BANQUE AFRICAINE DE DÉVELOPPEMENT
AVIS DE VACANCE DE POSTE RÉF. ADB/21/042

INTITULÉ DU POSTE :	**CHEF D'UNITÉ — RISQUES CYBERNÉTIQUES**
COMPLEXE :	**SERVICES INSTITUTIONNELS ET RESSOURCES HUMAINES (CHVP)**
DÉPARTEMENT/DIVISION :	**SERVICES INSTITUTIONNELS ET RESSOURCES HUMAINES (CHVP)**
GRADE :	**PL1**
SUPÉRIEUR HIÉRARCHIQUE :	**VICE-PRÉSIDENT CHARGÉ DES SERVICES INSTITUTIONNELS ET DES RESSOURCES HUMAINES (CHVP)**
LIEU D'AFFECTATION :	**ABIDJAN, CÔTE D'IVOIRE**
INFORMATIONS SUR LE POSTE :	**CE POSTE BÉNÉFICIE DU STATUT INTERNATIONAL ET OUVRE DROIT AUX CONDITIONS D'EMPLOI Y AFFÉRENTES.** **Si vous rencontrez des difficultés techniques lors de l'enregistrement de votre candidature, veuillez envoyer un courriel avec une description précise du problème et/ou une capture d'écran indiquant le problème à : HR Direct HRDirect@AFDB.ORG**
N° SAP :	**50101122**
DATE DE CLÔTURE :	**12 Mars 2021 (à 23 h 59 GMT)**

LA BANQUE :

Créée en 1964, la Banque africaine de développement (BAD) est la première institution panafricaine de développement. Elle a pour mission de promouvoir la croissance économique et le progrès social sur l'ensemble du continent. La Banque compte 81 pays membres, dont 54 pays africains (les pays membres régionaux). Le Programme de développement de la Banque vise à fournir l'appui financier et technique nécessaire aux projets porteurs de transformation, qui permettront de réduire sensiblement la pauvreté grâce à une croissance économique inclusive et durable en Afrique. Pour davantage se concentrer sur les objectifs de la Stratégie décennale (2013-2022) et réaliser un plus grand impact sur le développement, cinq grands domaines (*High 5*), dans lesquels les interventions devront s'intensifier pour l'Afrique, ont été identifiés, à savoir : l'énergie, l'agro-industrie, l'industrialisation, l'intégration et l'amélioration de la qualité de vie des populations africaines. La Banque entend constituer une équipe de direction qui pilotera avec succès la mise en œuvre de cette vision.

LE COMPLEXE :

La Vice-présidence des services institutionnels et des ressources humaines (CHVP) assure la fourniture de services institutionnels efficaces, centrés sur les personnes et répondant aux besoins des clients, afin de garantir une efficacité institutionnelle globale dans tous les aspects des services institutionnels de la Banque. Le Complexe mène les efforts visant à numériser et à transformer la Banque en un vivier de talents, à promouvoir des politiques de ressources humaines qui renforcent le talent, à conduire une culture axée sur la performance, et à s'assurer la compétitivité de la Banque en tant qu'employeur de choix. Le Complexe veille à ce que les ressources humaines et les services institutionnels soient en harmonie pour améliorer leur performance, et exécuter la vision stratégique et les priorités de la Banque. Le Complexe est chargé d'assurer le leadership dans la formulation et la mise en œuvre des stratégies de la Banque concernant la gestion des personnes, les technologies de l'information, les services généraux et les achats institutionnels, les services linguistiques, la continuité des affaires, ainsi que la santé et la sécurité.

LE DÉPARTEMENT/LA DIVISION QUI RECRUTE :

Le chef de l'Unité en charge des risques cybernétiques créera une nouvelle unité au sein de la Banque, afin de fournir une expertise et une assistance pour assurer une protection effective des actifs relatifs aux infrastructures et aux informations de la Banque. L'Unité en charge des risques cybernétiques sera responsable de la sauvegarde de tous les actifs de la Banque relatifs aux technologies de l'information et de la communication (TIC), sur l'ensemble des plateformes, en tous lieux, et pour l'ensemble des parties prenantes. L'Unité en charge des risques cybernétiques fera partie de la gestion du cycle de vie des TIC de la Banque, et lui offrira des solutions TIC sécurisées. Elle pilotera les solutions technologiques sécurisées à la Banque et les fournira. Ces activités incluent, sans s'y limiter, le Centre d'opérations de la sécurité (SOC), la réponse aux incidents cybernétiques, la veille en matière de menaces, l'attaque et la défense de type « zéro day », la sécurité des données en nuage, la sécurité mobile, la sécurité des données ainsi que la sécurité des applications. L'Unité en charge des risques cybernétiques mettra l'accent sur l'élaboration et la mise en œuvre de stratégies, de politiques et de normes en matière de risques liés à l'information, et veillera à la mise en place de solutions efficaces, de politiques et de procédures appropriées, notamment les règles de connexion et d'authentification des utilisateurs, la violation des règles de sécurité, les procédures de recours à la hiérarchie, et les procédures d'évaluation de la sécurité. L'Unité en charge des risques cybernétiques appliquera les politiques et les procédures en matière de sécurité de l'information, surveillera les profils de sécurité des données sur toutes les plateformes et mènera des enquêtes sur les scénarios de risque.

