David LARBONI

Consultant indépendant en Cybersécurité
CISO as a Service

ISO 27001, HDS, WLA, CISSP

Conférencier

Contact

+33 6 62 74 25 63

davidlarboni@gmail.com

Compétences

- ✓ ISO 27001 / ISO 27005 / HDS
- ✓ Sécurité de l'information (SMSI)
- ✓ Gestion des risques fournisseur
- ✓ Management de projets
- ✓ RGPD

Langues

Anglais (Courant)

Allemand (Professionnel)

Formation

ESCP EUROPE *(1994 - 1997)*

Master's Degree, Marketing & IT

Résumé

- **Interim Management : RSSI**
  *(**R**esponsable de la **S**écurité des **S**ystèmes d'**I**nformation)*
- **Certifications**
  - ✓ ISO 27001 « Lead Implementer » *(versions 2013 & 2022)*
  - ✓ CISSP
  - ✓ NIST
- **Création d'un outil de notation du SMSI des entreprises (CyberVadis ®)**
- **Management de projets**
  - ✓ Déploiement de solutions informatiques
  - ✓ ISO 10006 « Quality Management Systems »
- **Management d'équipes**
  - ✓ jusqu'à 10 collaborateurs
  - ✓ jusqu'à 18 prestataires
- **Gestion de contrats de service**
  - ✓ 11 contrats (SSII et conseil)

Loisirs

- Sports *(tennis, ski nautique, kitesurf, snowboard)*
- Musique *(batteur dans un groupe de rock)*
- Œnologie

J'organise des dégustations de Champagnes pour faire découvrir la richesse de ce terroir.

Expérience professionnelle *(consultant indépendant)*

Disponible pour de nouveaux défis à partir de Septembre 2023

Premier opérateur de jeux d'argent en France, deuxième loterie européenne et quatrième loterie mondiale, mon client gère également des activités ouvertes à la concurrence – principalement les paris sportifs en ligne.

Principales réalisations :

- Accompagnement aux certifications PCI-DSS v3.2.1 RoC[A], ISO/IEC 27001:2013 et WLA-SCS:2020 (World Lottery Association) → **Certifications obtenues par la FDJ à l'issue de la mission**.
- Mise à jour de l'ensemble des politiques, procédures et points de contrôles afin de garantir le maintien en conformité du SMSI.
- Accompagnement des équipés opérationnelles (IT, métiers) dans la mise en conformité des processus pour satisfaire aux exigences des normes ISO/IEC 27001:2013 et WLA-SCS:2020.
- Réalisation d'un audit à blanc basé sur les référentiels ISO/IEC 27001:2013 et WLA-SCS:2020 pour vérifier le respect des exigences et préparer à la certification.
- Suivi et résolution avec l'aide des équipes opérationnelles du reliquat de non-conformités.
- Animation et accompagnement lors de tous les entretiens de l'audit de certification avec l'auditeur externe et les équipes opérationnelles (7 jours).
- Réalisation et accompagnement à la transition vers la version 2022 de la norme ISO/IEC 27001.

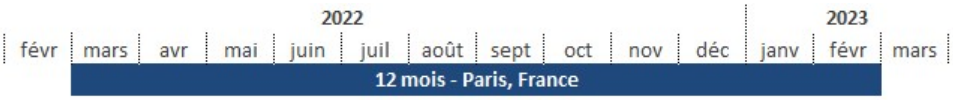
****

Mon client est une association loi de 1901, reconnue d'utilité publique, qui a pour but « d'aider et d'apporter une assistance bénévole aux personnes démunies, notamment dans le domaine alimentaire ».

Principales réalisations *(mission à temps partiel, 2 jours / semaine)* **:**

- Management par Interim: RSSI – Responsable de la Sécurité des Systèmes d'Information.
- Mise en place d'un plan de sécurisation à 3 ans issu d'un audit externe de sécurité.
- Rédaction puis promotion/diffusion et maintien de la politique de sécurité des SI.
- Mise en œuvre d'un plan de continuité des activités.
- Diffusion au sein de l'association d'une culture sécurité (savoir et faire savoir).
- Définition au sein du Pôle SI et au sein de l'association d'une gouvernance sécurité (reporting, risques, suivi des actions, alertes).
- Benchmark et choix puis acquisition d'un outil de sensibilisation.
- Réalisation de sessions de sensibilisation sur les risques et bonnes pratiques en matière de sécurité.

****



LINEDATA est un éditeur international de logiciels, de services et de données à valeur ajoutée dédiés à l'industrie financière.

