

MB
CYBER RISK & SECURITY SENIOR CONSULTANT / RISK MANAGER

FORMATION ET CERTIFICATIONS

2015 : Université Polytechnique, Master Cyber-Défense et Sécurité de l'Information

Certifications :

- ISO 27001 Lead Implementer
- Attestation de suivi GDPR
- CyberArk Certified Trustee
- SecNumAcademie
- Fortinet NSE 1 & 2
- ISO 27005 Risk Manager

COMPETENCES PRINCIPALES

Gestion des risques IT & Cybersécurité

- Réalisation d'analyses de risques SSI (EBIOS RM, ISO 27005, méthodes internes bancaires).
- Cartographie des risques IT et suivi des plans de remédiation.
- Évaluation des impacts métier, réglementaires et opérationnels.

Contrôles IT et dispositif de contrôle interne IT

- Mise en œuvre et exécution des contrôles IT de niveau 1, 2 et 3.
- Réalisation de contrôles permanents SSI (N2) : accès logiques, conformité PSSI, sécurité applicative.
- Vérification de la conformité des dispositifs de sécurité et identification des écarts.
- Suivi des plans d'actions correctifs et gestion des recommandations d'audit.

Audit et conformité sécurité

- Préparation, accompagnement et suivi des audits SSI (internes, inspection générale, PASSI).
- Coordination des réponses aux audits et consolidation des éléments de preuve.
- Pilotage de la remédiation suite aux recommandations d'audit.
- Contribution aux dispositifs de conformité (NIST, RGPD, LPM).

Sécurité des projets IT

- Intégration de la sécurité dans les projets (ISP).
- Analyse de l'architecture sécurité et revue des dossiers techniques (DAT).
- Définition des exigences sécurité et validation des solutions techniques.
- Suivi des vulnérabilités et des plans de remédiation.

Gestion des incidents et vulnérabilités

- Analyse et traitement des incidents de sécurité (phishing, malware, compromission).
- Suivi des alertes cyber et coordination des actions de remédiation.
- Analyse technique des vulnérabilités et priorisation des corrections.

Compétences techniques :

Framework Cybersécurité :

- NIST

Méthodologies & standards de sécurité

- ISO 27001 Lead Implementer
- ISO 27005 Risk Manager
- EBIOS Risk Manager
- MESARI (Méthodologie Client Bancaire)

Autres méthodologies :

- ITIL

Réseaux & sécurité

- Protocoles & normes : Modèle OSI, TCP/IP, DNS, SSL, SMTP, LDAP, TLS, SFTP, SSH, SSL HTTPS
- Réseaux : LAN, WAN, VPN, Réseau physique
- Sécurisation des réseaux : Sécurité physique Datacenter. Chiffrement : Asymétrique/symétrique, Signature électronique, Certificat., chiffrement applicatif

Langage informatique

- Connaissance des langages C et Python

Systèmes & Solution

- Windows (serveurs/postes de travail), Kali-Linux
- Virtualisation : VMware
- RSA Archer (Solution GRC)

Autres

- Maîtrise des outils et solutions d'authentications
- Maîtrise des principes d'architecture sécurisée et de sécurité by design
- Bonne connaissance des solutions du marché

Soft Skills :

