Cesare Gallotti

# *Curriculum Vitae*

**Cesare Gallotti**
(Milan – Italy, 11 February 1973)
Address: Ripa di Porta Ticinese 75 - 20143 Milan - Italy
Web: http://www.cesaregallotti.it

**Educational background**

University degree in Mathematics, achieved in Università degli Studi of Milan, in March 1999. The degree thesis was about "Cryptography, protocols and cryptanalysis"

**Certificates of competence**

- Lead Auditor ISO/IEC 27001 qualified by AICQ-SICEV;
- Quality Lead Auditor (ISO 9001) qualified by AICQ-SICEV;
- ITIL Expert and ITIL 2011 Foundation certificates issued by Exin;
- ITIL 4 Foundation certificate issued by Axelos on 2019;
- ITIL 4 Managing Professional Certificate issued by Axelos on 2020;
- Lead Auditor ISO/IEC 20000 following itSMF schema and accredited trainer for related courses;
- Auditor ISO 28000;
- Lead auditor ISO 22301;
- Certified Information Systems Auditor (CISA) qualified by ISACA;
- Post-University Degree in Computer Forensics year 2009;
- "Pass with Merit" Business Continuity Institute examination in 2011;
- Agile Scrum Master by Exin;
- Prince 2 Foundation and Prince 2 Practitioner issued by Exin;
- Service Integration and Management Foundation issued by Exin;
- Certified Information Privacy Professional Europe (CIPP/E) issued by IAPP in 2018.
- Europrivacy implementer course and auditor course.

**Languages**

English and French, very good in writing and reading, with professional practice in several projects in Europe and Africa.

**Professional experience**

FROM NOVEMBER 2008

Free-lance consultant.

- Italian expert at ISO/IEC JTC 1 SC 27 WG1, with the participation to the editing groups for ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27003, ISO/IEC 27006, ISO/IEC 27013, ISO/IEC 27701.
- For the Italian standardization body (UNINFO), member of the translation group for the ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27005 standards.
- Consultancy for the implementation of information security management systems according to ISO/IEC 27001 (also with extension to ISO/IEC 27017 and 27018).
- Consultancy for the implementation of IT service management systems according to ISO/IEC 20000-1.
- Consultancy for risk assessment and establishment of the information security treatment plan.
- Consultancy for the implementation of business continuity management systems.
- Consultancy for the implementation of quality management systems according to ISO 9001.
- Consultancy for the compliance with personal data protection (GDPR) legal requirements.
- Consultancy for the compliance with administrative responsibility (similar to SOX) legal requirements.
- Third party audits and assessments on information security, quality and service management systems in Italy, Morocco, Spain, Greece, Hungary and South Africa for the Certification Body DNV GL Business Assurance.
- Third party audits as Technical expert for the certification body DNV GL Business Assurance for software medical devices UE marking against applicable directives and standards.
- Trainer for AICQ-SICEV and IRCA accredited Lead Auditor ISO/IEC 27001 courses in Italy and Spain.
- Trainer for ISO/IEC 20000 courses for DNV GL Business Assurance.
- Trainer for ITIL Foundation courses accredited by Exin and APMG.
- Trainer for Business Continuity and ISO 22301 courses for DNV Italia.
- Design and supply of a 5-days Quality Assurance course in English for an organization in the engineering sector.

APRIL 2008 – NOVEMBER 2008

Consultant and trainer for Quint Wellington Redwood (www.quintgroup.com) for Information Security, IT Service Management based on ITIL and Quality Management.

- Trainer, in Italy and abroad, for ITIL Foundation and ISO/IEC 20000 courses accredited by Exin or itSMF.
- Consultancy for the implementation of an IT Service Management System implementation.
- Consultancy for the implementation of a Quality Management System.

Collaboration with Exin (www.exin.nl) for the development of professional certification schemes in Information Security.

NOVEMBER 2002 - MARCH 2008

Lead Auditor and ICT Schemes Responsible in Det Norske Veritas Italia (now DNV GL Business Assurance Italia S.r.l.), Agrate Brianza (MI).

