# David LARBONI

**Cybersecurity freelance consultant**
**CISO as a Service**

**ISO 27001, HDS, WLA, CISSP**

**Keynote Speaker**

## Contact

📱 +33 6 62 74 25 63

@ davidlarboni@gmail.com

## Top skills

- ✓ ISO 27001 / ISO 27005 / HDS
- ✓ Information Security (ISMS)
- ✓ Vendor Risk Management
- ✓ Project Management
- ✓ GDPR

## Languages

🇬🇧 English (Full Professional)

🇩🇪 German (Professional Working)

## Education

ESCP EUROPE    *(1994 - 1997)*

**Master's Degree**, Marketing & IT

## Summary

- **Interim Management: CISO**
  *(Chief Information Security Officer)*

- **Information Security Certifications**
  - ✓ ISO 27001 « Lead Implementer »
    *(2013 & 2022 revisions)*
  - ✓ CISSP
  - ✓ NIST

- **Creation of a Vendor-Risk Management rating tool (CyberVadis®)**

- **Project Management**
  - ✓ Large scale deployment of hardware
  ISO 10006 « Quality Management Systems »

- **Management of internal staff**
  - ✓ up to 10 subordinates
  - ✓ up to 18 contractors

- **Contractor Management**
  - ✓ 11 contracts (computing services & consulting)

## Leisure

- Sports *(tennis, water-ski, snowboard)*

- Music *(piano & drums in a rock band)*

- Wine tasting

*I organize (as a hobby) premium Champagne learning & tasting dinners in fancy restaurants*

## Available for new challenges, beginning of September 2023

| 2022 | | | | | | | | | 2023 | | | |
| sep | oct | nov | dec | jan | feb | mar | apr | may | jun | jul | aug | sep |

**9 months - Paris, France**



No. 1 gambling operator in France, second largest European lottery and fourth largest in the world, FDJ also manages competitive activities – primarily online sport betting.

**Main achievements:**

- Supported PCI-DSS v3.2.1 RoC$^A$, ISO/IEC 27001:2013 and WLA-SCS:2020 (World Lottery Association) re-certification → **All three Certifications successfully obtained**.

- Updated all policies, procedures and control points to ensure maintenance of ISMS compliance.

- Supported operational staff (IT, business lines) in bringing processes into conformity to meet the requirements of the ISO/IEC 27001:2013 and WLA-SCS:2020.

- Carried-out a mock audit based on the compliance frameworks to verify compliance with requirements and prepare for ISO/IEC 27001:2013 and WLA-SCS:2020 certifications.

- Monitored and resolved the remainder of non-conformities with the help of operational teams.

- Organised, drove and provided support during all certification audit interviews (7 days).

- Implementation and support for the transition to the 2022 version of the ISO/IEC 27001 standard.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

| 2022 | | | | | | | | | 2023 | | |
| sep | oct | nov | dec | jan | feb | mar | apr | may | jun | jul | aug |

**9 months - Paris, France**



Les Restos du Coeur is an association law of 1901, recognized as being of public utility, which aims "to help and provide voluntary assistance to the poor, particularly in the food sector".

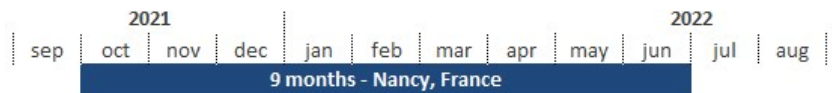**Main achievements** *(part-time assignment, 2 days / week)*:

- Interim Management: CISO – Chief Information Security Officer.

- Implemented the 3-year security plan resulting from an external security audit.

- Wrote, then promoted/disseminated and maintained the IS security policy.

- Established a business continuity plan and coordinated its implementation.

- Established and disseminated a safety culture within the association.

- Defined and implemented a security governance framework (reporting, risks, follow-up of actions, alerts).

- Provided awareness sessions on IS risks and best practices.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

|  | | | | | 2022 | | | | | | | | 2023 | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| jan | feb | mar | apr | may | jun | jul | aug | sep | oct | nov | dec | jan | feb | mar |
| | | 12 months - Paris, France | | | | | | | | | | | | |

LINEDATA is a global provider of software, services and value-added data dedicated to the financial sector.

