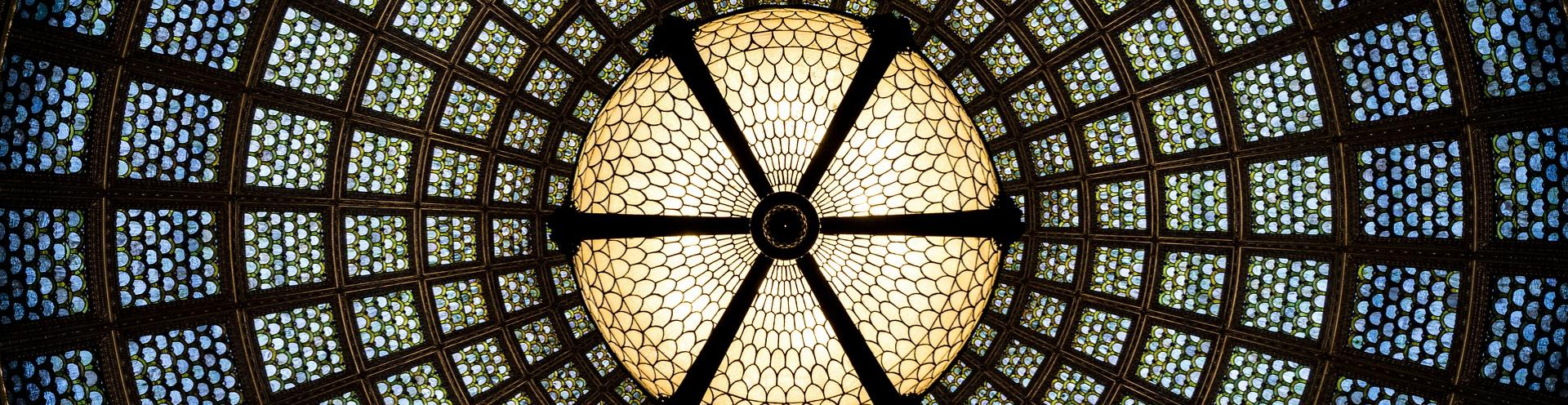




Adeguamento DORA

Interventi operativi di compliance e attività ricorrenti

Gennaio 2026

Premessa e contesto di riferimento

- Il **Regolamento DORA** (2554/2022) per la **resilienza digitale nel sistema finanziario**, è diventato operativo dal 17 gennaio 2025
- Le **entità finanziarie** hanno **redatto** nei primi mesi del 2025 il **diagnostico previsto da Banca d'Italia** finalizzato a rilevare lo **stato di avanzamento** delle attività di **adeguamento**
- Con tale diagnostico, le entità finanziarie hanno dichiarato il **loro piano di adeguamento in termini di scadenze e di attività da svolgere**, generalmente previste nel corso del 2025 e nei primi mesi del 2026:
 - Impostazioni di governance, regolamenti, linee guida entro settembre 2025
 - Metodologie di analisi del rischio ICT, classificazione e segnalazione incidenti entro dicembre 2025
 - Prime attivazioni operative nei primi mesi del 2026 (es. analisi di rischio ICT, rilevazione incidenti).

Per le entità finanziarie **meno strutturate** o con rilevante **esternalizzazione ICT** (es. **SGR**), gli adempimenti possono risultare complessi, date le **limitate risorse ICT interne** e comunque la **piena responsabilità** in capo agli **organi apicali prevista dal Regolatore**

L'impianto normativo DORA e DORA RTS prevede l'intervento su più dimensioni operative, sotto la piena responsabilità degli organi apicali



Con il diagnostico, il Regolatore ha richiesto la pianificazione dei principali adempimenti previsti dai Regolamenti DORA e DORA RTS



L'adeguamento a DORA richiede interventi sia in fase di IMPOSTAZIONE sia nel **CONTINUO**

La Governance sui rischi informatici comporta precise responsabilità in capo all'Organo di Gestione

L'Organo di Gestione rappresenta il fulcro strategico della resilienza operativa digitale, con responsabilità chiare e dirette nella governance dei rischi informatici.

