IDEAS | PEOPLE | TRUST

Digital Operational Resilience Act (DORA)

Contesto attuativo e implementazione del Regolamento EU

BDO

A fronte della crescente dipendenza del settore finanziario dalle tecnologie digitali nelle attività e nella prestazione dei servizi finanziari, il Digital Operational Resilience Act (DORA) si pone 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 finanziari in un contesto tecnologico sempre più complesso.

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.

Applicabilità: i soggetti coinvolti

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

I principali impatti

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.

IIª 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.

Iª 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 alle AEV.
- Strategie e processi di comunicazione interna/esterna.

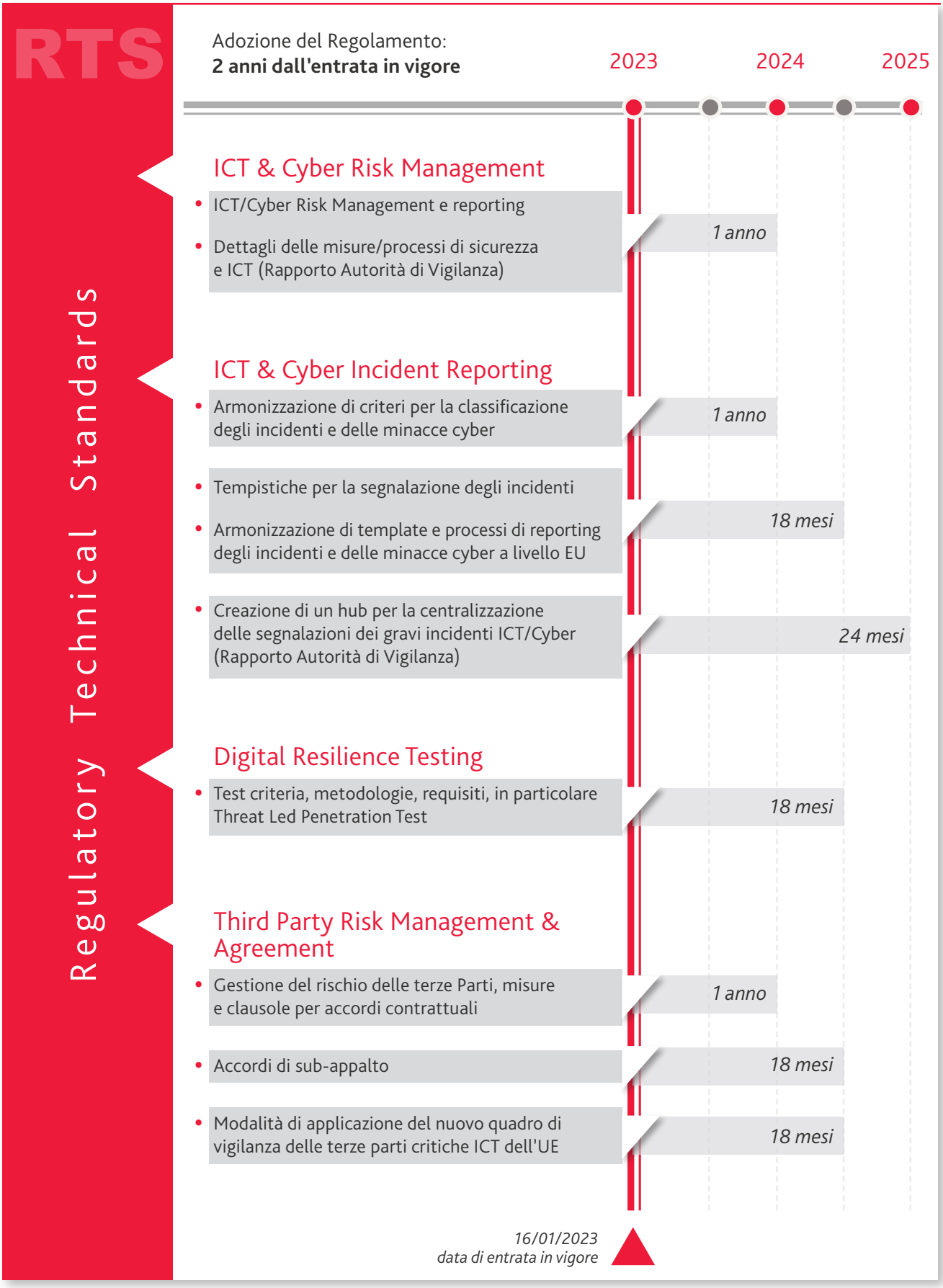
Digital Resilience Testing | articoli 24-27

- 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 FS, 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 da parte delle AEV nei confronti dei Fornitori ICT designati critici.

