

COMPETENCES CYBER SECURITE ET GOUVERNANCE

Responsable de la Sécurité des Systèmes d'Information. Gestion opérationnelle, incidents, relations clients. Conseil de direction, transformation numérique. Management d'équipes. Gouvernance Risk Compliance. Elaboration de normes et de référentiels de sécurité. Audit, état des lieux, et expertise sur les systèmes d'information, réseaux et Internet. Constats d'écart et défauts de sécurité. Revues de direction et plan d'action suite aux audits.

Assistance à maîtrise d'ouvrage, accompagnement appel d'offres. Analyse de risque. Politique de sécurité. Contrôle conformité réglementaire et normative : RGPD, LPM, directive NIS (OIV / OSE). Système de management de la sécurité de l'information (SMSI ISO 27001). Autres directives et réglementations. Travaux juridiques.

Définition de tableaux de bord : stratégiques, pilotage et opérationnels.

Formation, sensibilisation et responsabilisation des acteurs. Coaching. Animation de groupes de travail. Etudes stratégiques, enquêtes et marketing sur les solutions de sécurité. Elaboration de business plans. Outillage pour travaux de groupes et méthodes pour le cyber sécurité. Publications.

EXPERIENCE PROFESSIONNELLE

Depuis septembre 2018 Directeur conseil fondateur Cyber Sécurité Gouvernance Risk Management	<b style="color: red;">Dominique CIUPA Security Consulting (DCSC : conseil de direction cyber sécurité) RSSI de transition pour une importante ESN. Reprises des politiques de sécurité. Des analyses de risques, avec la solution EGERIE Risk Manager. Gouvernance en vue de renouveler une certification ISO 27001. Refonte de l'approche de formation et sensibilisation à la cybersécurité. Approche en vue de définir des solutions de cyber-assurances. Réponse aux incidents de sécurité en permanence. Comités de pilotage avec tous les acteurs de la sécurité. Recrutement et formation d'un RSSI adjoint. Travaux sur les solutions IaaS et SaaS. Notamment O365 et Microsoft Azure. Travaux préparatoires pour la mise en œuvre d'une gouvernance ISO 27001 pour une société d'économie mixte. Lancement de l'activité de conseil en cyber sécurité : <ul style="list-style-type: none"> ◆ Conseil de direction. Prise en compte de la cyber sécurité dans la stratégie. ◆ Conformité réglementaire Loi Programmation Militaire, directive NIS. Dossiers homologation. EBIOS 2010 / EBIOS Risk Manager 2018, FEROS, plan de sécurité. ◆ Accompagnement à la conformité au RGPD, protection des données à caractère personnel, DPO externe (délégué à la protection des données). PIA / EIVP. ◆ Préparation à la certification ISO 27001 d'un SMSI. Analyse de risque. PSSI. ◆ Formation, animation de conférences, et groupes de travail.
2017- 2018 Manager Consultant Cyber Sécurité	<b style="color: blue;">ATEXIO (conseil en cyber sécurité) RGPD - règlement de protection des données à caractère personnel EU 2016-679 : <ul style="list-style-type: none"> ◆ Offre de conseil pour mise en conformité : audit, état des lieux ; registre des activités de traitement ; contrats sous-traitants ; contrats clients pour opérateurs software as a service ; durées de conservation des données et archivage des données. ◆ Prestations pour : opérateurs de services, éditeurs de logiciels, sociétés d'investissements, activités commerciales, sociétés industrielles, établissements de santé. SMSI - ISO 27001 : <ul style="list-style-type: none"> ◆ Analyse de risque préparatoire à la certification ISO 27001 d'une ESN. Premières politiques de sécurité. Pré-audit de certification avec LRQA. ◆ Travaux pour la conformité d'une agence européenne.
Juin-Octobre 2017 RSSI	<b style="color: blue;">IDNOMIC (éditeur IGC / PKI) RSSI de transition. PKI. Reprise des conditions habilitation IGI 1300.

