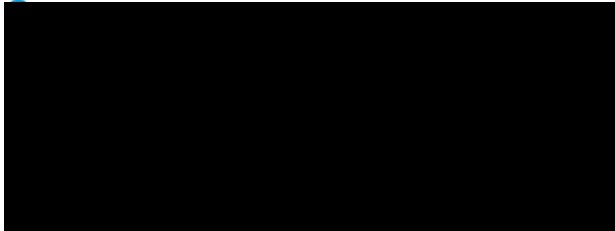
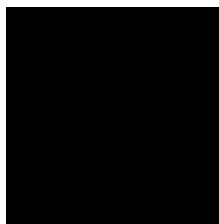


PERSONAL INFORMATION

Federica Magna



POSIZIONE RICOPERTA

Director Cybersecurity & Resilience

Ricopro il ruolo di Director all'interno della practice di Cyber Security di PwC con un'esperienza di circa 19 anni in tale ambito.

Possiedo profonde conoscenze in ambito Information e Cyber Security Strategy & Governance, acquisite attraverso l'esecuzione di attività in ambito quali: Security and Privacy by Design assessment (in particolare in ambito SAP) sui livelli di maturità di Information Security e/o Cyber Security e gap analysis rispetto a best practice e standard di riferimento nonché normative europee e nazionali quali NIS2; PSNC; DL Cyber; definizione e implementazione di Framework per l'Information Security e/o Cyber Security, attività di supporto per la compliance al Nuovo Regolamento sulla Data Privacy, stesura di procedure e linee guida di Information Security e/o Cyber Security e definizione di processi di Information Security e/o Cyber Security, Information Security e/o Cyber Security Risk Assessment, Vulnerability Assessment e Penetration Test, definizione e implementazione di Incident Management Process, nBusiness Continuity Plan e Disaster Recovery Plan. Inoltre, ho acquisito esperienza in attività di verifica della compliance a normative quali 262/05 e L.231, attività di analisi e implementazione della Segregation of Duties al livello di processo e a livello di sistema (autorizzazioni/profili/ruoli associati agli utenti di un sistema informativo) su diverse tipologie di sistemi (S/4 HANA; SAP R/3; AS 400; Hyperion).

Ho inoltre acquisito esperienza in ambito europeo in qualità di PM per la stesura di report in ambito cybersecurity (ad es.: Cyber Theft of Trade Secrets; Study on Remote Identity Proofing Practices: Attack Scenarios and Countermeasures)

Completano il profilo certificazioni specialistiche in ambito Information Security (ISO/IEC 27001:2022 Lead Auditor; ISO/IEC 27001:2013 Lead Auditor; OPST - OSSTM Professional Security Tester; ISO/IEC 22301:2012; ITIL v3 Foundation; TOGAF 9.1 Foundation)

Esperienza lavorativa in ambito Information Security; Cyber Risk Management; Continuità Operativa e Resilience

ESPERIENZA LAVORATIVA

ESPERIENZA PROFESSIONALE

Giugno 2015 – in corso

Cyber Security Director

PwC, Largo Angelo Fochetti 29, Roma

Progetti rilevanti in ambito Cyber Security e analisi funzionali:

Aprile 2025 - Ongoing

Supporto in ambito continuità operativa e alla Business Continuity con esecuzione di BIA, identificazione delle strategie di continuità, stesura e revisione periodica del Piano di Continuità Operativa in linea con ISO 22301 per il principale operatore aeroportuale nazionale al fine di definire un sistema integrato ed efficace in caso di scenari di interruzione dell'operatività

Attività o settore: Operatore aeroportuale

Luglio 2024 - Ongoing

Attività di supporto al CISO Office relativamente all'Information Security Assessment, identificazione delle azioni di trattamento del rischio di sicurezza in linea con attività di prioritizzazione e tenendo conto dei requisiti e obblighi di base in ambito NIS2. Definizione di una roadmap implementativa e del modello organizzativo e operativo di cybersecurity.

Attività o settore: Principale operatore settore farmaceutico

Dicembre 2020 - Ongoing

Supporto in ambito Security Strategy e adempimenti normativi ivi incluse attività legate alla continuità

operativa e alla Business Continuity con esecuzione di BIA, identificazione delle strategie di continuità, stesura e revisione periodica del Piano di Continuità Operativa in linea con ISO 22301.

