INFORMAZIONI PERSONALI

Claudio Cilli

ESPERIENZA PROFESSIONALE

(2007 - oggi)

Università degli Studi di Roma "La Sapienza"

Dipartimento di Informatica – Facoltà di Ingegneria dell'Informazione, Informatica e Statistica

- *Docente nel corso di laurea in Informatica*
- *Docente nel Master di I e II livello sulla Sicurezza*
- *Membro del Comitato Scientifico dei Master di I e II livello*
- Aree di interesse: Sicurezza dei Sistemi Informativi (Crittografia e applicazioni, Intrusion Detection Systems, Tecniche di attacco), Protocolli di comunicazione e vulnerabilità (Man-in-the-middle), Reti neurali (modelli comportamentali), Sistemi Informativi (Progettazione, revisione e pianificazione, analisi organizzativa dei flussi informativi, controllo e revisione dello sviluppo del software), Tecniche di valutazione dello sforzo di programmazione (FP, Kloc)

Attività o settore Insegnamento e ricerca

(2005 - 2007)

Università Politecnica delle Marche

Dipartimento di Ingegneria Informatica, Automatica e Gestionale – Facoltà di Ingegneria

- Docente del corso di Fondamenti di Informatica

Attività o settore Insegnamento e ricerca

(2011 - oggi)

Net Partner Consulting S.r.l. – Presidente e Amministratore Delegato

Torino, Roma – www.netpartnerconsulting.com

- Audit dei sistemi informatici, sia nel settore bancario e finanziario che in quello industriale, sistemi informativi di produzione, adempimenti legislativi e normativi (Sarbanes-Oxley, D.L. 231/2001, tutela della privacy, ecc.), sicurezza dei sistemi informativi e delle installazioni
- Realizzazione di Piani di Business Continuity e di Disaster Recovery, relativa implementazione e test
- Analisi revisione dei processi aziendali e analisi organizzativa. Previsione e pianificazione degli interventi di modifica/miglioramento dei processi al fine dell'ottimizzazione degli stessi per consentire alle organizzazioni di incrementare le proprie prestazioni e ottenere una riduzione dei costi. Individuazione dei fattori critici di successo e (KPI) e pianificazione degli interventi di attuazione.
- Progettazione, revisione e implementazione delle modifiche ai processi e all'organizzazione aziendale. Assistenza organizzativa alla direzione generale per guidare il processo di cambiamento. Pianificazione e controllo dei progetti di change management
- Architetture dei sistemi, acquisizione o realizzazione del software applicativo, organizzazione, gestione dei certificati di firma digitale, sicurezza. Consulente per progetti riguardanti la realizzazione di Certification Authority ai sensi delle normativa: aspetti tecnici e procedurali.
- Certificazione della sicurezza dei sistemi informativi secondo gli standard ISO27001-27002, ITSEC/ITSEM e Common Criteria

Attività o settore Consulenza nelle tecnologie dell'informazione

(2015 - oggi)

European Union Agency for Network and Information Security (ENISA)

Expert for assisting in the implementation of the ENISA Work Programme

- Contratto per le attività di assistenza alle attività di ENISA:

- Emerging application areas: e.g. transportation and automotive, eGovernment, eHealth, etc.
- Information security risk management: expertise and experience in conducting risk assessment and risk management exercises, using appropriate risk management methodologies and tools

Attività o settore Information Systems Security

(2010-2011) **United Nations (new York) – IT Auditor**

Office of Internal Oversight Services

- Contratto per le attività di IT Audit e IT Govcernance
- "The Office assists Member States and the Organization in protecting its assets and in ensuring the compliance of programme activities with resolutions, regulations, rules and policies as well as the more efficient and effective delivery of the Organization's activities; preventing and detecting fraud, waste, abuse, malfeasance or mismanagement; and improving the delivery of the Organization's programmes and activities to enable it to achieve better results by determining all factors affecting the efficient and effective implementation of programmes" (UN OIOS Mission)

Attività o settore Information Systems Audit

(2003-2005) **Value Partners S.p.A. – Responsabile delle attività di Risk Management**

Milano - Roma

- Coordinamento e pianificazione degli interventi presso i clienti. Le responsabilità comprendono: pianificazione, analisi organizzativa e dei flussi informativi, gestione dei gruppi di lavoro, preparazione e revisione dei rapporti finali, verifica e approvazione delle relazioni operative, controllo e revisione dello sviluppo del software, controllo e revisione delle applicazioni, pianificazione e verifica dei controlli interni, revisione della sicurezza e dei controlli, gestione del personale, sviluppo e implementazione del software e dei sistemi.

