

TERMES DE REFERENCE POUR LE RESPONSABLE SECURITE DE L'INFORMATION, CONTINUITE D'ACTIVITE & PROTECTION DES DONNEES

OBJECTIFS DU POSTE

- ✓ Assurer des services de qualité en matière de sécurité de l'information, de protection des données et de gestion de la continuité des activités au niveau de l'organisation ;
- ✓ Contribuer à l'amélioration et la gestion des informations sensibles, anticiper régulièrement des audits internes de sécurité et agir comme principal point de contact entre la banque et les autorités de protection des données ;
- ✓ Évaluer le cadre existant de protection des données, identifier les domaines de non-conformité ou de conformité partielle pour un accompagnement garantissant une conformité totale
- ✓ Promouvoir une culture de conformité en matière de protection des données au sein de l'organisation.
- ✓ S'assurer chaque fois que les politiques et procédures de protection des données et de la gestion de la continuité d'activité sont à jour.

PRINCIPALES RESPONSABILITES

- ✓ Agir en tant que Responsable de la Sécurité de l'Information et assurer la mise en œuvre de la stratégie globale de sécurité de l'information du Groupe au niveau de la filiale ;
- ✓ S'assurer du maintien de la conformité aux exigences sectorielles et réglementaires (PCIDSS, SWIFT CSP, ISO 27001, ISO 27701, ISO 22301, exigences de cybersécurité du Groupe, etc.) ;
- ✓ Assurer le monitoring régulier de la conformité aux politiques et procédures de sécurité de l'information, de la gestion de la continuité d'activité et transmettre les exceptions au Directeur des Opérations & Technologies ainsi qu'au responsable CISO du Groupe ;
- ✓ Travailler en étroite collaboration avec la Sécurité de l'Information du Groupe pour mettre en œuvre, au niveau de la filiale, les initiatives de sécurité du Groupe Ecobank ;
- ✓ Initier, faciliter et promouvoir des activités visant à créer et renforcer la sensibilisation à la sécurité de l'information au sein de la banque ;
- ✓ Fournir des conseils et orientations pour la protection physique et logique des ressources technologiques et de l'Information au bénéfice des autres systèmes fonctionnels ;
- ✓ Examiner tous les plans de sécurité liés aux systèmes à travers le réseau de la banque

- ✓ Mettre en place un processus de reporting afin de garantir que le management soit informé de l'efficacité de la Sécurité des Technologies de l'Information ainsi que de la résolution des problèmes identifiés ;
- ✓ Exécuter toute autre tâche assignée par le Superviseur.

Gestion des risques

- ✓ Conception et élaboration des politiques et un cadre de gestion des risques de sécurité conformes aux normes de l'industrie ;
- ✓ S'assurer qu'annuellement une formation de sensibilisation à la sécurité de l'information sous la supervision directe est faite par tous les employés conformément aux politiques et procédures de sécurité de l'information établies par la banque ;
- ✓ Examiner l'infrastructure technologique des systèmes de paiement, identifier les lacunes critiques et recommander des actions de correction ;
- ✓ Réaliser une évaluation interne des risques fondée sur la conformité de sécurité SWIFT Customer Security (CSP) chaque année, dans le cadre des systèmes de paiement ;
- ✓ Réaliser une évaluation interne des risques ainsi qu'une évaluation des risques liés aux tiers, conformément aux exigences obligatoires de la norme ISO 27001, chaque année, afin de garantir la conformité et de maintenir la certification.

Protection des données

- ✓ Concevoir, mettre en œuvre une stratégie de Protection et de Confidentialité des Données de l'organisation ;
- ✓ S'assurer de la mise en œuvre du Système de Gestion des Informations relatives à la Vie Privée (PIMS) au sein de l'organisation en collaboration le management de la banque et le groupe ;
- ✓ Veiller au respect intégral de la loi locale sur la Protection des Données et de la Vie Privée ainsi que des réglementations en matière de cybersécurité au sein de l'organisation ;
- ✓ développer de nouvelles politiques et procédures internes de protection des données ou réviser périodiquement celles existantes, en consultation avec les parties prenantes clés ;
- ✓ Effectuer des évaluations périodiques et veiller à ce que les procédures et processus soient conformes aux exigences en matière de protection des données ;
- ✓ Promouvoir une culture de conformité à la protection des données dans toutes les unités de la Banque.

Coordination de la continuité d'activité

- ✓ Travailler en étroite collaboration avec le responsable de la continuité des activités du Groupe afin de mettre en œuvre les initiatives de continuité des activités pour la filiale ;
- ✓ Travailler avec tous les segments de la banque et élaborer le plan de continuité des activités de la filiale en veillant à ce que tous les segments soient intégrés ;
- ✓ Veiller à ce qu'un comité de crise soit constitué et s'assurer de fournir des orientations concernant l'activation des plans de réponse aux incidents ou situations d'urgence ;
- ✓ Coordonner les tests de continuité des activités et veiller à ce que tous les segments de la banque y participent et que les tests soient concluants. Identifier toutes les lacunes, les documenter, attribuer des responsabilités et en assurer le suivi jusqu'à leur clôture ;

PROFIL DU CANDIDAT

- Bac+4 en informatique au minimum
- Une formation en sécurité informatique serait un atout
- La possession des certifications Cisco serait un grand atout
- Minimum deux ans d'expérience dans un poste similaire ;
- Avoir des compétences en Réseaux et systèmes sans fil ;
- Aptitudes de gestion des troubles de réseaux ;
- Connaissance des produits IT ;
- Avoir une bonne maîtrise du français et de l'anglais ;
- Le candidat doit faire preuve de rigueur, collaboration, disponibilité, patience, avoir le sens de priorité et d'initiatives, honnêteté et un sens élevé d'anticipation.