AFG HOLDING Atlantic Group	RECRUTEMENT	Rèf : F-HR-0	
	FICHE DE DESCRIPTION DE POSTE	Rédigé le :	Révisé le :

1. Informations Administratives

Titre de Poste	CHEF DE DEPARTEMENT DE LA SECURITE DES SYSTEMES D'INFORMATIONS (H/F)
Direction	DIRECTION SECURITE GLOBALE
Responsable Directe	DIRECTRICE DE LA SECURITE GLOBALE
Responsable Indirecte (Fonctionnel)	
Nombre de dépendants hiérarchiques	
Grade du Poste	CADRE
Organigramme	DIRECTRICE GENERALE ADJOINTE SUPPORT DIRECTRICE DE LA SECURITE GLOBALE CHEF DE DEPARTEMENT DE LA SECURITE DES SYSTEMES D'INFORMATIONS

2. Domaines de résultats

Raison d'être du poste		
Le Chef de département de la Sécurité des Systèmes d'Informations assure un rôle de conseil, d'assistance technique, d'information, de formation et d'alerte, en particulier auprès de l'ensemble des Collaborateurs de la Banque. Il préconise et est force de conseils sur toute décision d'intervention sur les systèmes d'information, en cas d'attaques potentielles ou avérées. Il effectue un travail de veille technologique et réglementaire sur son domaine et propose des évolutions qu'il juge nécessaires pour garantir la sécurité logique et physique du système d'information dans son ensemble.		
Livrables-clé du poste		
Domaines de Résultats *(Sur quels domaines le poste doit-il délivrer des résultats ?)*	**Activités principales** *(Quelles sont les activités à mener dans chaque domaine de résultats ?)*	**Résultats attendus** *(Quels résultats attendus dans le cadre d'une bonne performance ?)*
1 Gouvernance, Risques & Conformité (GRC) Cyber	• S'assurer que les pratiques de l'entreprise respectent les régulations légales et les normes internes et externes, telles que le RGPD, ISO 27001, ISO 27005, NIS2, DORA via la veille réglementaire ; • Contribuer à l'acculturation Cybersécurité des collaborateurs d'AFG BANK en s'impliquant dans la déclinaison du Programme Groupe annuel de sensibilisation ;	• Axes stratégiques définis ; • Innovations proposées ; • Outils de gestion et tableaux de bords pour le suivi des performances ; • Placer l'amélioration continue de la performance au cœur de ses actions stratégiques.

		• Maintenir des reportings réguliers (KPI & KRI) sur l'état de la sécurité de l'information, analyser les tendances des incidents de sécurité et fournir des recommandations stratégiques à la Direction Générale.	
2	Cyber Risk Management	• Identifier et évaluer les actifs informationnels critiques, classer les risques selon leur probabilité et leur impact potentiel sur l'organisation. • Utiliser des techniques et/ou méthodologies (FAIR, ISO 27005 EBIOS RM) afin d'évaluer les menaces existantes et émergentes, analyser les vulnérabilités dans les systèmes et les processus. • Développer des stratégies pour atténuer les risques identifiés, y compris l'adoption de technologies de sécurité appropriées et la révision des politiques et procédures. • Collaborer avec les équipes IT et les RSSI des autres filiales pour assurer l'implémentation des mesures de sécurité, suivre les progrès et ajuster les plans selon les besoins.	
3	IAM / PAM (Identity and Access Management / Privileged Access Management)	▪ Participer à la mise en œuvre du programme Groupe IAM/PAM sur son périmètre. ▪ Via la plateforme IAM, gérer l'accès des utilisateurs d'AFG BANK aux systèmes, applications et données. ▪ Surveillance et reportings : effectue une surveillance en temps réel pour détecter les utilisations anormales ou non autorisées des accès, générer des rapports détaillés pour les audits. ▪ Former régulièrement les utilisateurs aux politiques d'accès, aux risques associés aux négligences, et renforcer la conformité aux procédures de sécurité.	
4	Sécurité Opérationnelle	▪ Mettre en application et décliner opérationnellement la politique de sécurité de l'entreprise (PSSI) ; ▪ Conseiller le Top Management sur les solutions de sécurité adaptées à leurs besoins tout en rationalisant les différents outils de sécurité présents sur le marché et, ainsi, garantir une meilleure interopérabilité des systèmes ; ▪ Piloter sur son périmètre la sécurité des réseaux, des terminaux (postes de travail, appareils mobiles, etc.), et contribuer à la mise en œuvre de la sécurité périmétrique (firewall, proxy) ; ▪ Scanner régulièrement l'environnement dans le but de détecter des vulnérabilités ; ▪ Piloter et traiter les alertes et incidents de sécurité ;	