Attività o settore: Pubblica Amministrazione

Marzo 2021 – Dicembre 2021

Supporto nell'esecuzione di un'attività di Assessment per gli aspetti di security and privacy by design nell'ambito di un progetto di digital transformation (migrazione da SAP ECC a S/4HANA) al fine di identificare i requisiti di sicurezza e privacy del nuovo sistema. In particolare l'attività ha previsto le seguenti fasi:
threat modelling
design dei requisiti di security e privacy
identificazione dei test di sicurezza da eseguire (VA; PT; Secure code review)

Attività o settore: Trasporti e Logistica

Dicembre 2021 – 2023

Supporto nell'esecuzione di un'attività di Assessment in grado di fornire evidenza della postura tenuta nell'AS-IS dal cliente rispetto a quanto prescritto dai perimetri NIS e Perimetro Sicurezza Nazionale Cibernetica. In particolare, le attività in oggetto hanno l'obiettivo di:

- verificare il livello di compliance raggiunto dal cliente nell' AS-IS rispetto al perimetro NIS e individuare eventuali gap e azioni di miglioramento;
- verificare il livello preliminare di compliance rispetto ai vari DPCM in ambito Perimetro Sicurezza Nazionale Cibernetica e individuare delle Readiness che possano proattivamente accompagnarla in un eventuale processo di inclusione nel Perimetro;
- verificare la rispondenza della metodologia di analisi e trattamento dei rischi attualmente adottata dal cliente rispetto a quanto prescritto dai perimetri PSNC e NIS.

Attività o settore: Trasporti e Logistica

Dicembre 2019 – Aprile 2020

- Supporto nella esecuzione di una Business Impact Analysis sui processi aziendali e mappatura dei sistemi aziendali a supporto dei processi (IT e OT)
- Supporto nella stesura di un Piano di Continuità Operativa

Attività o settore: Oil & Gas

Maggio 2019 – Dicembre 2021

- Supporto nella esecuzione di una Business Impact Analysis sui servizi aziendali esterni e interni
- Supporto nell'esecuzione di un Risk Assessment sugli asset aziendali
- Supporto nella stesura di un Piano di Continuità Operativa, istruzioni operative tecniche e nella stesura del Piano di Disaster Recovery

Attività o settore: Ente Pubblico

Febbraio 2019 – Aprile 2019

- Supporto nelle attività di assessment e adeguamento rispetto al nuovo regolamento Europeo per il Data Protection
- Definizione e analisi delle misure di sicurezza specifiche per la gestione ottimale della data protection
- Identificazione e supporto all'implementazione delle azioni di rimedio identificate

Attività o settore: Ente Pubblico

Ottobre 2018 – Gennaio 2019

Esecuzione di un'attività di Cyber Security Audit volto alla verifica dell'efficacia ed efficienza del Sistema di Controllo Interno in ambito Cyber per 6 aziende del Gruppo, identificando le aree di miglioramento e le azioni di rimedio da implementare. Esecuzione di 10 Vulnerability Assessment e Penetration Test sui sistemi/applicativi delle società in perimetro, individuando quelli particolarmente critici per l'operatività del business. Attività di supporto nel monitoraggio dell'implementazione delle azioni correttive concordate al fine di verificarne la corretta esecuzione.

Attività o settore: Trasporti e Logistica

Gennaio 2018 – Dicembre 2018

Studio tecnico volto a stabilire gli impatti del cyber spionaggio per le aziende europee e definizione di azioni di rimedio verso policy maker al fine di supportare le imprese nell'implementazione di azioni volte a contrastare il fenomeno del furto di dati segreti aziendali attraverso attacchi cyber.

Maggio 2017 – Ottobre 2017

Studio tecnico di supporto ed Impact Assessment volto a stabilire gli impatti della creazione di un nuovo Framework Europeo di Cyber Security per la Certificazione ed etichettatura dei prodotti ICT/IoT. Le attività progettuali hanno previsto inoltre:

- Mappatura di Framework di Cyber Security (e.g. NIST, Italian Cyber Security Framework, COBIT etc.) e Schemi di Certificazione Nazionali (e.g. CPA, CSPN, BSPA, Cyber Essentials etc) ed Internazionali (e.g. Common Criteria) utilizzati all'interno della Comunità Europea.
- Mappatura delle principali normative e degli standard relativi alla Cyber Security utilizzati all'interno della Comunità Europea
- Case Studies riguardanti gli impatti economici dovuti all'implementazione di un nuovo Framework Europeo di Cyber Security su 3 diversi settori di mercato: smart-meters, alarm systems, cloud-computing.

