Cesare Gallotti

Curriculum Vitae

Cesare Gallotti
Nato a Milano il 11 febbraio 1973
Residente in Ripa di Porta Ticinese 75 - 20143 Milano - Italia
Web: http://www.cesaregallotti.it

Titolo di studio

Laurea in Matematica presso l'Università degli Studi di Milano, conseguita nel marzo 1999, a pieni voti legali; titolo della tesi: "Crittografia, protocolli e crittoanalisi"

Attestati di competenza

Lead Auditor ISO/IEC 27001 qualificato AICQ-SICEV.

Lead Auditor 9001 qualificato IRCA.

Certificati ITIL Expert e ITIL 2011 Foundation emessi da Exin nel 2008.

Certificato ITIL 4 Foundation emesso da Axelos nel 2019.

Lead Auditor ISO/IEC 20000 per DNV GL Business Assurance, Auditor ISO/IEC 20000 secondo lo schema itSMF e accreditato come docente (classificazione Auditor – Tutor 1) per i relativi corsi.

Auditor ISO 28000.

Lead auditor ISO 22301.

Certified Information Systems Auditor (CISA) secondo lo schema dell'ISACA.

Perfezionamento post-laurea in "Computer Forensics e investigazioni digitali" presso l'Università Statale di Milano AA 2008/2009.

"Pass with Merit" Business Continuity Institute examination nel 2011.

Agile Scrum Master rilasciato da Exin.

Prince 2 Foundation e Prince 2 Pratictioner rilasciato da Exin.

Service Integration and Management Foundation rilasciato da Exin.

Lingue

Inglese e francese, lettura e scrittura ottime, praticati in ambito professionale con la partecipazione a diversi progetti in Europa e Africa.

Esperienze professionali

DA NOVEMBRE 2008
Consulente free-lance.

- Esperto italiano per i lavori dell'ISO/IEC JTC 1 SC 27 WG1, con la partecipazione ai gruppi di redazione degli standard ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27003, ISO/IEC 27006, ISO/IEC 27013, ISO/IEC 27701.
- Consulenza per l'attuazione di sistemi di gestione per la sicurezza delle informazioni in accordo alla ISO/IEC 27001 (anche con estensione alle ISO/IEC 27017 e ISO/IEC 27018).
- Consulenza per l'attuazione di sistemi di gestione per i servizi IT in accordo alla ISO/IEC 20000-1.
- Consulenza per il risk assessment e la redazione di piani per la sicurezza delle informazioni.
- Consulenza per l'attuazione di sistemi di gestione per la continuità operativa (business continuity, anche in accordo alla ISO 22301).
- Consulenza per l'attuazione di sistemi di gestione per la qualità in accordo alla ISO 9001.
- Consulenza per gli adempimenti richiesti dalla normativa in materia di protezione dei dati personali.
- Consulenza per l'attuazione del modello organizzativo ai sensi del D. Lgs. 231/2001.
- Audit di terza parte e assessment su qualità, sicurezza delle informazioni e gestione dei servizi IT in Italia, Marocco, Spagna, Grecia, Ungheria e Sud Africa per l'organismo di certificazione DNV GL Business Assurance.
- Audit di terza parte, in qualità di esperto in ambito software, per dispositivi medici (medical devices) da marcare secondo le Direttive e i Regolamenti europei applicabili per l'organismo di certificazione DNV GL Business Assurance.
- Erogazione di corsi Lead Auditor ISO/IEC 27001 accreditati AICQ-SICEV e IRCA in Italia e all'estero per DNV GL Business Assurance.
- Erogazione di corsi ITIL Foundation, con qualifica Exin e APMG.
- Erogazione di corsi ISO/IEC 20000 per DNV GL Business Assurance.
- Erogazione di corsi su Business Continuity e ISO 22301 per DNV GL Business Assurance.
- Progettazione ed erogazione di un corso in inglese di Quality Assurance di 5 giornate per un'azienda multinazionale di ingegneria (in Italia e all'estero).

DA APRILE 2008
Consulente e docente per Quint Wellington Redwood, Milano.