2015-2017	SOPRA-STERIA (ESN)
Manager Consultant Cyber Sécurité	<p>Domaine bancaire :</p> <ul style="list-style-type: none"> ◆ Travaux sur la sécurité de projets de migration des systèmes d'information dans le cloud computing. Grille d'éligibilité. ◆ Analyse exigences réglementaires dans le secteur bancaire pour identification projets transversaux : LPM, directive NIS, DSP2, secrets des affaires, RGPD, etc. <p>Domaine Santé :</p> <ul style="list-style-type: none"> ◆ Politiques de sécurité du dossier médical partagé (DMP) et protection des données à caractère personnel (RGPD). Travaux audités et validés par la CNIL.
2013-2014	OUTSCALE (opérateur IaaS – infrastructures cloud computing)
RSSI : Système management et qualité	<p>SMSI certifié ISO 27001 : 2013, par la BSI (British Standards Institution) en août 2014 (sans aucune non-conformité). Documentation rédigée entièrement en anglais.</p> <ul style="list-style-type: none"> ◆ Animation de 5 « risk owners » dans un métier d'IaaS (cloud computing). Gestion des risques et exploitation de la notion de presque-accidents. ◆ Gestion du changement, responsabilisation des acteurs au management dans une entreprise « très technique ».
2011-2013	ACTIVITÉ INDÉPENDANTE (diverses entreprises)
Manager Consultant Cyber Sécurité	<p>Préparation certification ISO 27001 d'une ESN pour clients opérateurs télécoms et banques pour des activités de tierce maintenance applicative (TMA) et développements applicatifs. Analyse de risque pour une certification ISO 27001 pour des activités IaaS et SaaS (Infrastructure et Software à la demande – en mode Cloud). Étude sécurité des Smartphones, données à caractère personnel. Informatique et Libertés. Dossier d'homologation d'un système d'information militaire. Etude EBIOS. Préparation FEROS. Préparation des dossiers d'architecture de sécurité.</p>
2007-2011	BULL SERVICES (équipementier informatique, ESN)
Manager Consultant Cyber Sécurité	<p>Sécurité de différentes activités internes au groupe BULL :</p> <ul style="list-style-type: none"> ◆ Certification ISO 27001 par LSTI activités hébergement, dont gouvernementales. ◆ Appui pour des référencements sécurité de développements et maintenance. <p>Domaine énergie :</p> <ul style="list-style-type: none"> ◆ Gestion de risque du réseau gaz avec exigences Directives Nationales Sécurité. ◆ Norme ISO 27005 et NEI 0404 (USA) infrastructures SCADA nucléaires. ◆ Veille sur Internet. Spécificités techniques, intelligence économique, ROSO. <p>Ministères :</p> <ul style="list-style-type: none"> ◆ Études de scénarios de fraudes. Enquêtes terrain. Contre-mesures et plan d'actions pour corriger les erreurs d'implémentation d'une application nationale. <p>Domaine militaire :</p> <ul style="list-style-type: none"> ◆ Sécurité de furtivité-anonymat sur Internet. Information et renseignement. ◆ Approche offensive avec l'École de Guerre Économique. <p>Domaine santé :</p> <ul style="list-style-type: none"> ◆ Audit du système d'information, plan d'actions. Approche norme ISO 27001. Estimation des écarts. Mesures de sécurité ISO 27002 et ISO 27799. <p>Conseil Général :</p> <ul style="list-style-type: none"> ◆ Formation SSI : compréhension des risques, fraudes, Informatique et Libertés, introduction à ISO 27001, 27002, 27005, méthode EBIOS. Politique de Sécurité.
2005-2007	ACTIVITÉ INDÉPENDANTE (diverses entreprises clientes)
Consultant Cyber Sécurité	<p>Domaine bancaire :</p> <ul style="list-style-type: none"> ◆ Maîtrise d'ouvrage choix d'une solution de ToIP pour 2 200 agences. Analyse Cisco, Avaya, Alcatel. Evolution des roadmaps pour le Comité de Qualification Technique. <p>Divers :</p> <ul style="list-style-type: none"> ◆ Maîtrise d'ouvrage. Projets internationaux pour l'Union Européenne. ◆ Intérim RSSI Groupe. Revue de la politique de sécurité et contrôle de conformité en relations avec 27 filiales.

