


PERSONAL INFORMATION **Dan Cimpean**

 Bucharest, Romania + Brussels, Belgium

 + 40 724 714 657 +32 497 59 38 27 +32 494 167 187

 dan.cimpean@cert.ro dcimpean@outlook.com

 <https://www.linkedin.com/in/dan-cimpean/>

Sex Male | Date of birth 26/08/1970 | Nationality Romanian

CURRENT

General Director, CERT-RO

WORK EXPERIENCE

FEB 2020 – APRIL 2020

Independent Consultant - Brussels, Belgium

Since February 2020 – following own decision to resign from Deloitte – operating as independent consultant and advisor in the areas of cyber security, threat intelligence, risk management, technology and digital transformation, compliance, cloud security and controls, policy, audit and assurance.

SEPT 2001 – JAN 2020

Partner - Deloitte Cyber Risk Services, Belgium, Brussels**Overall experience**

Over 18 years of full-time experience with Deloitte Belgium out of which 10 and half years at Cyber Risk Partner level, leading the Deloitte cyber risk services towards European Institutions for 7 years. Member of Deloitte North-South Europe Public Sector Cyber Leadership team. Leader of Deloitte NIS Directive Workgroup. Member of Board of Directors of Deloitte Consulting and Advisory, Belgium.

Thanks to the cyber engagements executed for ENISA, European Commission, other European agencies, Dan had an extensive involvement with Operators of Essential Services (OES) and Digital Service Providers (DSP) in all sectors listed by the NIS Directive. A key focus of these was establishing capabilities for cyber risk and threat identification, on profiling cyber threat actors and on preparing the involved stakeholders for developing threat and risk mitigation processes and mechanisms.

Dan directly led multiple contracts, assignments and projects for the European Commission (DIGIT, DG CONNECT, DG EMPL, DG AGRI, DG ECHO, DG HOME, DG JUST, DG REGIO, DG GROW, DG EAC, DG COMM, DG BUDGET, DG MOVE, DG SANTE, Secretariat General, IAS), for the European Council, European Investment Bank and key European agencies like: ENISA, eu-LISA, EUIPO, EMSA, ESMA, SRB, EDA, EMA, EFSA, EIOPA, ECDC, ECHA, CEDEFOP, EBA, F4E, EDPS, EASA, CDT. He also assists key trans-national major organisations in Brussels, like NATO and EUROCONTROL.

Actively involved in supporting major European cyber security policy, regulatory, legal and operational initiatives, programmes and developments, in particular related to NIS Directive, GDPR, Cybersecurity Act, EU data strategy, AI, capacity building and funding at EU and national level. Dan is active in key European-level technology and cyber security workgroups focused on international cooperation, certification and standardization, trust building, information exchange and capability building initiatives, assisting for these several major organisations, EU Member States competent authorities, law enforcement, national/governmental CSIRTs/CERTs and private actors.

Dan has proven experience in a variety of cyber advisory projects, in cyber capacity and capability building, advanced threat readiness and preparation, red/purple/blue teaming exercises, SIEM intelligence, technology architecture, cyber crisis management and response, and risk assessments and investigations. He performed multiple reviews of technology infrastructure, organizational and governance for compliance with regulations, standards, frameworks and good practices. Also, was leading on regular basis cyber incident response, ransomware investigations and data loss incidents.

He has extensive expertise in performing a variety of policy-related engagements with main focus on technology, regulatory compliance, cyber security, privacy and data protection, but also on cloud, IoT, resilience, crisis management, net neutrality, top level domains, audio-visual media, 5G, etc. In terms of policy making, impact assessment and rollout, Dan succeeded to build and lead a professional team specialized in stocktaking, analysis and recommendations on latest policy, compliance and regulatory developments, and on roll-out of regulatory, data protection, privacy and cyber technologies, standards and frameworks at EU, national and industry sector level.

Strong experience and track record in interacting with CXOs, CIOs, CISOs, Heads of Units, technology leaders and other senior executives for public and private sector clients. Leading complex engagements, tenders, contractual and operational delivery of large-size contracts (multi-million Euro, many of them with involvement of consortium partners, subcontractors and independent experts).

Operational experience (for over 6 years) as the Functional Risk Leader (FRL) for Deloitte Risk Advisory Belgium business unit:

- > 550 full-time professionals,
 - > 70 Million Euro business on annual basis,
 - > 1000 clients portfolio overall,
 - > 500 projects and engagements for professional services delivered on annual basis.
- ✓ Responsible for the overall risk and quality management (risks related to reputation, regulatory compliance; contracts, confidentiality, quality, third parties, privacy);
 - ✓ Responsible for the review and approval (from a risk management perspective) of all contracts and projects of Deloitte Risk Advisory business unit at the pre-sales and sales phase;

Extensive track record as speaker and facilitator of trainings, workshops and exercises for decision makers, policy officers, operational teams, data protection coordinators and cyber technical experts from European institutions, NATO, governmental organisations, and from the private sector actors.

Dan also did lead for several years the group of professionals within Deloitte Belgium that provides ICT audit, information security audit, data mining for the purposes of fraud detection, cloud risk assessment and compliance, and third party assurance services. This group is focused on executing reviews, audits and validations based on a variety of standards and frameworks: ISO 2700X family of standards, COBIT, ITIL, PCI-DSS, Cloud Security Alliance, ISAE 3402, SSAE 18, SOC 1, 2 & 3; ISRS 4400, Webtrust, or based on European Commission's frameworks, decisions and regulations.

- In particular, for European Institutions and/or for large international organisations,
- ✓ Professional support and solutions to comply with the EU legal framework and advice on key policy, legislative and regulatory developments in Brussels and EU Member States;
 - ✓ Cyber research and studies: CCB Belgium, European Commission, ENISA, EMSA, ISACA, CEPS;
 - ✓ Information security and IT audits: European Commission (DG DIGIT, DG EMPL, DG GROW, DG AGRI, DG COMM), European Agencies (F4E, EIOPA, ECHA, EBA, ENISA, FRA);
 - ✓ Security and Privacy Risk Assessments: European Commission (Secretariat General, DG ECHO, DG EMPL, DG DIGIT, DG EAC, DG GROW, DG HOME, DG JUST, IAS), European Agencies (EDPS, ECDC, CDT, EMA, EMSA, CEDEFOP, ENISA, Shift2Rail), MasterCard, Worldline, ING, Isabel, Société Internationale de Télécommunications Aéronautiques (SITA);
 - ✓ Business Continuity and Crisis Management: ENISA, SRB, EASA, EIOPA, DIGIT, DG EMPL;
 - ✓ SOX compliance: Mastercard, Kaneka, Daikin, BNPP Fortis, Campbell, Avnet;
 - ✓ Internal Audit: ISABEL, Mastercard, NATO, EUROCONTROL, European Commission, Worldline;
 - ✓ Third Party Assurance Audits: Synsis, Worldline, CACEIS, Belfius, BICS, Nexans, Mambu, Société Internationale de Télécommunications Aéronautiques (SITA), European Union Intellectual Property Office (EUIPO), European Commission DG DIGIT (WiFi4EU).

Relevant recent operational projects and clients (see below only a selection)

2009 – 2019 for European Union Agency for Cybersecurity (ENISA) multiple research studies, reports and cyber advisory projects

Role: Leader of Deloitte cyber security team executing the work, quality assurance responsible, contract responsible and subject matter expert. Dan has directly served the EU Agency for Cybersecurity (ENISA) with a variety of cyber security research, governance and operational advisory services since 2007. In particular, Dan supported ENISA operational departments and units but also gained extensive experience in interacting with and in advising the key governance bodies of the Agency:

- ✓ Executive Director, Core Operations Department, Resources Department;
- ✓ Management Board;
- ✓ Advisory Group (former Permanent Stakeholders Group);
- ✓ National Liaison Officers (NLOs).