LE POSTE :

Le poste vise les objectifs suivants :

1. Se charger de la sauvegarde de tous les actifs de la Banque relatifs aux technologies de l'information et de la communication (TIC), sur l'ensemble des plateformes, en tous lieux, et pour l'ensemble des parties prenantes. En outre, le titulaire du poste jouera un rôle décisif dans le programme élargi de la Banque relatif aux risques liés aux technologies de l'information, et sera chargé d'assurer la conformité aux normes de sécurité de l'information auprès de tous les fournisseurs externes.

2. Élaborer une vision exhaustive des pratiques en matière de sécurité cybernétique pour la Banque, dans le cadre de la gestion des politiques de sécurité, des procédures, des orientations et des normes. Cette vision inclura entre autres des feuilles de route de l'architecture sécuritaire des TIC, les outils associés et les procédures sécuritaires.

3. Diriger l'innovation de la sécurité cybernétique au sein de la Banque, et offrir des solutions TIC novatrices, de sorte à répondre aux défis opérationnels et technologiques.

4. Proposer des solutions à l'équipe de projet opérationnelle et TIC de la Banque, veiller à la gestion des exigences en matière de sécurité de l'information et de la technologie, notamment la confidentialité, l'intégrité et la disponibilité, et veiller à atteindre les objectifs des projets.

5. Planifier, exécuter et gérer des projets multidimensionnels liés à la gestion des risques cybernétiques, à l'atténuation et à l'intervention, à la conformité, à l'assurance du contrôle et à la sensibilisation des utilisateurs.

6. Actualiser, tenir à jour et documenter les systèmes de contrôle de l'information, et apporter un appui

direct aux structures informatiques internes de la Banque.

7. Piloter et coordonner, structurer et suivre les mesures liées à l'élaboration et à la mise en œuvre d'une nouvelle unité des risques cybernétiques. Celle-ci assurera la gestion efficace de ces risques, la planification axée sur les risques et veillera à la collaboration avec les départements opérationnels sur divers aspects des risques cybernétiques, à l'effet de réaliser les objectifs opérationnels de la Banque.

8. Superviser les activités qui lui sont confiées, principalement dans le cadre de la gestion des risques, et piloter des projets techniques dans tous les domaines techniques, afin d'atténuer les risques cybernétiques.

PRINCIPALES FONCTIONS :

Les domaines de responsabilité du chef de l'Unité relèvent des catégories suivantes :

- Gouvernance et stratégie : S'assurer de la gestion sans heurt de toutes les initiatives énumérées plus haut, de l'obtention de leur financement, et de la compréhension de leur importance auprès des responsables institutionnels ;
- Opérations en matière de sécurité : Analyser en temps réel les menaces imminentes, et trier les problèmes qui se posent ;
- Risque et veille cybernétiques : Se tenir au courant des menaces sécuritaires en cours, et aider le Conseil à comprendre les problèmes sécuritaires potentiels susceptibles de découler des acquisitions et d'autres mouvements opérationnels importants ;
- Perte des données et prévention de la fraude : S'assurer que le personnel interne utilise correctement les données et ne les vole pas ;
- Architecture de la sécurité : Planifier, acquérir et mettre en service le matériel et le logiciel, et veiller à la conception de l'infrastructure du réseau informatique en gardant à l'esprit les meilleures pratiques en matière de sécurité ;
- Gestion des identités et des accès : S'assurer que seules les personnes habilitées ont accès aux données et aux systèmes restreints ;
- Gestion des programmes : Se tenir au courant des besoins sécuritaires, en mettant en œuvre des programmes ou des projets qui atténuent les risques ;
- Enquêtes et expertise judiciaire : Déterminer les dysfonctionnements en cas de violation, gérer les responsables s'ils sont internes, et planifier en vue d'éviter que la crise ne se reproduise.