Erogazione di corsi ITIL e ISO/IEC 20000 accreditati Exin o itSMF in Italia e all'estero.

Consulenza per l'attuazione di un IT service management system.

Consulenza per l'attuazione di un sistema di gestione per la qualità.

Collaborazione con Exin per lo sviluppo degli schemi di certificazione professionale nell'ambito della sicurezza delle informazioni.

NOVEMBRE 2002 – MARZO 2008
Lead Auditor e ICT Schemes Responsible in Det Norske Veritas Italia (oggi DNV GL Business Assurance), Agrate Brianza.

- Responsabile tecnico per gli schemi di certificazione in ambito ICT, dell'aggiornamento dei servizi offerti da DNV GL Business Assurance, delle competenze del personale impiegato nelle attività di verifica e del mantenimento degli accreditamenti Sincert (ora Accredia).
- Aggiornamento del personale sulle novità legali, in particolare privacy, responsabilità amministrativa delle imprese, computer crime, firma digitale e archiviazione ottica sostitutiva, e-commerce e accessibilità ai sistemi informatici.
- Lead Auditor di sistemi di gestione per la sicurezza delle informazioni secondo la ISO/IEC 27001, anche all'estero.
- Lead Auditor per le attività connesse alla certificazione degli IT Service Management System secondo la ISO/IEC 20000-1:2005 e alla loro valutazione anche secondo le best practices ITIL.
- Lead Auditor di sistemi di gestione per la qualità secondo la ISO 9001:2000 per aziende informatiche, di servizi alle imprese, del settore finance e manifatturiere.
- Technical Reviewer per i progetti di certificazione dei contact center secondo la UNI 11200.
- Progettista e docente per i corsi di Auditor e Lead Auditor ISO/IEC 27001 e ISO/IEC 20000, incluso il "Corso per I.S.M.S. Auditor" qualificato CEPAS e AICQ-SICEV.
- Partecipazione ai lavori dell'UNINFO per la redazione delle norme internazionali (in particolare per la ISO/IEC 20000).

DA LUGLIO 2001 A NOVEMBRE 2002
Consulente e Project Manager in Intesis S.p.A., Milano.

DA APRILE 1999 A GIUGNO 2001
Consulente e Project Manager in Securteam S.r.l., Milano.

Con le responsabilità di:

- realizzazione di Sistemi di Gestione per la Sicurezza delle Informazioni e delle relative procedure;
- studi e consulenza sulla realizzazione di algoritmi crittografici da implementare su un sistema di comunicazione, sulla realizzazione di sistemi di pagamento attraverso carte di credito e di debito in ambito europeo e su un sistema automatizzato per ottimizzare la distribuzione di farmaci nei reparti ospedalieri;
- adeguamento alla normativa in materia di privacy.

Sono state utilizzate metodologie di analisi del rischio quali Defender e CRAMM e, per la Intesis, è stata sviluppata la metodologia proprietaria per la progettazione di un Sistema di Gestione per la Sicurezza delle Informazioni.

Progetti Vedere Appendice A

Pubblicazioni e presentazioni

Attività continuative

- Da Ottobre 2008: autore della Newsletter mensile "*IT Service Management News*" (http://www.cesaregallotti.it/newsletter.htm);
- dal 2017: autore di articoli per la rivista "ICT Security" (www.ictsecuritymagazine.com).

Altre attività:

- Dicembre 2002: pubblicazione del libro "*Sicurezza delle informazioni - Analisi e Gestione del Rischio*", ed. FrancoAngeli, 2002;
- 2003-2005: relatore per la lezione "*Criteri di valutazione e certificazione della security dei sistemi informativi*" per il corso "Le aziende e gli atti illeciti: progettare la Business Security" presso lo Space Bocconi, Milano;
- Febbraio 2006: articolo "*Le novità della ISO 27001:2005 rispetto alla BS 7799-2:2002*", su ICT Security, febbraio 2006;
- Dicembre 2006: presentazione dell'articolo "*Le novità della ISO 27001:2005 rispetto alla BS 7799-2:2002*" alla sessione di studio dell'AIEA (Associazione Italiana IS Auditors);
- Gennaio 2009: autore della metodologia di Risk Assessment per la sicurezza delle informazioni "*VERA*";
- Giugno 2009: relatore a ECL 2009 su "*Privacy e Sistemi Organizzativi*";
- Agosto 2009: articolo *"Acquisizione e analisi di un dispositivo iPhone (Apple)"*, su *Cyberspazio e Diritto*, vol. 10 no. 2 agosto 2009;
- Settembre 2009: articolo "*Un metodo di risk assessment semplice*", su ICT Security, settembre 2009;
- Marzo 2010: presentazioni "Un metodo di Risk Assessment semplice" per AIEA Milano e AIEA Roma;
- Ottobre 2010: intervista per Salotto Tecnologico su "Sicurezza delle informazioni, privacy e organizzazione: che deve fare una PMI per ottenere risultati concreti?";
- Novembre 2010: intervento dal titolo "IT Governance: scelte e soluzioni" per il convegno "Stanco di fare l'equilibrista - Lasciatevi condurre sul cammino sicuro verso una corretta IT Governance" organizzato da ECS;
- Novembre 2010: intervento a Parigi "Appréciation conjointe ISO/IEC 27001 et ISO/IEC 20000-1" per il Club 27001 (www.club-27001.fr);
- Marzo 2011: intervento al Security Summit "Sistemi di gestione integrati - Come la ISO/IEC 20000 può essere di supporto alla ISO/IEC 27001";
- Novembre 2011: intervento per DFA "Standard ISO/IEC 270xx";
- Gennaio 2012: intervento per Assintel "Usare il Cloud in sicurezza: spunti tecnici";

- 7 giugno 2012: intervento "*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*" a Rabat (Marocco) per "Les 2 èmes assises de la Certification", organizzato dall'Association des Certificateurs du Maroc ;
- Luglio 2012: articolo "*Sicurezza delle informazioni e gestione dei servizi IT*", U&C luglio/agosto 2012, Milano;
- 2013: Partecipazione al gruppo di ricerca AIEA per l'analisi del futuro regolamento europeo sulla privacy;
- 2013: Partecipazione al gruppo di ricerca AIEA per la traduzione del manuale CISA;
- 2013: con Fabio Guasconi, Quaderno Clusit 009, "*Certificazioni Professionali in Sicurezza Informatica 2.0*";
- 2013: partecipante al Gruppo di Lavoro UNINFO sulla serie di norme ISO/IEC 27000 per la pubblicazione di "*La gestione della sicurezza delle informazioni e della privacy nelle PMI*";
- 2019: partecipante al gruppo di lavoro per la pubblicazione "Consapevolmente cloud" della Oracle Community for Security;
- 2020: partecipante al gruppo di lavoro per la pubblicazione "Sicurezza IoT" della Clusit Community for Security;
- 2014, 2017 e 2019: libro "*Sicurezza delle informazioni*", in self publishing.

Gli articoli e le presentazioni sono pubblicate, quando possibile, su http://www.cesaregallotti.it/art_pres.htm.

Altre esperienze professionali

- Partecipazione alle RFC del BSI per la redazione della BS 25999 (Business Continuity Management) e BS 25777 (IT Service Continuity Management).
- Dal 2002: collaborazione con Selexi per la realizzazione dei test di selezione del personale e per concorsi pubblici per le aree tematiche connesse all'informatica.
- Dal 2017: presidente dell'associazione Digital forensics alumni dei partecipanti ai corsi di perfezionamento post-laurea in "Computer Forensics e investigazioni digitali" e in protezione dei dati personali presso l'Università Statale di Milano.