Background: ENISA works closely together with the EU Member States and other key stakeholders from the industry to deliver advice and solutions as well as improving their cyber security capabilities. It also supports the development of a cooperative response to relevant threat actors, emerging cyber threats and risks, large-scale cross-border cyber incidents or crises and since 2019, it has been drawing up cyber security certification schemes. Dan executed hands-on the following projects for ENISA:

- ✓ *Good practices in innovation on cyber security under National Cyber Security Strategies (NCSS) – 2019*
- ✓ *Support for organizing the European Cyber Security Challenge – 2019, 2018, 2017*
- ✓ *Good practices in interdependencies' risk assessment – 2018*
- ✓ *Good practices on interdependencies between Operators of Essential Services (OES) & Digital Service Providers (DSP) – 2018*
- ✓ *Incident Reporting Framework for the NIS Directive – 2018*
- ✓ *Study and guidelines for the implementation of mandatory cyber incident reporting – 2017*
- ✓ *Dependencies of Essential Services Operators (OES) on Digital Service Providers (DSP) – 2017*
- ✓ *Assessing Cyber Security in Member States in the Air Transport Sector – 2017*
- ✓ *Assessing Cyber Security in Member States in the Finance Sector – 2017*
- ✓ *Cyber Security Incident Tracking & Taxonomies Study – 2016*
- ✓ *A good practice guide of using taxonomies in incident prevention and detection – 2016*
- ✓ *Study on EU-level Crisis Management and Applicability to Cyber Crises – 2015*

- ✓ *Study on Cyber Security Information Sharing: Overview of Regulatory & Non-regulatory Approaches – 2015*
- ✓ *Report on Information Sharing and Common Taxonomies between CSIRTs and LEAs – 2015*
- ✓ *ENISA's CSIRT-related capacity building activities – Impact Analysis Update 2015*
- ✓ *Supporting the CERT community: Impact Assessment and Roadmap Study – 2014*
- ✓ *International Conference on Cyber Crisis Cooperation and Exercises – 2013*
- ✓ *Inventory of CERT activities in Europe – 2012*
- ✓ *Study on Minimum Security Measures for Smart Grids – 2012*
- ✓ *Study on CERT Operational Gaps and Overlaps – 2011*
- ✓ *Study on cyber security challenges in the Maritime Transportation Sector – 2010*
- ✓ *Policy Recommendations on Baseline Capabilities of National & Governmental CERTs – 2010*
- ✓ *Provision of Network and Information Security Country Reports for 30 Countries – 2011, 2010*
- ✓ *Study on Measurement Frameworks and Metrics for Resilient Networks and Services: Challenges and Recommendations Report – 2010*
- ✓ *Analysis of regulatory and policy issues related to the resilience of the Public eCommunications networks – 2009.*

2018 – 2019 for National CSIRT-CY and Cyprus Office of the Commissioner of Electronic Communications and Postal Regulation (OCECPR) <https://csirt.cy>

Role: Deloitte project team leader for project CEF 2016-CY-IA-0129 financed by European Commission for establishing, development and enhancement of capabilities for Cyprus National CSIRT.

Background: Dan was leading the Deloitte cyber security and advisory services for the following:

- ✓ Activity 1 – Project Administration / Project Management / Risk Management
- ✓ Activity 2 – Improvement of the CSIRT-CY Domain Network and Security Design
- ✓ Activity 3 – Improvement of the CSIRT-CY Domain Network and Security Configuration
- ✓ Activity 4 – Preparatory actions for connecting the CSIRT-CY infrastructure to the already implemented infrastructures (of other CSIRTs/CERTs in EU etc.)
- ✓ Activity 5 – Prepare CSIRT-CY for the accreditation process
- ✓ Activity 6 – Procurement, Support and Maintenance of CSIRT-CY Infrastructure (HW and SW)
- ✓ Activity 7 – Increasing the maturity of the CSIRT-CY internal policies, procedures, guidelines
- ✓ Activity 8 – Training of CSIRT/CERT staff on Advanced Digital Forensics
- ✓ Activity 9 – Overall trainings to the CSIRT/CERT personnel and key stakeholders
- ✓ Activity 10 – Liaising with other CEF cyber security projects
- ✓ Activity 11 – Design, Requirements, Recommendation and Implementation support for new or existing CSIRT/CERT tools
- ✓ Activity 12 – Communication and stakeholder interaction activities for the CSIRT-CY
- ✓ Activity 13 – Activities to prepare and improve CSIRT-CY for the compliance with the General Data Protection Regulation (GDPR – Regulation (EU) 2016/679) and with the applicable laws and regulations from the Republic of Cyprus
- ✓ Activity 14 – Activities to prepare CSIRT-CY for compliance with new regulations coming from the rollout of the NIS Directive
- ✓ Activity 15 – Implementation, support and testing activities for CSIRT-developed or -adopted tools
- ✓ Activity 16 – Review, improvements, development and deployment of increased CSIRT/CERT capabilities including security and resilience of own organization and infrastructure

2019 – 2020 for European Commission DG DIGIT feasibility study for the future EU Open Source Intelligence (OSINT) service 'ShadowFinder'

Role: Leader of the Deloitte tender team, cyber subject matter expert

Background: The European Commission will develop and maintain a future cloud security service named 'Pro-active OSINT-based cloud security service - ShadowFinder'. This will use open source intelligence data to identify risks to the Commission and initiate risk remediation processes. Key tasks:

- ✓ Draft and validate the ShadowFinder vision document, in line with best practices;
- ✓ Perform a detailed requirement analysis (including preliminary legal/functional/interoperability analysis) and document the technical and organisational requirements and key functionalities;
- ✓ Define the ShadowFinder OSINT processes, assets and use cases, detailed organisational functionalities, required information models and security controls, high-level solution architecture and detailed technical specifications;
- ✓ Identify mature OSINT technologies, data sources and providers suitable for ShadowFinder service;
- ✓ Draft and validate the roadmap for ShadowFinder implementation;
- ✓ Draft a formalised Final Report for validation by the European Commission.

2018 – 2019 for Security Made In Letzebuerg G.LE. (SMILE / CIRCL) for the Distributed Denial of Services Detection Devices (D4) Platform – project CEF 2017-LU-IA-0099

Role: Deloitte team leader for the project CEF 2017-LU-IA-0099 financed by European Commission

Background: The Deloitte Cyber Risk team led by Dan has supported SMILE (CIRCL) Luxembourg for:

- ✓ Improving the visibility and situational awareness of Distributed Denial-of-Service (DDoS) attacks at national, European and global levels;
- ✓ Enhancing faster and more effective CSIRT cooperation and information sharing mechanisms to detect, monitor, and react to denial of service traffic accurately;
- ✓ Improving the preparedness and cooperation of the CSIRTs in EU through advisory and support services regarding DDoS, secure coding and delivery;
- ✓ Ensuring legal and regulatory compliance of the D4 platform with among other General Data Protection Regulation (GDPR) and the NIS Directive.