Le titulaire du poste assumera notamment les fonctions suivantes :

1. Appropriation de la vision, de la stratégie et de l'assurance relatives à la conformité à la sécurité de l'information, y compris des éléments suivants :

    - Planification stratégique du système de gestion des risques cybernétiques de la Banque, notamment de l'évaluation de la situation, de la vision et de la mission, des objectifs, et des

feuilles de route à court, moyen et long termes.

- Évaluation et interprétation des meilleures pratiques de l'industrie pour le compte de la BAD (NIST, ISO, SANS, COBIT, CERT), et exigences de conformité (juridiques et réglementaires).
- Selon qu'il conviendra, appropriation, parrainage, gestion, appui et supervision des évaluations en matière de sécurité de l'information, des audits, et du suivi.
- Gestion des menaces posées à la sécurité de l'information et de la vulnérabilité, établissement de rapports concernant les incidents, gestion d'événements, enquêtes sur les événements ainsi que leur analyse.
- Appropriation du portefeuille de projets relatifs à la sécurité de l'information, y compris le développement de capacités nouvelles ou améliorées, et gestion des domaines nécessitant des mesures correctives.
- Conduite et parrainage de la stratégie de la BAD relative à la gestion des risques informatiques institutionnels.

2. Planification stratégique, gestion des risques et actions :

- Développer une stratégie de gestion des risques cybernétiques, de sorte à répondre aux besoins à court, moyen et long termes.
- Concevoir, élaborer et entretenir l'Architecture de sécurité de l'information d'entreprise (EISA - *Enterprise Information Security Architecture*) par l'alignement des processus opérationnels, du matériel et du logiciel informatiques, des réseaux locaux et au-delà, des personnes, des opérations et des projets, dans le cadre de la stratégie globale de l'organisation en matière de sécurité
- Procéder à une analyse externe de l'organisation (par exemple, une analyse des clients, de la concurrence, des marchés et de l'environnement de l'industrie), et à une analyse interne (gestion des risques, capacités de l'organisation, mesure de la performance, etc.). Utiliser ces analyses pour faire correspondre le programme en matière de sécurité aux objectifs de l'organisation
- Identifier et consulter les principales parties prenantes, en vue d'assurer une compréhension des objectifs de l'organisation
- Définir un plan stratégique prospectif, visionnaire et novateur, dans le cadre du rôle à jouer pour le programme de sécurité de l'information, contenant des cibles et des objectifs clairs qui aident à répondre aux besoins opérationnels de l'organisation

3. Implication des intervenants du secteur

- Collaborer avec les dirigeants du secteur d'activité sur des questions de risque allant des politiques et de la gouvernance aux opérations liées aux risques de sécurité.
- Offrir un appui de niveau expérimenté et actif à l'équipe de projet opérationnelle, de sorte à

garantir la livraison des projets conformément aux cibles, aux délais impartis et au budget, dans le but de répondre aux besoins de l'institution.

- La BAD a adopté une stratégie axée sur la « priorité au nuage ». Les plateformes qui hébergent des services en nuage et les logiciels en tant que service (SaaS – *software-as-a-service*) sont largement utilisés au sein des unités opérationnelles et des unités informatiques de la Banque. Le titulaire du poste dirigera l'Unité et élaborera une stratégie en matière de sécurité en nuage. Il sera responsable de la mise en œuvre de la stratégie.

- Fournir des mesures administratives et de suivi au Vice-président de CHVP, tout en entretenant des relations avec les Unités chargées de la continuité des activités, de la sécurité physique, le Département des technologies de l'information, l'Équipe chargée des risques opérationnels et le Chef de la gestion des risques du Groupe.

- Diriger et assurer la coordination et le consensus avec les autres équipes de la Banque, afin d'harmoniser les processus et les procédures, et assurer une approche commune des activités de gestion des risques cybernétiques.

4. Mener l'innovation de la technologie en matière de sécurité cybernétique au sein de la Banque, et proposer des services de conseil d'expert du plus haut niveau à la Haute direction.

5. Veiller à ce que tous les processus et l'accès soient conformes aux politiques de la Banque.

6. Apporter un soutien dans le cadre des audits internes et externes.

7. Gérer des projets multiples de grande envergure, ambigus et très complexes.

8. Entretenir des connaissances spécialisées sur tous les principes, les technologies et les éléments relatifs au risque de cybersécurité.

9. Comprendre la structure et les opérations du programme global de la Banque et appuyer la stratégie des priorités *High 5*.

COMPÉTENCES (qualifications, expérience et connaissances) :

1. Être titulaire au moins d'un Master 2 en génie électrique, génie des systèmes, sciences informatiques, génie informatique, technologies de l'information, systèmes d'information de gestion, gestion des risques et de la sécurité, ou dans des disciplines connexes.