- Technical responsibilities for ICT certification schemes, updating of services, knowledge management for employees and contractors, accreditation schemes compliance.
- Lead Auditor for Information Security Management Systems according to ISO/IEC 27001:2005, carrying out audits in Italy and abroad.
- Lead Auditor for activities related to IT Service Management System according to ISO/IEC 20000-1:2005 and ITIL best practices.
- Lead Auditor for Quality Management Systems according to ISO 9001:2000 in IT, servicing, finance and manufacturing sectors.
- Technical Reviewer for Contact Centres certification projects according to UNI 11200:2006.
- Designer and trainer for Auditor and Lead Auditor courses according to ISO/IEC 27001:2005 (accredited by CEPAS and AICQ-SICEV) and ISO/IEC 20000.
- Participant of reviews of ISO International Standards for UNINFO.

JULY 2001 - NOVEMBER 2002

Consultant and Project Manager in Intesis S.p.A., Milano

APRIL 1999 - JUNE 2001

Consultant and Project Manager in Securteam S.r.l., Milano

With responsibilities for:

- implementing information security management systems and related procedures;
- advising and consultancy for the implementation of cryptographic algorithms to be used in communication systems, for the analysis of payment systems based on credit and debit cards in Europe, for the implementation of an automated systems for drugs delivery in hospitals;
- consultancy for the compliance to personal data protection laws in the manufacturing, health, insurance, banking and engineering sectors;
- development, for Intesis S.p.A., of its proprietary risk assessment methodology.

All the consultancies were based on the delivery of solutions according to customers' needs from a strategic and governance point of view. For the Risk Assessments, methodologies such as Defender and CRAMM were used.

**Projects** See Annex A

**Publications**

Continuous activities:

- From October 2008: editor of the "*IT Service Management News*" Newsletter (http://www.cesaregallotti.it/newsletter.htm);
- from 2017: articles for "ICT Security magazine" (www.ictsecuritymagazine.com).

Other activities

- 2002: book "Information Security - Risk Analysis and Management", ed. FrancoAngeli (www.francoangeli.it), whose table of content and presentation you can read (in Italian);
- 2003-2005: coach in the post-university degree "Organizations and illegal actions: how to design Business Security" by Space Bocconi of Milan, for the "Evaluation and certification criteria for the information systems security" module;
- February 2006: article "The new ISO 27001:2005" published in ICT Security;
- December 2006: lecturer for AIEA (Associazione Italiana IS Auditors, www.aiea.it) about requirements in ISO/IEC 27001:2005 against BS 7799-2:2002;
- January 2009: publishing of the Risk Assessment methodology "*VERA*" for Information Security;
- June 2009: lecturer at ECL 2009 on "*Privacy and Organizations*";
- August 2009: paper *"Acquisition and analysis of an iPhone (Apple) device*, on *Cyberspazio e Diritto*, vol. 10 no. 2 August 2009;
- September 2009: paper "*An easy Risk Assessment method*", on ICT Security, September 2009;
- November 2010: lecturer for Club 27001 in Paris on "*Case study: ISO/IEC 27001 and ISO/IEC 20000-1 assessment*";
- March 2011: lecturer to the Security Summit on "Integrated Management Systems – How ISO/IEC 20000 can support the ISO/IEC 27001";
- November 2011: lecturer for DFA on "ISO/IEC 270xx standards";
- January 2012: lecturer for Assintel on "Using the Cloud in security: technical hints";
- 7 June 2012: lecturer in "Les 2 èmes assises de la Certification", for the Association des Certificateurs du Maroc in Rabat (Maroc) on "*Protéger vos actifs informationnels dans un contexte concurrentiel: L'ISO 27001 un outil incontournable. Les méthodes pratiques pour identifier les vulnérabilités et les menaces. Retours d'expérience de Logica North Africa*" ;
- July 2012: paper "*Information security and IT service management*", U&C July/August 2012, Milan;
- 2013: participation in the AIEA research group on the new European Regulation on data protection;
- 2013: participation in the AIEA group for the translation of CISA manual;
- 2013: with Fabio Guasconi, Quaderno Clusit 009, "*Certificazioni Professionali in Sicurezza Informatica 2.0*";