2019 – 2020 for European Commission DG MOVE Transport Cyber-Security Toolkit

Role: Leader of the Deloitte tender team, cyber subject matter expert

Background: The project performs a study on the main cyber security threats that transport companies are exposed to, the potential consequences and cyber-risk mitigation actions, and creation of an interactive “cyber-security toolkit” that will contain all these information. Intended target audience of the results of the study consists of the entire workforce active in the transport sector: aviation, maritime and land (rail and road) transport. The key tasks executed:

- ✓ Stock taking, analysis and review of cybers threats and consequences on transport operations;
- ✓ Document practices enhancing cyber security in transport companies;
- ✓ Develop a toolkit of good cyber security practices (proof of concept, pilot of the electronic version);
- ✓ Develop the awareness documents (proof of concept, awareness materials and visuals);
- ✓ Present the project at meetings of the stakeholders advisory groups;
- ✓ Final report for the Commission and external members of the security committees/experts group.

2018 – 2019 for X-ISAC Luxembourg establishing best practices for setting up an ISAC - project CEF 2016-LU-IA-0098

Role: Deloitte team leader for the project CEF 2016-LU-IA-0098 financed by European Commission

Background: The Deloitte Cyber Risk team led by Dan has supported X-ISAC Luxembourg in the delivery of the project for preparing a key actions and guidance documents on how to set up an ISAC. X-ISAC (pronounced cross-ISAC) is the supporting Information Sharing and Analysis Center for other ISACs, information sharing communities or CSIRT networks and provides core software, cross-sector threat intelligence, taxonomies and open standards. Information sharing is now a key requirement in cyber security as well as in intelligence, and counter-terrorism. The activities performed included:

- ✓ Preparing materials for awareness workshops on ISACs and compliance with the General Data Protection Regulation (GDPR) and the Network and Information Systems Directive (NIS Directive);
- ✓ Recommendations and guidelines in ensuring compliance with the GDPR and NIS Directive in information-sharing communities published by entities such as CIRCL, ENISA, IAPP, the Article 29 Working Party or other bodies with the relevant legal, policy and technical expertise;
- ✓ Drafting a guidance article on setting up ISACs including:
 - First steps: where to start when establishing an ISAC (e.g. funding mechanism, benefits of participating in the community of Information Sharing and Analysis Centers);
 - Legal: how to ensure compliance with the GDPR and the NISD;
 - Technical aspects: tools and platforms available in information sharing community (MISP);
- ✓ Best practices and recommendations towards ISAC stakeholders.

2018 – 2020 for eu-LISA professional services for Maintenance in Working Order (MWO) of the Schengen Information System (SIS II)

Role: SIS II MWO Deputy Security Officer, Deloitte Leader for SIS II MWO - Security Risk Management

Background: The European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA) is responsible for the management and the operation of SIS II. A Maintenance in Working Order (MWO) contract for SIS II was awarded.

Dan is responsible for the following transversal services of SIS II MWO Security Risk Management:

- ✓ SIS II MWO Security Risk Management Plan + SIS II MWO Security Plan;
- ✓ SIS II MWO ISMS implementation report and Security Report (monthly);
- ✓ SIS II MWO Audit questionnaires and Business Continuity Plan;
- ✓ Contribute to the cyber incident management actions;
- ✓ Contribute to security audits organised by eu-LISA.

2013 – 2020 for European Commission DG EMPL advisory services to support the Electronic Exchange of Social Security Information (EESSI) system security, privacy and data protection in operational mode

Role: Deloitte Project Leader and Security and Data Protection Team Leader of the EESSI project

Background: the Electronic Exchange of Social Security Information (EESSI) is an ICT system built and operated by the European Commission and connecting the EU Member States' administrations in charge of social security. EESSI aims to connect > 20.000 social security institutions across Europe and support over 900 million data exchanges per year. Data exchanges takes place between national competent administrations of participating countries in following areas governed by the EU Regulations:

- ✓ Sickness, maternity and equivalent paternity benefits
- ✓ Old-age pensions, pre-retirement and invalidity benefits
- ✓ Survivors' benefits and death grants
- ✓ Unemployment benefits, family benefits
- ✓ Benefits in respect of accidents at work and occupational diseases

Dan was leading since 2013 the Deloitte team's work related to EESSI project (approximately 1.000 man-days of cyber security, data protection and privacy consulting and advisory services per year).

- ✓ Defining and reviewing the implementation of the EESSI security requirements;
- ✓ Coordination and execution of EESSI security testing in line with frameworks: OWASP, ISO 27001, NIST, ENISA and using specific tools: CAST, SonarQube, READY API (SOAP UI, LOAD UI);
- ✓ Operational security and data protection guidance towards the Member States using EESSI;
- ✓ Cyber incident response & cyber forensics support for the EESSI system in production mode;
- ✓ Implementing the processes and infrastructure for detection, monitoring and addressing of cyber threats, and for reporting on the threat evolution and on the involved risk posture;

- ✓ Security monitoring of the EESSI environment and management of cyber issues and incidents;
- ✓ Preparation steps for security certification of the EESSI software components;
- ✓ Disaster Recovery Plan (DRP) / Business Continuity Plan (BCP) for EESSI and business continuity support to the Member States in view of using EESSI;
- ✓ Ethical hacking campaigns, cyber security awareness focused on EESSI stakeholders and users;
- ✓ Static security source code review for each major release of system's components, pen-testing;
- ✓ Support to Member States for defining and integrating the EESSI Security Plan;
- ✓ Elaborate the EESSI Personal Data Protection Guide and provide GDPR compliance support;
- ✓ Organise Member State GDPR-focused workshops/trainings
- ✓ Establish EESSI privacy and data protection programme and communication;
- ✓ Ongoing data protection and privacy helpdesk services.

2019 – 2020 for European Commission DG CONNECT for the maintenance and evolution of the Core Service Platform Cooperation Mechanism for CSIRTs (MeliCERTes Facility)

Role: Leader of Deloitte tender team for this project (SMART 2018/1024), cyber subject matter expert

Background: MeliCERTes is a tool provided by DG-CONNECT to the national and governmental CSIRTs for supporting them in their daily operation. It establish a common base foundation for a minimal interconnected toolset for CSIRTs. This project aims to the existing foundation as bootstrapped in MeliCERTes into long-term maintainable and a more operationalised platform, meant to support the cooperation efforts within the CSIRTs Network. For this project, Dan led the effort for assembling an operational delivery consortium formed by Deloitte, Belgium & Luxembourg and:

- ✓ NASK (Naukowa i Akademicka Sieć Komputerowa), Poland
- ✓ SMILE/CIRCL (Security Made in Lëtzebuerg), Luxembourg
- ✓ CERT.AT (nic.at GmbH), Austria
- ✓ CERT-EE/RIA (Riigi Infosüsteemi Amet), Estonia
- ✓ SK-CERT, Slovakia

2018 – 2020 for European Commission DG DIGIT Open Source Software audits via Bug Bounties (OSS-BB) for EU Institutions (contract jointly delivered by Deloitte and intigrity)

Role: Dan is the Deloitte Team Leader and responsible/owner of this framework contract

Background: The performed contract is under the European Commission's EU-FOSSA 2 (Free and Open Source Software Auditing) programme and involve execution of security audits via bug bounties supported by the ICT platform of intigrity (www.intigrity.com) and involving management of stakeholders, validation and reporting of bugs, interaction with the community of ethical hackers executed by Deloitte. The project target open-source software or software produced by the European Commission's services in preparation for open sourcing. To date, the following open source software components have been tested: KeePass, FluxTL, 7-ZIP, Digital Signature Services (DSS), Drupal, GNU C Library (glibc), PHP Symfony, Apache Tomcat and WSO2.

