Prof. Ing. Claudio Cilli, CIA, CISA, CISSP, CISM, CGEIT, CSSLP, CRISC, M.Inst.ISP
Via Berna, 25
00144 Roma
Telefono: 06-5293614
Portatile: 392-3905055

DATI PERSONALI

LINGUE CONOSCIUTE: INGLESE

NATO A CITTÀ S. ANGELO (PE) IL 17/05/1957

CONIUGATO

PERMANENZE ALL'ESTERO PER LAVORO: GERMANIA, REGNO UNITO, STATI UNITI, REPUBBLICA CECA, BELGIO, LUSSEMBURGO, POLONIA, FRANCIA

STUDI

Università degli Studi di Roma "La Sapienza"
Roma

Laurea conseguita nel 1983

Laurea in Ingegneria Elettronica (votazione 110/110 e Lode)

Corsi post-universitari e di specializzazione compiuti presso diversi istituti italiani e stranieri, quali: IBM, Università californiana di Berkeley, ELEA, COMSIS (USA), SAP Institute

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.

ESPERIENZE LAVORATIVE

2005 – 2007

Università Politecnica delle Marche
Ancona

Dipartimento di Ingegneria Informatica Automatica e Gestionale

Docente del corso di Fondamenti di Informatica

Università degli Studi di Roma "La Sapienza" *2007 – oggi*
Roma

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).

IS Audit Group. S.r.l. *2005 – oggi*
Roma

Presidente

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 ISO17799-27001 (BS7799), ITSEC/ITSEM e Common Criteria.

Office of Internal Oversight Services
United Nations (New York) *2010 – 2011*

Consulente per le attività di IT Audit e IT Governance

"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)

ValuePartners S.p.A.
Milano – Roma *2003 – 2005*

Responsabile attività di Risk Management

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.

KPMG S.p.A.
Roma *2001 – 2003*

Responsabile Information Risk Management

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.

ERNST & YOUNG *1997 – 2000*
Roma

Senior Manager: E-Business e EDP Audit

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.

GRUPPO DATAMAT S.p.A. *1989 - 1995*
Roma

Coordinamento dei servizi di consulenza nel settore militare

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.

YALE SECURITY PRODUCTS S.p.A. *1986 - 1988*
Aprilia - Birmingham (UK) - Charlotte, NC (USA)

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

SELENIA S.p.A. *1985 - 1986*
Roma

Progettista di sistemi di Guerra Elettronica per applicazioni terrestri e navali

LITTON ITALIA S.p.A. *1983 - 1985*
Roma

Progettista di sistemi di guida e controllo per aerei civili e militari

Altre Notizie

Insegnante universitario. Corsi di Sistemi Informativi, Fondamenti di Informatica, Linguaggi e Traduttori, Sistemi Operativi.

Chair dello CRISC Certification Board presso l'ISACA/ISACF (Information Systems Audit and Control Association/Foundation.

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.

Esperienze tecniche

Consulente - Data processing professional con 12 anni di esperienza nell'audit e 20 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.

1. Realizzazione dell'architettura di una delle principali banche italiane, inclusi il progetto e la realizzazione delle soluzioni tecniche e la scrittura delle procedure organizzative.
2. Consulenza presso molte aziende e istituzioni in merito alla Legge 675 sul trattamento dei dati personali e relativo regolamento (misure minime di sicurezza).
3. Progetto e realizzazione delle soluzioni tecniche per alcune grandi aziende, incluse l'implementazione del software, la scrittura delle procedure organizzative e gli adempimenti legali.
4. 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
5. Progetto e realizzazione di sistemi informativi per la Marina Militare Italiana.
6. Consulenza e training sulle applicazioni della multimedialità e il software engineering per una grande azienda di servizi EDP
7. Progetto e implementazione del Piano di Disaster Recovery per una delle principali aziende petrolifere italiane
8. 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
9. Implementazione delle misure di sicurezza logica per le comunicazioni tra la sede centrale e le sedi periferiche per una principale azienda ferroviaria
10. 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.
11. Progettazione, realizzazione e implementazione del Piano di Business Continuity per una grande banca italiana.

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 (FrontPage).

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 NT. In particolare l'implementazione e la revisione della sicurezza nelle implementazioni di reti con server Unix e Windows NT.

Information Systems Auditing svolto in numerosi e diversi ambienti informatici:

12. *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);
13. *Revisioni delle applicazioni software:* Identificazione e analisi dei processi, identificazione dei controlli esistenti, test dei controlli, test delle interfacce;
14. *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;
15. *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:

16. *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;
17. *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.

Pubblicazioni e conferenze

- “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 segeregation of duties”, PolCACS 2001, Krakov 2001
- 7 CISO Summit 2011 – Keynote on Security Methodologies
- 8 CISO & Cloud Computing 2011 – Chair of IS Managers roundtable