**Main achievements:**

- Interim Management: CISO – Chief Information Security Officer.

- Supported SOC II certification.

- Monitored and resolved the remainder of non-conformities, following an external audit (pentest), with the help of operational teams.

- Provided awareness sessions on IS risks and best practices (~800 employees trained).

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

| | 2021 | | | | | | | | 2022 | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| sep | oct | nov | dec | jan | feb | mar | apr | may | jun | jul | aug |
| | 9 months - Nancy, France | | | | | | | | | | |

As part of its public service missions and as a public health establishment and support establishment for the GHT Sud Lorraine, the Nancy CHRU must ensure and guarantee the security of the data it holds for itself and on behalf of others as well as the services it provides.

**Main achievements:**

- Supported ISO/IEC 27001:2013 and HDS V1.1 2018 certification (Hosting of Health Data) - Health Information Privacy equivalent → Certification successfully obtained.

- Updated all policies, procedures and control points to ensure maintenance of ISMS compliance.

- Supported operational staff (IT, business lines) in bringing processes into conformity to meet the requirements of the ISO/IEC 27001:2013 standard for the HDS perimeter.

- Carried-out a mock audit based on the HDS compliance framework to verify compliance with requirements and prepare for HDS certification.

- Monitored and resolved the remainder of non-conformities with the help of operational teams.

- Organised, drove and provided support during all certification audit interviews (10 days).

- Provided awareness sessions on IS risks and best practices (~100 employees trained).

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Lazard Frères is a global financial group focusing on its financial advisory activity (strategic advice, mergers and acquisitions, restructuring, capital markets, fundraising), as well as on asset management for institutional, corporate and individual clients.

**Main achievements:**

- Drumbeat and rationalised the compliance approach.

- CSP-SWIFT: conducted an independent assessment and ensure a compliant position by the end of 2021, in the context of a partial migration of SWIFT operations to cloud service provider.

- Overviewed the self-assessment posture and ensured a compliant position:

  o EBA: supported the creation of an action plan and engaged follow-up actions accordingly

  o ACPR: as per a voluntary commitment to ensure compliance with ACPR standards, I managed compliance gaps and corrective actions

- Created and delivered a "one shop stop" approach for cybersecurity reporting to Lazard counterparts (authorities, clients, partners, etc.).

**************************************************************************************************

2021
jan | feb | mar | apr | may | jun | jul | aug | sep | oct | nov | dec
**3 months - Marseille, France**

**KLANIK**

IT and Engineering consulting company, specialized in the fields of Digital, wishes to embark on an ISO/IEC 27001:2013 certification project.

**Main achievements:**

- Interviews with management (CEO, CFO, CTO, CIO, CISO, HR) to understand the challenges and needs within the framework of this project.

- Identifid assets & processes to protect.

- Carrid-out an initial assessment of exposure to major risks (risk analysis based on ISO 27005).

- Carrid-out a gap analysis with the 114 control points required for ISO/IEC 27001:2013 to size the project and the load for the customer.

- Determined of the scope for certification.

- Identified internal and external resources that will be allocated to the project.

**************************************************************************************************

| | | | | | | | | | **2021** | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| jan | feb | mar | apr | may | jun | jul | aug | sep | oct | nov | dec | | | | | |

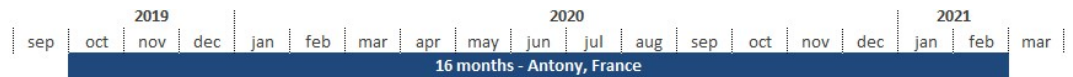**6 months - Paris, France**

AXA Groupe Operations (GO) has established in 2020 a risk indicator strategy (KRI) to measure the performance and effectiveness of its security controls (KPI).

As AXA GO proceeds to the full deployment of the KPI / KRI strategy, it is essential to ensure the relevance and systematic repeatability of the measurement of indicators.

