Mario ZANNOU

Consultant en Cybersécurité

CISM, CRISC, ISO 27001 | Cybersécurité - Gouvernance - Conformité et Risques SSI

Permis de conduire
mario@zannou.fr
33699831183
92290 Chatenay-Malabry
France

Consultant senior en cybersécurité, certifié **CISM** ***(Certified Information Security Manager)***, **CRISC** ***(Certified in Risk and Information Systems Control)***, **ISO 27001 Lead Implementer** et **PECB Trainer**, j'interviens sur des missions de gouvernance, gestion des risques, conformité et projets SSI. J'accompagne également les organisations en tant que RSSI, renfort sur projets SSI, audits ISO 27001, intégration de la sécurité dans les projets (ISP) et analyse de risques, pour renforcer leur posture cybersécurité et conformité réglementaire.

EXPÉRIENCES

CYBERSECURITY OFFICER (CSO)

HEINEKEN - Depuis février 2023

- *En tant que responsable cybersécurité de l'OpCo France, je suis chargé de piloter la stratégie locale de cybersécurité en alignement avec les cadres globaux de HEINEKEN, tels que le NIST et l'ISO 2700X. Mon rôle englobe la mise en oeuvre de mesures pour maîtriser les risques de sécurité, notamment à travers l'analyse de sécurité des systèmes et processus, la gestion des risques, et l'élaboration de plans de continuité et de reprise d'activité (DRP). J'assure également la sensibilisation des collaborateurs pour renforcer la posture de sécurité de l'OpCo France tout en garantissant la conformité avec les exigences du groupe.*

- **Pilotage des programmes de sécurité**: Gestion des budgets et ressources alloués à la cybersécurité. Suivi des indicateurs de performance (KPI, KRI) et animation des comités de gouvernance de la sécurité pour garantir une prise de décision stratégique et proactive avec le groupe.
- **Opérations de sécurité** : Mise en œuvre et mise à jour des stratégies de sécurité (SIEM, SOC), gestion des audits (ISO 27001, NIST), conformité réglementaire (RGPD), et pilotage des incidents (EDR, XDR, SOAR).
- **Sensibilisation**: Déploiement des campagnes de formation à la cybersécurité (phishing, Zero Trust), gestion des accès et renforcement des bonnes pratiques en entreprise.
- **Stratégie de sécurité**: Analyse des risques (PRA/PCA, Pentest, Risk Assessment), recommandations sur la gestion des vulnérabilités (CVSS, patch management), et amélioration continue des contrôles de sécurité.
- **Contrôle des processus**: Supervision des incidents via ServiceNow, suivi des correctifs (WSUS, SCCM), gestion des sauvegardes (Veeam, Acronis), et conformité des équipements de sécurité (firewall, VPN, DLP).
- **Gestion des changements (CAB)**: Validation des évolutions technologiques (Cloud Security, DevSecOps, IAM), alignement des changements avec les normes de sécurité (ISO 27005, ITIL, SOC 2).

CONSULTANT SENIOR CYBERSÉCURITÉ - RÉFÉRENT SI & CONFORMITÉ

SWISSLIFE - Février 2022 à février 2023

- *En tant que consultant cybersécurité et référent SI & conformité, j'ai assuré des missions stratégiques et opérationnelles pour renforcer la posture sécurité du groupe SwissLife, en alignant les pratiques locales sur les standards internationaux et les exigences de conformité.*

- **Politiques et conformité** : Déploiement et suivi des politiques de sécurité (ISO 2700X), gestion des règles et normes via les dossiers de sécurité, et supervision de la conformité avec le CISO en utilisant des frameworks comme NIST CSF et COBIT.
- **Suivi opérationnel de la sécurité**: Pilotage des analyses de risques et intégration de la sécurité dans les projets (ISP), suivi des contrôles de premier niveau (SIEM, SOAR), gestion des revues périodiques des habilitations (IAM, PAM) et coordination des tests d'intrusion (Pentest, Red Team, SAST/DAST), avec suivi des plans de remédiation.
- **Continuité et reprise d'activité (PCI/PCA)** : Organisation et pilotage des tests annuels (Disaster Recovery Testing, Tabletop Exercises), validation des plans de continuité et évaluation de la résilience des systèmes critiques via des simulations réelles.
- **Sensibilisation et formation**: Gestion des campagnes de sensibilisation à la cybersécurité (phishing simulation, social engineering awareness), développement de programmes de formation interactifs basés sur le Security Awareness Framework.
- **Référent sécurité**: Interface entre la gouvernance et les équipes opérationnelles, coordination des initiatives stratégiques avec des méthodologies comme Zero Trust Security et suivi des indicateurs de sécurité au COMSEC (Comité de Sécurité).

