DORA compliance operativa: implementazione pratica per financial entities e test di resilienza



La DORA compliance è diventata realtà operativa per il settore finanziario europeo dal 17 gennaio 2025, data di applicazione del Digital Operational Resilience Act. Migliaia di entità finanziarie si confrontano oggi non più con l'eventualità di un adeguamento normativo, ma con la concretezza di un regime di vigilanza che ridefinisce il rapporto tra tecnologia, rischio e governance nel sistema finanziario.

Nonostante mesi di preparazione, molte organizzazioni stanno scoprendo che il vero banco di prova della DORA compliance non è stato superare l'audit di conformità, ma trasformare principi regolamentari in prassi operative efficaci. La distanza tra il documento di compliance e la resilienza effettiva è il territorio dove oggi si gioca la partita più significativa.

Il paradosso dell'implementazione della DORA compliance

C'è un paradosso interessante nell'implementazione della **DORA compliance** che emerge con particolare chiarezza nelle conversazioni con i responsabili delle financial entities. Da un lato, il Regolamento (UE) 2022/2554 è stato accolto come strumento necessario per standardizzare approcci frammentati alla gestione del rischio ICT. Dall'altro, la sua natura *principle-based* lascia ampi margini interpretativi che generano incertezza operativa, soprattutto nelle

organizzazioni di dimensioni medio-piccole.

Prendiamo l'articolo 6 del regolamento DORA, che impone l'implementazione di un framework di gestione del rischio ICT "completo, solido ed efficace". Questi tre aggettivi, apparentemente semplici, racchiudono in realtà una complessità implementativa notevole. Cosa rende un framework "completo" nel contesto specifico di una banca regionale con un'infrastruttura *legacy* complessa? Come si misura la "solidità" di un sistema di classificazione degli incidenti? E soprattutto, come si dimostra l'efficacia quando molti scenari di rischio sono per loro natura probabilistici e difficilmente quantificabili *ex ante*?

La risposta che sta emergendo dalla pratica della DORA compliance è che il regolamento richiede un cambio di paradigma culturale prima ancora che tecnologico. Non si tratta di implementare nuovi tool o aggiornare policy esistenti, ma di ripensare il modo in cui l'intera organizzazione percepisce e gestisce il rischio tecnologico.

Governance e ruolo dell'organo direttivo nella DORA compliance

Un elemento distintivo della DORA compliance riguarda il coinvolgimento diretto dell'organo direttivo nella gestione del rischio ICT. L'articolo 5 del regolamento stabilisce responsabilità precise e non delegabili per il *board*, segnando un cambio di paradigma rispetto al passato quando la cybersecurity era spesso relegata a questione puramente tecnica.

L'organo di gestione delle entità finanziarie deve ora approvare, supervisionare e assumersi la responsabilità finale del framework di gestione del rischio ICT. Questo significa che i membri del *board* devono possedere conoscenze sufficienti per comprendere e valutare criticamente i rischi informatici e

il loro impatto potenziale sull'organizzazione. Nella DORA compliance, non è più accettabile che il consiglio di amministrazione si limiti ad approvare formalmente documenti preparati dai dipartimenti tecnici senza comprenderli realmente.

Le organizzazioni più avanzate stanno implementando programmi di *board education* specifici, con sessioni di formazione dedicate che vanno oltre le presentazioni generiche sulla cybersecurity. Questi programmi includono simulazioni di scenari di crisi cyber, analisi di casi reali di incidenti nel settore finanziario, e sessioni di *war gaming* che mettono il *board* di fronte a decisioni strategiche in condizioni di stress e incertezza.

La funzione di controllo ICT: architettura organizzativa della DORA compliance

L'articolo 6, paragrafo 4, del regolamento introduce un requisito organizzativo specifico: le entità finanziarie diverse dalle microimprese devono attribuire la responsabilità della gestione dei rischi informatici a una funzione di controllo indipendente. Questo rappresenta una delle questioni più dibattute nell'implementazione della DORA compliance.

Il regolamento non prescrive una collocazione organizzativa specifica, lasciando alle entità la flessibilità di adattare la funzione alle proprie strutture di governance. Tuttavia, la Banca d'Italia nella sua comunicazione del 30 dicembre 2024 ha chiarito che la scelta sulla collocazione organizzativa non deve pregiudicare l'efficace svolgimento di tutti i compiti attribuiti alla funzione di controllo ICT.