2019 for Single Resolution Board (SRB) benchmarking and fit analysis for SRB's crisis management software application system

Role: Leader of Deloitte team, contract responsible and benchmark subject matter expert.

Background: The benchmarking and fit analysis was executed to assist SRB in its efforts for assessing the market readiness for providing specialised software application to support SRB's crisis management processes, both in preparatory phases and during the response phases. This benchmarking and fit analysis was performed based on information provided by the software application providers contacted, or based on available information and documentation collected and analysed. The work also included:

- ✓ Further defining the list of criteria for the market analysis;
- ✓ Performing an in-depth analysis for the top 5 software applications fitting the SRB business and ICT requirements (including demos);
- ✓ Performing a SWOT analysis and fit gap assessment for the top 3 selected software applications;
- ✓ Presenting the conclusions (including results and roadmap for implementation) in a comprehensive report followed by a presentation to SRB management.

2019 for European Commission DG DIGIT pilot project for readiness and compliance with data protection rules for European Commission's Microsoft Office365 and internal e-mail system

Role: Leader of Deloitte team, contract responsible and benchmark subject matter expert.

Background: This project, conducted by Deloitte team led by Dan for DG DIGIT, was the first large-scale project launched by the European Commission in order to evaluate and manage data protection and information security risks related to Microsoft Office365 and the internal e-mail system of the view of Regulation (EU) 2018/1725 on the protection of individuals with regard to the processing of personal data by EU institutions, bodies, offices and agencies and on the free movement of such data:

- ✓ Assessed current readiness to efficiently tackle the obligations arising from the new regulation;
- ✓ Set priorities on the basis of an approach that takes into account the purpose of the law, the operational realities and an understanding of the relevant risk;
- ✓ Proposed concrete actions to support the achievement of compliance;
- ✓ Compared processing activities described by Microsoft technical specifications of various Office365 applications and the processors agreement offered by Microsoft to the European Commission;
- ✓ Implemented a complete Data Protection Impact Assessment (DPIA) for Microsoft Office365 and the internal email system of the European Commission, in line with Regulation (EU) 2018/1725.

2019 for eu-LISA study on the future architecture for Interoperable IT Systems

Role: Leader of the security architecture track of the study, subject matter expert

Background: The European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (i.e. eu-LISA) provides operational management of essential large-scale IT systems asylum, border management and migration policies of EU. Performed a study to define future architectures for interoperable IT Systems, conduct impact assessments, integration and migration plans. The scope included new and existing interoperability components:

- ✓ New – European Search Portal (ESP); Shared Biometric Matching Service (S-BMS); Common Identity Repository (CIR); Multiple-Identity Detector (MID); Common Repository for Reporting and Statistics (CRRS);
- ✓ Existing – Entry/Exit System (EES); European Travel Information Authorisation System (ETIAS); European Criminal Records Information System for Third-Country Nationals (ECRIS-TCN).

2019 – 2020 for European Maritime Safety Agency (EMSA) study on security and interoperability solutions for SafeSeaNet (SSN)

Role: Leader of the Deloitte team, subject matter expert, quality assurance responsible

Background: EMSA serves EU's maritime interests for a safe, secure, green and competitive maritime sector. SafeSeaNet is the European Union's maritime information and exchange platform. It supports the maritime safety, port and maritime security, marine environment protection, and safety and efficiency of maritime traffic. SSN is composed of a network of 27 National SSN systems operated by EU Member States and a Central SSN system operated by EMSA. The main objective of the project is provision of consultancy services to elaborate a comprehensive study on security and interoperability solutions for SSN under the Common Information Sharing Environment (CISE) maritime domain initiative context.

The results of the study will define the measures and implementation options to ensure that within SSN:

- ✓ Data will be genuine and from bona fide sources (authenticity);
- ✓ Data will be accessible and usable upon request by an authorised entity (availability);
- ✓ Data will not be disclosed to unauthorized recipients (confidentiality);
- ✓ Data exchanged during the transactions will not be altered (integrity);
- ✓ All transactions will take place and will be attributable to identifiable individuals (non-repudiation);
- ✓ Access will only be granted to those who are authorized to (authorization);
- ✓ Exchanging data will require prior authentication of the parties (authentication);
- ✓ SSN information will be exchanged between all information systems involved (interoperability).

2019, 2015, 2012 for EUROCONTROL ICT Service Provision Benchmark for the European Aeronautical Information Service (AIS) Database (EAD)

Role: Leader of Deloitte team, contract responsible and benchmark subject matter expert:

Background: The EAD services of EUROCONTROL provide a reference database of quality-assured critical aeronautical information:

- ✓ Safety, high-level data validation contributing to the improvement of aeronautical information/data integrity, thus improving the overall safety levels;
- ✓ Economics, reducing the overall costs of the provision of AIS throughout the ECAC area;
- ✓ Uniformity, the EAD Service is provided to AIS data users at all times;
- ✓ Quality, procedures for data provider users based on ISO 9001 and compliance with the ED-153 - Guidelines for ANS Software Safety Assurance.

The Deloitte team led by Dan performed an in-depth ICT service provision benchmark for the outsourced EAD services (IT Services, Software Development, Data Operations and Training Services) delivered by the involved two key EUROCONTROL contractors from Germany and Austria.

2019 & 2014 for European Union Intellectual Property Office (EUIPO, ex-OHIM) SOC 2 service auditor report for the database supporting enforcement of intellectual property rights and the related processes (i.e. the EUIPO Enforcement Database)

Role: Leader of Deloitte team who performed the service audit examination and issuance of the SOC 2 certification report for EUIPO's Enforcement Database.

Background: The audit confirmed the suitability of design and operating effectiveness of controls for the security, availability, processing integrity and confidentiality for EUIPO processes and controls supporting the database for enforcement of intellectual property rights.

2013 – 2019 European Commission DG EMPL – Support for the Security Expert Forum (SEF) for EESSI - Electronic Exchange of Social Security Information system

Role: Dan was the project leader for the support work provided to DG EMPL concerning the regular interaction and work with the members of the Security Expert Forum (SEF) established by European Commission and the involved 35 countries in the EESSI project.

Background: The support activities involve:

- ✓ Direct support to the SEF, including preparation of the SEF quarterly meetings hosted in Brussels, communication of meeting agenda, preparation of the deliverables to be debated and approved in the SEF meeting, preparation of meeting minutes and report;
- ✓ Managing the content of the published information security artefacts information exchange platform used to share the information with the involved SEF members from 35 countries;
- ✓ Documenting the decisions taken and the approval of EESSI security artefacts, including addressing the SEF comments, remarks and recommendations for improvement;
- ✓ Formal communication towards both EC and the involved representatives of the Member States.

2016 – 2018 for European Commission DG CONNECT SMART 2014/1079 preparatory activities for the launch of the Connecting Europe Facility (CEF) Core Cooperation Platform for Computer Emergency and Response Teams (CERTs/CSIRTs) in the European Union

Role: Leader of the consortium executing the project and cyber security subject matter expert

Background: European Commission DG CONNECT is responsible for the cyber security strategy of the EU to ensure a safe, secure, trustworthy and resilient digital environment. In the overall context of the Connecting Europe Facility (CEF) Cyber Security work programme, the preparatory activities for the CEF Core Service Platform (CSP) for cooperation mechanisms aimed for:

- ✓ Establishment and maintenance of a governance structure of the information sharing platform with The European Commission, ENISA, CERT-EU, representatives of EU Member States, of National Competent Authorities and of the national / governmental CSIRTs, to steer the process;
- ✓ Identification by the Governance Board of the detailed technological functionalities for the technical part of the core cooperation platform from the list of available and mature options and the preparation of its physical infrastructure and definition of the required security levels of the platform;
- ✓ Providing individual organisational and technical support to an initial group of n/g CSIRTs aimed to identify their individual (technical, organisational and legal) challenges for enabling interoperability with the future CSP, including the requirements from European legislation (NIS Directive, GDPR);
- ✓ Promotion of best practice support of other CSIRTs to facilitate alignment to the core cooperation platform and mechanisms;
- ✓ Engagement of the Member States to outline a medium-term roadmap on how to implement and extend the core platform to ensure it is available to all Member State CSIRTs. This included awareness-raising activities and training with the European CSIRTs stakeholder community;
- ✓ Establish cooperation with existing EU-level and Member States cyber security initiatives and will create links with existing infrastructure, processes and tools and apply existing standards.