RÉFÉRENT CYBERSÉCURITÉ & MANAGER IAM

CREDIT AGRICOLE ASSURANCES - Juillet 2020 à février 2022

- *En tant que référent cybersécurité et manager IAM, j'ai joué un rôle stratégique au sein de l'équipe CISO de Crédit Agricole Assurances, en pilotant des projets complexes de sécurité des systèmes d'information (SI) et en optimisant la gestion des identités et des accès (IAM).*

- **Sécurité des projets** : Qualification et évaluation des projets nécessitant un accompagnement en cybersécurité avec une approche de risk-based security. Réalisation des analyses de risques (MESARI), identification des risques résiduels, et mise en œuvre de plans de sécurité adaptés. Supervision des tests d'intrusion (boîte noire et grise, Pentest) et suivi des actions de remédiation (Patch Management, CVSS scoring). Pilotage de la gouvernance sécurité en intégrant des mesures stratégiques dans les projets critiques.
- **Gestion des identités et des accès (IAM)** : Élaboration et déploiement de plans projet IAM, identification des applications critiques et intégration des revues des habilitations métiers et hiérarchiques (JML – Joiner, Mover, Leaver). Implémentation des recommandations issues des audits de l'Inspection Générale Groupe (IGL) et suivi des résultats pour garantir la conformité. *Environnement technique* : **BrainWave**
- .**Amélioration continue et gouvernance IAM**: Renforcement des processus de gestion des rôles, profils et droits d'accès pour une meilleure maîtrise des accès. Optimisation des délais de désactivation des comptes en cas de départ/mobilité et gestion des dérogations via PAM (Privileged Access Management). Supervision des politiques de mots de passe et couverture des applications critiques via des outils de contrôle IAM.
- **Revue périodique des habilitations** : Coordination des revues régulières des accès (RBAC, ABAC) pour assurer la conformité et minimiser les risques liés aux accès non autorisés. Suivi des écarts et actions correctives pour garantir la sécurité des systèmes d'information
- **Gouvernance des projets Cyber** : Pilotage des projets de sécurité en lien avec les parties prenantes, intégration des exigences de sécurité dès la phase de conception (Security by Design), gestion des budgets et coordination avec les directions IT et métiers.

CONSULTANT EN CYBERSÉCURITÉ / RÉFÉRENT SSI & CONFORMITÉ

EGIS - Janvier 2019 à juillet 2020 - Freelance - Guyancourt - France

- *En tant que consultant senior en cybersécurité, j'ai occupé un rôle stratégique et opérationnel au sein de la DSI du groupe EGIS, avec pour mission de renforcer la sécurité des systèmes d'information, d'optimiser la gestion des risques et de garantir la conformité aux exigences réglementaires et normatives.*

- **Stratégie SSI et conformité** : Conception et mise en œuvre d'une stratégie de sécurité globale, intégrant les standards ISO 2700X, RGPD, RGS, ANSSI. Définition et pilotage du Plan d'Assurance Sécurité (PAS) pour évaluer et garantir la sécurité des prestataires externes. Supervision des solutions de sécurité (antivirus, IDS, firewall, antispam) et anticipation des évolutions techniques face aux nouvelles menaces.
- **Gestion des risques et des vulnérabilités** : Réalisation d'analyses de risques (EBIOS RM, MEHARI) pour identifier et traiter les vulnérabilités des systèmes internes et des filiales du groupe. Pilotage du Patch Management pour assurer une mise à jour proactive des correctifs de sécurité. Mise en place d'une veille SSI pour surveiller en temps réel les menaces émergentes et coordination des tests d'intrusion et scans de vulnérabilités, avec suivi rigoureux des plans de remédiation.
- **Gestion des identités et habilitations (IAM)** : Déploiement d'une solution IAM structurée pour la gestion des identités et des accès. Supervision des revues périodiques des habilitations, gestion rigoureuse des accès et dérogations, optimisation des processus d'arrivées, départs et mutations des collaborateurs afin de garantir une maîtrise stricte des accès.
  Résilience et continuité d'activité : Organisation et tests réguliers des stratégies de continuité d'activité (PCA, PRA, PRI) pour garantir la disponibilité des systèmes critiques en cas d'incident majeur. Mise à jour des processus documentaires pour assurer la pertinence et l'efficacité des plans de secours.
- **Gestion des incidents et leadership en cybersécurité** : Pilotage du processus de gestion des incidents, depuis la détection jusqu'à la remédiation et l'analyse post-incident pour renforcer les mesures préventives. Supervision des projets classés confidentiel défense, garantissant un haut niveau de conformité et de sécurité des données sensibles. Accompagnement des équipes projets pour intégrer la sécurité by design dès les phases initiales des développements.

