

## RECRUTEMENT

INTITULÉ DU POSTE	DOSSIER À ENVOYER
<b>CHARGE DU SUIVI DU RISQUE SI</b>	<b>Lettre de motivation, CV et Diplôme</b>

Nous vous prions de bien vouloir adresser vos candidatures (Lettre de motivation + Curriculum Vitae + dernier diplôme), en mentionnant l'intitulé du poste, à l'adresse [recruitmenthr@nsiabanque.com](mailto:recruitmenthr@nsiabanque.com).

Date limite de dépôt des candidatures : **Mardi 21 février 2023**

**Par ailleurs, seules les candidatures retenues seront contactées.**

### RAISON D'ÊTRE DE LA FONCTION

- Cartographier les risques liés à la sécurité SI
- Suivre l'appétence aux risques SI et alerter sur les cas d'infraction
- Mettre à jour les politiques et procédures de sécurité SI
- Sensibiliser à la culture du risque informatique
- S'assurer de la conformité du dispositif de gestion des risques SI
- Renforcer le dispositif existant pour la maîtrise du risque SI

### POSITION DANS L'ORGANIGRAMME

CHEF DE DEPARTEMENT IDENTIFICATION ET SUIVI DES RISQUES

CHEF DE SERVICE SUIVI DES RISQUES DES RISQUES OPERATIONNELS & INFORMATIQUES

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

**PROFIL EXIGE PAR L'EMPLOI**

<b>Formation initiale (Diplôme)</b>	<b>Bac 4/5 en sécurité des SI, Informatique, audit et contrôle, réseau informatique</b>
<b>Formation professionnelle</b>	<b>Risque, contrôle, audit, sécurité des SI, gouvernance informatique</b>
<b>Connaissances particulières</b>	<b>Cybersécurité, si possible : certificat CISA, Norme ISO 27001</b>
<b>Expérience indispensable</b>	<b>Minimum 2 ans dans les domaines (contrôle, audit, sécurité, réseau)</b>
<b>Compétences spécifiques</b>	<b>Suite office, normes et référentiel de sécurité, normes bancaires</b>
<b>Qualités requises</b>	<b>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.</b>

**« Cette annonce ne fait lieu d'aucune discrimination de handicap, d'origine, de religion, d'appartenance politique ou de genre . »**