

COORDONNEES

Adresse: 7 Chemin de saint blin 95500 Gonesse

Telephone: +33625068841

Email: bfredeuphel@yahoo.fr

Disponibilité: ASAP

CERTIFICATIONS OBTENUES

- Finance & Banque: Advanced Corporate Governance for Financial Institutions (LCT - 2018)
- COSO ERM: Enterprise Risk Management (IMA - 2022)
- COSO Internal Control: Auditing (IMA - 2022)
- COBIT: IT GRC Expert des SI (ISACA - 2016)
- CISSP: En cours

FORMATIONS PROFESIONNELLES

- IT GRC Expert (Pilotage - Protection - Prévention - Innovations)
- PMP (Management de Projets)
- NIST (Conformité des évolutions des SI)
- PCI DSS (Conformité de la Sécurité de paiements)
- ISO 31000 - 27001 - 27002 - 27005
- ITILv3 (Amélioration des Services IT)
- SOC 2 - CSA CCM - DoD CSR - CMMC
- APPSEC - DevSecOps - OWASP - ASVS - CIS CSC - STRIDE - DREAD - MITRE ATT&CK - NVD - CVE
- TOGAF (Security Architecture & Design)

COMPETENCES

- Pilotage: Evolution des SI - SMSI - PSSI - Audits - COPIL - Reporting - IT Performance - CAPEX - OPEX
- Protection: Veille technologique - Security and Privacy By Design (SPBD) - Conformité des SI - Sécurité des SI (Infras. - Réseaux - Applis - Sys.)
- Prévention: Gestion de risques - Gestion de Vulnérabilités - BCP/DRP - Sensibilisation
- Innovation: Habilitations - Mobilité Sécurisée - Adaptation du SI à la stratégie - Messagerie
- Cloud: IaaS - PaaS - SaaS - Logiciels médiateurs (API - CASB...)
- Asset Mgmt.: Infrastructure - Systèmes - Data - MDM - Services
- Contrôles: Scans - SIEM - SOAR - habilitations - EDR/XDR - Incidents - Hardening - Monitoring
- Supervision: IAM - SIEM - MDM - Cloud - Infrastructure - Systèmes - Messagerie
- Conformité SI: FFIEC - ISO 2700X - NIST - PCI DSS - HIPAA - NIS2 - DORA - SDLC - ASVS - CIS - OWASP
- Reporting: COPIL des projets - IT Performance (PKI & KRI) - Budget (CAPEX...) - Gestion des Incidents

OUTILS

- Solutions Anti-malveillants
- Equipements (FW, IDS/IPS, AD, Routeurs, Switch...)
- APPSEC (OWASP - ASVS - CIS - Pentest - SCANS...)
- QRADAR, Splunk, Usercube, CISCO, Fortinet
- Méthodes (SDLC, STRIDE, DREAD, PASTA...)
- VPN (IPSEC, TLS, SSL, PKI...)
- EDR, XDR, SOAR

FORMATION

- 2008: Mastère Spécialisé en Cybersécurité (Télécom Paritechs)
- 2006: Ingénieur Télécom et Réseaux (EPMI - ECAM)
- 2003: BTS Electronique (EST LOKO - Abidjan)
- 2000: BAC S

LANGUES

- Anglais: Bilingue
- Espagnol: Notions

CENTRES D'INTERETS

- Activités sportives et bénévoles
- Voyages
- Passion de cuisine
- Loisirs culturels

Fred Euphel BATTI BITECK

DIRECTEUR de PROGRAM CYBERSECURITE & IT GRC EXPERT (+15 ans)
(Finance - Banque - Assurance - Télécoms)

PROFIL

Réussite reconnue de mon **coaching RSSI** dans l'évolution des systèmes d'informations qui s'alignent aux besoins stratégiques et métiers. Gestion des risques cybersécurité par l'analyse des processus et des opérations ainsi que des évolutions réglementaires afin d'adapter les systèmes d'informations aux objectifs et aux missions des entreprises. Coordination des **équipes expérimentées** autour des projets de mise en conformité opérationnelle des SI aux normes cybersécurité. Vision globale des enjeux cybersécurité (**Security By Design and Privacy**) par l'intégration de la sécurité dans les acquisitions. Accompagnement des équipes de la continuité d'activité et de la cyber résilience dans l'implémentation des mesures de sécurité. Participation aux comités architectures en vue de proposer des solutions de sécurité. Pilotage d'audits de sécurité afin de remédier aux vulnérabilités, Assistance des équipes CSIRT lors de la gestion d'incidents.