RESPONSABILITÀ ULTIMA

L'Organo di Gestione assume la **responsabilità finale** per la gestione complessiva dei **rischi informatici** dell'entità finanziaria. Questa **responsabilità è indelegabile** e richiede una supervisione attiva e continua di tutti gli aspetti legati alla sicurezza digitale. Essa opera anche nei confronti dei fornitori e dei sub-fornitori

SUPERVISIONE STRATEGICA

L'organo definisce e **approva l'attuazione** di tutte le **disposizioni** previste dai **Regolamenti Europei e nazionali** per la **Gestione dei Rischi Informatici**, vigilando costantemente sulla sua corretta applicazione in tutte le funzioni aziendali.

COMPETENZE OBBLIGATORIE

I **membri** devono mantenere attivamente **conoscenze e competenze adeguate** per **comprendere e valutare** i rischi informatici. È obbligatoria una **formazione specifica su base regolare** per garantire l'aggiornamento continuo sulle evoluzioni tecnologiche e normative.

L'Organo di gestione definisce e approva espressamente gli interventi e l'organizzazione per l'attuazione delle disposizioni del Regolamento DORA

Normative interne e processi operativi

Definizione del quadro di gestione rischi: Il quadro definisce come la Società affronta le minacce digitali e misura il rischio corrispondente.

Strategia di resilienza operativa e tolleranza al rischio: la strategia approvata include la determinazione della tolleranza al rischio e precisi obiettivi di protezione dei dati.

Integrazione e monitoraggio: le politiche di protezione devono essere integrate nei processi e monitorate per garantire la conformità normativa.

Processo dinamico e aggiornamenti: La resilienza digitale richiede rilevazioni e aggiornamenti continui delle politiche e delle metodologie per adattarsi alle nuove minacce e assicurare la continuità operativa.

Ruoli e responsabilità e governance operativa

Governance e ruoli TIC: La normativa DORA richiede ruoli chiari in tutte le funzioni ICT per ridurre ambiguità e migliorare coordinamento.

Funzione di controllo indipendente: È obbligatorio istituire un controllo indipendente per gestire e sorvegliare i rischi informatici in modo obiettivo.

Modello delle tre linee di difesa: Le tre linee di difesa separano funzioni operative (1° liv.), controllo (2° liv.) e audit (3°liv.) per un sistema di controllo robusto e trasparente.

Monitoraggio e Supervisione sistematici

Gestione delle risorse finanziarie: devono essere assegnate e riesaminare le risorse finanziarie per supportare sicurezza informatica e formazione continua

Piani di continuità operativa: i piani di risposta e ripristino devono essere aggiornati sistematicamente e monitorati per garantire la ripresa rapida dopo incidenti.

Ruolo dell'audit interno: i piani di audit sull'IT devono essere approvati e riesaminati periodicamente dall'organo di gestione

Documentazione e revisione normativa: Il quadro di gestione dei rischi deve essere documentato, riesaminato annualmente e formalizzato con relazioni dettagliate.

Rilevazione e segnalazione incidenti: devono essere previsti sistemi strutturati per la rilevazione cla

Gestione dei fornitori terzi

Gestione dei rischi da fornitori terzi: fornitori terzi di servizi TIC introducono rischi che richiedono una gestione attenta e continua.

Ruolo di supervisione dedicato: È fondamentale designare un responsabile di alto livello per monitorare gli accordi con i fornitori terzi.

Comunicazione efficace e tempestiva: devono essere istituiti canali di comunicazione per segnalare incidenti gravi e misure correttive rapidamente.

