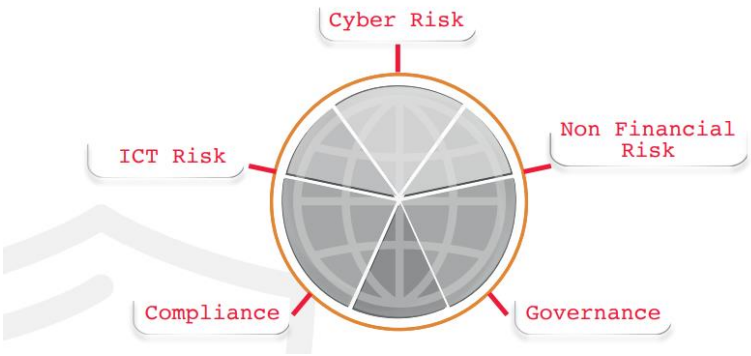
POLICY DI RESILIENZA OPERATIVA DIGITALE (DORA)

Versione: 01

Data: 01.09.2025

Responsabile: Cirillo Gianluigi



1. Premessa e Scopo

Questa policy definisce gli obiettivi e i principi di resilienza digitale e gestione dei rischi ICT per Consoft Informatica. Obiettivo: garantire continuità operativa, sicurezza dei sistemi ICT e conformità al Regolamento DORA.

2. Ambito di Applicazione

- I sistemi ICT coperti dalla presente policy sono quelli critici per il trattamento, la protezione, la gestione e la disponibilità dei dati personali, nonché per il funzionamento dei servizi IT e delle attività di business. In particolare, sono inclusi ad esempio, sistemi di gestione documentale e archiviazione elettronica, database aziendali, applicativi software sviluppati internamente o per conto terzi, sistemi di autenticazione e autorizzazione degli utenti, piattaforme cloud e ambienti virtualizzati utilizzati per l'elaborazione e conservazione dei dati personali, sistemi di backup e disaster recovery, infrastrutture di rete e dispositivi perimetrali (firewall, IDS/IPS, VPN).

- Processi aziendali interessati: Progettazione, sviluppo e realizzazione di applicativi software e di soluzioni web. Erogazione di servizi di consulenza informatica.

- Personale e funzioni coinvolte: Area IT e Prodotti

POLICY DI RESILIENZA OPERATIVA DIGITALE (DORA)

3. Ruoli e Responsabilità

| Ruolo | Responsabilità |

| Direzione Generale | Ing. Campofranco Luigi
| Responsabile ICT / CISO | Cirillo Gianluigi
| Risk Manager ICT | Cirillo Gianluigi
| Vendor Manager | Area commerciale
| Internal Audit / Compliance | external audit team

Intro

DORA è l'occasione per valutare in maniera olistica e integrata la resilienza dei sistemi aziendali e il rischio ICT, attuando un monitoraggio nel continuo. Consoft ha deciso di impostare un assessment efficace sul quale fondare il framework di resilienza: identificazione congiunta delle aree su cui prioritizzare gli interventi, in relazione al modello di business e delle componenti di rischio con maggior esposizione. Per costruire un framework robusto e resiliente nel tempo, occorre definire fin dall'assessment KPI e parametri di sintesi volti al raffronto di elementi tra loro non omogenei a prima vista. Potendo contare su professionisti ad alte competenze specialistiche e su team multidisciplinari, garantiamo tutto il supporto necessario per affrontare le sfide che DORA pone alle organizzazioni.

POLICY DI RESILIENZA OPERATIVA DIGITALE (DORA)

Principali aspetti normativi

• Uniformare e semplificare le attività degli intermediari finanziari nella gestione dei rischi ICT e Cyber, tramite l'adozione di modelli e procedure comuni.

• Affrontare a livello UE le necessità in materia di Cyber Security, derivanti dalla rapida evoluzione tecnologica dei servizi finanziari, stabilendo meccanismi di verifica dei sistemi ICT.

• Aumentare l'awareness delle entità finanziarie sui rischi informatici/cyber e sugli incidenti ICT al fine di garantire una gestione efficace; con conseguente obbligo di predisporre e adottare un framework di Governance basato su principi e requisiti chiave sul quadro di gestione del rischio ICT.

• Introdurre nuovi poteri per le Autorità di vigilanza finanziaria sia in ambito di controllo e valutazione dei presidi adottati dalle entità finanziarie che nella gestione degli incidenti e valutazione dei rischi derivanti dalla dipendenza delle entità finanziarie dai fornitori di servizi ICT terzi.

Inoltre, il Regolamento DORA impone analisi interpretative approfondite sotto il profilo legale e regolamentare degli impatti delle novità introdotte in materia di resilienza operativa digitale sui diversi quadri normativi e regolamentari di settore.

Contesto normativo

Il Regolamento DORA si interseca trasversalmente nel contesto delle diverse normative applicabili ai vari segmenti del settore Financial Services.