Attività o settore: Ente governativo europeo

Dicembre 2015 – Settembre 2018

Supporto continuativo alla funzione di governo della sicurezza per il Top Management in attività quali:

- Definizione di processi in ambito Information Security
- Analisi funzionali e calcolo di function point per progetti di sviluppo, per progetti di manutenzione evolutiva e per applicazioni esistenti
- Stesura di procedure e linee guida di Information Security e definizione di processi di Information Security
- Assessment sui livelli di maturità di Information Security e/o Cyber Security e gap analysis rispetto a best practice e standard di settore;
- Definizione e implementazione di Framework per l'Information Security e/o Cyber Security specifico per gli utenti appartenenti al Top Management

Attività o settore: Energy & Utility

Luglio 2015 – Febbraio 2016

Definizione e implementazione di un Cyber Security Framework basato sul Cyber Security Framework del NIST.

Il progetto ha previsto:

- Cyber Security Assessment al fine di identificare l'attuale livello di maturità del cliente in ambito Cyber Security, attraverso la valutazione di risorse e tecnologie, policy e processi in uso per Operational Technology, Information Technology e Industrial Control System; le attività hanno coinvolto componenti ICS, SCADA e sistemi aziendali e gestionali.
- Definizione di un Framework di Sicurezza Integrato, volto a sviluppare un approccio proattivo di security by design per la Cyber Security riducendo il rischio legato alla Sicurezza delle Informazioni, migliorando la risposta ad attacchi cyber e prendendo in considerazione le differenze fra gli Industrial Control Systems e Corporate Systems.
- Calcolo di function point per applicazioni esistenti

Attività o settore: Energy & Utilities

Dicembre 2015 – Aprile 2016

Assessment sui livelli di maturità di Cyber Security e gap analysis rispetto a best practice e standard di settore:

- Definizione di un set di controlli di Sicurezza IT applicabili sulla base di standard di riferimento, compresa la ISO 27001 e il COBIT;
- Assessment organizzativo e documentale per la verifica dell'aderenza al set di controlli definito;
- Selezione di un campione di sistemi ed applicativi per la verifica dell'efficacia dei controlli disegnati dall'organizzazione;
- Definizione di una serie di iniziative per il sanamento di eventuali controlli risultati non efficaci.

Attività o settore: Media & Entertainment

Luglio 2015 – Dicembre 2015

Assessment sui livelli di maturità di Cyber Security e gap analysis rispetto a best practice e standard di settore, tra cui ISO27001 e COBIT

- Esecuzione di un Security Assessment sul Sistema di Governo della Sicurezza IT aziendale, attraverso analisi documentale e l'esecuzione di interviste con personale chiave;
- Gap analysis rispetto ad un framework di controlli costruito sulla base dei requisiti di Sicurezza IT definiti dai principali standard e normative selezionati, tra cui ISO27001 e COBIT;
- Definizione di un piano di azioni di miglioramento, di quick win e di una roadmap strategica di interventi;
- Supporto nell'implementazione di alcuni dei quick win identificati

- Analisi funzionali e calcolo di function point per progetti di sviluppo e per progetti di manutenzione evolutiva

Attività o settore Ente pubblico – Servizi di distribuzione idrica

Novembre 2014 – Marzo 2015

Definizione e implementazione di Framework di ICT Security Assurance

- Assessment del framework di ICT Security Assurance secondo le best practice e i leading standard di settore (ISO/IEC 27001:2013; ISO/IEC TR 15443-1:2005; NIST SP800-100) e valutazione del livello di maturità attuale di ICT Security Assurance mediante benchmarking con altre Società Nazionali e Internazionali operanti nel settore Energy
- Definizione del nuovo ICT Security Assurance Framework conforme ai requisiti di sicurezza espressi dalla normativa ISO/IEC 27001:2013, definizione delle attività da implementare o modificare mediante la proposta di Quick Win da eseguire in integrazione del nuovo framework all'interno del processo aziendale di Information Security Risk Management
- Definizione e implementazione di una roadmap per l'ICT Security Assurance Framework per aumentare il livello di maturità di Sicurezza delle Informazioni e consolidare l'ICT Security Assurance Framework