Continuità operativa e resilienza: devono essere previsti sistemi di contingency in caso di incidente informatico e previsti test di resilienza operativa digitale su cui effettuare analisi di efficacia e di robustezza

L'adeguamento a DORA richiede interventi sia in fase di IMPOSTAZIONE sia nel CONTINUO

A

GESTIONE DEI RISCHI INFORMATICI

FASE DI IMPOSTAZIONE

- **Regolamento interno** sulla gestione dei **RISCHI INFORMATICI e di SICUREZZA**
 - Ruoli e Responsabilità, Obiettivi, Principi, Strategie
 - Propensione al Rischio, Tolleranza, Rischio residuo accettato
 - Controllo dl Rischio, Rendicontazione
- **Metodologia di Analisi del Rischio Informatico e di Sicurezza**
 - Minacce, Rischi, Presidi d mitigazione
 - Modello di misurazione e valutazione dei rischi
 - Strumenti di supporto
- **Processo di gestione e controllo** dei rischi
- **Mappatura risorse IT** (anche quelle in outsourcing)
- **Mappatura processi** supportati da **tecnologie ICT**

ATTIVITÀ NEL CONTINUO (annualmente)

- **Aggiornamento annuale del modello di rischio**
 - Minacce ICT, rischi ICT, presidi di controllo applicabili
 - Processi operativi impattati
 - Inventario asset tecnologici (anche presso outsourcer)
- **Applicazione del modello di valutazione** del rischio ICT
 - Scoring e Rating per ogni minaccia/Rischio
 - Valutazione dei presidi
 - Agility Risk
 - Calcolo del **rischio netto** e del **rischio residuo**
- **Valutazione del Rischio** sui servizi **esternalizzati**
 - Valutazione delle analisi degli outsourcer e integrazione nel modello interno
- **Rendicontazione** alla Direzione
 - **Formalizzazione** e Passaggio in CDA

L'adeguamento a DORA richiede interventi sia in fase di IMPOSTAZIONE sia nel CONTINUO

B

GESTIONE DEGLI INCIDENTI

FASE DI IMPOSTAZIONE

- **Regolamento interno** sulla gestione degli **INCIDENTI ICT E di SICUREZZA**
 - Obiettivi, Principi, Strategie
 - Ruoli e Responsabilità
- **Modello di classificazione incidenti e livelli di emergenza**
 - Livelli di emergenza, gravità degli incidenti, attività
- **Strumento** applicazione delle **Regole di classificazione**
 - Gestione dei parametri caratteristici **DORA RTS** (danni, volumi)
- **Registro degli incidenti**
 - Responsabile raccolta dati e Integrazione con gli outsourcer
- **Indicatori di allerta precoce**
- **Segnalazione** all'autorità competente
 - Responsabile segnalazione e **eventuale esternalizzazione**
- **Contenuti reporting** sistematico per la **Direzione**

ATTIVITÀ NEL CONTINUO (annualmente)

- **Gestione incidenti**
 - Rilevazione dati di ogni incidente (non solo quelli gravi)
 - Applicazione tool di classificazione incidenti
 - Valorizzazione registro incidenti
 - Escalation su livello di emergenza
 - Rilevazione impatti e danni
- **Interazione con outsourcer ICT**
- Valorizzazione **Alert preventivi**
- **Segnalazione incidenti**
 - Valorizzazione Form di segnalazione e segnalazione
- **Analisi delle cause**
 - Formalizzazione dell'analisi delle cause
- **Reporting** sistematico

L'adeguamento a DORA richiede interventi sia in fase di IMPOSTAZIONE sia nel CONTINUO

C

CONTINUITÀ OPERATIVA

FASE DI IMPOSTAZIONE

- **Regolamento di Continuità Operativa**
 - Strategie di continuità
 - Principi e obiettivi
 - Rischio residuo accettato
- **Piano di Continuità Operativa**
 - Ruoli e responsabilità
 - BIA e Processi critici
 - Disaster Recovery
 - Livelli di emergenza
 - Piani di verifiche della BC
- **Responsabile della BC e Gestione della Crisi**
 - Regole di attivazione Comitato di Crisi
 - Attività in Stato di crisi
 - Rientro alla normalità

ATTIVITÀ NEL CONTINUO (annualmente)

- **Organizzazione Piani di verifiche di BC**
 - Verifiche autonome
 - Verifiche con outsourcer
 - Verifiche con il sistema
- **Redazione BIA e aggiornamento sistematico**
 - Schede di BIA
 - Analisi criticità processi
- **Integrazione con gestione incidenti**
- **Definizione Scenari di Crisi**
- **Reporting**
 - Documentazione prove
 - Rendicontazioni e statistiche