Cesare Gallotti

Appendice A: Progetti

Anno	*Tipo progetto*	*Settore cliente*
1999	Realizzazione di un sistema di gestione per la sicurezza delle informazioni e delle relative procedure	Istituto bancario
1999	Studi e consulenza sulla realizzazione di algoritmi crittografici da attuare su un sistema di comunicazione	TLC
2000	Adeguamento alla normativa in materia di Privacy	Ospedale
2000	Studi e consulenza sulla realizzazione di sistemi di pagamento attraverso carte di credito e di debito in ambito europeo	Istituto di ricerca
2000	Adeguamento alla normativa in materia di Privacy	Manifatturiera: costruzione macchine
2000	Adeguamento alla normativa in materia di Privacy	Assicurazioni
2000	Realizzazione di un sistema di gestione per la sicurezza delle informazioni e delle relative procedure	IT SP per istituti bancari
2001	Studi e consulenza su un sistema automatizzato per ottimizzare la distribuzione di farmaci nei reparti ospedalieri	Istituto di ricerca
2001	Realizzazione di un sistema di gestione per la sicurezza delle informazioni e delle relative procedure - Standard ISO/IEC 15408	Chimico
2001	Adeguamento alla normativa in materia di Privacy	Provider contabilità
2001	Adeguamento alla normativa in materia di Privacy	Ingegneria
2002	Realizzazione di un sistema di gestione per la sicurezza delle informazioni e delle relative procedure - Standard ISO/IEC 27001	IT SP - Centrale Rischi
2002	Realizzazione di un sistema di gestione per la sicurezza delle informazioni e delle relative procedure.	Distribuzione alimentare
2002	Adeguamento alla normativa in materia di Privacy	TLC
2002	Realizzazione di un sistema di gestione per la sicurezza delle informazioni e delle relative procedure	Assicurazioni
2008	Consulenza per l'attuazione di un Sistema di Gestione per i Servizi IT secondo la ISO/IEC 20000-1.	Trasporti e logistica
2008	Consulenza per l'attuazione di un sistema di gestione per la qualità	IT SP
2009	Consulenza per l'attuazione del modello organizzativo ai sensi del D. Lgs. 231/2001	Ingegneria
2009	Realizzazione di un sistema di gestione per la sicurezza delle informazioni e delle relative procedure	Vendita di strumenti per ufficio
2009	Assessment sulla correttezza tecnica e organizzativa del processo di raccolta dati e reportistica	Manifatturiera: costruzione macchine
2010	Consulenza per l'attuazione di un sistema di gestione per i servizi IT secondo la ISO/IEC 20000-1:2005 e per la sicurezza delle informazioni secondo la ISO/IEC 27001	IT SP per il settore bancario
2010	Adeguamento alla normativa in materia di Privacy	Cosmetica
2010	Consulenza per il la valutazione del rischio e la redazione di piani per la sicurezza delle informazioni	Logistica
2010	Consulenza per il la valutazione del rischio e la redazione di piani per la sicurezza delle informazioni	TLC
2010	Consulenza per l'attuazione del modello organizzativo ai sensi del D. Lgs. 231/2001 e di gestione licenze	IT SP per PA
2011	Consulenza per l'attuazione del modello organizzativo ai sensi del D. Lgs. 231/2001	Ingegneria
2011	Realizzazione BCP	Istituto bancario
2011	Realizzazione BCP	Advertising
2011	Consulenza per la redazione di procedure per la sicurezza delle informazioni	Istituto bancario
2011	Consulenza per la realizzazione di un sistema di Data Loss Prevention	Istituto bancario