2014 – 2017 for European Commission DG AGRI audits of information systems security of the Paying Agencies in the EU Member States, Candidate and Potential Candidate Countries

Role: Dan was project coordinator, subject matter expert and contract responsible for this framework contract for audits of Information Systems Security (ISS) for Paying Agencies in 35 countries.

Background: this contract involves executing audits in line with criteria regarding information security under Regulation (EC) 885/2006 and ISO 27001:

- ✓ Analysis of the legal basis and validation of the technical of the ISS audit;
- ✓ Defining the technical aspects of the testing methods employed for the ISS Audit;
- ✓ Review of IT, infrastructure and Information Systems Security architecture and key controls;
- ✓ Execute the test plans, prepare and review workpapers, reporting and recommendations.

2013 for European Commission DG CONNECT feasibility study and preparatory activities for the implementation of a European Early Warning and Response System (EWRS) against cyber-attacks and disruptions

Role: Leader of Deloitte team, cyber security subject matter expert and quality assurance responsible

Background: The overall aim of EWRS is to provide operational support and facilitate the technical cooperation between the relevant response capabilities within the European Union:

- ✓ Analyse the feasibility of implementing a European early warning and response system against cyber-attacks and disruptions; assessment of interoperability aspects;
- ✓ Define in detail its scope and the technical, organisational, legal and economic aspects of such a system; and to propose an implementation plan.

2012 – 2015 for EASA, ECHA, EBA, EIOPA, F4E, BEREC system compliance validation for the local IT system of European Agencies (IT systems that provide accounting information)

Role: Dan was the leader and key subject matter expert of the work executed by Deloitte in order to ensure an independent IT system compliance validation.

Background: The key tasks performed included:

- ✓ Verification of access controls to systems software, databases, data files, user ID's and passwords;
- ✓ Verification of procedures in place for safeguarding data (backup system);
- ✓ Verification of data exchange between modules, of control systems in place for storage of data;
- ✓ Verification of protection measures in place, which control the production and output of legally binding documents and confidential information in printed as well as electronic format;
- ✓ Verification of the reliability and correctness of the output of statistical data delivered;
- ✓ Defining the overall approach, executing the key technical reviews and security testing of the involved IT systems versus the framework defined by European Commission DG BUDGET;
- ✓ Analysis of the IT architecture and security compliance aspects;
- ✓ Review of software security and testing performed by the Agency against compliance requirements.

2011 for European Commission DG COMM assessment of the contractors, processes and infrastructure supporting the European Commission's media monitoring activities

Role: Dan was the project leader of this project and subject matter expert

Background: The key tasks executed included:

- ✓ Identification of issues, gaps and risks, proposed recommendations and action plans
- ✓ Assessment of current IT systems / software / information flows that support DG COMM processes for production of media monitoring products (e.g. DPR, DNS, DND) and for publication and printing;

- ✓ Review of organisational aspects within the current processes in scope;
- ✓ Analysis of interdependencies and constraints in the current overall contractual, operational and governance architecture / structure.
- ✓ Detailed report with actions and recommendations.

ICT & Information Security audit and compliance reviews

Role: Dan did lead for several years the group of professionals within Deloitte Belgium that provides ICT & information security audit and compliance reviews and third party assurance services. This group also performed data mining and audit services as part of the financial audit mandates performed by Deloitte:

- ✓ Audit of internal controls in the key business processes (e.g. revenue, expenditure, accounting, HR, inventory, fixed assets, treasury, budgeting);
- ✓ Audit of IT processes (Information Security, IT Operations, Change Management, Problem Management, Incident Management, IT Budgeting);
- ✓ Data mining procedures, data analytics, cyber forensics investigations;
- ✓ Agreed upon-procedures focused on security, incident response, ransomware response;
- ✓ Audits in line with international assurance standards: ISAE 3402, SSAE 18, SOC (1, 2 & 3), ISRS 4400, Webtrust, Systrust, SAS 70, COSO letters etc.

Business or sector Professional services – cyber risk services, general advisory, ICT and security audit

1999 - 2001 Senior Consultant - Ernst & Young, Bucharest, Romania

As Senior Consultant, Dan has focused on information security, forensics, internal audit, external audit, risk management, business continuity planning, change management, performance/processes improvement and development of policies/procedures. His key clients were mainly located in Romania, Greece, Turkey and Hungary. Amongst the key roles and responsibilities:

- ✓ Audit of client's ICT processes, ICT organisation and ICT infrastructure based on internationally accepted standards and frameworks;
- ✓ Investigation of fraud incidents and of ICT security incidents;
- ✓ Review the application controls and implementation of large-scale integrated application suites (e.g. SAP, MFG/PRO, Oracle, Exact) and made recommendations for risk mitigation;
- ✓ Perform walkthrough, inquiries and sample tests. Issuing recommendations on specific controls related to the IT processes which support the client's business and accounting processes;
- ✓ Assess the strategy and systems of the clients; assist the clients in strategy planning, business-IT alignment, software implementation and partners/vendors selection;
- ✓ Review of client's business plans, industry trends, market environment and financial key indicators;
- ✓ Develop client relationship and representing the company in pre-sale contacts, presentations.

Business or sector Professional services – audit and advisory

1996 - 1999 IT Department Deputy Manager - Transdata, Ploiesti, Romania

As IT Department Deputy Manager, Dan has focused on:

- ✓ Managing the activity of a 19 persons team (IT staff, engineers, computer operators, technicians).
- ✓ Reviews of technical IT and security architecture (pre- and post- implementation reviews) to ensure compliance with government regulations and internal security and IT policies and procedures.
- ✓ Responsible for defining and implementation of the IT Security policy of the company. Reviewing on daily basis the IT security incidents and taking action for risk mitigation.
- ✓ ICT quality management, testing and conformity review for applications and ICT solutions provided by the company to its clients.
- ✓ Manage Service Level Agreements (SLAs), Operational Level Agreements (OLAs) and Key Performance Indicators (KPIs) in the field of overall ICT and information security
- ✓ Implementation of company's own IT infrastructure (hardware, software, databases, telecommunication network, web site and interfaces with key business partners)
- ✓ Represent the company in relationship with clients, business partners, and authorities.
- ✓ Identify the technical and security needs of client's projects, developing implementation and action plans, preparing budgets and providing the best solutions for the customer requirements.
- ✓ Negotiating of contracts, technical details, financial and delivery terms with the clients.

