INFORMAZIONI PERSONALI Ivan Bitocchi

PROFILO SINTETICO

Profilo professionale specializzato in consulenza organizzativa con 20 anni di esperienza, maturata sia nel settore della **Pubblica Amministrazione** che in quello Privato.
Principali ambiti di attività:

- **Cyber Security Governance, Risk Management and Compliance:** Definizioni di modelli organizzativi, definizione e implementazione di Information Security Management Systems, produzione di politiche, standard e procedure, Cyber Risk Management, definizione di KRI e KPI
- **Analisi dei processi e Business Impact Analysis**
- **Program Management delle iniziative in ambito Cyber Security ed IT**
- **Security Manager** per gli aspetti di Sicurezza Fisica, Sicurezza Logica e Sicurezza di produzione di produzioni manufatturiere ad alto valore (carta banconote ed elementi di sicurezza)
- **Internal Audit** sui sistemi di gestione, in particolare sugli schemi: 27001, 22301, 14298
- Implementazione e monitoraggio della **Compliance** in relazione a standard e normative nazionali e internazionali quali 27001, 22301, Perimetro di Sicurezza Nazionale Cyber Security, NIS e NIS2, Cloud PA, Cyber Security Framework, GDPR

ESPERIENZA PROFESSIONALE

Da 2018 – Corrente

Istituto Poligrafico e Zecca dello Stato S.p.A.

- Manager della struttura Physical Security & monitoring Operations ed in precedenza della struttura Security Governance Security Risk
  Principali Attività svolte:
  - **Security Manager** produzione Carta per Banconote: Referente per Ispettori BCE e Indirizzo e Gestione dei requisiti di compliance e del processo di risk assessment su Sicurezza Fisica, Sicurezza Logica e Sicurezza di produzione di carta banconote e relativi elementi di sicurezza
  - **Gestione della Sicurezza Fisica a livello nazionale**: presidio delle sedi e relativi servizi di vigilanza e progettazione e operatività dei sistemi di supporto ed al monitoraggio della sicurezza fisica
  - **Cyber Security Governance, Risk Management and Compliance**: Definizioni di modelli organizzativi, definizione e implementazione di Information Security Management Systems, produzione di politiche, standard e procedure, Cyber Risk Management, definizione di KRI e KPI
  - **Analisi dei processi e Business Impact Analysis**
  - **Program Management** delle iniziative in ambito Cyber Security ed IT
  - **Risk Assessment** di processo e specifici
  - Progettazione e **definizione dei requisiti di sicurezza** (Logica e Fisica) sui nuovi progetti secondo l'approccio Security by Design

Da 2006 – 2018

EYFBA - Ernst & Young Financial Business Advisors S.p.A

- Progettazione, Implementazione, monitoraggio e manutenzione del Sistema di Gestione della Sicurezza delle Informazioni ai fini della conformità allo standard ISO 27001 e alle misure AGID per la PA
- Supporto nella definizione, governo e monitoraggio del piano e del programma di sicurezza delle informazioni
- Definizione dei requisiti di gara per piattaforme System Service Management e prodotti e servizi sulla Sicurezza delle informazioni
- Rilevamento e descrizione dell'adeguatezza ed efficacia del sistema di controllo interno sul reporting finanziario implementato dal management aziendale al fine di soddisfare gli obiettivi di controllo della Section 404 del Sarbanes-Oxley Act ed alla legge 262/2005
- Attività di analisi e costruzione di modelli Organizzativo-Gestionale di controllo con finalità preventive ai fini del rispetto della normativa sulla responsabilità amministrativa degli Enti per reati commessi nel loro interesse o a loro vantaggio (Legge 231/2001)

Da 2001 – 2005

Getronics

- analisi dei rischi del sistema informativo
- redazione di Politiche di Sicurezza dei Sistemi Informativi

- assistenza alla fase di progettazione del sistema di gestione della sicurezza delle informazioni ed esecuzione di audit finalizzati alla certificazione in base allo standard di sicurezza delle informazioni BS 7799 (ISO 17799)
- redazione di piani relativi alla Business Continuity o al Disaster Recovery di sistemi informativi
- redazione di Piani di Sicurezza seguendo la normativa CNIPA (marzo 2004) per diversi enti della Pubblica Amministrazione
- Rilevamento e descrizione dell'adeguatezza ed efficacia del sistema di controllo interno rispetto ai principali standard sulla sicurezza delle informazioni

ISTRUZIONE E FORMAZIONE

ANNO 2000

Laurea
Economia e Commercio
Presso Università di Tor Vergata - Roma

ANNO 2001 – 2002

Master
ISTUD sul ruolo (competenze e capacità relazionali) del consultant con particolare riferimento al mondo dell'Information & Communication Technology

COMPETENZE PERSONALI

Lingua madre: Italiano

Altre lingue

	COMPRENSIONE		PARLATO		PRODUZIONE SCRITTA
	Ascolto	Lettura	Interazione	Produzione orale	
Inglese	C1	C1	C1	C1	C1

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

Competenze informatiche: Ottima conoscenza del pacchetto Office, conoscenze base dei linguaggi di programmazione e dei protocolli di rete

ULTERIORI INFORMAZIONI

EVENTUALI REFERENZE o CERTIFICAZIONI

Certificato Lead Auditor ISO / IEC 27001
British Standard Institute
Certificato Lead Auditor ISO / IEC 22301
British Standard Institute

Certified Information Systems Auditor (CISA)
ISACA (Information Systems Audit and Control Association)
Audit informatici secondo gli standard, le linee guida e le prassi ottimali, così da garantire che l'IT ed i sistemi di business di un'organizzazione siano adeguatamente controllati e protetti.
Cybersecurity Fundamentals (CSX)
ISACA (Information Systems Audit and Control Association)
Principi relativi gli scenari di cyber security e ruolo delle figure addette alla protezione delle informazioni dai nuovi scenari di minacce

Ivan Bitocchi