Attività o settore: Energy & Utilities

Gennaio 2006 – Giugno 2015

Information Security Senior Consultant

EY – Ernst & Young Financial Business Advisory S.p.A, Via Po 32, Roma

Principali progetti rilevanti in ambito Cyber Security:

Gennaio 2013 – Luglio 2015

- **Definizione e implementazione di Framework per l'Information Security** di multicompliance contenente requisiti di sicurezza espressi dalle principali normative in ambito Information Security (i.e. ISO/IEC 27001) e dalle normative vigenti in ambito privacy (i.e. D.lgs. 196/03, Provvedimento per gli Amministratori di Sistema)
- Valutazione dell'attuale Sistema di Gestione della Sicurezza delle Informazioni rispetto ai requisiti di sicurezza definiti all'interno della normativa internazionale ISO/IEC 27001
- **Revisione e stesura di procedure e linee guida di Information Security e/o Cyber Security e definizione di processi di Information Security e/o Cyber Security** a supporto del SGSI
- Analisi funzionali e calcolo di function point per progetti di sviluppo, per progetti di manutenzione evolutiva e per applicazioni esistenti

Attività o settore Government & Public Services

Marzo 2013 – Dicembre 2013

Definizione e implementazione di un framework per l'Information Security

- Definizione e implementazione di modelli di multicompliance
- Analisi del Sistema di Gestione della Sicurezza delle Informazioni e valutazione della compliance agli standard internazionali in ambiti di Information Security (i.e. ISO27001)
- Analisi dei controlli implementati sui principali sistemi aziendali, in particolare SAP R/3 e AS 400.
- Analisi dei bisogni di business e definizione di una strategia di Information Security, analisi funzionali e calcolo di function point per progetti di sviluppo, per progetti di manutenzione evolutiva e per applicazioni esistenti
- Definizione di roadmap strategiche al fine di supportare e raggiungere gli obiettivi di business in ambito di Information Security
- Revisione e **definizione di processi di Information Security** in molte aree (Risk Management, Identity Management, Asset Management, Vulnerability & Threat Management, etc.)
- Definizione e implementazione di strumenti di monitoraggio per la valutazione dell'efficienza di pratiche e controlli in ambito Information Security
- Definizione di metodologie ed esecuzione di **Information Security Risk Assessment** e definizione di Risk Treatment Plan
- Identificazione dei requisiti di continuità per la **definizione e implementazione di Business Continuity Plan e Disaster Recovery Plan** in linea con gli obiettivi di business e di sicurezza aziendali

Attività o settore Banking

Gennaio 2012 – Giugno 2013

- **Assessment sui livelli di maturità di Information Security** attraverso l'esecuzione di IT Audit sugli IT General Control implementati ai fini della compliance SOX

- Supporto nella fase di implementazione del piano di remediation individuato a seguito dell'assessment
- Supporto nella **stesura di Linee Guida e Procedure operative in ambito IT e ICT Security**
- Supporto alle Funzioni Internal Audit del Gruppo nell'esecuzione di test semestrali e annuali sui controlli applicativi e IT General per la valutazione della Compliance SOX con particolare attenzione ai sistemi SAP R/3; Hyperion e AS 400.

Attività o settore Energy & Utilities

Gennaio 2007 – Luglio 2013

- **Assessment sui livelli di maturità di Cyber Security e gap analysis rispetto a best practice e standard di settore**
- Analisi di dettaglio sui rischi connessi alla segregazione delle responsabilità (SoD)
- Analisi dello stato AS-IS dei profili presenti nel contesto SAP r/3; Hyperion e AS400
- Attività mirate alla verifica dei controlli implementati su diverse tipologie di sistemi a supporto dei processi di business aziendali (SAP R/3; AS 400)
- Definizione di una matrice dei rischi sulla base delle esigenze espresse dal cliente
- Analisi di possibili gap tra l'attuale livello della sicurezza delle informazioni e quello desiderato
- Definizione di un nuovo framework sulla base dei risultati della gap analysis
- Definizione di nuovi ruoli e profili nel contest SAP
- Supporto nell'implementazione del tool GRC al fine di garantire un monitoraggio continuo della SoD
- Analisi funzionali e calcolo di function point per progetti di sviluppo, per progetti di manutenzione evolutiva e per applicazioni esistenti

Attività o settore Aerospace and Defence

Ulteriori progetti:

Marzo 2009 – Luglio 2013

- Supporto alle Funzioni Internal Audit del Gruppo nell'esecuzione di test semestrali e annuali sui controlli applicativi e IT General per la valutazione della Compliance alla Legge 262/05
- Analisi dello stato AS-IS dei controlli IT General implementati ai fini della compliance alla Legge 262/05 in accordo con il framework Cobit.