- 2013: co-author for "*Information security management and personal data protection in SME*", UNINFO;
- 2019: book "Consapevolmente cloud" ("Consciously cloud") as member of the Oracle Community for Security;
- 2020: book "IoT Security" as member of the Clusit Community for Security;
- 2021: book "Artificial intelligence and security" as member of the Clusit Community for Security;
- 2022: book "Digital risk. Innovation and resilience. Knowing, addressing, and mitigating the digital risk" as member of the Clusit Community for Security;
- 2022: member of the working group for the Italian translation of ISO/IEC 27002:2022;
- 2014, 2017, 2019 and 2022: book "*Information security*", self-published;
- 2023: member of the working group for the Italian translation of ISO/IEC 27001:2022;
- 2023: book "Supply chain security" as member of the Clusit Community for Security.

All free available publications are on http://www.cesaregallotti.it/art_pres.htm.

**Other professional experiences**

- Since 2002: collaboration with Selexi (www.selexi.it) for the production of tests for selection of personnel.
- Since 2019: President of the Digital forensics alumni (DFA) association (members are the attendants to the Post-University courses on Computer Forensics and Personal data protection managed by the Università Statale di Milano.

Cesare Gallotti

**Annex A: Projects**

| *Year* | *Project Type* | *Sector* |
|---|---|---|
| 1999 | Implementation of an information security management system and related procedures | Bank |
| 1999 | Advising and consultancy for the implementation of cryptographic algorithms to be used in communication systems | TLC |
| 2000 | Consultancy for the compliance to Italian Data Protection laws | Health |
| 2000 | Advising and consultancy for the analysis of payment systems based on credit and debit cards in Europe | Research centre |
| 2000 | Consultancy for the compliance to Italian Data Protection laws | Automotive |
| 2000 | Consultancy for the compliance to Italian Data Protection laws | Insurance |
| 2000 | Implementation of an information security management system and related procedures | IT SP for banking |
| 2001 | Advising and consultancy for the implementation of an automated systems for drugs delivery in hospitals | Research centre |
| 2001 | Implementation of an information security management system and related procedures based on ISO/IEC 15408 | Chemical |
| 2001 | Consultancy for the compliance to Italian Data Protection laws | Accounting |
| 2001 | Consultancy for the compliance to Italian Data Protection laws | Engineering |
| 2002 | Consultancy for the implementation of an information security management system according to ISO/IEC 27001 | IT SP - Credit risk |
| 2002 | Implementation of an information security management system and related procedures | Food |
| 2002 | Consultancy for the compliance to Italian Data Protection laws | TLC |
| 2002 | Implementation of an information security management system and related procedures | Insurance |
| 2008 | Consultancy for the implementation of an IT service management system according to ISO/IEC 20000-1 | Transport and logistic |
| 2008 | Consultancy for the implementation of a quality management system according to ISO 9001 | IT SP |
| 2009 | Consultancy for the compliance with Administrative Responsibility (similar to SOX) legal requirements | Engineering |
| 2009 | Consultancy for the implementation of an information security management system according to ISO/IEC 27001 | Reselling of electronic components |
| 2009 | Assessment on the technical and organizational accuracy of customer satisfaction data gathering and reporting process. | Automotive |
| 2010 | Consultancy for the implementation of an information security management system according to ISO/IEC 27001 and an IT service management system according to ISO/IEC 20000 | IT SP - Banking |
| 2010 | Consultancy for the compliance to Italian Data Protection laws | Cosmetic |
| 2010 | Consultancy for risk assessment and establishment of an information security plan | Logistic |
| 2010 | Consultancy for risk assessment and establishment of an information security plan | TLC |