Business or sector Telecom operator, software house and ICT integrator

1994 - 1996 Quality Assurance Engineer**UZUC, Ploiesti, Romania**

As Quality Assurance Engineer, Dan has focused on:

- ✓ Managing the corporate quality management and quality assurance program and procedures. In charge with the application and maintaining in accordance with ISO 9001, DIN, ASME, and ASTM requirements, and with contractual specifications.
- ✓ Defining and documenting the Quality Management System processes, in line with the structure and content of ISO 9001. Preparing the Quality Assurance Lab for the ISO 9001 certification.
- ✓ Providing internal trainings on the quality management principles and concepts:
 - The Plan, Do, Check, Act (PDCA) cycle
 - The relationship between quality management and customer satisfaction
 - Commonly used quality management terms and definitions as given in ISO 9000
 - The process approach used in quality management
- ✓ Executing quality assurance tests, audits and analyses, observing the preparation, distribution and

- ✓ revision of quality assurance documents.
- ✓ Managing the activity of the Non-Destructive Testing Laboratory, drafting, implementing and bringing up-to-date the Quality Manual and Quality Assurance procedures.

Business or sector Manufacturing

EDUCATION AND TRAINING
PAST 2 YEARS TRAININGS

TRAININGS FOLLOWED IN THE PAST 2 YEARS

- ✓ 2019 – ITS² (IT Security Risk Management) by European Commission DG DIGIT
- ✓ 2019, 2018, 2017 – Deloitte European Union Business University – classes focused on the services tailored for the European Institutions (2 days)
- ✓ 2018, 2017 – Attending the CERT-EU Conference, Brussels – (conference, 2 days)
- ✓ 2018 – General Data Protection Regulation (GDPR) Training – by Deloitte (classroom, 2 days)
- ✓ 2018 – Deloitte EMEA Cyber Wargaming training (1 day) – Brussels
- ✓ 2018 - Cyber Academy - CIRO 102 - Security Incident Response (e-Learning, 30 hours)
- ✓ 2018 - Responding to Non-Compliance With Laws and Regulations (NOCLAR) For Client Service Professionals Performing Non-Audit Services (DPM 1553) (e-Learning, 2 hours)
- ✓ 2018 - Responding to Non-Compliance With Laws and Regulations (NOCLAR) for Auditors (ID: GLB4199) (e-Learning, 2 hours)

2012 & 2010 ISACA Information Security & Risk Management Certificate

ISACA

- ✓ Information Security & Risk Management

2012 Certified Information Security Manager (CISM) License 1321466

ISACA

- ✓ Common body of knowledge for information security management
- ✓ Information risk management as the basis of information security
- ✓ Proof of minimum five years of work experience in the field of information security, with at least three years in the role of information security manager

2009 Certified in the Governance of Enterprise IT (CGEIT) License 0903060

ISACA

- ✓ Framework for the Governance of Enterprise IT
- ✓ Strategic Management, Benefits Realization
- ✓ Risk management and risk optimization
- ✓ Resource management and optimization, performance measurement
- ✓ Experience supporting the governance of an enterprise's information technology

2009 Isabel 6 eBanking Technical Consultant Certificate

ISABEL NV/SA, Belgium

- ✓ Electronic Banking Technology Architecture, Electronic Banking Infrastructure

2006 Certified Internal Auditor (CIA) License 63771

The Institute of Internal Auditors (IIA)

- ✓ The only globally accepted certification for internal auditors and remains the standard by which individuals demonstrate their competency and professionalism in the internal auditing field
- ✓ Proof of minimum five years verified experience in internal audit

2005 ITIL V3 Foundation Certified License 803586

Examen Instituut voor de Informatica (EXIN), Netherlands

- ✓ Awareness of the key elements, concepts and terminology used in the ITIL Service Lifecycle
- ✓ Knowledge of the linkages between lifecycle stages, the processes used and their contribution to service management practices

2004 Certified Information Systems Auditor (CISA) License 0435538

ISACA

- ✓ Audit, control, monitor and assess an enterprise's IT and business systems.
- ✓ Assurance knowledge, skills, experience and credibility to leverage standards
- ✓ Manage vulnerabilities, ensure compliance, offer solutions, institute controls
- ✓ Proof of minimum five years of professional IS auditing, control or security work experience

1999 Business Management Diploma

Institut Franco-Roumain d'Administration des Entreprises, Bucharest, Romania

- ✓ Corporate management, operations management
- ✓ Accounting, human resources, financial accounting
- ✓ Programme and project management

1994 Quality Testing Diploma

Quality Testing School of Physics Institute Bucharest, Bucharest, Romania

- ✓ Quality testing standards and frameworks
- ✓ Quality testing procedures and management

1994 Master in Physics and Engineering "Magna Cum Laude"

University of Bucharest, Romania

- ✓ Master in Physics and Engineering

PERSONAL SKILLS

Mother tongue(s) Romanian

Other language(s)

	UNDERSTANDING		SPEAKING		WRITING
	Listening	Reading	Spoken interaction	Spoken production	
English	C2	C2	C2	C2	C2
French	B1	B1	B1	B1	B2

Levels: A1/A2: Basic user - B1/B2: Independent user - C1/C2 Proficient user
[Common European Framework of Reference for Languages](#)

- Communication skills**
- ✓ Regular speaker at conferences and seminars and provides both internal and external trainings in the area of policy, regulatory compliance, international cooperation, information security, cyber, ICT and information security audits, assurance standards, risk management;
 - ✓ Excellent skills in summarising value propositions and in presenting/translating complex situational and operational data into actionable intel for decision makers and non-technical management;
 - ✓ Extensive experience in facilitating workshops, seminars, conferences and trainings that involve a variety of stakeholders, security, and ICT professionals, business representatives;
 - ✓ Design and delivery of trainings and exercises, including awareness, onboarding and technical trainings with the aim of improving the capabilities and skills of the teams, management, boards;
 - ✓ Experience in facilitating workshops and meetings for validation of results and findings.

- Organisational / managerial skills**
- ✓ Experience in leading the Deloitte Cyber Risk services team for the European Institutions;
 - ✓ Strong business network and connections and ability to work in public-private and private-private alliances, partnerships and initiatives;
 - ✓ Interaction and coordination with multiple internal (Board, top management, legal, risk, compliance, etc.) and external actors (regulators, government agencies, EU bodies, CSIRTs, cyber service providers, private business partners etc.);
 - ✓ Leading sensitive cyber incident response, ransomware investigations and data loss incidents;
 - ✓ Coordination of projects, missions, planning, preparation, request for information, scheduling;
 - ✓ Project coordination and management for large cross-border engagements in line with international project management frameworks and methodologies (PRINCE2, PMBOK, PM³);
 - ✓ International coordination skills – multiple projects covering all EU Member States, EEA and US;
 - ✓ Responsible for operating teams of more than 20-30 cyber and risk management advisors;
 - ✓ Operational experience (for over 6 years) as the Functional Risk Leader (FRL) for Deloitte Risk Advisory Belgium business unit:
 - > 550 full-time professionals;
 - > 70 Million Euro business on annual basis;
 - > 1000 clients portfolio overall;
 - > 500 projects and engagements for professional services delivered on annual basis;
 - ✓ Strong experience in leading the business relationship, tendering and contractual aspects for large-size tenders and contracts for the public and private sector.

