aux activités critiques de la BCEAO existe déjà, afin qu'elle puisse servir de référence pour orienter la conception du plan de réponse ?

Réponse : Une analyse des risques relatifs à la cybersécurité et aux activités critiques a été initiée mais pas finalisée.

Question : Attendez-vous que le plan soit conçu selon un référentiel spécifique (ISO 27035, NIST 800-61, cadre interne BCEAO…) ?

Réponse : Il revient au soumissionnaire de proposer le référentiel qu'il juge adéquat en la matière.

Question : Les "outils" mentionnés concernent-ils uniquement des supports méthodologiques (procédures, workflows) ou également des outils techniques à mettre en œuvre ou configurer dans l'environnement BCEAO ?

Réponse : Il revient au soumissionnaire de proposer d'évaluer la pertinence et la portée des outils à recommander (procédures, workflows, solutions technologiques, etc..).

Question : Attendez-vous que le prestataire conçoive uniquement les scénarios d'exercices, ou qu'il organise et anime également les simulations avec vos équipes ?

Réponse : Le soumissionnaire est invité à faire des propositions qu'il juge pertinentes.

Question : Pouvez-vous préciser si la formalisation attendue doit se limiter à des procédures générales de gestion des incidents, ou si elle doit inclure des instructions opérationnelles détaillées par type d'incident (ex. fiches réflexes, modèles de communication, schémas d'escalade, rôles et responsabilités) afin d'assurer une application concrète du dispositif ?

Réponse : L'offre du soumissionnaire doit permettre d'assurer une opérationnalisation complète et concrète du dispositif.

Question : Souhaitez-vous que la formalisation des procédures et instructions opérationnelles porte uniquement sur la structure globale du processus de réponse aux incidents, ou qu'elle détaille également les actions spécifiques à mener pour chaque type d'incident ?

Réponse : La réponse à la question est l'objet de l'appel d'offre

Question : Pouvez-vous préciser les types de formation attendus : sensibilisation générale à la réponse aux incidents, formation technique pour les équipes opérationnelles, ou formation spécifique pour les responsables et décideurs ? Pouvez-vous préciser le nombre approximatif de participants et la répartition par profil ?

Réponse : Il revient au soumissionnaire de faire les propositions des formations adéquates et pertinentes. Pour le nombre de participants et le profil, voir la réponse ci-dessus.

Question : Souhaitez-vous que le prestataire élabore les plans d'exercices de simulation comme mentionné sur "II.4 Résultats attendus", ou qu'il assure également la conduite effective des simulations ? Pouvez-vous préciser le nombre d'exercices à élaborer ou réaliser, les types de scénarios attendus (exemples : compromission, ransomware, fuite de données, etc.), ainsi que le format souhaité des simulations (table-top, techniques) ?

Réponse : Le soumissionnaire est invité à faire des propositions

Question : Pouvez-vous indiquer si l'exécution de toute la mission est attendue d'être en mode hybride (Présentiel / Distanciel) ou seulement en présentiel ?

Réponse : Le soumissionnaire est invité à faire des propositions