2003-2005	INTRANODE (start-up, éditeur de logiciel de sécurité français)
Consultant Manager Cyber Sécurité	Repositionnement d'Intranode (scanner vulnérabilités), vente à Netasq et à Criston pour créer une suite logicielle gérant et corrigeant les vulnérabilités (aujourd'hui devenu Airbus Cyber Security). Différents projets de gestion des vulnérabilités des systèmes gouvernementaux, avec règles d'isolation.
2001 – 2003	CONCORD COMMUNICATION (éditeur de logiciels américain)
Account manager Supervision performance SI	Analyse des besoins de qualité de service des offres de transmissions de données pour les entreprises. Pilotage, mise en œuvre et stabilisation des solutions de supervision et d'exploitation des systèmes d'information.
1998 – 2001	LUCENT TECHNOLOGIES (équipementier télécommunications)
Directeur de l'activité Conseil	Audit de l'exploitation du réseau Noos (câblo-opérateur). Analyse technique, mesure de la performance. Organisation de l'exploitation avec externalisation : infogérance de 3 ans avec 45 personnes. Sécurité du Système d'Information. Demandes de licences à l'Autorité de Régulation des Télécoms pour nouveaux opérateurs.
1996 – 1998	KPMG PEAT MARWICK (conseil en organisation)
Manager Consultant	Conseil en organisation, définition de processus. Préparation à la mise en œuvre de différentes solutions logicielles. Audit. Analyse de la régulation des télécommunications : France (ART), puis Irlande (Ofcom).
1992 – 1998	ACTIVITÉ INDÉPENDANTE (différentes entreprises clientes)
Manager Consultant	Maîtrise d'ouvrage des services de sécurité : contrôle accès, énergie, télécom, salles blanches, câblage, climatisation, anti-incendie. Reprise et continuité d'activités. Offres de téléphonie alternatives et services managés : aspects juridiques et économiques. Veille, information, sur la libéralisation du marché des télécommunications.
1990 – 1992	MAZARS (audit et conseil de direction)
Consultant - audit	Formation à l'audit des sociétés : participation à la réponse du Cabinet Mazars pour l'audit des comptes d'un grand client des télécoms. Différentes missions de conseil : audit d'organisation, Schéma Directeur Informatique.
1988 – 1989	SAGATEL (conseil en télécommunications)
Consultant junior	Analyse de marchés en vue de la libéralisation des télécommunications. Travaux avec la DGT (avant la création de France Telecom) et avec la Commission européenne (DG XIII).

DIVERS

Études :	1987 : Ingénieur Télécom. École Nationale Supérieure des Télécommunications de Bretagne, devenue Institut Mines Télécom. 1991 : Formation à l'audit des comptes à HEC avec le cabinet Mazars. 2007 et 2015 : Certifié Lead Auditor ISO 27001 par LSTI (norme 2005, puis norme 2013).
Langues :	Français : langue maternelle. Anglais : courant et professionnel, parlé et écrit.
Expertise :	<ul style="list-style-type: none"> ◆ Membre de la CN27 à l'AFNOR : normes ISO 27001, 27005. ◆ Adhérent du Club EBIOS (www.club-ebios.org/) : analyse de risque avec l'ANSSI. ◆ Ex-Membre de l'ANAJ – IHEDN (Hautes Etudes Défense Nationale) ◆ Ex-adhérent de l'AFCDP (www.afcdp.net/) : protection des données personnelles.
Rédacteur :	Participation au livre de l'AFCDP : « Correspondant Informatique et Libertés ». Auteur de différents articles SSI professionnels.
Divers	<ul style="list-style-type: none"> ◆ Officier de Réserve : CCR Marine (commandant), réserviste cyberdéfense groupe de travail GT7 / LPM (2015-17). Missions (2016-17) avec l'officier général cyberdéfense. ◆ Conférences SSI : BlackHat, Hack in Paris, Cercle de la sécurité, Assises de la sécurité, FIC, Celar, ARCSI, Clusif, SSTIC, ANAJ-IHEDN, CESM, CDEC.