- Capacité d'analyse
- Communication

Anglais : courant

EXPERIENCE PROFESSIONNELLE**BPCE, 09/2024 à 02/2026****Consultant IT Risk**

- Définition et déploiement du programme TRM (Technology Risk & Management) pour l'ensemble des entités de BPCE SA (~30 entités) - modèle de gestion des risques Cyber et Informatique du Groupe
- Animation de comités et coordination : Préparation et animation de réunions de pilotage sécurité
- Politique de sécurité SI : Déclinaison de la politique sécurité, définition des besoins et mise en place de procédures adaptées
- Réalisation d'analyses de risques IT et cyber et mise à jour de la cartographie des risques.
- Mise en œuvre de contrôles SSI de niveau 2 sur les dispositifs de sécurité et la conformité PSSI.
- Identification des écarts de sécurité et suivi des plans de remédiation avec les équipes IT.
- Contribution à la préparation des audits internes et réglementaires et suivi des recommandations.
- Analyse des incidents de sécurité et proposition de mesures correctives.
- Analyse des incidents : Identification des menaces, évaluation des impacts et proposition de solutions correctives
- Cartographie des risques : Mise à jour, diffusion et suivi de la cartographie des risques SI, présentation des cartographies des risques aux CDG-1 de BPCE SA
- Accompagnement projets : Intégration des exigences sécurité dans les nouveaux projets et produits.
- Gestion de crises et alertes cyber : Suivi et résolution des incidents de sécurité
- Conseil et sensibilisation : Formation et accompagnement des collaborateurs et managers sur les enjeux de la cybersécurité.

CGI FINANCE (Filiale de la Société Générale), 09/2022 à 10/2024**Consultant Cybersécurité**

- Pilotage de projets sécurité (bastion d'administration, cloisonnement réseau centralisation des logs, sécurité Cloud Azure)
- Déploiement de solutions de protection (OME pour chiffrement des emails, DLP pour prévenir des fuites de données)
- Gestion des incidents de sécurité (phishing, malwares, intrusions) et coordination des plans de remédiation
- Analyse de risques techniques et métiers (ASA, ARA, flux, projets applications, besoins utilisateurs).
- Evaluation de la sécurité des applications (revue, tests, conformité) et accompagnement RGPD.
- Contribution aux activités de qualification / validation sécurité des applications suivi et remédiation des vulnérabilités sur l'environnement Azure et applications critiques.
- Participation au programme de suivi basé sur le NIST (contrôle, audit et conformité)
- Sensibilisation des utilisateurs et reporting régulier auprès du RSSI
- Participation aux revues de sécurité applicatives et aux audits SSI.

FRANCE TELEVISIONS, 01/2023 à 04/2024**Consultant sécurité**

- Intégration de la sécurité dans les projets (ISP)
- Accompagnement sécurité sur l'ensemble des projets (Direction de l'informatique, Numérique, Media Factory, CDE).
- Rédaction des exigences sécurité dans les projets selon les besoins en sécurité
- Intégration de la sécurité dans les contrats avec les fournisseurs techniques ou métiers

- Analyse et évaluation des propositions des fournisseurs métiers techniques ou métiers.
- Analyse sécurité sur des applications de type Saas/hors Saas (EBIOS RM).
- Pilotage et suivi d'une mission d'homologation sécurité LPM (secteur audiovisuel : Centre de Diffusion et d'Echange)
 - Identification et suivi des comités opérationnels, gestion budgétaire
 - Exigences détaillées liées au règles LPM
 - Validation de la conformité des solutions techniques, analyse de la sécurité selon les besoins des développeurs

SOCIETE GENERALE, 12/2020 à 12/2022***Expert fonctionnel Sécurité des SI***

- Intégration de la sécurité dans les projets (ISP)
- Accompagnement sécurité sur l'ensemble des projets (Audit, Inspection, Direction Générale .)
- Classification des applications, Evaluation des impacts (opérationnel, image, réglementaire etc.)
- Etude des mesures de sécurité implémentées (analyses de risques applicative, revue contractuelles, Plan Assurance Sécurité Fournisseur)
- Participation aux différents comités métiers et SSI (COMOP, COPIL, COSEC, etc.)
- Responsable du programme de mise en conformité LPM
 - Identification et suivi des comités opérationnels, gestion budgétaire
 - Exigences détaillées liées au règles LPM
 - Validation de la conformité des solutions techniques, analyse de la sécurité selon les besoins
 - Homologation & audit : Préparation et participation à la commission d'homologation, Réponse au rapport de l'audit PASSI, Analyse de risques