Attività o settore Servizi professionali di consulenza IT

(2001-2003) **KPMG S.p.A. – Responsabile Information Risk Management**

Milano - Roma

- Analisi revisione dei processi aziendali e analisi organizzativa. Previsione e pianificazione degli interventi di modifica/miglioramento dei processi al fine dell'ottimizzazione degli stessi per consentire alle organizzazioni di incrementare le proprie prestazioni e ottenere una riduzione dei costi.
- Progettazione, revisione e implementazione delle modifiche ai processi e all'organizzazione aziendale. Assistenza organizzativa alla direzione generale per guidare il processo di cambiamento. Pianificazione e controllo dei progetti di change management.
- Audit dei sistemi informatici, sia nel settore bancario e finanziario che in quello industriale, sistemi informativi di produzione, adempimenti legislativi, sicurezza dei sistemi informativi e delle installazioni.

Attività o settore Servizi professionali di consulenza IT

(1997-2000) **Ernst & Young – Senior Manager: Information Systems Audit and Advisory Services (ISAAS)**

Roma

- Audit dei sistemi informatici, sia nel settore bancario e finanziario che in quello industriale, sistemi informativi di produzione, adempimenti legali e revisione organizzativa. Interventi di due-diligence e valutazione dell'efficacia dell'organizzazione aziendale.
- Coordinamento e pianificazione degli interventi presso i clienti: gestione dei gruppi di lavoro, preparazione e revisione dei rapporti finali, controllo e revisione delle applicazioni, pianificazione e verifica dei controlli interni, revisione della sicurezza e dei controlli.
- Architetture dei sistemi, acquisizione o realizzazione del software applicativo, organizzazione, gestione dei certificati di firma digitale, sicurezza.
- Certificazione della sicurezza dei sistemi informativi secondo gli standard ISO17799 (BS7799) e ITSEC/ITSEM. Realizzazione di Piani di Business Continuity e di Disaster Recovery, implementazione e test.

Attività o settore Servizi professionali di consulenza IT

(1989-1996) **Gruppo Datamat S.p.A. – Coordinamento dei servizi di consulenza nel settore mlitare**

Roma

- Pianificazione, gestione dei gruppi di lavoro, preparazione e revisione dei rapporti finali, verifica e approvazione delle relazioni operative, controllo e revisione dello sviluppo del software e delle applicazioni, revisione della sicurezza e dei controlli, gestione del personale. Realizzazione di Piani di Business Continuity e di Disaster Recovery, implementazione e test.

Attività o settore Sicurezza militare

(1986-1988) **Yale Security Products S.p.A.**

Roma – Birmingham (UK) – Charlotte, NC (USA)

- Responsabile dei sistemi elettronici e assistente del Direttore Generale per l'organizzazione tecnica e la progettazione

Attività o settore Progettazione e sviluppo di sistemi di sicurezza

(1985-1986) **Selenia S.p.A.**

Roma

- Progettista di sistemi di Guerra Elettronica per applicazioni terrestri e navali

Attività o settore Sicurezza militare – Progettazione e sviluppo

(1983-1985) **Litton Italia S.p.A.**

Roma

- Progettista di sistemai di guida e controllo per aeromobili civili e militari

Attività o settore Progettazione e sviluppo di sistemi elettronici per la navigazione aerea

ISTRUZIONE E FORMAZIONE

(1976-1983) **Dottore in Ingegneria Elettronica**

Università degli Studi di Roma “La Sapienza”

- Laurea in Ingegneria Elettronica (votazione 110/110 e lode)

(1983) **Abilitazione all’esercizio della professione di Ingegnere**

Università degli Studi di Roma “La Sapienza”

- Superamento dell’Esame di Stato per conseguire l’abilitazione all’esercizio della professione

(1983-oggi) **Corsi post-universitari e di specializzazione**

Corsi frequentati presso diversi istituti italiani e stranieri, quali: IBM, Università californiana di Berkeley, ELEA, COMSIS (USA), SAP Institute, ecc.

- Sistemi di Sicurezza
- Sistemi di navigazione inerziale
- Sistemi integrati di gestione aziendale (ERP)
- Architetture dei sistemi informatici
- Tecniche di software engineering
- Gestione progetti
- Gestione delle risorse umane

(1996-oggi) **Certificazioni professionali**

Information Systems Audit and Control Association (ISACA), USA – The Institute of Internal Auditors (IIA), USA – International Information Systems Security Certification Consortium $(ISC)^2$, USA

- Certificazione CISA (Certified Information Systems Auditor) ottenuta nel 1996.