- Job-related skills** Good knowledge and practical experience with:
- EU regulations, directives, frameworks, standards, methodologies, policies**
- ✓ European Commission DIGIT - IT Security Risk Management (ITSRM²) methodology
 - ✓ European Commission Decision 2017-46 Security of communication and information systems in EC
 - ✓ European Commission Decision 2017-8841 - Implementation Rules for C2017-46
 - ✓ European Commission Decision 2018-559 - Implementation Rules for C2017-46 Art.6.pdf
 - ✓ European Commission Decision 2006-3602 concerning the security of information systems used by the European Commission and its implementing rules and standards
 - ✓ European Commission DG BUDGET - guidelines and check list for evaluation of local IT systems
 - ✓ European Commission - Risk Management Implementation Guide
 - ✓ European Commission DIGIT - ISIP Web applications secure development guidelines
 - ✓ Regulation (EU) 2018/1725 on the protection of individuals with regard to the processing of personal data by EU institutions, bodies, offices and agencies and on the free movement of such data
 - ✓ Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation GDPR)
 - ✓ Regulation (EU) 2019/881 on ENISA and on information and communications technology cybersecurity certification (The Cybersecurity Act)
 - ✓ Directive (EU) 2018/1808 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive)
 - ✓ ENISA Information Assurance Framework
 - ✓ EU Guide to Financial Issues relating to FP7 Indirect Actions

ICT, information security, risk management frameworks and standards

- ✓ COBIT 4.1 & 5; CobiT Online, RiskIT, ValIT – ISACA
- ✓ ITSRM², ITIL, TOGAF, PCI DSS, CRAMM, BSI-Standards 100-1, 100-2
- ✓ ISO 9001:2015 “Quality Management”

- ✓ ISO/IEC 27001:2013 "Information technology - Security techniques – Information security management systems requirements specification"
- ✓ ISO/IEC 27002:2013 "Information technology - Code of practice for information security mgmt.."
- ✓ ISO/IEC 27005:2008 "Information security risk management"
- ✓ ISO/IEC 27031:2011 "Information technology - Security techniques - Guidelines for information and communications technology readiness for business continuity"
- ✓ ISO 22301:2012 "Societal security – Business continuity management systems"
- ✓ ISO 31000 "Risk Management"
- ✓ NIST Special Publication 800-53, NIST Special Publication 800-53A - Guide for Assessing the Security Controls in Federal Information Systems and Organizations
- ✓ Risk management methodologies: EBIOS, CRAMM, ISO 2700X, COSO ERM
- ✓ COSO Enterprise Risk Management - Integrated Framework - Committee of Sponsoring Organizations of the Treadway Commission

Audit standards and frameworks, other standards and frameworks

- ✓ International Standards for Audit (ISA)
- ✓ IIA Standards (Institute of Internal Auditors)
- ✓ International Public Sector Accounting Standards (IPSAS)
- ✓ ISRS 4400 - International Standard on Related Services (ISRS) 4400, "Engagements to Perform Agreed-upon Procedures Regarding Financial Information"
- ✓ ISAE 3402 - International Standard on Assurance Engagements (ISAE) 3402 – "Assurance Reports on Controls at a Service Organization"
- ✓ ISAE 3000 - International Framework for Assurance Engagements, "Assurance Engagements Other than Audits or Reviews of Historical Financial Information"
- ✓ SSAE 18 (and previously SSAE 16); SOC 1, 2 & 3

Project management

- ✓ PM², PMBOK, PRINCE 2

Digital competence

SELF-ASSESSMENT				
Information processing	Communication	Content creation	Safety	Problem solving
Proficient User	Proficient User	Proficient User	Proficient User	Proficient User

Levels: Basic user - Independent user - Proficient user
[Digital competences - Self-assessment grid](#)

Computer skills acquired as part of the ongoing project work

- ✓ Microsoft® Office suite (Word, Excel, PowerPoint, Visio, Project), Microsoft® SharePoint
- ✓ Deloitte Cyber Security Framework Platform
- ✓ MISp, RTIR, MONARC, MITRE ATT&CK™
- ✓ CAST, BlackDuck, SecurEnds, Okra, Hive, Mattermost, Barac, LINEAL, Egress
- ✓ KNIME, ELK, Splunk, Qlik, Maltego
- ✓ Nessus, IntelMQ, RetroShare, Cuckoo Sandbox, Ghidra
- ✓ Atlassian JIRA, Atlassian Confluence
- ✓ Qualitative and quantitative analysis tools: NVIVO, SPSS, STATA
- ✓ Operating Systems: Windows 10, 8, 7, Vista, Win XP, MS-DOS, Linux, UNIX, OS/400
- ✓ Networks: TCP/IP Ethernet networks, switching & routing
- ✓ ERPs: SAP R/3, MFG/PRO, Baan, JD Edwards, Exact, Navision, Axapta, Oracle eBusiness
- ✓ ACL, IDEA, SekCheck, AS2, eQSmart, Eurekfy SAGE
- ✓ Industry Print 4 & 5: process modelling
- ✓ Security protocols (SSL/TLS, IPsec, VPN), Unified Modeling Language (UML)
- ✓ RUP@EC and Agile RUP@EC (software development methodology)

Computer skills acquired as part of self-study, e-Learning and on-job training

- ✓ Cylance, Aves NetSec, CounterCraft, BlueDog, Tessian,
- ✓ Eclipse for Testers (Jubula and Mylyn)
- ✓ MySQL, ABAP, Business Objects; MediaWiki software; Microsoft BizTalk
- ✓ Rational Quality Manager (RQM), Rational Team Concert (RTC), Rational Unified Process (RUP)
- ✓ Apache Jmeter, Apache Maven

Computer skills acquired by attending training sessions, presentations and workshops

- ✓ AbuseHelper, QRadar, READY API (SOAP UI, LOAD UI, Hermes JMS)
- ✓ Cymulate, PatrOwl, Sunbren, SureVine, ClearView, ImmersiveLabs, RazorSecure

ADDITIONAL INFORMATION

<ul style="list-style-type: none"> Publications Presentations Projects Conferences Seminars Honours and awards Memberships References Citations Courses Certifications 	<p>Publications</p> <ul style="list-style-type: none"> ✓ Co-author of “Women in cyber in context of the European Cyber Security Challenge” – 2019 ✓ Co-author of “Deloitte’s view on the implementation of Regulation (EU) 2018/1725 – GDPR for European Union Institutions” – 2019 ✓ Task Force Member for the Report: “Strengthening the EU’s Cyber Defence Capabilities” published by the Centre for European Policy Studies (CEPS) Brussels – 2018 ✓ Co-author of reports for ENISA - European Union Agency for Network and Information Security: <ul style="list-style-type: none"> • <i>Good practices in innovation on cyber security under National Cyber Security Strategies</i> – 2019 • <i>Report of the European Cyber Security Challenge</i> – 2019, 2018, 2017 • <i>Good practices on interdependencies between OES and DSPs</i> – 2018 • <i>Good practices in interdependencies’ risk assessment</i> – 2018 • <i>Incident Reporting Framework for the NIS Directive</i> – 2018 • <i>Study and guidelines for the implementation of mandatory incident reporting</i> – 2017 • <i>Study on Dependencies of Essential Services Operators on Digital Service Providers</i> – 2017 • <i>Assessing Cyber Security in Member States in the Air Transport Sector</i> – 2017 • <i>Assessing Cyber Security in Member States in the Finance Sector</i> – 2017 • <i>Incident Tracking & Taxonomies Study</i> – 2016 • <i>A good practice guide of using taxonomies in incident prevention and detection</i> – 2016 • <i>Study on EU-level Crisis Management and Applicability to Cyber Crises</i> – 2015 • <i>Study on Cyber Security Information Sharing: Overview of Regulatory & Non-regulatory Approaches</i> – 2015 • <i>Report on Information Sharing and Common Taxonomies between CSIRTs and LEAs</i> – 2015 • <i>Leading the way - ENISA’s CSIRT-related capacity building activities - Impact Analysis</i> – 2015 • <i>Supporting the CERT community: Impact Assessment and Roadmap Study</i> – 2014 • <i>International Conference on Cyber Crisis Cooperation and Exercises</i> – 2013 • <i>Inventory of CERT activities in Europe</i> – 2012 • <i>Study on Minimum Security Measures for Smart Grids</i> – 2012 • <i>Study on CERT Operational Gaps and Overlaps</i> – 2011 • <i>Study on cyber security challenges in the Maritime Transportation Sector</i> – 2010 • <i>Policy Recommendations on Baseline Capabilities of National & Governmental CERTs</i> – 2010 • <i>Network and Information Security Country Reports - 30 European Countries</i> – 2011, 2010 • <i>Study on Measurement Frameworks and Metrics for Resilient Networks and Services: Challenges and recommendations</i> – 2010 • <i>Analysis of regulatory and policy issues related to resilience of Public eCommunications networks</i> – 2009. ✓ Co-author of report for Assessment of the Public Procurement System in Romania, published by European Commission DG REGIO – 2011 ✓ Co-author of ISACA book “CobiT and Application Controls – A Management Guide” ✓ Co-author of the Risk Map for European Institutions – prepared by Deloitte for the use of European Commission, European Parliament and European regulatory agencies - 2010 ✓ Co-author of Cloud Security Alliance Security Controls Framework for Cloud Providers and Consumers (the Cloud Controls Matrix - CCM v1.2).
---	---