GROUPE BPCE, 05/2020 à 11/2020***Responsable Risques et Sécurité***

- Réalisation des contrôles permanents SSI de niveau 2 (PSSI-G, Contrôle d'accès logique, ...).
- Cartographie des risques SSI, pilotage et suivi des risques et de leur traitement (Conformité et cybersécurité).
- Traitement et/ou pilotage du traitement de recommandations de l'inspection générale ou de l'audit.
- Révision de la classification des applications du SI bancaire et interne, de la cartographie des risques métier (en relation avec les MOA banques).
- Mise à jour et garant de la qualité des résultats et de la matière contrôles SSI, risques SSI, vulnérabilités SSI, plan d'actions, conformité PSSI-G dans l'outil groupe Archer (Drive)
- Pilotage, coordination, qualité des réponses lors d'audit et/ou questionnaires SSI réglementaires
- Cadrage d'expression de besoin pour la réalisation d'audit et tests d'intrusion sur des plans du SI ou des applications spécifiques
- Animation de groupe de travail (GT) avec les Banques Populaires, au sein de la filière SSI groupe, représentation RSSI dans des GT Groupe
- Accompagnement des Banques sur les exigences Conformité en RGPD
- Préparation du comité des risques (mensuellement) et contrôle interne (trimestriellement).

CREDIT AGRICOLE, 01/2019 à 05/2020**Consultant Cybersécurité**

- Analyse des risques applicatives/projets selon la méthodologie client (MESARI, EBIOS Risk Manager)
- Instruction sécurité de solutions techniques : accompagnement des MOE, MOA, Responsable Métier, préconisations de solutions de sécurité, revue d'architecture sécurité
- Qualification des critères de DICP
- Gestion des tests d'intrusion
- Suivi des plans de remédiation
- Rédaction et mise en œuvre de la politique de sécurité du système d'information
- Analyse des impacts sur la confidentialité des données (DPIA)
- Assistance RSSI/CISO :
- Reporting d'activité auprès du RSSI et des responsables d'applications.
 - Audit et revue de la sécurité de l'information.
 - Activités liées au programme annuel de sécurité du groupe (CARS).
 - Evaluation de la sécurité du fournisseur externe dans le cadre d'un appel d'offres, y compris le fournisseur de services cloud
 - Qualification de la sécurité des applications et des infrastructures

SOCIETE GENERALE, 10/2018 à 12/2018**Consultant Cybersécurité**

- Élaboration d'un questionnaire de sécurité lié à la gestion des données personnelles (RGPD) dans le processus d'analyse de risques
- Évaluation de la sensibilité des applications avec l'intégration des questions liées au RGPD (interactions avec les entités juridiques, les représentants de la conformité).
- Validation des rôles et des responsabilités des équipes devant intervenir sur l'analyse d'impact et la mise en conformité dans le cas où l'application gère des données personnelles au sens RGPD.
- Validation des moyens de mise en conformité à appliquer dans le cas où l'application gère des données personnelles au sens RGPD.

EDF, 08/2017 à 10/2018**Consultant Sécurité**

- Relecture et validation sécurité des DAT (Dossier d'Architecture Technique).
- Qualification des critères DICT
- Relecture et validation sécurité des guides de sécurisation
- Rédaction des RSIS (Rédaction des procédures, politiques et directives de sécurité).
- Accompagnement projet (contribution aux exigences sécurité .)
- Analyse sécurité sur des FED (Fiche d'écart et dérogation)
- Analyse sécurité sur des applications de type Saas/hors Saas (Méthodologie EBIOS RM)
- Accompagnement RSSI (Suivi des campagnes de sensibilisations, GDPR, Gouvernance...).

AUCHAN, 08/2015 à 08/2017

Consultant Sécurité

- Validation du risque sécurité SI pour les nouveaux projets
- Mise en place de la gouvernance autour de la sécurité du SI.
- Mise en place d'une cartographie des risques (applicatifs) sur le périmètre de la DPC
- Construction de supports de sensibilisation à la gestion des risques SI
- Pilotage des risques (Cadrage Audit, GDPR, Objets connectés IoT .)
- Suivi des campagnes de sensibilisations
- Analyse des risques projets (ISO 27005, EBIOS RM)