- Certificazione CIA (Certified Internal Auditor) ottenuta nel 2002.
- Certificazione CISSP (Certified Information Systems Security Professional) ottenuta nel 2002.
- Certificazione CISM (Certified Information Security Manager) ottenuta nel 2003.
- Certificazione CGEIT (Certified in the Governance of Enterprise IT) ottenuta nel 2007.
- Certificazione CSSLP (Certified Software Security Lifecycle Professional) ottenuta nel 2008.
- Certificazione CRISC (Certified in Risk and Information Systems Control) ottenuta nel 2010.
- Accreditamento in Internal Quality Assessment/Validation istituita dall'Institute of Internal Auditors (IIA) ottenuta nel 2006.
- Qualifica di Full Member dell'Institute of Information Security Professionals (Londra) ottenuta nel 2008

COMPETENZE PERSONALI

Lingua madre: Italiano

Altre lingue

	COMPRENSIONE		PARLATO		PRODUZIONE SCRITTA
	Ascolto	Lettura	Interazione	Produzione orale	
Inglese	C2 – Avanzato	C2 – Avanzato	C2 – Avanzato	C2 – Avanzato	C2 – Avanzato

Livelli: A1/2 Livello base - B1/2 Livello intermedio - C1/2 Livello avanzato
Quadro Comune Europeo di Riferimento delle Lingue

Competenze comunicative

Competenze comunicative acquisite durante l'esperienza di insegnante universitario e nelle molte presentazioni e conferenze cui è stato invitato

Competenze organizzative e gestionali

Leadership. In tutte le aziende in cui ha lavorato è stato responsabile di gruppi di lavoro di grandi dimensioni (fino a circa 50 risorse)

Competenze professionali

15 anni di esperienza nell'audit e 22 anni di esperienza nei sistemi informativi, progettazione e programmazione dei sistemi, gestione degli elaboratori e programmazione di applicazioni. Progettista di sistemi EDP, inclusi gli elaboratori, il software, l'installazione e l'addestramento degli utenti. Consulente di alcune aziende americane fornitrici dell'U.S. Department of Defence

- Realizzazione dell'architettura di una delle principali banche italiane, inclusi il progetto e la realizzazione delle soluzioni tecniche e la scrittura delle procedure organizzative
- Consulenza presso molte aziende e istituzioni in merito alla Legge 675 e D.L. 196/2003 sul trattamento dei dati personali e relativo regolamento (misure minime di sicurezza)
- Progetto e realizzazione delle soluzioni tecniche per alcune grandi aziende, incluse l'implementazione del software, la scrittura delle procedure organizzative e gli adempimenti legali.
- Realizzazione della documentazione, progettazione e implementazione di sistemi IT basati su mainframe IBM 30xx per una compagnia aerea, incluse la realizzazione del Piano di Disaster Recovery e le misure di sicurezza logiche e fisiche
- Progetto e realizzazione di sistemi informativi per la Marina Militare Italiana
- Consulenza e training sulle applicazioni della multimedialità e il software engineering per una grande azienda di servizi EDP
- Progetto e implementazione del Piano di Disaster Recovery per una delle principali aziende petrolifere italiane
- Progetto mirante all'implementazione e alla certificazione del sistema di contromisure per la protezione dei dati e del Disaster Recovery per un'azienda alimentare internazionale
- Implementazione delle misure di sicurezza logica per le comunicazioni tra la sede centrale e le sedi periferiche per una principale azienda ferroviaria
- Progettazione e revisione delle fasi di progettazione e sviluppo del software, implementazione delle misure di sicurezza logica e fisica per due delle principali compagnie di telefonia mobile
- Progettazione, realizzazione e implementazione del Piano di Business Continuity per una grande banca italiana

Competenze informatiche

Esperienze sugli elaboratori IBM e DEC/VAX, sistemi informativi di pianificazione e gestione della produzione: SAP R/3, MRP, MRP-II: MAPICS, MAC-PAC PHARMA, ecc.

Conoscenze approfondite del sistema operativo Unix e dei linguaggi di programmazione C and C++, Pascal, Basic, ADA, Prolog, dBase, SQL. Programmazione e gestione dei server Web (Apache, IIS) e strumenti per la creazione di pagine Web

Conoscenze approfondite e lunga esperienza nel software per EDP audit, Disaster Recovery Planning e I/S Security: Charismatek Function Point Workbench, SPR Checkpoint, The Buddy System, AIM Safe 2000, CPA RecoveryPac, CPA RiskPac, tools per analisi della sicurezza (ISS, COPS, Satan, ecc.)

