Information Security Manager

Rejoignez une jeune société active au Luxembourg et dans les pays voisins.
Nous accompagnons nos clients pour mettre la sécurité au Cœur de leur transformation digitale.
Bien que notre domaine soit profondément numérique, nous mettons l'Humain au Cœur de notre métier.

Votre profil

Diplôme en informatique, en sécurité de l'information ou équivalent.
Expérience : **3 à 5 ans** dans le domaine de la sécurité de l'information ou dans un rôle similaire.
Certifications souhaitées : **ISO 27001, ISO 27005, CISM, CISSP** ou équivalent.
Capacité à travailler dans un environnement multiculturel et à respecter des délais serrés.

Vos compétences :

- **Compétences techniques**
  - Maîtrise des normes ISO 27001, ISO 27005 et des cadres réglementaires tels que NIS2 et DORA.
  - Expertise en matière d'analyse des risques, de tests de pénétration et de gestion des incidents.
  - Solide compréhension des outils de sécurité informatique (IAM, SIEM, outils GRC).
- **Gestion et communication**
  - Solides compétences en matière de gestion de projets et capacité à coordonner des équipes interfonctionnelles.
  - Capacité à communiquer les défis de la cybersécurité à des équipes non techniques.
  - Maîtrise de l'anglais et du français (l'allemand et le luxembourgeois sont un plus).
- **Réglementation et conformité**
  - Expérience avérée dans des projets garantissant la conformité avec les cadres juridiques et réglementaires en Europe.

Information Security Manager

ADRONH FUNDAMENTAL SECURITY

Vos responsabilités

Gestion de la sécurité de l'information

- Concevoir, mettre en œuvre et maintenir un système de gestion de la sécurité de l'information (SGSI) conforme aux normes **ISO 27001 et ISO 27005.**
- Assurer l'alignement des pratiques de sécurité sur les exigences de la directive **NIS2 et du règlement DORA.**
- Identifier et évaluer les risques liés aux systèmes de formation et proposer des mesures correctives appropriées.

Gouvernance, risques et conformité (GRC)

- Élaborer et maintenir un cadre efficace de **gouvernance, de risque et de conformité.**
- Créer et mettre à jour les politiques et procédures relatives à la sécurité de l'information.
- Coordonner les audits internes et externes afin de garantir la conformité réglementaire et contractuelle.

Gestion des incidents et continuité des activités

- Établir et superviser les processus de gestion des incidents de sécurité.
- Élaborer et maintenir des plans de continuité des activités **(BCP)** et des plans de reprise après sinistre **(DRP)** en fonction des risques identifiés.

Communication et sensibilisation

- Sensibiliser les équipes internes aux défis de la cybersécurité.
- Collaborer avec les parties prenantes internes et externes pour garantir une approche coordonnée de la sécurité.

Gestion des projets de sécurité

- Superviser les projets liés à la conformité avec **NIS2, DORA** et d'autres exigences réglementaires.
- Évaluer et intégrer des outils de sécurité afin d'améliorer la position globale de l'organisation en matière de sécurité.

+

Une société respectueuse de l'humain et engagée socialement
Nous privilégions les échanges, l'autonomie et le respect
Nous laissons une place à vos projets sociétaux.
Des conditions salariales compétitives en accord avec vos expériences, compétences... et vos intêrets.

Envoyez votre candidature à carriere@adronh.com