**Main achievements :**

- Analysed the adequacy and aggregation of defined KRIs to provide meaningful information on the extent of achievement of security objectives.

- Rationalised the number of measures to be monitored and maintained (only the KPIs that trigger management decisions are maintained).

- Ensured that the Plan-Do-Check-Act (PDCA) cycle is taken into account.

- Deployed the KPI measurement process and associated reporting. KPI measurements must be validated during a committee meeting and communicated to all relevant stakeholders.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

| | **2019** | | | | | | | **2020** | | | | | | | | | **2021** | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| sep | oct | nov | dec | jan | feb | mar | apr | may | jun | jul | aug | sep | oct | nov | dec | jan | feb | mar | |

**16 months - Antony, France**

VERISURE is the leading provider of professionally monitored security solutions in Europe and present in Latin America.

**Main achievements:**

- Interim Management: CISO – Chief Information Security Officer. Management of a team of 3 security experts.

- Implemented security projects in order to cover some control points related to ISO/IEC 27001:2013 standard *(access management, application security, Windows hardening, server management (EOL, patching), Identity & Access Management).*

- Increased the workstation security to enable the staff to work from home during the Covid-19 crisis (USB blocking, hard disk encryption, user awareness).

- Provided information security updates at the Management Committee (once a month).

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

| | 2019 | | | | | | | | | | |
|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|
| jan | feb | mar | apr | may | jun | jul | aug | sep | oct | nov | dec |
| **10 months - Nanterre, France** | | | | | | | | | | | |

ADP is a comprehensive global provider of cloud-based human capital management (HCM) solutions that unite HR, payroll, talent, time, tax and benefits administration, and a leader in business outsourcing services, analytics and compliance expertise.

The relocation of the assets and staff of the Information Systems Department has led to a change in the statement of applicability (SOA) of the ISO/IEC 27001:2013 standard, requiring a complete revision of the ISMS before the venue of auditors in view of a recertification.

**Main achievements:**

- Updated the ADP ISMS to ensure that the ADP Global Enterprise Technology & Solutions organization maintains the confidentiality, integrity, availability, and privacy of client information.

- Updated all procedures and control points to ensure the maintenance of ISMS compliance.

- Analysed and updated the mapping of the ADP Security Policy and Standards against the ISO/IEC 27001:2013 security controls.

- Organised the venue of the external auditors (5 days) and the interviews with the operational teams.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

## Experience *(permanent position)*

# cybervadis

### Information Security Research Director

*(September 2016 - September 2018 (2 years)) - Paris, France*

CyberVadis operates the 1st collaborative platform, allowing companies to assess the Cybersecurity performance of their global suppliers.

CyberVadis combines technology and expertise to deliver simple and reliable "Cybersecurity scorecards", covering 20 Cybersecurity indicators, 150 purchasing categories and 120 countries.

**Main achievements:**

- Creation of the reference model based on International standards and frameworks (NIST, ISO-27001, Shared Assessments, PCI-DSS, GDPR)

- Conception of an evidence-based questionnaire tailored to a company's size and business sector

- Implementation of GDPR-related questions to assess a company's GDPR readiness

- Conception of a rating model providing an objective assessment of a company's Information Security Management System (ISMS)

- Development of a cloud-based tool to perform the assessments and automate the rating

- Implementation of the processes to on-board and assess a company's Cybersecurity (ISMS) performance

- Recruiting, building and training a team of (17) security experts in charge of assessing companies' Cybersecurity (ISMS) performance

- Mapping of our questionnaire against ISO-27001, NIST, SIG (Shared Assessment)

- Pre-sales engineering: presentation of the assessment model to prospects & clients

- Evangelism / Speaker at events:

  - 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*

**Corporate and Investment Banking**

## Information Security Risk Manager

*(May 2007 - August 2016 (9 years, 4 months)) - Paris, France*

## FDJ - Française des Jeux (french Lottery)

## Internal Auditor

*(April 2001 - May 2007 (6 years) - Paris, France*

## KPMG Peat Marwick (CSC)

## Senior Consultant

*(October 1997 - April 2001 (3 years, 7 months)) - Paris, France*