	Banking & Payments Markets	Investement Services	Asset Management	Insurance
INTERNAZIONALE	CRD/CRR	MiFIR	UCITS IV	Solvency II
	PSD2	EMIR	AIFMD	IDD
	EMD2	MiFID2		IORPII
	EBA Guidelines	ESMA Guidelines		EIOPA Guidelines
	GDPR			
	SFDR			
	NIS2 Directive			
	TIBER-EU Framework			

	TUB	TUF	CAP
NAZIONALE	Bol Circ. 285	Regolamento Emittenti	IVASS Reg. 38
	Bol Circ. 288	Regolamento Intermediari	IVASS Reg. 40
	Disp. Vig. IMEL	Reg. attuat. artt. 4-undecies TUF	IVASS Reg. 41
	Perimetro Nazionale di Sicurezza Cibernetica		

POLICY DI RESILIENZA OPERATIVA DIGITALE (DORA)

Consoft Informatica S.r.l. è una società di consulenza informatica che dal **2006** opera su tutto il territorio nazionale, con sedi a Roma, Milano, Napoli e Padova.
Una impresa dinamica e in costante crescita, con oltre 120 dipendenti e ricavi superiori ai 10 milioni di euro (dati esercizio 2024). Sosteniamo il percorso di Digital Transformation dei nostri clienti implementando soluzioni basate su piattaforme tecnologiche leader di mercato, realizzando applicativi custom ed erogando servizi professionali di qualità.
Abbiamo solide competenze verticali e conoscenze tecnologiche trasversali nei settori di mercato a cui ci rivolgiamo, ed I ns sistemi di gestione sono certificate da enti terzi accreditati secondo I seguenti standard internazionali:

9001:2015
14001:2015
45001:2018
27001:2022
37001:2016

Azienda con modello organizzativo gestionale conforme ai requisiti della ISO 25010

A fronte della crescente dipendenza del settore finanziario dalle tecnologie digitali nelle attività e nella prestazione dei servizi finanziari, **Consoft** ha deciso di adottare **il Digital Operational Resilience Act (DORA)** nell'ottica di armonizzazione del contesto regolamentare inerente alla sicurezza delle reti e dei sistemi informativi utilizzati nell'Unione Europea, garantendo la robustezza dei servizi offerti in un contesto tecnologico sempre più complesso. Di seguto una escursus complete sugli adempimenti e le metodologie implementate:

ICT & Cyber Risk Management | articoli 5-16

Governance, Strategia e Struttura Interna

• Istituzione, adozione e approvazione della strategia ICT inclusiva di chiari obiettivi in materia di sicurezza dell'informazione.
• Ruolo centrale dell'organo di gestione che definisce l'assetto organizzativo, metodologico e procedurale per il processo di gestione del rischio ICT e di sicurezza.
• Monitoraggio della corretta applicazione delle politiche e del processo di gestione del rischio ICT.
• Reporting continuo da parte delle funzioni ICT/Cyber sugli incidenti e relative soluzioni correttive implementate.
• Formazione adeguata in materia di rischi ICT e di sicurezza a tutto il personale, incluso il personale che riveste ruoli chiave.

II^ Linea di Difesa

• Politiche e Metodologie di valutazione del rischio ICT/Cyber come rischio operativo.

• Visione ICT/Cyber Risk impostata sui servizi di business forniti alla clientela e al mercato (critical function).
• Continuous improvement process in caso di incidenti.
• Coinvolgimento attivo nei progetti di modifica sostanziale del sistema informativo e, in particolare, nei processi di controllo dei rischi relativi a tali progetti.

I^ Linea di Difesa

• Visione per servizi di business (critical functions), mappatura processi e CMDB.
• Strategia Cybersecurity e implementazione di processi e tecnologie che comprendano la tutela dei dati dei clienti finali in termini di riservatezza, integrità e disponibilità.
• Misure tecniche ed organizzative per la protezione e la prevenzione dai rischi ICT/Cyber, inclusiva di logiche di Zero Trust Security Model.
• Progettazione e realizzazione di infrastrutture ed architetture resilienti.
• Adozione di misure di monitoraggio predittivo e early detection delle anomalie.
• Continuous improvement, root cause e incident post-mortem analysis.
• Strategie di business continuity, back-up, ICT continuity e disaster recovery basate su scenari plausibili e con vista sui servizi di business.

ICT & Cyber Incident Reporting | articoli 17-23

• Implementazione di un processo di gestione per monitorare e registrare gli incidenti ICT/Cyber.
• Classificazione degli incidenti sulla base di soglie di rilevanza e dei criteri stabiliti dal DORA ed ulteriormente sviluppati dalle Autorità Europee di Vigilanza (AEV).
• Segnalazione alle autorità competenti degli incidenti ICT/Cyber in funzione della gravità.
• Armonizzazione dei contenuti e modelli di reporting utilizzati per segnalare gli incidenti.
• Strategie e processi di comunicazione interna/esterna.

Digital Resilience Testing | articoli 24-27

• Definizione di un programma onnicomprensivo di test basici di resilienza operativa digitale per tutti gli intermediari finanziari.
• Definizione di un programma avanzato di Threat Led Penetration Test nei confronti di particolari Istituti Finanziari individuati dalle Autorità Competenti.

Third Party Risk Management & Agreements | articoli 28-44

• Adozione di una strategia per la valutazione, il monitoraggio e la gestione dei rischi derivanti da fornitori di servizi ICT/Cyber di terze parti.
• Previsione di clausole minime uniformi per i diversi operatori del mercato, per la redazione e revisione dei contratti esistenti di outsourcing e di fornitura con provider di servizi ICT/Cyber.

• Istituzione e aggiornamento nel continuo di un apposito Registro delle Informazioni su tutti gli accordi con fornitori ICT/Cyber.
• Monitoraggio dello stato di implementazione delle misure ICT/Cyber da parte dei fornitori di servizi ICT/Cyber.
• Integrazione negli obblighi specifici dei fornitori di aspetti relativi a: Configuration & Asset Management; Incident Management; Location e Storage dei dati; Programma di Test di Resilienza Digitale.
• Previsione di modalità di sorveglianza diretta nei confronti dei Fornitori ICT designati critici.