

AQ
Consultant Cybersécurité GRC / PMO

FORMATION ET CERTIFICATIONS

2021 Ingénieur, spécialité cybersécurité, ESIEE

Certifié ISO 27001 Lead Implementer

COMPETENCES PRINCIPALES

- Gouvernance, gestion des risques, compliance
- Gestion de projet, suivi de planning et mise en place de KPI
- Animation de réunions
- Rédaction de livrables
- Analyse de risques
- Audit de conformité aux politiques de sécurité
- PRA / PCA
- Intégration de la sécurité dans les projets
- Contrôle permanent N1 et N2

Compétences techniques :

- Outils, solution et logiciel : GRC Archer
- EBIOS 2010, EBIOS RM, ISO 27005, PASSI
- Règlementations DORA, NIST, TISAX
- Systèmes : Unix/Linux, Windows

Anglais : courant

EXPERIENCE PROFESSIONNELLE

AXA, 07/2025 à 02/2026
Consultant cybersécurité

Contexte : au sein de la Direction Sécurité et Protection des Données, réalisation de la mission d'assurance sécurité en deuxième ligne de défense.

Missions

- Contribution à la définition de la mission d'assurance sécurité sur trois piliers de la sécurité
 - Sécurité de l'information
 - Résilience opérationnelle et ITSCM
 - Sécurité physique des biens et des personnes
- Définition d'un planning de contrôles annuels
 - Phase d'analyse et phase d'échanges avec les différentes fonctions métier
 - Rédaction des fiches de contrôles
 - Présentation des résultats de contrôles en CoPil
- Réalisation des revues d'assurance annuelles
 - Identification des écarts potentiels
 - Formulation des recommandations
 - Suivi des remédiations

Résultats

- Revue d'assurance effectuée sur les 3 piliers IS, OR et PSS
- Planning de contrôles réalisé et approuvé par la direction Groupe en CoPil

Environnement

- Direction du Groupe
- Suite Office et SharePoint
- GRC Archer
- Travail en équipe, répartition des activités

ALLIANZ, 10/2022 à 07/2025

Assistant RSSI et IT Risk Manager

Contexte : Au sein du bureau du Directeur des Systèmes d'Information, réalisation d'analyses de risques sur l'ensemble des applications internes et cloud au niveau local, régional et central. Mise en place et accompagnement de l'ensemble des collaborateurs vers un nouvel outil de gestion et analyse de risques.

Missions :

- Réalisation d'analyses de risques et risk assessments cloud
 - Organisation de réunions d'avancement avec les équipes métiers
 - Demandes et revues des évidences exigées aux différents interlocuteurs métiers et techniques
 - Réalisation de rapports d'assessments
- Contribution au pilotage des chantiers sécurité sur l'ensemble du périmètre
 - Évaluation des risques
 - Bilan de conformité des applications du périmètre
 - Mise en place de contrôles et indicateurs clefs
 - Mesures de sécurité, traitement du risque
- Contribution au partage des meilleurs pratiques en matière de gestion des risques informatiques
 - Formation et sensibilisation
 - Assistance aux différentes fonctions métiers
- Transition vers un nouvel outil de management, de gestion et d'analyses de risques (Prévalent)
 - Formation des équipes métiers

- Mise en place de l'outil : écriture des nouveaux questionnaires de sécurité, création des risques associés et onboarding des équipes
- Création d'un questionnaire de sécurité pour évaluer les risques liés à l'utilisation de l'IA
- Résultats
 - Plus d'une centaine d'analyses de risques réalisées
- Respect des KPI prévus par le groupe et reporting associé
 - Transition vers Prévalent réussie : ensemble des collaborateurs formés, gestion des risques 100% intégrée au nouvel outil, présentation de l'outil en interne
- Environnement
 - Contexte international, en anglais
 - Prévalent : outil de management et d'analyses de risques
 - Suite Office et SharePoint
 - GRC Archer
 - Travail en équipe, répartition des activités

BPCE, 10/2021 à 09/2022 ***Ingénieur cybersécurité***

Contexte : Au sein de la Direction Sécurité Groupe de l'entreprise, réalisation de contrôles permanents de niveau 2 sur les périmètres mail et antivirus et réalisation d'un plan d'audit pour l'évaluation des prestataires du groupe.