2. Plus de huit (8) ans d'expérience professionnelle à un poste pertinent de gestion du risque lié à la sécurité de l'information, et plus de deux (2) ans d'expérience à un poste de gestion ou à un poste similaire. Des compétences et une expérience équivalentes sont hautement recherchées. Expérience pratique de la norme ISO 27000 est exigée. Expérience de plus de trois (3) ans dans la réalisation ou la conduite d'évaluations de la sécurité de l'information fondées sur le risque serait un avantage supplémentaire.

3. Expérience de niveau expert dans au moins deux domaines CISO

4. Certifications obligatoires en sécurité TIC (à moins de pouvoir démontrer le même niveau de connaissances) :

   - CISSP
   - CISM et/ou CISA

5. Certifications et expérience en sécurité désirées (une ou plus) :

   - Hacker éthique certifié
   - Sécurité CCIE
   - Défense cybernétique SANS
   - Veille des menaces
   - Test d'intrusion Kali

6. Expérience structurée de la gestion de projets dans le déploiement d'initiatives liées aux risques cybernétiques.

7. Vaste expérience des systèmes réseau et informatiques, axée sur les technologies de l'information et les risques cybernétiques.

8. Expérience de la gestion d'équipes.

9. Connaissance de la conformité, des normes et des cadres réglementaires tels que ISO, NIST, COBIT et PCI DSS.

10. Compréhension avérée des procédures et des méthodologies d'évaluation des risques en matière de sécurité de l'information et de gestion des risques.

11. Capacité de mettre en corrélation les risques de l'entreprise avec les contrôles administratifs et les techniques appropriés en matière de sécurité.

12. Connaissance et expérience de diverses architectures, d'environnements de traitement de transactions à grande échelle, de services hébergés externes et d'environnements de services informatiques hébergés en nuage.

13. Compréhension et connaissance pratiques des principes, des normes et des processus en matière de risques liés aux technologies de l'information, tels que l'authentification et le contrôle d'accès, le renforcement des infrastructures, l'analyse du trafic réseau, la sécurité des terminaux, l'architecture des plateformes, la sécurité des applications, le cryptage et la gestion des clés, la sécurité du nuage, etc.).

14. Connaissance pratique de tous les systèmes d'exploitation.

15. Dynamisme et motivation personnelle à fournir d'excellents services aux utilisateurs.

16. Excellentes aptitudes en relations interpersonnelles et sens de la collaboration.

17. Solides compétences en communication pour favoriser l'engagement efficace des membres de l'équipe

et des fournisseurs externes.

18. Compétences en matière de résolution de conflits.

19. Capacité à conseiller la Haute direction sur le développement de systèmes complexes et les questions y afférentes, qui sont d'une importance capitale pour l'Institution ; capacité d'analyse conceptuelle et stratégique à comprendre les systèmes d'information et les questions opérationnelles liées aux activités, de sorte à pouvoir analyser et à évaluer de façon minutieuse les enjeux touchant les systèmes essentiels.

20. Expérience avérée de l'amélioration des processus et des approches ; faculté d'adaptation indéniable aux priorités en constante évolution.

21. Aptitude à se tenir informé des nouvelles évolutions du métier et de la profession ; bonne compréhension des nouvelles technologies et des tendances de l'industrie.

22. Excellent esprit d'équipe, aptitudes à la communication orale et écrite.

23. Maîtrise de l'anglais, du français, ou des deux, avec une bonne connaissance pratique de l'autre langue.

Seul(e)s les candidat(e)s répondant à toutes les exigences du poste et retenu(e)s pour une évaluation plus approfondie seront contacté(e)s. Les candidat(e)s devront soumettre un curriculum vitæ (CV) concis, et tout autre document complémentaire pouvant être requis. *Le Président de la Banque africaine de développement se réserve le droit de nommer un candidat à un grade inférieur à celui du poste annoncé. La Banque africaine de développement est un employeur garantissant l'égalité des chances, et les candidatures féminines sont vivement encouragées.* **http://www.afdb.org**

Le Groupe de la Banque africaine de développement ne perçoit aucun frais ou contribution de quelque nature que ce soit des candidats tout au long de son processus de recrutement (dépôt des candidatures, étude des CV, entretien d'embauche, traitement final des candidatures). En outre, le Groupe de la Banque ne demande aucune information relative aux comptes bancaires des candidats. Le Groupe de la Banque africaine de développement décline toute responsabilité de publications frauduleuses d'offres d'emploi en son nom ou, de manière générale, d'utilisation frauduleuse de son nom, de quelque manière que ce soit.