L'adeguamento a DORA richiede interventi sia in fase di IMPOSTAZIONE sia nel CONTINUO

D

GESTIONE FORNITORI E FORNITURE

FASE DI IMPOSTAZIONE

- Identificazione **servizi essenziali e importanti** fruiti
- **Regolamento interno gestione terzi parti e rischio concentrazione**
- **Aggiornamento contratti con terze parti** (addendum contrattuali) sui requisiti DORA RTS (2024/1773), fra cui (di seguito i principali):
 - Gestione incidenti, misure e formazione Cyber di terze parti
 - Accountability, ricostruibilità, qualità dei dati
 - Change management di tecnologie e applicazioni
 - Penetration Test, Diritto di accesso, Audit
 - Assunzione di responsabilità del terzo sui subappalti
 - Obblighi di Business Continuity e Disaster Recovery
 - Valutazione dei rischi ICT e comunicazione al cliente
 - Obblighi di reporting verso il cliente

ATTIVITÀ NEL CONTINUO (annualmente)

- Aggiornamento **registro centralizzato** informazioni sulle terze parti, fra cui essenziali e importanti
- **Analisi** annuale del **rischio di terze parti**
- **Comunicazione annuale** fornitori essenziali e importanti **al Regolatore**
- Verifica adeguatezza contrattualistica terze parti essenziali e importanti
- **Aggiornamento** annuale **del rischio ICT di terze parti** e dei loro **subappaltatori**
- **Aggiornamento** annuale del **rischio di concentrazione**
- **Verifica** del **rispetto** dei nuovi **requisiti** contrattuali **DORA** da parte del **fornitore**

L'adeguamento a DORA richiede interventi sia in fase di IMPOSTAZIONE sia nel CONTINUO

E

GESTIONE COMPLESSIVA DELLA SICUREZZA
(Sistemi, reti, basi dati, cambiamenti)
Regolamenti o Linee Guida

FASE DI IMPOSTAZIONE

- Regolamenti interni o **almeno Linee Guida** su tematiche di **dettaglio** previste da **DORA RTS**:
 - **Gestione chiavi crittografiche** e certificati di sicurezza
 - Regole di **protezione basi dati**
 - **Gestione identità e accessi utenti** e tecnici ICT
 - **Gestione cambiamento tecnologico** (anche outsourcer ICT)
 - **Salvataggio, archiviazione, ripristino dati**
- In caso di **outsourcing** ICT/backoffice:
 - **verifica adeguatezza** dei **regolamenti** interni previsti dai fornitori
 - **Integrazione linee guida** per le **attività** ICT e backoffice gestite «in house» (es. elaborazioni excel rilevanti)

ATTIVITÀ NEL CONTINUO (annualmente)

- **Gestione chiavi di crittografia** e certificati di sicurezza
 - **Censimento e aggiornamento chiavi crittografiche** perimetro «in house»
 - **Verifica «eccezioni di aggiornamento»** comunicate dagli **outsourcer**
 - **Mappatura servizi essenziali e importanti da crittografare**
 - **Verifica cifratura «dati at rest»**
- **Regole protezione basi dati**
 - **Verifica adeguata gestione dati dell'outsourcer** e in perimetro «in house»
- **Gestione identità e accessi**
 - **Verifica adeguata gestione accessi outsourcer** e in perimetro «in house»
- **Gestione cambiamento tecnologico**
 - **Verifica adeguata gestione change management dell'outsourcer** e in perimetro «in house»
- **Salvataggio, archiviazione, ripristino dati**
 - **Test di leggibilità backup** e ripristino (compliance **outsourcer** e «in house»)