Attività o settore Aerospace and Defence

Gennaio 2011 – Marzo 2012

- Definizione dei requisiti funzionali per l'implementazione di un tool a supporto delle attività per la gestione della Compliance alla Legge/262
- Verifica attraverso test utente delle funzionalità effettivamente implementate a sistema
- Supporto nell'attività di caricamento dei dati relativi ai processi IT in ambito 262
- Training agli utenti sia funzionali, sia IT, sia della funzione Internal Audit per l'utilizzo del tool

Attività o settore Aerospace and Defence

Settembre 2005 –
Dicembre 2005

Stage

West LB AG, Via Canova, Milano

Attività svolte nell'ambito dell'IT Security in particolare per i processi Export Finance, Project Finance e Credit

Settore : Banking

CERTIFICAZIONI

- ISO/IEC 27001:2013 Lead Auditor
- ITIL v3 Foundation
- TOGAF 9.1 Foundation
- OPST - OSSTM Professional Security Tester
- ISO/IEC 22301:2012 Lead Auditor
- ISO/IEC 27001:2022 Lead Auditor

ISTRUZIONE E FORMAZIONE

2002 – 2005

Laurea in Economia e Management delle Imprese

Università Cattolica del Sacro Cuore sede di Roma

COMPETENZE PERSONALI

Lingua madre Italiano

Altre lingue

	COMPRENSIONE		PARLATO		PRODUZIONE SCRITTA
	Ascolto	Lettura	Interazione	Produzione orale	
Inglese	C1	C1	C1	C1	C1
Spagnolo	B1	B1	B1	B1	B1
Tedesco	A2	A2	A2	A2	A2

Levels: A1/2: Basic user - B1/2: Independent user - C1/2 Proficient user
Common European Framework of Reference for Languages

Competenze professionali

- Eccellente conoscenza di MS Excel, Outlook, Word, Access
- Eccellente conoscenza del sistema operativo Windows
- Eccellente conoscenza del web e dei motori di ricerca
- Ottima conoscenza di SAP R/3
- Ottima conoscenza di AS 400
- Ottima conoscenza di MS Access e Project
- Buona conoscenza dei sistemi operativi Unix
- Buona conoscenza dei database Oracle e Sql
- Buona conoscenza del mondo hardware
- Buona conoscenza del software di simulazione Arena
- Buona conoscenza di Lotus Notes
- Buona conoscenza del software AcL
- Buona conoscenza del software Monarch
- Buona conoscenza delle principali infrastrutture di rete

Conoscenza approfondita e competenze relative a tematiche di Information Security e Cyber Security, tra cui:

- NIST Framework for Improving Critical Infrastructure Cybersecurity
- Framework Nazionale per la Cyber Security italiano, definito dal CIS-Sapienza e dal Laboratorio Nazionale di Cyber Security
- Assessment sui livelli di maturità di Information Security e/o Cyber Security e gap analysis rispetto a best practice e standard di settore
- Definizione e implementazione di Framework per l'Information Security e/o Cyber Security
- Definizione e implementazione di SGSI
- Stesura di procedure e linee guida di Information Security e/o Cyber Security
- Definizione di processi di Information Security e/o Cyber Security
- Information Security e/o Cyber Security Risk Assessment,
- Vulnerability Assessment e Penetration Test
- Definizione e implementazione di Business Continuity Plan e Disaster Recovery Plan

Conoscenza di standard, framework e normative, tra cui:

- ISO 27001
- ISO 27002
- ISO 27005
- ISO 31000
- ISO 22301
- Nuovo Regolamento Europeo sulla Data Privacy
- NIST Framework for Improving Critical Infrastructure Cyber Security
- Framework Nazionale per la Cyber Security – CIS Sapienza
- COBIT
- ITIL
- NERC
- ISO/IEC 15408:1999 Common Criteria for Information Technology Security
- Risk Management standard
- Identity e Access Management
- ICT Security Incident e Crisis Management