EXPÉRIENCES

IT GRC Expert (COSO ERM - IT Operational Risks)

02/2023 - 08/2023

Barclays London - Freelance (Gestion des Risques IT Opérationnels)

ERM Program: (Information, Comm. & Reporting - 18. Leverages Information and Technology)

Améliorer le programme ERM, en établissant des bonnes pratiques (référentiels) en matière de gestion des risques Opérationnels liés à l'IT (cybersécurité et technologiques), choisir les méthodologies et les outils adéquats, pour une meilleure approche d'identification, d'évaluation, de priorisation, de quantification, de remédiation et de reporting des IT Operational risks au management et au comité d'audit. (Compliance FFIEC - Investissement Bank)

Zones de couvertures - IT Infrastructures support models (ITISM):

Change management, data management, Gestion des Habilitations, Gestion des Incidents, Gestion des Vulnérabilités, du backup, vendor management, Continuité et Reprise d'activités, les postes de travail, penetration tests, secure baselines, pour s'assurer que la sécurité IT (activités informatiques) s'aligne aux exigences réglementations, des politiques de sécurité définies par l'équipe **IT Risk Management (ITRM)**.

- Investiguer sur la robustesse et l'adéquation des mesures de sécurité dans les édifices **ITISM**.
- Accompagner les DPO à évaluer l'efficacité des mesures de sécurité qui protègent les données (PII, PCI DSS, GDPR, GBLA, HIPPA...)
- Identifier et évaluer les risques ITGC opérationnels de l'entité, y compris ceux liés aux TPRM, établir le profil de risques par interview des collaborateurs, benchmark sur les tendances du secteur, sur les risques émergents, ainsi que des évolutions des réglementaires et des normes.
- Classer les risques par priorité selon les critères définis par l'**ITRM** et les exigences **FFIEC**, établir la procédure pour signaler les échecs et les lacunes des remédiations aux risk owners.
- Élaborer et valider avec les collaborateurs les plans de remédiation des risques ITISM prioritaires selon les bonnes pratiques (Security By Design and Privacy) et préparer les reportings COPIL
- Implémenter les mesures de sécurité (security by design and privacy) et les méthodologies de gestion de risques **ITRM/ERM**, s'assurer qu'elles sont conformes aux exigences du ERM program
- Maintenir les mesures de sécurité par des tests périodiques pour s'assurer que les risques sont réduits, revue des contrats avec les fournisseurs (TPRM) et sensibiliser les parties prenantes.

IT GRC EXPERT (COSO Internal Control - ITGC)

02/2022 - 12/2022

Expéris - Paris - CDI (IT Internal Control & ERP UPDATES)

La mise en place des dispositifs efficaces du contrôle interne par le biais de ITGC/CGI dans le but de développer et d'implémenter des systèmes d'informations qui adhèrent à la business stratégie, à la crédibilité financière par processus, à fiabilité des opérations et aux évolutions réglementaires et légales (**Control Activity - 11. Selects and develops general controls over technology**)

- Cartographie les processus organisationnels/métiers et hiérarchisation des risques associés
- Conception des dispositifs de contrôle interne dans les activités IT par l'analyse des risques auprès du métier et des chefs de projets SI (Infras., Applications, Données, habilitations, flux)
- Déploiement du cadre de contrôle interne pour les ITGC/CGI, en garantissant la conformité aux normes réglementaires de gestions (Stocks - Comptables - Projets - Ventes - Services...)
- Gestion des habilitations (Provisionnement/deprovisionnement, transferts, revue des comptes)
- Implémentation des plans de remédiation des directives ITGC/CGI vulnérables, en collaborant avec les parties prenantes de gestions (Stocks - Comptables - Projets - Ventes - Services...)
- Pilotage des audits ITGC et remédiation des déficiences en identifiant les domaines d'amélioration, tester et maintenir continuellement les mesures de sécurité.
- CoPil sur l'état des ITGC, les indicateurs de suivi d'activités et les efforts de remédiation.
- Benchmarking de bonnes pratiques métiers, veille technologique des ITGC, valider du cadre contrôle interne lié à l'IT (ITGC/CGI), sensibilisation des collaborateurs.