Cesare Gallotti

Anno	*Tipo progetto*	*Settore cliente*
2012	Consulenza per l'attuazione del modello organizzativo ai sensi del D. Lgs. 231/2001	Gestione rifiuti
2012	Consulenza per l'attuazione del modello organizzativo ai sensi del D. Lgs. 231/2001	Editoria
2012	Consulenza per l'attuazione di un sistema di gestione per i servizi IT secondo la ISO/IEC 20000-1:2005 e per la sicurezza delle informazioni secondo la ISO/IEC 27001	IT SP per PA
2012	Realizzazione di un sistema di gestione per la sicurezza delle informazioni e delle relative procedure	PA
2012	Consulenza per l'attuazione di un sistema di gestione per la sicurezza delle informazioni secondo la ISO/IEC 27001	IT SP - Security Operation Center
2012 - 2015	Consulenza attuazione del Sistema di Gestione per la Qualità in accordo alla ISO 9001:2008.	Centro media
2013	Consulenza per l'attuazione del modello organizzativo ai sensi del D. Lgs. 231/2001	Compagnia assicurazione
2013	Assunzione ruolo Data Protection Officer	Sviluppo software
2014	Analisi della sicurezza IT	Farmaceutica
2014	Analisi della sicurezza IT	Servizi postali
2014	Supporto per l'adozione di ITIL	Banca
2014	Adeguamento alla normativa in materia di Privacy	Sviluppo software per il settore sanità
2015	Valutazione del sistema di gestione per i servizi secondo la ISO/IEC 20000-1.	Fornitore di servizi IT
2015	Valutazione del sistema di gestione per la sicurezza delle informazioni e la privacy per i servizi cloud secondo la ISO/IEC 27018	Fornitore di servizi IT
2015	Consulenza per l'attuazione di un sistema di gestione per la sicurezza delle informazioni secondo la ISO/IEC 27001	Spedizioni e dogana
2015	Consulenza per l'attuazione di un sistema di gestione per la sicurezza delle informazioni secondo la ISO/IEC 27001	Sviluppo software per il settore sanità
2015-2018	Consulenza per l'attuazione di un sistema di gestione per la sicurezza delle informazioni secondo la ISO/IEC 27001	Erogazione di servizi gestiti in ambito IT (assistenza hardware, NOC e cloud)
2010-2016	Consulenza per l'attuazione e la manutenzione di un sistema di gestione per la qualità in accordo alla ISO 9001:2008	Consulenza
2011-2016	Consulenza per l'attuazione e la manutenzione di un sistema di gestione per la sicurezza delle informazioni secondo la ISO/IEC 27001	IT SP - Gestione documentale
2017	Gap Analysis ISO/IEC 27001 e GDPR	Produzione dispositivi IoT
2017	Gap Analysis ISO/IEC 27001	Logistica
2017	Gap Analysis ISO/IEC 27001	Produzione dispositivi IoT
2017	Consulenza per l'attuazione del modello organizzativo ai sensi del D. Lgs. 231/2001.	Negozi di profumeria
2017	Consulenza per la conformità eIDAS (valutazione del rischio).	Firma digitale
2018	Consulenza per la valutazione del rischio di un prodotto informatico in ambito farmaceutico.	Produzione prodotti farmaceutici
2018	Adeguamento alla normativa in materia di Privacy	Servizi IT per il meteo
2018	Adeguamento alla normativa in materia di Privacy	Fornitore di servizi IT di contabilità e ERP
2018	Adeguamento alla normativa in materia di Privacy	Firma digitale
2018	Adeguamento alla normativa in materia di Privacy	Cosmetica
2018	Adeguamento alla normativa in materia di Privacy	Servizi amministrativi
2018	Adeguamento alla normativa in materia di Privacy	Manifatturiera: viti
2018	Adeguamento alla normativa in materia di Privacy	Ricerche di mercato
2019	Consulenza per il recepimento dei requisiti di sicurezza delle informazioni di un cliente.	Sviluppo e manutenzione software per la sanità

