

FORMATIONS & CERTIFICATIONS

Sept. 2019 – 2021 : Master
Cyber Défense et sécurité de
l'information INSA Haut de
France
Sept. 2018 – 2019 : Licence
professionnelle en Réseaux et
Télécommunications Univ.
Polytechnique Haut de France
Sept. 2014 – 2017 : BTS
Télécommunications INSFP
Béjaïa
Certifications · ISO 27005 –
PECB (en cours)

LANGUES

Anglais : courant

RM

CYBERSECURITE / RISK / COMPLIANCE / GRC

COMPÉTENCES

Domaine / Métier : Cybersecurity (GRC), Réseaux et Télécommunications.

Normes : ISO 27001 • RGPD • NIS 2 ISO 27005 • DORA

Risque Et Conformité : Audit, Ebios, Mehari.

Outils : DiagCyber / Finare / MyDataCompliance / Tanium / Microsoft 365 / G-Suite / AutoCAD.

Réseaux : PAM / WAF / DLP / EDR.

Gestion des accès : IAM Thales.

Méthodes : Agile, Lean Management.

EXPÉRIENCES

Société :

BPI France

Février 2025 à
Septembre 2025

Poste :

Consultant Gouvernance Risk and Compliance

Environnement technique

Windows, Microsoft 365, Audit DiagCyber.Ebios RM

Missions réalisées :

Piloter et gérer différents projets de sécurités des systèmes d'informations, à travers un audit de maturité, des analyses de Risques via Ebios RM et un accompagnement organisationnel et technique complet du SI, sur DiagCyber de BPI France.

Tâches effectuées :

- Utilisation de DiagCyber de BPI France pour un Audit de conformité et de maturité du SI.
- Évaluer le niveau de sécurité des infrastructures SI via 12 chapitres de gouvernance IT en suivant les différentes directives ANSSI.
- Recommandations à travers un plan d'actions priorisé, pour la sécurisation du SI, et une sensibilisation du comité de Direction et des collaborateurs face à la menace Cyber.
- Analyse de risques via méthodologie Ebios RM à travers les 05 Ateliers, :
 - AT1 : Définition du périmètre avec MOA/MOE, identification des valeurs métiers, besoins DICT, événements redoutés (AT1+AT3) et biens supports avec la MOE (liste réf trouvable sur l'ANSSI). Vérification du socle de sécurité et des exigences PSSI.
 - AT2 : Analyse des différentes sources de risque en évaluant leurs motivations, moyens et capacités d'action. Construction d'un panorama des menaces crédibles en tenant compte du contexte métier, technique et organisationnel.
 - AT3 : Travail mené avec la MOE pour identifier les parties prenantes internes/externes et évaluer leur niveau de dépendance ou de pénétration potentielle dans le SI. Définition des zones de confiance et zones de menace selon la maturité du SI. Construction des scénarios stratégiques (chemins d'attaque majeurs) et évaluation de leur gravité.
 - AT4 : Décomposition des scénarios opérationnels selon les quatre étapes "Connaître – Entrer – Trouver – Exploiter".

Analyse des vecteurs et modes d'attaque avec MITRE ATT&CK pour modéliser les enchaînements réalistes. Évaluation de la vraisemblance via la facilité et la probabilité d'exploitation.
 -AT5 : Calcul du niveau de risque (gravité × vraisemblance) pour positionner chaque scénario. Élaboration du PACS pour recommander les mesures techniques, organisationnelles ou procédurales les plus pertinentes.
 Appui à la décision pour l'acceptation, la réduction, le refus ou le transfert du risque selon la stratégie de sécurité retenue.
 (Processus d'homologation après AR non pris en charge sur la liste des risques résiduels).

Société :

EDF

**Janvier 2024 à
Décembre 2024**

Poste :

Risk Manager

Environnement technique

Windows, Microsoft 365, Outils de gestion des DAT EDF.

Missions réalisées :

Relecture et évaluations des Dossiers d'architectures Techniques (DAT) pour les projets et applications d'EDF, en veillant à leur alignement avec les standards de l'entreprise (PSSI) et les exigences réglementaires.

Tâches effectuées :

- Vérification des dossier architectures techniques (DAT) selon les critères DICT en répondant aux besoins spécifiques des projets et applications.
- Assurer la cohérence et l'interopérabilité des solutions proposées avec l'écosystème informatique global d'EDF selon la PSSI.
- Fournir un soutien technique pour la résolution des problèmes suivant les écarts (Protocoles / Sécurisation des connexions etc...) à travers la fiche OSCAR.
- Attribuer des dérogations aux écarts mineurs et conseiller les équipes sur les recommandations prioritaire afin d'éviter la clôture projet.

