

Data & Risk Management Specialist

Mission

Le/la Data & Risk Management Specialist est responsable du cadre de gestion des risques cyber de l'organisation. Il/elle assure l'identification, l'évaluation, le traitement et le suivi des risques conformément aux exigences NIS2 et au Risk Management Framework de l'entreprise (ISO27005).

Principales responsabilités

- Définir et maintenir le Cybersecurity Risk Management Framework.
- Définir les méthodologies d'identification et d'évaluation des risques cyber.
- Maintenir la taxonomie des risques de cybersécurité.
- Organiser et coordonner les Cyber Risk Assessments.
- Consolider les risques provenant des différentes équipes de cybersécurité.
- Assurer le suivi des plans de mitigation.
- Maintenir le Cyber Risk Register.
- Définir et suivre les seuils d'appétence et de tolérance au risque.
- Identifier les risques résiduels et préparer les dossiers d'acceptation de risque.
- Challenger les plans de traitement proposés par les équipes techniques.
- Intégrer les risques liés aux fournisseurs et aux tiers.
- Contribuer à la gestion des risques liés aux projets et transformations IT.
- Produire les KPI/KRI et les dashboards destinés au CISO et au Risk Committee.
- Préparer les éléments de reporting pour le management et les instances de gouvernance.
- Assurer l'alignement avec NIS2, ISO 27001, NIST et les politiques internes.
- Contribuer aux audits et aux contrôles réglementaires.
- Contribution à la mise en œuvre et au maintien du NIS2 Cybersecurity Framework.
- Mapping des contrôles avec les exigences NIS2.
- Participation aux *NIS2 gap assessments*.
- Définition et maintenance des politiques, standards et procédures.
- Suivi des exceptions et risques acceptés.
- Définition des KPI/KRI.
- Reporting régulier au CISO.
- Coordination avec IT, Infrastructure, Cloud, Engineering, Risk, Legal, Compliance et Internal Audit.
- Gestion des plans de remédiation.
- Préparation et maintien des preuves d'audit.
- Contribution aux exercices de résilience et de gestion de crise.
- Veille réglementaire et adaptation du framework aux nouvelles exigences.

Profil recherché

- 5+ ans d'expérience en IT Risk, Cyber Risk ou Information Security Governance.
- Solide expérience en gestion des risques dans de grandes organisations.
- Très bonne connaissance des méthodologies de risk assessment.
- Connaissance de NIS2, ISO 27001, ISO 27005 est un plus.
- Expérience avec des outils GRC.

- Capacité à challenger des interlocuteurs techniques.
- Très bonnes capacités analytiques et rédactionnelles.
- Capacité à présenter des risques à des audiences non techniques.

Certifications appréciées

- CRISC
- CISM
- CISSP
- ISO 27001 Lead Implementer
- ISO 27005
- FAIR certification