I nostri servizi a supporto dell'adeguamento a DORA e DORA RTS

	IMPOSTAZIONE	SUPPORTO NEL CONTINUO
 NORMATIVE INTERNE E LINEE GUIDA	• Redazione Regolamenti interni e Linee Guida • Verifica compliance a DORA degli outsourcer	• Aggiornamento regolamenti • Verifiche adeguatezza dei Regolamenti degli outsourcer
 MODELLO DI RISCHIO ICT	• Impostazione modello di rischio ICT ▪ Minacce, Rischi, Presidi ▪ Parametri e Soglie di tolleranza	• Tool di calcolo del Rischio • Aggiornamento set Minacce/ Rischi/ Presidi • Report sistematico alla Direzione
 MODELLO GESTIONE INCIDENTI	• Impostazione modello gestione incidenti ▪ Tool classificazione incidenti ▪ Registro incidenti ▪ Processi gestione incidenti ▪ Alert Preventivi	• Gestione incidenti ▪ Raccolta informazioni e classificazione ▪ Registro e segnalazioni formali ▪ Reporting alla Direzione • Gestione Comitato di Crisi
 MODELLO GESTIONE CHIAVI CRITTOGRAFICHE E CERTIFICATI	• Impostazione modello gestione • Censimento chiavi crittografiche ▪ Censimento chiavi e registro ▪ Analisi adeguata sicurezza per ambito applicativo e sistemistico	• Valutazione adeguata sicurezza parametri di crittografia per ambito applicativo e sistemistico

Dettagli operativi ed esempi

MODELLO DI VALUTAZIONE DEL RISCHIO ICT: i parametri caratteristici della metodologia si basano su standard internazionali riconosciuti

Minacce

- **Minacce NIST:** circa 80 minacce codificate (Volontarie e involontarie)
- **Minacce ENISA:** circa 100 minacce articolate su 2livelli
- **Scelta preventiva** delle **minacce** applicabili in base all'analisi preliminare di rischio
- **Minacce** su **app** e su **infrastrutture**.
- **Minacce** su **IT in house** o in **outsourcing**

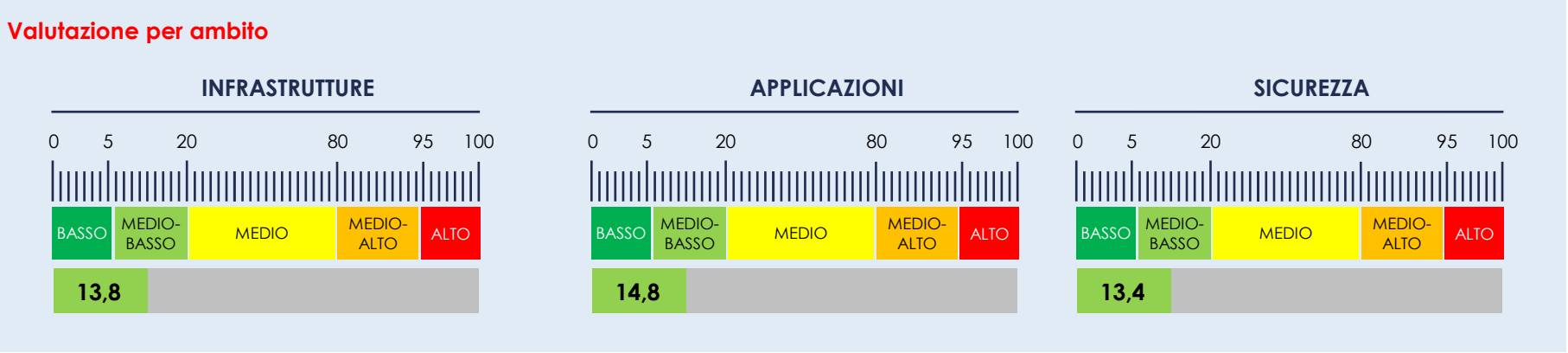
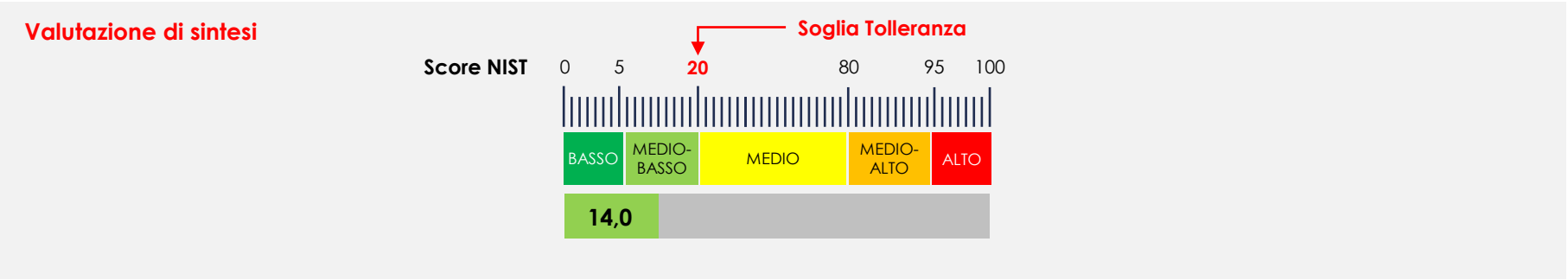
Scenari di rischio sul business