Missions

- Opération des contrôles permanents de niveau 2
 - Périmètres mail et antivirus
 - GRC Archer
 - Revue et analyses des preuves
- Construction d'un plan de contrôle de niveau 2
 - Organisation des ateliers avec les équipes des contrôles de niveau 1 associés
 - En lien avec les règles de la PSSI Groupe
 - Processus, points de contrôle, fréquence et planification
- Réalisation d'un plan d'audit pour l'évaluation des fournisseurs / prestataires externes du groupe
 - Exigences, thématique, criticité, preuves, interlocuteurs, vérifications et évaluation
 - Règles EBA (European Banking Authority)
 - Support de présentation à destination du Top Management
- Réalisation de formation à destination des RSSI et DSI du Groupe sur l'outil de GRC Archer
 - Ateliers hebdomadaires
- Résultats
 - Contrôles de niveau 2 opérés avec succès
 - Plan d'audit validé par le Top Management et prêt pour utilisation
 - Construction du plan de contrôles finalisé et prêt pour opération en vue d'une migration vers l'étranger

- Environnement
 - Mission dans une équipe de 12 personnes
 - GRC Archer
 - Teams

LA POSTE **06/2021 à 09/2021** **Consultant cybersécurité**

Contexte : Réalisation d'une méthodologie d'intégration de la sécurité dans des projets agiles (méthode SAFe) orientés Cloud.

Missions

- Réalisation d'une méthodologie ISP
 - Analyse des besoins et immersion au sein des équipes pour proposer une méthodologie adaptée au contexte du client
 - Présentation au management et RSSI
- Cartographie du parc applicatif Cloud
 - Réalisation d'un questionnaire sécurité d'évaluation de la criticité des applications
 - Organisation et réalisation des ateliers avec chaque responsable de projet
- Traitement des tickets (JIRA)
 - Organisation des réunions avec les différents acteurs
 - Proposer un accompagnement sécurité
 - Communication et sensibilisation auprès des différents acteurs
- Résultats
 - Méthodologie approuvée par le RSSI et appliquée
 - Vingtaine d'ateliers réalisés dans le cadre de la cartographie du parc applicatif Cloud
- Environnement
 - Mission en binôme
 - Suite Office (Word, Excel, PowerPoint)
 - JIRA

HEADMIND **01/2019 à 06/2019** **Consultant cybersécurité**

Contexte : dans le cadre de la préparation à un audit de sécurité PASSI, revue de l'ensemble du corpus documentaire, mise en conformité et mise à jour puis refonte de l'analyse de risques.

Missions

- Préparation audit de sécurité
 - Suivi du planning d'audit
 - Organisation de réunions d'avancement
 - Demandes et revue des preuves d'audit aux différents interlocuteurs métiers et techniques pour la mise en conformité du corpus documentaire ainsi que la réalisation de contrôles sur l'existant
- Analyse de risques avec les méthodes EBIOS 2010 et EBIOS RM 2018

- Cadrage et socle de sécurité, contexte
- Évènements redoutés
- Scénarios de menace
- Risques
- Mesures de sécurité et traitement du risque
- Revue et mise en conformité du corpus documentaire
 - Politique de sécurité (PSSI)
 - Convention d'audit
 - Plan d'audit
 - Processus d'audit
 - Matrice de données
 - Méthodologies
- Résultats
 - Audit passé avec succès
 - Poursuite de la mission pour la préparation du plan de remédiation des écarts
- Environnement
 - Projet en autonomie
 - Suite Office (Word, Excel)
 - EBIOS 2010 et EBIOS RM 2018
 - Référentiel d'exigences PASSI de l'ANSSI