Presentations, Conferences, Seminars

- ✓ 2020 – Speaker at the Let’s Manage IT Live online event on “Addressing cyber risks while managing uncertainty and complexity”
- ✓ 2019 May – Speaker at the MITRE ATT&CK User Workshop, EUROCONTROL, Brussels
- ✓ 2018 Oct – Facilitator of Deloitte European-wide webinar training “NIS Directive”
- ✓ 2018 May – Facilitator of Deloitte European-wide webinar training “Opportunities for cyber funding: Connecting Europe Facility (CEF) & Horizon 2020 programmes of the European Commission”
- ✓ 2016 May – Speaker at EuroCACS Conference, Dublin
- ✓ 2013 June - Facilitator of ISSA-BE workshop “Security frameworks for smart grids”, Brussels
- ✓ 2013 Apr – Speaker at the Trust in Digital Life & Cyber Security and Privacy EU Forum Conference, Brussels. Topic: “A European view on assurance frameworks for cloud computing”
- ✓ 2013 Jan – Facilitator of Deloitte European-wide training “Standards for Attestation Engagements 16 (SSAE 16, also known as SOC 1) to Deloitte Audit Managers, Directors and Partners
- ✓ 2012 May - ENISA – EC Workshop on Certification and Cyber Security of Smart Grid Components
- ✓ 2011 Dec - Deloitte European-wide webinar for Deloitte Managers, Directors and Partners: International assurance standards - ISAE 3402 standard
- ✓ 2011 Nov – Facilitator of ENISA Maritime Cyber Security Seminar, Brussels
- ✓ 2011 Nov – Facilitator of Deloitte European-wide webinar training “International Assurance standards - ISAE 3402”
- ✓ 2011 Feb – Facilitator of Deloitte European-wide training “International Assurance Standards - ISAE 3402”, Prague. This training was addressed to Deloitte audit Managers and Directors
- ✓ 2010 Sept – Speaker at the North American Information Security and Risk Management Conference 2010, ISACA, Las Vegas – “Assurance Frameworks for Cloud Computing”
- ✓ 2010 Nov - European Information Security and Risk Management Conference ISACA, Vienna – “Assurance Frameworks for Cloud Computing”
- ✓ 2010 Sept – Facilitator of Deloitte European-wide training International Assurance Standards - ISAE 3402, SAS 70, ISRS 4400”, Prague
- ✓ 2010 March – Speaker at ISACA EuroCACS Conference
- ✓ 2009 Oct – Facilitator of Deloitte European-wide training, Prague: Business Process and System Risk Assessment

- ✓ 2008 Apr – IT Internal Audit in Banking Event, Brussels
- ✓ 2008 Oct – Facilitator of Deloitte EU training “Business Process and Risk Assessment”, Prague
- ✓ 2008 Sept – Facilitator of Deloitte EU training “Design & Execute Internal Audit Programs”, Lisbon

Major contracts won as where Dan was the tender leader or key contributor

- ✓ European Commission DG EMPL Framework Contract CASIS Lot 1 Information System Development Services (Business Intelligence Applications, Data Processing and Information Management Applications, Data Modelling, Data Warehouse, Enterprise Architecture, Workflow and Business Management) – overall value 100.000.000 Euro
- ✓ European Commission DG EMPL Framework Contract CASIS Lot 2 Information System Supporting Services (IS Quality & Audit, IS Security, IS Requirement Analysis, IS Specific Studies, User Assistance, Administration, Coordination) – overall value 85.000.000 Euro
- ✓ European Commission DG DIGIT Framework Contract DIGIT/A3/PO/2017/037 for Open Source Software audits via Bug Bounties for the EU Institutions (OSS-BB) – overall value 1.000.000 Euro
- ✓ European Defence Agency 19.CAP.OP.302 Framework Contract for the provision of “Cyber Defence Capability Development Services” - LOT II: exercises related to “Comprehensive Cyber Senior Decision-Making (CC SDM)” and “OHQ/FHQ Level Cyber Defence Operational Planning (Cyber Phalanx)” – overall value 800.000 Euro
- ✓ European Commission DG DIGIT Framework Contract for Advice, Benchmarking and Consulting Services in Information and Communication Technology – ABC IV Lot 2 – Benchmarking services (Benchmarking and Delivery Quality Review) – overall value 24.500.000 Euro
- ✓ European Commission DG DIGIT Framework Contract for Advice, Benchmarking and Consulting Services in Information and Communication Technology – ABC IV Lot 3 – Consulting Services (High Level Consultancy and Studies) – overall value 144.000.000 Euro
- ✓ ENISA F-COD-13-T22 Framework Contract for supporting the CSIRT/CERT community – overall value 1.000.000 Euro
- ✓ ENISA F-COD-13-T26 Framework Contract for supporting cyber crisis cooperation exercises & other related activities – overall value 250.000 Euro
- ✓ ENISA F-COD-16-T32 Framework Contract for Supporting Critical Information Infrastructures Protection activities – overall value 600.000 Euro
- ✓ European Commission DG AGRI Framework Contract AGRI/2013/J1/01 for the audit of Information Systems Security of the Paying Agencies in the EU Member States, Candidate and Potential Candidate Countries – overall value 2.800.000 Euro
- ✓ European Commission DG AGRI Framework Contract AGRI/2017/H1/02 for audit of Information Systems Security and IT applications of the Paying Agencies in the EU Member States and in IPARD II Beneficiary Countries – overall value 1.090.000 Euro

Memberships

- ✓ Active member of ISACA (www.isaca.org)
- ✓ Active member of ISSA Information Systems Security Association (www.issa.org)
- ✓ Active member of Institute of Internal Auditors (www.iaa.org)
- ✓ Active member of the C-SIG Certification Group organised by DG CONNECT and ENISA
- ✓ Active member of the Deloitte North-South Europe Public Sector Cyber Leadership team
- ✓ 2009 – 2016 Member of the Board of Directors of Deloitte Bedrijfsrevisoren / Réviseurs d'Entreprises, Belgium
- ✓ 2016 – 2020 Member of the Board of Directors Deloitte Consulting and Advisory, Belgium