- **Definiti ad hoc** sulla base delle minacce selezionate e della realtà aziendale specifica
- **Direzioni di impatto:** modello CIDA (confidenzialità, Integrità, Disponibilità, Accountability/ Tracciabilità)
- **Includono anche i rischi** riferiti al **soggetto a influenza dominante (per controllante NIS2)** su decisioni a impatto rischi e sicurezza

Presidi e controlli

- **Presidi di Controllo NIST:** minacce valutate alla luce dei presidi e controlli dello standard NIST
- **Rischio netto:** consentono di valutare il rischio al netto della sussistenza e dell'efficacia di tali presidi

Esempio di valutazione quali-quantitativa del rischio ICT





Alberto Provedel

ICT Risk & Data Governance

C&P Advisory srl

BleedBlue – Data Handling for IT Governance

Viale Fratelli Cairoli, 159 – 31100 Treviso

(+39) 335 8214622

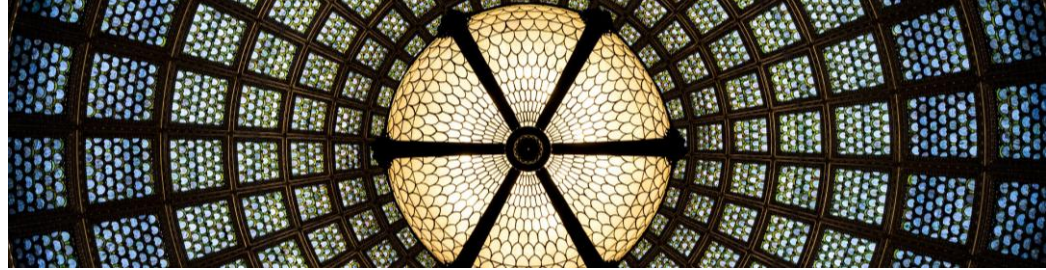
alberto.provedel@cpadvisory.eu

Profilo

Alberto ha oltre 35 anni di esperienza nel supporto alle aziende sui temi della gestione ICT e nel governo dei Rischi Informatici e Operativi. Ha lavorato dapprima come consulente di direzione presso aziende multinazionali di consulenza e successivamente ha operato come Dirigente in ambito bancario. Attualmente è ritornato alla consulenza supportando i clienti sull'adeguamento alla Resilienza Digitale e alla corretta applicazione delle tecniche di Machine Learning & Artificial Intelligence. Si occupa inoltre di sensibilizzazione sul tema esteso del Rischio Digitale.

Esperienze

Ha lavorato sui temi del Controllo dei sistemi ICT, della Sicurezza Informatica e dell'Ottimizzazione dei processi aziendali presso clienti di rilevanti dimensioni dei settori bancario, assicurativo e manifatturiero. Come dirigente di un Gruppo Bancario di rilevanza nazionale si è occupato di Operations, Information Technology e Risk Management. In tali contesti si è occupato di interloquire e collaborare con i Regolatori nazionali ed Europei



C&P Advisory srl

**Viale Fratelli Cairoli, 159
31100 Treviso**

Tel 0422 128 1106
www.cpadvisory.eu
alberto.provedel@cpadvisory.eu

BleedBlue
Data Handling for IT Governance

BleedBlue – Data Handling for IT Governance

**Viale Fratelli Cairoli, 159
31100 Treviso**

cell: 335 8214622
www.bleedblue.eu
info@bleedblue.it

C&P ADVISORY