



AVIS DE RECRUTEMENT

Type de contrat : **CDD 2 ans**

Disponibilité immédiate

Ingénieur(e) Sécurité en Gouvernance, Risque et Conformité (H/F)	
Employeur	Agence des Systèmes d'Information et du Numérique (ASIN)
Superviseur Hiérarchique	Responsable Conformité
Direction	Pôle Sécurité Numérique
Relation fonctionnelle	Tous directeurs et autres collaborateurs
Lieu d'affectation	Cotonou - BENIN
Candidature	Postulez en ligne sur le portail national des services publics https://service-public.bj/public/services/service/PS01334 en joignant CV détaillé, lettre de motivation, références et attestations, au plus tard le 23 octobre 2026 à 20h00 (heure de Cotonou).

INFORMATIONS GENERALES

La République du Bénin a lancé un programme ambitieux de développement de l'économie numérique visant à positionner le pays comme la référence en matière de plateforme de services numériques de l'Afrique de l'Ouest et de faire des Technologies de l'Information et de la Communication le principal levier de son développement socio-économique.

L'Agence des Systèmes d'Information et du Numérique (ASIN) est une agence gouvernementale sous la double tutelle du Ministère de l'Économie et des Finances et du Ministère du Numérique et de la Digitalisation, chargée d'assurer la mise en œuvre opérationnelle des programmes et projets entrant dans le cadre des stratégies de développement des services et systèmes d'information sécurisés au Bénin. À ce titre, elle conçoit, déploie et maintient les plateformes nationales de services publics numériques, les référentiels et les briques d'interopérabilité qui permettent aux administrations d'échanger leurs données et de servir les usagers de manière simple, sécurisée et continue.

OBJECTIF ET PORTEE DE LA MISSION

Rattaché(e) directement au Responsable de la conformité du Pôle Sécurité Numérique, l'Ingénieur(e) GRC a pour mission principale d'assurer la conformité aux politiques de sécurité et de protection, aux normes et aux meilleures pratiques en matière de Sécurité Numérique. Il/Elle participe activement aux activités relevant du Laboratoire des Opérations de Conformité dans le cadre de l'atteinte des objectifs qui lui sont assignés.

PRINCIPALES RESPONSABILITES

- Participer à la définition, l'élaboration, la mise en œuvre et le contrôle du plan d'inspection de Sécurité Numérique ;
- Réaliser les audits de conformité, présenter les analyses d'écarts en regard des référentiels en vigueur, exposer les conclusions aux structures auditées et aux équipes de contrôle ;
- Participer à l'analyse des risques, à la mise en œuvre et au suivi des plans de traitement des risques en Sécurité Numérique ;
- Contribuer à l'élaboration, la mise en œuvre, le suivi, la mise à jour et l'amélioration des documents de gouvernance de sécurité et des cadres de références (Stratégie de sécurité numérique, Politiques de sécurité, Politiques de protection, Documents de spécification) ;
- Contribuer à l'élaboration des processus et des procédures concernant les activités de sécurité de l'information ;
- Participer à la définition et à la gestion des KPI de sécurité ;
- Réaliser en autonomie des diagnostics de sécurité des fonctions informatiques et des processus métier informatisés ;
- Mener des contrôles permanents et/ou périodiques de sécurité, notamment sur la base de



revues documentaires, de collecte de preuves et aux rapports des outils de contrôle de conformité ;

- Participer au programme de sensibilisation/formation en sécurité de l'information ;
- Exécuter toutes autres tâches liées à la Sécurité Numérique assignées par le supérieur hiérarchique.

FORMATION, EXPÉRIENCES, CONNAISSANCES ET LANGUES

Formation

- Être titulaire au moins d'un Master (BAC + 5) portant sur le « management des SI » ou « en Ingénierie Informatique »,
- Avoir au moins l'une des certifications suivantes serait un atout : CISA, ISO 27001-Lead Auditor, ISO 27001- lead implementor, CRISC.

Expérience professionnelle

- Une expérience de trois (03) à cinq (05) ans minimums dans le domaine de la Sécurité Numérique dont au moins cinq (05) ans en audit, gouvernance, risque et conformité de la sécurité Numérique.
- Une bonne expérience de la gouvernance de la sécurité Numérique.

Connaissances

- Une bonne connaissance des outils, normes, référentiels et standards de l'industrie : ISO 27001, ISO 27002, ISO 20000, Top10 OWASP ;
- Une bonne connaissance des cadres nationaux : Stratégie Nationale de Sécurité Numérique, Politique de Sécurité des Systèmes d'Information de l'Etat, Politique de Protection des Infrastructures Critiques ;
- Une bonne connaissance du Code du Numérique ;
- Une bonne compréhension des dispositifs de contrôle et de gestion des risques.

Langues

- Une excellente maîtrise de la langue française aussi bien à l'oral qu'à l'écrit est exigée. Une bonne maîtrise de l'anglais à l'oral et à l'écrit serait un atout.

ETHIQUE, MANAGEMENT ET LEADERSHIP

- Être passionné(e) de la sécurité des technologies de l'information, avoir la volonté d'apprendre, être capable de travailler en équipe et sous pression.
- Avoir l'esprit de rigueur, d'analyse et une bonne capacité de traitement des urgences.
- Avoir une excellente capacité rédactionnelle.
- Avoir l'esprit de confidentialité et d'auto-formation.
- Avoir une excellente capacité de communication et de travail en équipe pour l'atteinte des objectifs.
- Bonne gestion du temps et des priorités.
- Avoir un bon sens de synthèse et d'analyse.
- Être de bonne moralité.

CADRE LÉGAL ET RÈGLES D'ENGAGEMENT

- Aucune action offensive ne peut être engagée sans mandat écrit préalable définissant le périmètre, les adresses et systèmes concernés, les fenêtres d'intervention, les actions interdites et les points de contact d'urgence
- Interdiction absolue de toute action hors périmètre, de toute exfiltration de données réelles au-delà de la preuve minimale nécessaire, et de toute action susceptible de dégrader un service en production sans autorisation explicite
- Journalisation exhaustive et horodatée de toutes les actions menées, conservée et communicable à l'entité testée et à la hiérarchie



- Destruction sécurisée des données collectées à l'issue de la mission, selon la procédure de rétention définie
- Notification immédiate à la hiérarchie et à l'entité en cas de découverte d'une compromission préexistante, avec bascule vers le processus de réponse à incident
- Interdiction d'utiliser les compétences, les accès, l'outillage ou les informations obtenus dans le cadre du poste à toute autre fin; engagement de non-divulgaration permanent, y compris après la fin du contrat
- Poste soumis à une enquête de moralité approfondie et à la production d'un extrait de casier judiciaire.

CONDITIONS PARTICULIERES D'EXERCICE

- Interventions possibles en dehors des heures ouvrables en cas de crise ou afin de limiter l'impact sur les services en production, et déplacements sur le territoire national.