Société :**EDF****Novembre 2023 à
Décembre 2023****Poste :****Asset Management Analyst****Environnement technique :**

Windows, Microsoft 365, Tanium AM

Missions réalisées :

Responsable de l'évaluation de la santé applicative dans un contexte de gestion et sécurisation des EndPoints avec Tanium, pour le monitoring, la gestion des vulnérabilités et le déploiement de correctifs sur un parc informatique.

Tâches effectuées :

- Conformité applicative et amélioration de la visibilité en temps réel sur les Endpoints, à travers un renforcement de la posture de cybersécurité via l'Asset Management.
- Inventaire automatisé des actifs IT, pour la détection et le suivi des endpoints sur Tanium Asset & Discover.
- Optimisation de la conformité avec la surveillance des logiciels, gestion des licences et identification des actifs obsolètes.
- Automatisation du reporting à travers des tableaux de bord et alertes pour améliorer la visibilité et la prise de décision.

Société :**AIRBUS (Toulouse)****Avril 2023 à
Octobre 2023****Poste :****PMO Cyber****Environnement technique :**

Windows, G-Suite, Outils de finance Airbus (Finare).

Missions réalisées :

En tant que PMO sur un projet de sécurité/Budget, au sein du Sous-département Aircraft Security, en charge de la sécurité des programmes A320/A330/A350/A380. J'étais impliqué dans la gestion et le suivi des activités de sécurité, en veillant à la bonne gestion du budget et à l'alignement des projets avec les objectifs stratégiques.

Tâches effectuées :

- Assurer l'exhaustivité des activités de bout en bout, et des risques associés à travers une posture PMO, en incluant l'impact sur la roadmap en alignement avec les différentes entités Airbusienne.
- Saisir le budget prévu ou accordé dans l'outil BCP/Finare et préparer les jalons de prévision trimestriels (FC1, FC2, FC3)
- Comparer avec la planification de la feuille de route et signaler les divergences et les confirmations suivant les différentes technologies associées.
- Construction d'une base de données (fichier tableur/croisé dynamique) combinant plusieurs types d'informations pour les KPI.

Société :

AIRBUS (Toulouse)

**Février 2022 à
Avril 2023**

Poste :

Risk Officer

Environnement technique :

Windows, Microsoft 365, G-Suite, Ebios RM, Audit, Outil Interne IAM.

Missions réalisées :

Contexte : Pour le pôle de protection des actifs critiques et des données (DSC), assister les propriétaires et gestionnaires des 7300 applications identifiées chez Airbus, dans un processus de classification selon les quatre axes de sensibilité interne, en utilisant l'outil MyDataCompliance.

Tâches effectuées :

- Évaluer l'importance et la sensibilité de chaque application dans le contexte opérationnel d'Airbus commercial à travers les différents sites mondiaux.
- Déployer et gérer l'outil MyDataCompliance pour la classification des applications selon les recommandations de sécurité Airbus.
- Former les propriétaires et les gestionnaires d'applications à l'utilisation de MyDataCompliance.
- Assister les équipes dans la classification des applications selon les quatre axes de sensibilité d'Airbus. Ex: Export control, Airbus corporate, National security et Personal data. Dans le but de faciliter la gestion de l'écosystème SI Airbus.

- Participer à l'amélioration continue des pratiques de sécurité en lien avec la classification des applications, via Reporting, KPI, Livrable mensuel.

Société :

LABROUP Luxembourg SA

Poste :

Consultant GRC Junior

**Mars 2021 à
Février 2022**

Environnement technique :

Windows, Microsoft 365, G-Suite, Ebios RM, Audit, Outil Interne IAM.

Missions réalisées :

Contribuer au suivi opérationnel de la gouvernance de la sécurité du SI, dans une entreprise luxembourgeoise spécialisée dans la dématérialisation de documents. (Stage fin d'études+CDD).

Tâches effectuées :

- Rédaction et mise en oeuvre des documents de sécurité du SI en lien avec la norme ISO 27001 et la norme PSDC du Luxembourg. Ex: Politiques/Procédures/Chartes de Sécurité..
- Conduite d'analyses de risques EBIOS RM à travers les cinq ateliers : Périmètre, identification des menaces, construction de scénarios stratégiques et opérationnels, évaluation des impacts, puis définition d'un plan de traitement (PACS) adapté aux besoins de sécurité et à la protection des actifs essentiels de l'organisation. Afin d'assurer la sécurité des missions essentielles, la protection des actifs vitaux, et la maîtrise des risques pesant sur la disponibilité, l'intégrité, la confidentialité et la traçabilité des systèmes.
- Audits de conformité interne. (Via Iso27001 et PSDC Luxembourg)
- Participer à la conception et à la mise en oeuvre de programmes de sensibilisation à la sécurité pour les employés.
- Effectuer des test PRA/PCA en rapport direct avec une filiale irlandaise.
- Support Opérationnel IAM en participant à la campagne de recertification.