| *Year* | *Project Type* | *Sector* |
|---|---|---|
| 2010 | Consultancy for the compliance with Administrative Responsibility (similar to SOX) legal requirements and to software licences management legal requirements | IT SP - Public Sector |
| 2011 | Consultancy for the compliance with Administrative Responsibility (similar to SOX) legal requirements | Engineering |
| 2011 | Consultancy for the implementation of a business continuity management system | Bank |
| 2011 | Consultancy for the implementation of a business continuity management system | Advertising |
| 2011 | Consultancy for information security procedures. | Bank |
| 2011 | Consultancy for the implementation of a Data Loss Prevention system | Bank |
| 2012 | Consultancy for the compliance with Administrative Responsibility (similar to SOX) legal requirements | Waste management |
| 2012 | Consultancy for the compliance with Administrative Responsibility (similar to SOX) legal requirements | Publishing |
| 2012 | Consultancy for the implementation of an information security management system according to ISO/IEC 27001 and an IT service management system according to ISO/IEC 20000 | IT SP - Public Sector |
| 2012 | Consultancy for the implementation of information security management systems according to ISO/IEC 27001 | Public sector |
| 2013 | Consultancy for the compliance with Administrative Responsibility (similar to SOX) legal requirements | Insurance |
| 2013 | DPO role | IT Service provider |
| 2014 | IT Security assessment | Pharmaceutical industry |
| 2014 | IT Security assessment | Postal services |
| 2014 | Support for ITIL implementation | Bank |
| 2014 | Consultancy for the compliance to Italian Data Protection laws | Medical software development and management |
| 2009-2015 | Consultancy for the compliance to Data Protection laws | IT SP - Insurance |
| 2012 - 2015 | Consultancy for the implementation of a quality management system according to ISO 9001 | Media centre |
| 2015 | Assessment of an IT service management system according to ISO/IEC 20000 | IT Service provider |
| 2015 | Assessment of data protection controls in cloud services to ISO/IEC 27018 | IT Service provider |
| 2015 | Consultancy for the implementation of an information security management system according to ISO/IEC 27001 | Medical software development and management |
| 2015 | Consultancy for the implementation and maintenance of an information security management system according to ISO/IEC 27001 | Logistic |
| 2010-2016 | Consultancy for the implementation and maintenance of a quality management system according to ISO 9001 | Consultancy |
| 2011-2016 | Consultancy for the implementation and maintenance of an information security management system according to ISO/IEC 27001 | IT SP - Document Management |
| 2015 - 2016 | Consultancy for the implementation of:<br>- a quality management system according to ISO 9001;<br>- an information security management system according to ISO/IEC 27001. | Debt collection |
| 2015 - 2018 | Consultancy for the implementation of an information security management system according to ISO/IEC 27001 | IT Service provider (hardware support, NOC, cloud) |
| 2016 | Consultancy for the implementation of an information security management system according to ISO/IEC 27001. | Legal IT service provision |

| *Year* | *Project Type* | *Sector* |
|---|---|---|
| 2017 | Gap Analysis for ISO/IEC 27001 and the applicable personal data protection laws and regulations. | IoT devices production |
| 2017 | Gap Analysis for ISO/IEC 27001 | Logistic |
| 2017 | Gap Analysis for ISO/IEC 27001 | IoT devices production |
| 2017 | Consultancy for the compliance with Administrative Responsibility (similar to SOX) legal requirements. | Retail shops for luxury products |
| 2017 | Consultancy for the eIDAS compliance (risk assessment). | Trust service provider |
| 2018 | Consultancy for the risk assessment of an IT product in pharmaceutical field. | Pharmaceutical industry |
| 2018 | Consultancy for the compliance to personal data protection laws and regulations | IT service provider for a transportation provider |
| 2018 | Consultancy for the compliance to personal data protection laws and regulations | Weather forecast provider |
| 2018 | Assessment for the compliance to personal data protection laws and regulations | Accounting and ERP IT service provider |
| 2018 | Assessment for the compliance to personal data protection laws and regulations | Trust service provider |
| 2018 | Assessment for the compliance to personal data protection laws and regulations | Cosmetic |
| 2018 | Assessment for the compliance to personal data protection laws and regulations | Administrative services |
| 2018 | Assessment for the compliance to personal data protection laws and regulations | Manufacturing: screws |
| 2018 | Assessment for the compliance to personal data protection laws and regulations | Market research |
| 2019 | Support for the implementation of the information security requirements of a customer. | Health software development and maintenance |
| 2019 | Consultancy for the compliance to the applicable personal data protection laws and regulations. | Hosting, housing, website management |
| 2019 | Consultancy for the implementation of an information security management system according to ISO/IEC 27001, ISO/IEC 27017 e ISO/IEC 27018. | Software development and maintenance |
| 2019-2020 | Support for the qualification of a long preservation archiving system. | Software development, maintenance and operations |
| 2020 | Support for the implementation of the information security requirements of a customer and the ISO 13485 certification | Health software development and maintenance |
| 2020 | - Consultancy for the design process of software systems | Design and development of BI software |
| 2020 | Assessment of IT systems for personal data protection compliance | Energy provider |
| 2021 | • Consultancy for the compliance to the applicable personal data protection laws and regulations | HR management |
| 2012 - 2021 | Consultancy for:<br>- implementation of a quality management system according to ISO 9001;<br>- implementation of an information security management system according to ISO/IEC 27001;<br>- compliance to data protection law. | Software development |