		▪ Construire des tableaux de bord et des indicateurs de mesure du niveau de sécurité opérationnelle de l'entreprise ;	
5	Cyber Résilience	• Élaborer et maintenir des plans de continuité d'activité (PCA) et de reprise après sinistre (DRP) pour minimiser l'impact des incidents de sécurité sur les opérations commerciales. • Analyse post-incident : Conduire des revues après chaque incident majeur pour identifier les lacunes dans les politiques et les procédures, et recommander des améliorations pour prévenir les récurrences. • Pentests et simulations : Organiser régulièrement des tests de pénétration et des simulations d'attaques pour évaluer la robustesse des infrastructures et des réponses aux incidents, et pour former le personnel à la réactivité face aux crises.	

3. Clés du succès

Niveau requis *(Insérer le niveau requis conformément aux directives existantes.)*

En leur absence, se référer à l'échelle suivante : 1 = Basique, 2= Standard, 3 = Avancé, 4, = Formateur

Compétences -clé	Brève description *(Donner une courte description de la compétence ou du comportement attendu)*	Niveau requis
Compétences fonctionnelles *(Se référer aux compétences fonctionnelles de votre Département. Si non existantes, les déterminer avec le Supérieur directe)*		
Connaissances spécifiques	• Expérience avérée en Sécurité Informatique. • Connaissance approfondie des normes de sécurité (ISO 27001, NIST, ISO 27005, ISO 22301, NIS2). • Capacités de leadership, communication efficace et travail en équipe. • La connaissance des SI Bancaire est un plus. • Bonne connaissance de la sécurité des systèmes d'information et de communication • Aisance relationnelle » Bonne capacité d'écoute et d'anticipation • Bonne communication » Aisance relationnelle • Bonne capacité d'écoute et d'anticipation • Excellentes compétences linguistiques en anglais et en français	4
Veille et conseil	• Capacité à apporter le conseil et l'assistance aux opérationnels • Garantir le respect des normes et politiques internes et externes.	4
Management	• Excellent stratège avec une forte orientation sur la planification et le contrôle ; • Sens de l'observation, de l'analyse et de l'anticipation ; • Curiosité et ouverture d'esprit ; • Adaptation et remise en question ; • Charisme avéré qui lui confère une aisance à l'écrit et à l'oral ; • Faire preuve d'un leadership naturel et de solides compétences managériales ;	4

	• Maitrise des procédés de mise en œuvre d'une démarche préventive d'analyse des risques ; • Participer à la validation des projets d'investissement.	

4. Profil de candidat

Education / Formation	Niveau d'études : Bac 5, Master II Domaine : Sécurité Informatique ou équivalent
Expérience	Un minimum de sept (7) années d'expérience en sécurité d'information Certifications pertinentes en : • CISSP • ISO 27001 Lead Implementer / Lead Auditor • ISO 27005 Ebios Risk Manager • ISO 22301 Lead Implementer / Lead Auditor • CompTIA • Certified Ethical Hacker (CEH)
Langues	Français – courant, Anglais - Courant
Compétences informatiques	Pack office ; ERPs dédiés aux activités des assurances
Compétences transversales	• Discrétion et droit de réserve ; • Bonne expression et présentation ; • Très bon sens relationnel ; • Sens la relation client ; • Calme ; • Rigueur et Contrôle ; • Autonome ; • Capacité d'organisation ; • Sens de l'analyse et de la synthèse ; • Capacité d'anticipation ; • Capacité d'adaptation ; • Force de proposition ; • Sens de l'écoute ; • Savoir travailler en équipe ; • Capable de travailler sous pression.
EVOLUTION PROFESSIONNELLE (P+1)	• XXXXXXXXXXXXXXXXXXXXX • XXXXXXXXXXXXXXXXXXXXX