Principales réalisations :

- Management par Interim: RSSI – Responsable de la Sécurité des Systèmes d'Information.
- Accompagnement à la certification SOC II.
- Suivi et résolution avec l'aide des équipes opérationnelles du reliquat de non-conformités suite à un audit technique (pentest).
- Réalisation de sessions de sensibilisation sur les risques et bonnes pratiques en matière de sécurité (~800 employés sensibilisés).

****

Dans le cadre de ses missions de service public et en tant qu'établissement public de santé et établissement support du GHT Sud Lorraine, le CHRU de Nancy doit assurer et garantir la sécurité des données qu'il détient pour lui-même et pour le compte d'autrui ainsi que des services qu'il délivre.

Principales réalisations :

- Accompagnement à la certification ISO/IEC 27001:2013 / HDS V1.1 2018 (Hébergement des Données de Santé) → **Certification obtenue par le CHRU à l'issue de la mission**.
- Mise à jour de l'ensemble des politiques, procédures et points de contrôles afin de garantir le maintien en conformité du SMSI.
- Accompagnement des équipés opérationnelles (IT, métiers) dans la mise en conformité des processus pour satisfaire aux exigences de la norme ISO/IEC 27001:2013 sur le périmètre HDS.
- Réalisation d'un audit à blanc basé sur le référentiel de conformité HDS pour vérifier le respect des exigences et préparer à la certification HDS.
- Suivi et résolution avec l'aide des équipes opérationnelles du reliquat de non-conformités.
- Animation et accompagnement lors de tous les entretiens de l'audit de certification avec l'auditeur externe et les équipes opérationnelles (10 jours).
- Réalisation de sessions de sensibilisation sur les risques et bonnes pratiques en matière de sécurité (~100 employés sensibilisés).

****

Lazard Frères est un groupe mondial dont l'activité se concentre sur le conseil financier (conseil stratégique, fusions-acquisitions, marchés de capitaux, levées de fonds), ainsi que sur la gestion d'actifs pour des clients institutionnels, entreprises ou particuliers.

Principales réalisations :

- Rationalisation de la démarche de conformité.
- CSP-SWIFT : réalisation d'une évaluation indépendante afin de garantir une position conforme pour l'échéance fin 2021, dans le contexte d'une migration partielle des opérations SWIFT vers un fournisseur de services cloud.
- Surveillance de la posture d'auto-évaluation pour assurer une position conforme :
  - EBA : soutien à la création d'un plan d'action et pilotage des actions de remédiation.
  - ACPR : dans le cadre d'un engagement volontaire de mise en conformité avec les normes ACPR, j'ai géré les écarts de conformité et piloté les actions correctives.
- Création d'une approche « guichet unique » pour les rapports de Cybersécurité aux homologues de Lazard (autorités, clients, partenaires, etc.).

****

Société de conseil en IT et Ingénierie, spécialisée dans les métiers du Digital, souhaite se lancer dans un projet de certification ISO 27001.

Principales réalisations :

- Entretiens avec le management (CEO, CFO, CTO, CIO, CISO, HR) pour comprendre les enjeux et les besoins dans le cadre de ce projet.
- Identification des actifs & processus à protéger.
- Réalisation d'une première évaluation de l'exposition aux risques majeurs (analyse de risques basée sur l'ISO 27005).
- Réalisation d'une analyse d'écart avec les 114 points de contrôles requis pour l'ISO/IEC 27001:2013 permettant de dimensionner le projet et la charge pour le client.
- Détermination du périmètre pour la certification.
- Identification des ressources internes et externes qui seront allouées au projet.

****

AXA Groupe Operations (GO) a établi en 2020 une stratégie d'indicateurs de risques (KRI) afin de mesurer la performance et l'efficacité de ses contrôles (KPI) de sécurité, mis en place dans le cadre de la norme ISO/IEC 27001:2013 .

Alors qu'AXA GO procède au déploiement complet de la stratégie KPI/KRI, il est essentiel de garantir la pertinence et la répétabilité systématique de la mesure des indicateurs.

Principales réalisations :

- Analyse de l'adéquation et l'agrégation des KRI définis pour fournir des informations significatives sur l'étendue de la réalisation des objectifs de sécurité.
- Rationalisation du nombre de mesures à suivre et maintenir (seuls les KPI qui déclenchent des décisions de gestion sont maintenus).
- Veiller à ce que le cycle Plan-Do-Check-Act (PDCA) soit pris en compte.
- Déploiement du processus de mesure des KPI et du reporting associé. Les mesures des KPI ont été validées lors d'un comité et communiquées à toutes les parties prenantes concernées.