| *Year* | *Project Type* | *Sector* |
|---|---|---|
| 2008-2021 | Consultancy for:<br>- certification of the information security management system (ISO/IEC 27001 extended with ISO/IEC 27017 and ISO/IEC 27018);<br>- certification of the quality management system (ISO 9001);<br>- certification of the business continuity management system (ISO 22301);<br>- qualification of the long term preservation service;<br>- implementation of National authority directives for Public administration in ICT. | Public sector |
| 2022 | Expert for a research on the cybersecurity approach of SMEs in Italy: meetings with SMEs representatives for information gathering, development of a tool for measuring the "Cyber readiness level", final presentation. | Research centre |
| 2022 | Consultancy for the implementation of an information security management system according to ISO/IEC 27001.<br>Specific activities:<br>- preliminary assessment;<br>- risk assessment approach and contractual clauses for the supply chain management. | University |
| 2009 - 2022 | Consultancy for the compliance to Data Protection laws.<br>Consultancy for the business continuity management.<br>Consultancy for the maintenance of a quality management system according to ISO 9001. | Market research |
| 2015-2022 | Consultancy for the implementation of an information security management system according to ISO/IEC 27001 | Household cleaning and personal care products |
| 2016-2022 | Consultancy for the implementation of an information security management system according to ISO/IEC 27001. | Air transportation |
| 2023 | Consultancy for the information security risk assessment | Appliance production and assistance |
| 2023 | Consultancy for the security of 2 software applications. | Infrastructure for transportation |
| 2023 | Consultancy for the implementation of an information security management system according to ISO/IEC 27001 | Provisioning of professional services |
| 2024 | Support for a second party audit for a finance application | Software development and operation |
| 2018-2024 | Consultancy for the compliance to the applicable personal data protection laws and regulations and DPO. | Hosting, housing. |
| 2009 - on going | Consultancy for the implementation of a quality management system according to ISO 9001, ISO/IEC 27001 (with ISO/IEC 27017 and ISO/IEC 27018) and ISO/IEC 27701.<br>Consultancy for the implementation of the security requirements of the Italian Cybersecurity Agency.<br>Consultancy for the compliance to Data Protection laws and DPO.<br>Consultancy for the compliance to whistleblowing laws.<br>Member of the supervisory board. | Human Resources |
| 2011 - on going | Consultancy for the compliance to Data Protection laws | Certification Body and assessment provider. |
| 2011 - on going | Consultancy for the compliance to data protection law | Luxury |
| 2012 - on going | Consultancy for:<br>- implementation of an information security management system according to ISO/IEC 27001;<br>- supplier management and monitoring;<br>- IoT security;<br>- privacy impact assessment;<br>- Industry 4.0 security. | Design, development and production of electronic devices and IoT |