Anno	*Tipo progetto*	*Settore cliente*
2019	Adeguamento alla normativa in materia di Privacy.	Hosting, housing, gestione siti web
2008-in corso	Consulenza per: - certificazione del sistema di sestione per la sicurezza delle informazioni (ISO/IEC 27001 ed estensione a ISO/IEC 27017 e 27018); - certificazione del sistema di sestione per la qualità (ISO 9001); - certificazione del sistema di sestione per la continuità operativa (ISO 22301); - accreditamento AgID del servizio di conservazione; - attuazione delle misure minime AgID.	Pubblica amministrazione
2009-in corso	Adeguamento alla normativa in materia di Privacy	Assicurazioni - IT SP
2009-in corso	Adeguamento alla normativa in materia di Privacy. Consulenza per la gestione della business continuity. Consulenza per la manutenzione del SGQ certificato ISO 9001.	Istituto ricerche di mercato
2009-in corso	Consulenza per l'attuazione del Sistema di Gestione per la Qualità in accordo alla ISO 9001:2008. Adeguamento alla normativa in materia di Privacy.	Selezione del personale
2011-in corso	Adeguamento alla normativa in materia di Privacy	Organismo di Certificazione
2011-in corso	Adeguamento alla normativa in materia di Privacy	Oreficeria
2012-in corso	Consulenza per - manutenzione di un Sistema di Gestione per la sicurezza delle informazioni secondo la ISO/IEC 27001; - rapporti con i fornitori; - sicurezza nell'ambito IoT; - privacy impact assessment; - industria 4.0 (sicurezza).	Progettazione e produzione impianti elettrici e IoT
2012-in corso	Consulenza - attuazione del Sistema di Gestione per la Qualità in accordo alla ISO 9001:2008; - adeguamento alla normativa in materia di Privacy e GDPR. - attuazione di un Sistema di Gestione per la sicurezza delle informazioni secondo la ISO/IEC 27001.	Sviluppo software
2013-in corso	Consulenza per l'attuazione di un sistema di gestione per: - la qualità secondo la ISO 9001; - la sicurezza delle informazioni secondo la ISO/IEC 27001; - l'estensione del certificato ISO/IEC 27001 alle norme ISO/IEC 27017 e 27018; - la conformità ai requisiti eIDAS, PEC, SPID e timestamp authoritty.	Fornitore di servizi IT fiduciari (PEC, SPID e TA) e cloud (IaaS, PaaS, SaaS)
2015-in corso	Consulenza per l'attuazione di un sistema di gestione per la sicurezza delle informazioni secondo la ISO/IEC 27001	Produzione prodotti per la casa e l'igiene personale
2015-in corso	Consulenza per l'attuazione di un sistema di gestione per: - la qualità secondo la ISO 9001; - la sicurezza delle informazioni secondo la ISO/IEC 27001.	Recupero crediti
2016-in corso	Consulenza per l'attuazione di un sistema di gestione per la sicurezza delle informazioni secondo la ISO/IEC 27001.	Erogazione servizi IT eIDAS
2016-in corso	Consulenza per l'attuazione di un sistema di gestione per la sicurezza delle informazioni secondo la ISO/IEC 27001.	Trasporto aereo
2016-in corso	Consulenza per l'attuazione e la manutenzione di un sistema di gestione per la qualità e la sicurezza delle informazioni secondo la ISO/IEC 27001 e la ISO 9001. Adeguamento alla normativa in materia di Privacy.	Sviluppo software, manutenzione sistemi
2017-in corso	Adeguamento alla normativa in materia di Privacy.	PA

Anno	*Tipo progetto*	*Settore cliente*
2018-in corso	Supporto certificazione ISO/IEC 27001. Supporto alla qualifica del servizio di conservazione.	Conservazione documenti
2018-in corso	Adeguamento alla normativa in materia di Privacy e DPO.	Hosting, housing, gestione siti web, organizzazione campagne marketing.
2018-in corso	Adeguamento alla normativa in materia di Privacy e DPO.	Ordine professionale
2018-in corso	Adeguamento alla normativa in materia di Privacy.	Formazione professionale
2018-in corso	Consulenza per l'attuazione di un sistema di gestione per la sicurezza delle informazioni secondo la ISO/IEC 27001.	Servizi amministrativi
2018-in corso	Consulenza per l'attuazione e la manutenzione di un sistema di gestione per la qualità e la sicurezza delle informazioni secondo la ISO/IEC 27001 e la ISO 9001. Adeguamento alla normativa in materia di Privacy.	Sviluppo software, manutenzione sistemi per la pubblica amministrazione
2019-in corso	Adeguamento alla normativa in materia di Privacy e DPO.	Sviluppo e manutenzione software per la sanità
2019-in corso	Supporto alla manutenzione dei requisiti AgID per il servizio di conservazione.	Sviluppo e manutenzione software e esercizio servizi IT
2019-in corso	Consulenza per l'attuazione e la manutenzione di un sistema di gestione per la sicurezza delle informazioni secondo la ISO/IEC 27001, ISO/IEC 27017 e ISO/IEC 27018.	Sviluppo e manutenzione software
2019-in corso	Consulenza per l'attuazione e la manutenzione di un sistema di gestione per la sicurezza delle informazioni e a qualità secondo le ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018 e ISO 9001.	Fornitore di servizi cloud IaaS, PaaS e SaaS