COMPLEMENT DES EXPERIENCES	
❖ BNPP CIB et CARDIFF:	08/2017 – 12/2021
➤ APPROCHES FONCTIONNELLES	
▪ Gestion de Risques (ERM – Internal Control – RMP – CRA – IAP)	
▪ Cybersécurité (WISP – DSP – CSOP – COSO – NIST – ISO 2700X – FFIEC – KYC – PCI DSS – SANS...)	
▪ Sécurité des SI (SPDB – SDL – DevSecOps – IAM – COOP – DPP – BCP – SIEM...)	
▪ Gestion de vulnérabilités (VPMP – SBC)	
▪ Gestion d'incidents (IIRP – CIRP – CSIRT)	
▪ Gestion de Fournisseurs (TPRM – TSPM – C-SCRM)	
➤ APPROCHES TECHNIQUES	
▪ Pilotages Audits (OWASP – STRIDE – DREAD – CIS – ASVS – CVSS – NVD)	
▪ Gestion des apps. et leurs criticités (BAM+ – GSF)	
▪ Checklists du Core Banking (Prod Review – SAST – DAST – Pen Tests – ASVS – CIS – OWASP – MITRE)	
▪ Passerelles d'accès N-tiers (Web Access Security – Revamping – WAF – CASB)	
▪ Habilitations (ICAM/IDAM – StrongAuth – RBAC – ABAC – DAC – SSO – FIdM – Break Glass Access)	
▪ Data Management (Anonymisation – DPNP – Chiffrement ...)	
❖ Orange/OBS:	04/2016 – 07/2017
➤ APPROCHES FONCTIONNELLES	
▪ Cybersécurité (Asset Mgmt. – SIEM – DLP – Habilitations – Monitoring – 3rd Party Mgmt.)	
▪ Pilotage (SMSI – PSSI – IT performance – COPI – Audits – Rémediation des vulnérabilités)	
▪ Protection (Sécurité dans les projets – habilitations – Gestion des vulnérabilités – gestion des incidents)	
▪ Prévention (BCP – DRP – Gestion de risques)	
▪ Conformité (ISO 2700X – ISO 9001 – PCI DSS – SSAE 18 – OWASP – ASVS – CVSS – STRIDE – CIS CSC)	
➤ APPROCHES TECHNIQUES	
▪ Pilotage Audits (PenTests – ST&E – OWASP – ASVS – CIS – CVSS – CVE – STRIDE – DREAD...)	
▪ ST&E (SAST, DAST, SCA, Rémediations, Hardening)	
POINTS COMMUNS PROGRAM. PCI DSS (5 ANS)	
➤ APPROCHES FONCTIONNELLES	
▪ identifier des processus des paiements existants	
▪ Analyse Fonctionnelles et Techniques des processus de paiements existants (Réseaux – Infr. – Syst...)	
▪ Analyse des contrôles applicables à la sécurité de paiements (Infr. – Applis. – Syst...)	
▪ Security Architecture & Design et sécurité dans les projets (technologiques et techniques)	
▪ Endpoint Hardening (Réseaux – Systèmes – Applications – Postes de travail – Backup...)	
▪ COPI (Opérationnels, projets, métiers, 3 rd party...)	
▪ Pilotage d'Audits PCI DSS et Rémediation des écarts	
➤ APPROCHES TECHNIQUES	
Pilotage d'Audits (Vulnerability Management Program)	
▪ ASVS scans: (Systèmes – Applis. – Data Backups)	
▪ OWASP: Sécurité Applications web et vulnérabilités	
▪ CIS CSC : Prévention attaques Cybersécurité	
▪ NIST: Robustesse et Acquisitions des SI.	
▪ ISO 2700X: Robustesse des SI (SMSI et PSSI)	
▪ STRIDE: Threats Modeling (Business Logics...)	
▪ DREAD: Threats Modeling (Use cases...)	
▪ SAST: Scans statiques sur (Syst. – Applis – Backups)	
▪ DAST: Scans Dynamiques sur (NGAV – EDR – MDR – Syst. – Applis – Backups)	
▪ CSA CCM: Cloud Best pratiques (IaaS, PaaS, SaaS)	
▪ Tests: ETL – API – SOA	
▪ Habilitations:(StrongAuth – FIdM – MFA – SSO – RBAC – ABAC – PKI)	
▪ PKI: (Users – Services – Systèmes – Applis – Flux)	