| *Year* | *Project Type* | *Sector* |
|---|---|---|
| 2013 - on going | Consultancy for the implementation of:<br>- a quality management system according to ISO 9001;<br>- an information security management system according to ISO/IEC 27001;<br>- consultancy for the extension of the ISO/IEC 27001 certificate to ISO/IEC 27017 and ISO/IEC 27018;<br>- a conformity system for eIDAS (for TSA), registered email, identity trust provider and long time preservation of documents. | Trust service provider (registered email, TSA, Identity and long time preservation), SaaS (Email), IaaS and PaaS service provider |
| 2016 - on going | Consultancy for the implementation and maintenance of a quality and information security management systems according to ISO 9001 and ISO/IEC 27001.<br>Consultancy for the compliance to the applicable personal data protection laws and regulations.<br>Consultancy for the implementation of the security requirements of the Italian Cybersecurity Agency. | Software development and system management |
| 2017 - on going | Consultancy for the compliance to the applicable personal data protection laws and regulations.<br>Consultancy for the implementation of an information security management system according to ISO/IEC 27001. | Public sector |
| 2018 - on going | Consultancy for the implementation of an information security management system according to ISO/IEC 27001.<br>Support for the qualification of a long preservation archiving system. | Document management |
| 2018 - on going | Consultancy for the compliance to the applicable personal data protection laws and regulations and DPO. | Website management, web marketing |
| 2018 - on going | Consultancy for the compliance to the applicable personal data protection laws and regulations and DPO.<br>Consultancy for the compliance of an IT platoform to the regulations for the public administration e-procurement. | Professional association and register (Public body) |
| 2018 - on going | Consultancy for the compliance to the applicable personal data protection laws and regulations. | Competence for experts |
| 2018 - on going | Consultancy for the implementation of an information security management system according to ISO/IEC 27001. | Administrative, facility management and tax consulting services |
| 2018 - on going | Consultancy for the implementation and maintenance of a quality, information security and privacy management systems according to ISO 9001, ISO/IEC 27001 and ISO/IEC 27701.<br>Consultancy for the implementation of the security requirements of the Italian Cybersecurity Agency. | Software development and system management for the public administration |
| 2019 - on going | Consultancy for the compliance to the applicable personal data protection laws and regulations and DPO. | Software development and maintenance for the health sector |
| 2019 - on going | Consultancy for the implementation of a quality, information security and privacy management systems according to ISO 9001, ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018 and ISO/IEC 27701. | Cloud service provider (IaaS, PaaS and SaaS) |
| 2020 - on going | Consultancy for the implementation of an information security management system according to ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018, ISO 22301 and implementation of the CSA Control Matrix (version 3 and 4). | Cloud service provider (SaaS) for contact centres. |
| 2021- on going | Consultancy for the compliance to the applicable personal data protection laws and regulations and DPO. | Cloud service provider (IaaS, PaaS and SaaS) |
| 2021- on going | Consultancy for the implementation of a quality management systems according to ISO 9001 | IT service provider |
| 2021- on going | Consultancy for the implementation of an information security management system according to ISO/IEC 27001 | Production of machines for the logistics sector |

| *Year* | *Project Type* | *Sector* |
|---|---|---|
| 2021- on going | Consultancy for the implementation of an information security management system according to ISO/IEC 27001 | Cloud IT system management |
| 2021- on going | Consultancy for the implementation of an information security management system according to ISO/IEC 27001 | IT system management |
| 2023- on going | Consultancy for the implementation of an information security management system according to ISO/IEC 27001. | Consultancy |
| 2023- on going | Consultancy for the implementation of an information security management system according to ISO/IEC 27001. | Transport and logistic (food) |
| 2023- on going | Consultancy for the implementation of an information security management system according to ISO/IEC 27001 and ISO/IEC 27701. | Critical infrastructure |
| 2023- on going | Consultancy for the implementation of an information security management system according to ISO/IEC 27001 | SaaS antifraud solution |
| 2024- on going | Consultancy for the implementation of an information security management system according to ISO/IEC 27001 | Software development |
| 2024- on going | Consultancy for the implementation of an information security management system according to ISO/IEC 27001 with the extended control set with ISO/IEC 27017 and ISO/IEC 27018.<br>Consultancy for the implementation of the security requirements of the Italian Cybersecurity Agency. | Development and operation of cloud SaaS for the education sector |
| 2012 and 2024 | Consultancy for the implementation of information security management systems according to ISO/IEC 27001 | IT SP - Security Operation Centre |
| 2024- on going | Consultancy for the implementation of an information security management system according to ISO/IEC 27001 | Cloud IT system management |
| 2024- on going | Consultancy for the implementation of information security management systems according to ISO/IEC 27001 | IT SP - Security management |
| 2024- on going | Consultancy for the implementation of a quality and information security management systems according to ISO 9001, and ISO/IEC 27001. | Consultancy |
| 2024- on going | Consultancy for the implementation of information security management systems according to ISO/IEC 27001 | Food integration product production |