

RECRUTEMENT

INTITULÉ DU POSTE	DOSSIER À ENVOYER
CHARGE DU SUIVI DES RISQUES SI	Lettre de motivation, CV et Diplôme

Nous vous prions de bien vouloir adresser vos candidatures (Lettre de motivation + Curriculum Vitae + dernier diplôme), en mentionnant l'intitulé du poste et la référence du poste(REF/DGR/02) , à l'adresse recruitment@nsiabanque.com.

Date limite de dépôt des candidatures : **vendredi 11 juillet 2025**

Par ailleurs, seules les candidatures retenues seront contactées.

RAISON D'ÊTRE DE LA FONCTION

Identifier, analyser et traiter les risques liés à la sécurité du système d'information pour en minimiser l'impact et mettre en place des solutions pour garantir la disponibilité, la sécurité et l'intégrité du système d'information et des données.

POSITION DANS L'ORGANIGRAMME

CHEF DE DEPARTEMENT IDENTIFICATION ET SUIVI DES RISQUES

CHEF DE SERVICE SUIVI DES RISQUES OPERATIONNELS & INFORMATIQUES

CHARGE DU SUIVI DES RISQUES SI

FINALITÉS DE LA FONCTION

- Assister le chef de service Suivi des risques Opérationnels et Informatiques dans les actions suivantes :
- Identifier, documenter et évaluer les risques SI ;
- Analyser les incidents de sécurité du SI et proposer des actions de maîtrise ;
- S'assurer de la mise en œuvre du plan de traitement des risques SI identifiés dans la cartographie des risques ;
- Calculer et suivre les indicateurs de risques (KRI) à la Sécurité du SI
- S'assurer du respect et de la mise en œuvre des politiques, procédures et chartes liées à la sécurité de l'information
- Veiller au respect des lois, réglementation et obligations en matière de sécurité du SI
- Suivre la mise en œuvre des plans d'actions résultants des audits de sécurité interne et externe
- Aider à la préparation des comités de sécurité du SI
- Diffuser la culture du risque informatique

DOMAINES D'ACTIVITÉS	TÂCHES PRINCIPALES
1)) Identifier et suivre les risques SI	<ul style="list-style-type: none"> ▪ Identifier les risques liés à la sécurité du SI et participer à la mise à jour de la cartographie des risques ; ▪ Participer à la collecte et l'analyse des incidents de sécurité SI ; ▪ Assister à l'identification des risques SI liés à la mise en place de nouveaux produits, process, systèmes et activités ; ▪ Faire le suivi des activités des prestataires de sécurité ; ▪ Proposer des actions de maîtrise des risques SI identifiés.
2) Mesurer et anticiper les risques SI	<ul style="list-style-type: none"> ▪ Calculer et suivre les différents indicateurs de risques (KRI) et identifier les dépassements des seuils ; ▪ Analyser les indicateurs d'efficacité du dispositif des risques SI et faire des recommandations ; ▪ Faire la veille technologique sur la cybersécurité en vue d'anticiper la survenance et la détection de certains risques SI ▪ S'assurer du respect des lois, réglementation et obligations en matière de sécurité du SI
3) Maitriser les risques SI	<ul style="list-style-type: none"> ▪ Suivre la mise en œuvre des politiques, des règles de gestion des procédures et des chartes de sécurité SI ▪ Participer activement à la mise en œuvre du plan de secours informatique ▪ Garantir la mise en œuvre du plan de traitement des risques issus de la cartographie des risques ▪ Participer à la prise en compte de la sécurité dans les projets ▪ Contribuer au renforcement du dispositif de gestion des risques SI en proposant des actions de maitrise
4) Diffusion de la culture du risque SI	<ul style="list-style-type: none"> ▪ Contribuer à la mise en place d'actions de sensibilisation au sujet du risque opérationnel auprès de l'ensemble des collaborateurs ; ▪ Former les utilisateurs sur les bonnes pratiques de sécurité ▪ Participer à la préparation des comités de sécurité SI

PROFIL EXIGE PAR L'EMPLOI

Formation initiale (Diplôme)	Bac 4/5 en sécurité des SI, Informatique, audit et contrôle, réseau informatique...
Formation professionnelle	Cybersécurité, si possible : certificat CISA, Norme ISO 27001
Connaissances particulières	Risque, contrôle, audit, sécurité des SI, gouvernance informatique
Expérience indispensable	Minimum 2 ans dans les domaines (contrôle, audit, sécurité, réseau).
Compétences spécifiques	Suite office, normes et référentiel de sécurité, normes bancaires
Qualités requises	Rigueur et fiabilité, dynamique et organisé, Sens de l'écoute et de la confidentialité, Aptitudes relationnelles, Esprit critique, capacité d'analyse (méthodologique) et de synthèse, Autonomie et réactivité, Aisance rédactionnelle, Capacité de travailler sous pression, Goût pour le travail en équipe et la gestion de projet