IT GRC Expert - Coordinateur de RSSI Régions	08/2017 – 12/2021
BNPP [CIB et CARDIFF]- Paris – CDI	(5 ans)
Conception, implémentation et maintenance des socles technologiques de CIB ITO et CARDIFF en vue d'aligner leurs systèmes d'information à la stratégie de BNPP, ainsi que la gestion des risques IT par l'adhésion à la conformité réglementaire et des bonnes pratiques (ITRM – ITOps)	
<ul style="list-style-type: none"> Aligner les bonnes pratiques IT aux objectifs organisationnels, protéger l'information et ses infras. de traitements, adhésion aux exigences légales, réglementaires et contractuelles. Elaboration des stratégies d'exécution des programmes infosec. (Back2Green, NIST, APPSEC) Coordination des RSSI des régions (EMEA – APAC – NAR – LATAM) lors des évolutions des SI COPI, planification budgétaire, arbitrages des priorités, gestion des risques et des tiers. Gestion des vulnérabilités et gestion d'incidents, ajustement des actifs aux évolutions des SI 	
Directeur de Programme Cybersecurité	04/2016 – 07/2017
Orange/OBS – Paris – CDI	
Accompagner les projets d'évolutions des infrastructures d'hébergement (Cloud – GW – ZOE), Auditer et tester leurs robustesses ainsi que leurs conformités aux normes de la cybersécurité.	
<ul style="list-style-type: none"> Participer aux Comités Architecture CoSo pour valider les édifices (Infrastructures, Applicatives, Données, systèmes) et renseigner les DAF (Docs Architecture Fonctionnel) Segmenter le LAN Client du réseau Interne (WIFI – VOIP – VPN Overlay – Amelie...) Raccorder les composants aux services communs d'infrastructures (DNS, DHCP, NTP, ...) Sécuriser les passerelles et Infrastructures d'accès au SI (Gassi – Axway – Metagate – SAI ...) habilitations et revue de comptes utilisateurs (Maghesta – Cactus – GASSI –TDIMG – TACACS) 	
Directeur de Programme Cybersécurité	02/2015 – 03/2016
Soc Gén. – Paris – CDI	
Assurer la cohérence des exigences sécurité des transactions Bancaires et des échanges de différentes plateformes de services par l'adhésion aux objectifs stratégiques cybersécurité	
<ul style="list-style-type: none"> Spécifications (Fonct, Tech) des composants et l'Intégration des solutions secure-Banking Sécurité dans les projets (COPI) - Gestion des risques – Gestion des incidents – Hardening Habilitations (StrongAuth, accounts Review, NAC, MDM, BYOD) – SIEM (fraudes) 	
Directeur de Programme Cybersécurité	08/2013 – 12/2014
BOURSORAMA – Paris – CDI	
Maîtriser l'évolution du SI et ses applications métiers e- Banking (Crédit, Epargne, Assurance, CB ...) par la gestion des risques IT et mesurer la performance du SI (e-Portail – Infr. – Syst. – Applis...)	
<ul style="list-style-type: none"> Rédaction des spécifications (SMSI, PSSI) – Piloter les audits – Rémediation (Roots causes) Qualifications des projets sécurité (Infra, Systèmes, Réseaux, Applications, Services...) CoPil (Projets, Sécurité, Risques, Conformité, Incidents...) – Indicateurs COPI (PKI, KRI) 	
❖ PLUSIEURS MISSIONS DE PROGRAMMES PCI DSS	(5 ANS)
Mission 4 – SFR – Paris – CDI	11/2011 – 07/2013
Validation d'une plateforme Banking services pour les paiements mobiles, notification des mouvements des comptes par la gestion des transactions bancaires (Achats, Transferts, Dépôts...)	
<ul style="list-style-type: none"> Rédiger des exigences SMSI/PSSI – Chiffrement des projets – Participer aux comités de pilotage Sécurité dans les projets (SDL – Tests – VABF – UAT) et des Transactions (PKI, Chiffrement...) 	
Mission 3 – OBERTHURCS – Paris – CDI	11/2010 – 10/2011
Evolution de la plateforme de service mobile e-Banking « ALM - Télépathic » pour gérer les transactions bancaires des applications du portefeuille mobile (Banques, mobiles, services...)	
<ul style="list-style-type: none"> Identification des besoins par le PCI DSS assessment tools (Assets, Risks, vulnérabilités...) Déploiement des modules ALM et Télépathic (Tests – VABF – UAT) – PKI (Services, Flux, Applis) 	
Mission 2 – SFR – Paris – CDI	11/2008 – 10/2010
Pilotage de la sécurité de la plateforme Banking services par le contrôle d'accès et la protection des transactions par des services communs IT (Crédit, CB movements, paiements, trésorerie, fraudes)	
<ul style="list-style-type: none"> Identification des besoins par le PCI DSS risques assessment (Assets, Risks, vulnérabilités...) StrongAuth des Accès et des échanges (PKI, AD, Systèmes, Services, SAML, SSO, SIEM...) 	
Mission 1 – Bouygues Télécoms – Paris – CDI	12/2006 – 10/2008
La conduite de changement de la plateforme de service facturation « Transactions Biling »	
<ul style="list-style-type: none"> Prise en compte des exigences d'évolutions (Infr., Applis., services, processus) Coordination chefs de projets (Cadage, BUILD, RUN) – Reporting (projets, Risques, budget...) 	
SFR – Paris – CDI	05/2005 – 10/2006
Augmentation capacitaire du réseau mobile 3G et migration des différents flux vers MGWR4	
<ul style="list-style-type: none"> Refonte de l'architecture des reseaux mobiles (Accès Radio & Coeur Réseau) – Différentiation et Convergence des flux “CAC 40, partenaires, mobiles, Internet, data”. 	