CHARGÉ DE MISSION ET CHEF DE PROJETS SÉCURITÉ SI

VIIA - Groupe SNCF - Octobre 2015 à janvier 2019 - Paris - France

- *En tant que chargé de mission et chef de projets sécurité SI au sein de la filiale VIIA du groupe SNCF, j'ai conduit des initiatives stratégiques en cybersécurité, piloté des projets complexes, et renforcé la gouvernance et la protection des systèmes d'information. Mon rôle incluait également l'accompagnement des équipes pour intégrer les exigences de sécurité dans les processus métiers et garantir la conformité réglementaire.*

- **Gouvernance et politiques de sécurité** : Élaboration et déploiement des politiques SSI (PSSI, Charte informatique, PAS) pour structurer et harmoniser la gouvernance SSI. Mise en œuvre d'un projet IAM global, incluant la ré-certification des comptes critiques, la gestion des entrées/sorties et la supervision des droits d'accès. Harmonisation des processus de sécurité entre les entités françaises et internationales pour garantir une approche cohérente.
- **Gestion des risques et conformité** : Cartographie et analyse des risques SSI avec EBIOS, ISO 27005, permettant une gestion proactive des vulnérabilités. Accompagnement à la conformité RGPD et certification ISO 27001 via la mise en place d'un SMSI (Système de Management de la Sécurité de l'Information). Continuité d'activité et résilience : Élaboration, tests et suivi des plans PCA, PRI, PRA pour garantir la disponibilité des systèmes critiques en cas d'incident. Mise à jour et optimisation des processus documentaires associés aux stratégies de secours.
- **Gestion des projets SSI** : Qualification des projets, analyse des besoins métiers et SI, et intégration des exigences de sécurité dès la conception (Security by Design). Rédaction des cahiers des charges, gestion des prestataires et suivi des livrables pour assurer le respect des délais et budgets.
- **Formation et accompagnement** : Assistance aux équipes métiers et techniques pour l'adoption des politiques de sécurité et outils SSI. Animation de formations sur la cybersécurité et les outils ERP métiers, ainsi que des campagnes de sensibilisation pour renforcer la posture sécurité des collaborateurs et prestataires.

Chef de Projets Etude et Développement

PROSODIE CAPGEMINI - Février 2015 à août 2015

- Pilotage et gestion projets web - Développement de plateforme web multilingue et multi-thèmes (international)
- Etude et analyse des fonctionnalités en relation avec les utilisateurs, rédaction expression de besoins et cahier de charges.
- Définition, coordination et réalisation des activités d'accompagnement du Changement lors des phases de déploiement.
- Réalisation de la recette utilisateurs et rédaction du cahier de recette.
- Intégration d'outils BI (QlikSense/QlikView) et CRM (Dimelo, Eptica...) et développement d'une application web
- Support technique et fonctionnel sur les outils métiers.