L'esperienza nelle reti locali di elaboratori comprende: Unix (Solaris, Linux, BSD, Be), Novell Netware e Windows. In particolare l'implementazione e la revisione della sicurezza nelle implementazioni di reti con server Unix e Windows

Information Systems Auditing svolto in numerosi e diversi ambienti informatici:

- Revisione della sicurezza: Accessi on-line e batch, sicurezza fisica, modifiche al software, gestione delle password, piani di Disaster Recovery e loro test, Business Continuity Plan, Piani di contingenza (Short Term Recovery);
- Revisioni delle applicazioni software: Identificazione e analisi dei processi, identificazione dei controlli esistenti, test dei controlli, test delle interfacce;
- Revisioni del System Development Life Cycle (SDLC): Avvio del progetto, studi di fattibilità, analisi costi/Benefici (Ritorno degli Investment), decisioni sull'acquisizione/realizzazione dei sistemi, progettazione iniziale, progettazione di dettaglio, programmazione, test delle singole unità, test di sistema, implementazione degli strumenti di conversione, controlli di accettazione, analisi di post-implementazione;
- Revisione delle attività operative I/S: Pianificazione strategica, supporto ai centri di profitto/dipartimenti/business unit, aderenza agli obiettivi aziendali, determinazione degli obiettivi I/S, controlli per ridurre la probabilità di un uso inadeguato dei beni aziendali.

Implementazione di architetture di E-Business e di Certification Authority:

- Definizione delle politiche di sicurezza, e delle soluzioni tecniche: Definizione dell'architettura, firewall e sicurezza, procedure utente, accessi on-line e batch, sicurezza fisica, gestione dei certificati X.509v3, accessi ai database di produzione, implementazione degli strumenti e tecniche per la sicurezza delle transazioni (SET), verifica della sicurezza e test di intrusione, certificazione a norme europee ISO17799 e ITSEC/ITSEM;
- Costituzione di una Certification Authority: Identificazione e analisi dei prodotti software/hardware compatibili alle direttive, organizzazione, verifica della certificazione ISO17799 e ITSEC/ITSEM, organizzazione, realizzazione del manuale operativo e degli altri documenti, procedure di gestione delle chiavi e delle smart-card.

Altre competenze

- Insegnante universitario. Corsi di Sistemi Informativi, Fondamenti di Informatica, Linguaggi e Traduttori, Sistemi Operativi
- Docente per conto dell'Associazione Italiana Internal Auditors per corsi riguardanti le certificazioni professionali e di sviluppo delle competenze
- Membro del Certification Board di International Information Systems Security Certification Consortium $(ISC)^2$ per le certificazioni CISSP e CSSLP
- Speaker nei seminari AFCEA (Armed Forces Communications & Electronics Associations)
- Membro dell'ESoCE (European Society of Concurrent Engineering)
- Autore di articoli pubblicati in diverse riviste e libri specializzati

Patente di guida

Categoria B

ULTERIORI INFORMAZIONI

Principali Pubblicazioni

- "Security Issues in the Concurrent Enterprise", CALS Europe '97, Frankfurt, Ottobre 1997
- "An extensive approach to risk analysis and countermeasures definition", European Conference on Security and Detection (ECOS) 97, London, Aprile 1997
- "IT Governance: Why a Guideline?", Information Systems Control Journal, Vol. 3, 2003
- "Privacy: An Opportunity for IS Auditors?", Information Systems Control Journal, Vol. 4, 2005
- "One of the Gang", Interview about status of security, Infosecurity, Nov/Dic 2005
- "Come sviluppare il piano della sicurezza", Informatica Pubblica Vol. 3, 1994
- "Il furto di identità", Computer Business Review Italy, Ottobre 2005

- "A comprehensive methodology for information systems security evaluation and improvement", Armed Forces Communication and Electronics Association (AFCEA) Europe, Roma, Maggio 1994
- "Logical Access Controls", PolCACS 2001, Krakov 2001
- "Selecting effective IS auditing and security tools", PolCACS 2001, Krakov 2001
- "Organizational structure of IT – Desired Segregation of duties", PolCACS 2001, Krakov 2001
- 7 CISO Summit 2011 – Keynote on Security Methodologies
- 8 CISO & Cloud Computing 2011 – Chair of IS Managers roundtable
- SecureRome Conference, 9th July 2013: Security in the 21st Century - Threats or Trends
- "Understanding Covert Channels of Communication", CSX Europe 2016, London
- "Deep & Dark Web", CSX Europe 2016, London
- "Cyber-warfare", CSX Europe 2016, London
- "Understanding Covert Channels of Communication", CSX Asia/Pacific 2016, Singapore
- "Understanding Covert Channels of Communication", IT STAR 2016
- "Defending Our Privacy – A True Story", The Nexus, Jan 9th, 2017

Riconoscimenti e premi	2009 International Who's Who of Professionals award 2009 International Information Systems Security Certification Consortium $(ISC)^2$ award 2010 International Madison Who's Who award
Appartenenza a gruppi / associazioni	Rotary International

Si autorizza il trattamento del presente curriculum ai sensi e per gli effetti del D.Lgs 196/03 "Codice in materia di protezione dei dati personali".

Si dichiara l'assenza delle cause di inconferibilità di funzioni dirigenziali e situazioni di incompatibilità, di cui alla legge n. 190/2012 ed al decreto legislativo n. 39/1993.