Le tempistiche



Ulteriori ambiti di attenzione

Condivisione delle informazioni (articolo 45)

Programma (su base volontaria) di condivisione delle informazioni inerenti alle minacce informatiche all'interno della community degli intermediari finanziari soggetti al DORA, con lo scopo di:

- potenziare la resilienza operativa digitale del settore finanziario europeo
- aumentare l'awarness delle minacce informatiche
- contenere la diffusione delle minacce informatiche
- sostenere le capacità di difesa e risposta delle entità finanziarie.

Autorità competenti (articolo 46-50)

Le AEV, attraverso Comitati congiunti e in collaborazione con le Autorità Competenti, la BCE e il CERS, promuovono risposte coordinate a livello europeo al fine di potenziare la resilienza dei sistemi utilizzati dai mercati finanziari.
A tal fine possono:

- istituire meccanismi di condivisione di pratiche efficaci per la creazione di un piano di condivisione dei rischi ICT/Cyber più comuni
- elaborare esercitazioni comuni a livello UE per la gestione delle crisi e delle emergenze, ove simulare scenari di attacchi informatici così da testare l'efficacia delle risposte.

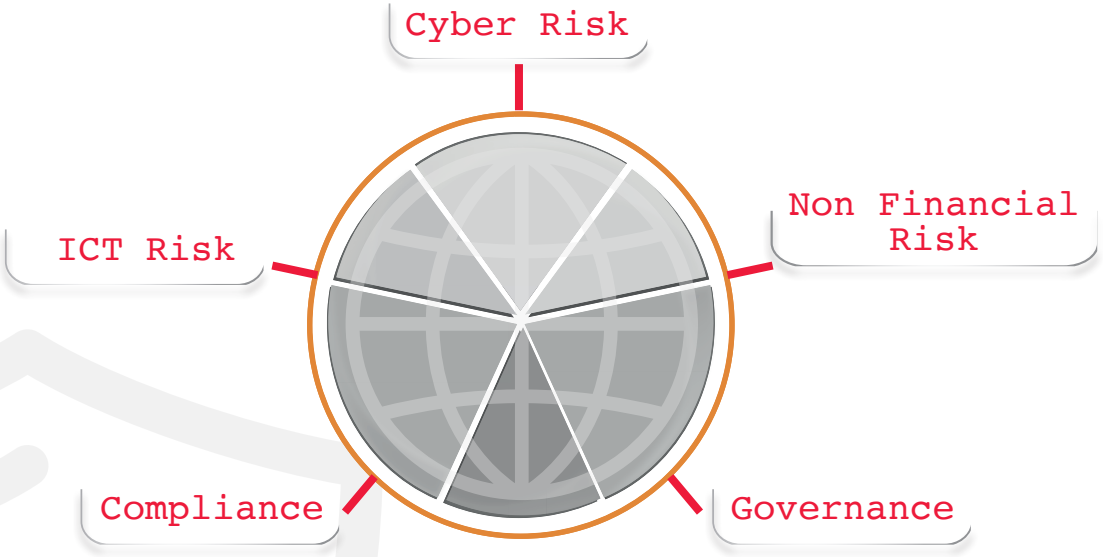
Le nostre soluzioni

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.

Con i nostri professionisti, aiutiamo i nostri clienti ad 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.



esempi

- Valutazione o definizione della strategia di resilienza e inserimento nel framework di rischio
- Progettazione del modello operativo per la gestione della resilienza in azienda
- Valutazione del programma di resilienza per fornire garanzie e assicurare la conformità
- Definizione di un percorso di implementazione per gli adempimenti DORA
- Valutazione del livello di maturità del modello di gestione della resilienza in essere
- Valutazione del quadro di gestione del rischio ICT\Cyber e dei processi di supporto
- Valutazione dei test di resilienza
- Valutazione dei processi di gestione del rischio di terze parti in ambito ICT e implementazione delle azioni per garantire la continuità operativa
- Supporto operativo alla funzione interna di controllo dei rischi ICT e di sicurezza ovvero esternalizzazione del monitoraggio e del controllo dei rischi IT e di sicurezza nel continuo, attraverso il coinvolgimento di un team di professionisti specializzato e qualificato sui principali standard internazionali di riferimento per la gestione ed il controllo dei rischi ICT e di sicurezza

Contatti:

BDO
Viale Abruzzi, 94
20131 Milano

dora@bdo.it

BDO è tra le principali organizzazioni internazionali di servizi alle imprese.

Audit | Advisory | Tax | Law

www.bdo.it

DORA_0723