****

VERISURE est le N°1 des Alarmes télé-surveillées en Europe.

Principales réalisations :

- Management par Interim: RSSI – Responsable de la Sécurité des Systèmes d'Information. Management d'une équipe de 3 experts sécurité.
- Mise en œuvre de projets de sécurité pour couvrir certains points de contrôles de la norme ISO/IEC 27001:2013 *(gestion des accès, sécurité des applications, Windows hardening, server management (EOL, patching), Identity & Access Management).*
- Accroissement de la sécurité des postes de travail dans le cadre de la mise en télétravail du personnel lors de la crise de Covid-19 *(blocage USB, chiffrement des disques durs, sensibilisation des utilisateurs).*
- Interventions régulières en Comité de Direction (1 fois par mois).

****

ADP est le leader mondial des solutions basées sur le Cloud proposant des services pour la gestion des Ressources Humaines, la gestion des temps et des activités, la paie, et la conformité.

Le déménagement des actifs et du personnel de la Direction des Systèmes d'Information a entraîné une modification du périmètre d'applicabilité (SOA) de la norme ISO/IEC 27001:2013 , nécessitant une révision complète du SMSI avant le passage des auditeurs en vue d'une recertification.

Principales réalisations :

- Mise à jour du Système de Management de la Sécurité de l'Information (SMSI) pour s'assurer que l'organisation ADP Global Enterprise Technology & Solutions maintient la confidentialité, l'intégrité et la disponibilité des informations clients.
- Mise à jour de l'ensemble des procédures et points de contrôles afin de garantir le maintien en conformité du SMSI.
- Analyse et mise à jour de la correspondance entre la politique de sécurité ADP et les contrôles de sécurité ISO/IEC 27001:2013 .
- Organisation et pilotage de l'intervention des auditeurs externes (5 jours).
- Animation des entretiens avec les équipes opérationnelles dans le cadre du processus de maintien de la certification ISO/IEC 27001:2013 (périmètre EMEA).

Expérience professionnelle *(CDI)*

cybervadis

Information Security Research Director

(Septembre 2016 - Septembre 2018 (2 ans)) - Paris, France

CyberVadis est la première plate-forme collaborative, permettant aux entreprises d'évaluer les performances en cybersécurité de leurs fournisseurs.

CyberVadis allie technologie et expertise pour fournir des "tableaux de bord de la cybersécurité" simples et fiables, couvrant 20 indicateurs de cybersécurité, 150 catégories d'achats et 120 pays.

Principales réalisations :

- Création d'un modèle de référence inspiré des standards Internationaux *(NIST, ISO27001, Shared Assessments, PCI-DSS, RGPD).*
- Conception d'un questionnaire d'évaluation d'un SMSI *(Système de Management de la Sécurité de l'Information d'une entreprise)* avec analyse de preuves, adaptable à la taille et au secteur de l'entreprise évaluée.
- Conception d'un modèle d'évaluation permettant une notation objective de la maturité du SMSI d'une entreprise.
- Intégration de questions pour vérifier la compatibilité des entreprises au RGPD.
- Développement d'un outil pour réaliser les évaluations et automatiser la notation.
- Recrutement et formation des analystes en charge de l'interprétation des questionnaires d'évaluation de la performance SMSI des entreprises.
- Avant-vente : présentation du modèle d'évaluation aux prospects dans le cadre de la démarche de commercialisation de la solution.
- Evangélisation / Intervention à divers événements pour promouvoir la solution :
  - Third Party and Supply Chain Cyber Security Summit (June 2017)
  - General Data Protection Regulation (GDPR) by Partech Ventures (Sept.2017) https://partechpartners.com/news/gdpr-seminar/
  - GDPR at Les Universités des Achats du CNA (May 2018) https://resources.ecovadis.com/fr/actualites-ecovadis/ecovadis-et-le-groupe-cr%C3%A9dit-agricole-aux-universit%C3%A9s-des-achats

SOCIETE GENERALE **Corporate and Investment Banking**

Information Security Risk Manager

(Mai 2007 - Août 2016 (9 ans et 4 mois)) - Paris, France

FDJ - Française des Jeux

Auditeur Interne

(Avril 2001 - Mai 2007 (6 ans) - Paris, France

KPMG Peat Marwick (CSC)

Consultant Senior

(Octobre 1997 - Avril 2001 (3 ans et 7 mois)) - Paris, France