COMPÉTENCES CLÉS

Management projets Cybersécurité

- **Pilotage des SMSI**: Expertise dans la conception, l'implémentation et la gestion de Systèmes de Management de la Sécurité de l'Information (ISO 2700X), avec un alignement stratégique sur les cadres internationaux (ISO, NIST) et réglementations (DORA, RGPD, ANSSI).
- **Gestion des vulnérabilités et des correctifs** : Mise en place de processus avancés pour identifier, analyser et corriger les vulnérabilités, garantissant une posture de sécurité optimale.
- **Management des risques** : Réalisation d'analyses d'impact métier (BIA), identification des menaces, évaluation approfondie des risques, et définition de stratégies de traitement adaptées.
- **Sécurité applicative** : Expertise en intégration des contrôles de sécurité dans le développement applicatif (OWASP) pour protéger les systèmes critiques.
- **Gestion des incidents de sécurité** : Conduite de bout en bout des processus de détection, réponse, atténuation, remédiation, et analyse post-incident pour garantir une amélioration continue.
- **Plans de continuité et de reprise d'activité(BCP/DRP)** : Élaboration et gestion de PCA et PRA robustes pour minimiser l'impact des interruptions et garantir la résilience des opérations.
- **Rédaction de politiques de sécurité** : Développement de PSSI, PAS, PRI et DRP alignés sur les meilleures pratiques pour une gouvernance efficace de la sécurité.
- **Gestion des identités et des accès (IAM)**: Mise en œuvre de solutions avancées pour sécuriser et gérer les droits d'accès dans des environnements complexes.
- **Veille stratégique en cybersécurité** : Maintien d'une expertise à jour grâce à une veille constante et l'application des meilleures pratiques pour anticiper les évolutions des menaces.

Gestion de projets

- **Pilotage stratégique de projets Cybersécurité et SSI**: Gestion complète de projets complexes, depuis la définition des besoins jusqu'à la livraison, en assurant l'alignement avec les objectifs métiers et les exigences de sécurité.
- **Maîtrise des méthodologies Agile et Scrum**: Expertise dans la mise en œuvre de frameworks agiles pour favoriser la collaboration, accélérer les cycles de développement et garantir la qualité des livrables.
- **Gestion des relations client/fournisseur**: Négociation et gestion des contrats, coordination avec les fournisseurs et externalisation de services via des Centres de Services pour maximiser l'efficacité et la satisfaction des clients.

Outils & Environnement technique

- **Systèmes** : Windows Server, Linux, Active Directory
- **Sécurité**: SentinelOne, QRadar, ElasticSearch, Qualys, Nessus, Splunk, Palo Alto
- **Systèmes et réseaux**: Windows, Linux, Active Directory, firewalls, proxy, VPN.
- **Outils de cybersécurité** : SIEM, SOC, EDR, ServiceNow ...
- **Cloud** : Azure, MS 365 ...

FORMATIONS

DIPLÔMES SUPÉRIEURS

INGÉNIEUR RÉSEAUX ET TÉLÉCOMMUNICATIONS
ECOLE D'INGÉNIEUR SUP GALILÉE - UNIVERSITÉ
PARIS 13 - *Paris FRANCE - Juin 2015*

EXÉCUTIVE MASTER OF BUSINESS ADMINISTRATION (EMBA)
IAE PARIS - SORBONNE BUSINESS SCHOOL (MBA) – *2023*
IFG EXECUTIVE EDUCATION (EXECUTIVE MBA) - *2023*

MASTER OF SCIENCE EN DATAMINING (PROGRAMME ERASMUS)
UNIVERSITY OF DEBRECEN
Debrecen HONGRIE – Février 2015

LICENCE PROFESSIONNELLE RÉSEAUX INFORMATIQUES
UNIVERSITÉ AFRICAINE DE TECHNOLOGIES ET DE MANAGEMENT *BÉNIN – Juin 2011*

DUT TÉLÉCOMMUNICATIONS
ECOLE SUPÉRIEURE DES TÉLÉCOMMUNICATIONS DE DAKAR
Dakar SÉNÉGAL – Juin 2010

CERTIFICATIONS EN CYBERSÉCURITÉ

- **ISO 27001** Lead Implementer (#ISLI1030127)
- **CISM** (Certified Information Security Manager)
- **CRISC** (Certified in Risk and Information Systems Control)
- **PECB** Trainer

FORMATIONS PROFESSIONNELLES ET SPÉCIALISÉES

- **SÉCURITÉ ÉCONOMIQUE ET PROTECTION DU PATRIMOINE**
  INSTITUT DES HAUTES ÉTUDES DE DÉFENSE NATIONALE (IHEDN) – *2019 (Promotion N° 322)*
  Lien : IHEDN Formation
- **GESTION DE PROJETS**
  Formation spécialisée dans le cadre de missions en cybersécurité et IT.
- **CISSP, ISO 27005 Risk Manager, ITIL, RGPD**