Nella pratica della DORA compliance, si stanno delineando diversi modelli organizzativi. Alcune organizzazioni

istituiscono una funzione autonoma dedicata, altre integrano i compiti nella funzione di *risk management*, altre ancora nella funzione di *compliance*. Il criterio discriminante non è tanto la collocazione formale quanto l'effettiva indipendenza, le competenze disponibili e la capacità di dialogare efficacemente sia con i team tecnici sia con il vertice aziendale.

È importante notare che la funzione di controllo ICT non può essere affidata alla struttura che svolge la funzione di *internal audit*, per evitare conflitti di interesse. Questo aspetto della DORA compliance richiede una chiara separazione dei ruoli all'interno dell'organizzazione.

Test di resilienza operativa digitale: dall'adempimento formale alla sostanza

Se c'è un ambito in cui il divario tra forma e sostanza della **DORA compliance** rischia di essere più evidente, è quello dei test di resilienza operativa digitale previsti dall'articolo 25. Molte financial entities hanno dovuto ammettere che i *penetration test* condotti negli anni precedenti, pur formalmente corretti, erano spesso esercizi circoscritti che poco rivelavano sulla capacità complessiva dell'organizzazione di resistere e reagire a stress tecnologici significativi.

La tassonomia dei test DORA

Il Regolamento DORA introduce una tassonomia articolata che prevede:

- Test di vulnerabilità e scansioni;
- Analisi *open source;*
- Valutazioni della sicurezza di rete;
- *Gap analysis;*

- Esami di sicurezza fisica;
- Questionari e soluzioni software di scansione;
- *Penetration test* basati su sorgenti;
- Threat-Led Penetration Testing (TLPT).

Quest'ultimo, obbligatorio per le entità finanziarie di maggiori dimensioni e da condurre almeno ogni tre anni, rappresenta un salto qualitativo rispetto alle pratiche convenzionali della DORA compliance.

Caratteristiche del threat-led penetration testing

Il TLPT, disciplinato dagli articoli 26 e 27 del regolamento DORA, non è un semplice test tecnico, ma una simulazione avanzata che mima le tattiche, le tecniche e le procedure di attori ostili reali. Richiede l'uso di *threat intelligence* aggiornata, l'impiego di tester qualificati che ragionino come veri avversari, e soprattutto un approccio che testi non solo la tenuta dei sistemi tecnologici, ma anche la capacità di *detection*, *response* e *recovery* dell'intera organizzazione.

Nella pratica della DORA compliance, un TLPT ben condotto può durare settimane, coinvolgere team *red* che operano senza preavviso sui perimetri di attacco, e generare scenari di stress che mettono alla prova non solo l'infrastruttura ma anche i processi decisionali, le comunicazioni interne, e la capacità di coordinamento tra diverse funzioni aziendali. Il framework segue le linee guida TIBER-EU, garantendo un approccio armonizzato a livello europeo.

Requisiti per i tester e certificazioni

Un aspetto critico della DORA compliance riguarda i requisiti per i soggetti che conducono i TLPT. L'articolo 27 stabilisce che i tester devono:

- Dimostrare il massimo grado di idoneità e reputazione;

- Possedere capacità tecniche e organizzative ed esperienza specifica nel campo delle analisi delle minacce, dei *penetration test* e dei test *red team;*
- Essere certificati da un ente di accreditamento in uno Stato membro o aver adottato codici formali di condotta o quadri etici;
- Fornire una garanzia indipendente o una relazione di audit concernente la solida gestione dei rischi derivanti dallo svolgimento di TLPT;
- Essere coperti da un'assicurazione di responsabilità professionale.

Particolare attenzione nella DORA compliance va posta sulla possibilità di utilizzare tester interni. Il regolamento lo consente, ma con condizioni stringenti: l'uso di tester interni deve essere approvato dall'autorità competente, deve essere garantita l'assenza di conflitti di interesse, e in ogni caso ogni terzo test deve essere condotto da tester esterni. Inoltre, la *threat intelligence* deve sempre essere fornita da un soggetto esterno, anche quando il team *red* è interno.

I sei criteri di classificazione degli incidenti ICT

Un aspetto fondamentale della DORA compliance riguarda la capacità di classificare correttamente gli incidenti ICT. L'articolo 18 del regolamento stabilisce sei criteri specifici che le entità finanziarie devono utilizzare per determinare se un incidente debba essere classificato come *major* e quindi segnalato alle autorità competenti.

I sei criteri di classificazione sono:

1. **Numero di clienti o controparti finanziarie interessate**: soglie quantitative specifiche determinano quando l'impatto è considerato significativo;

2. **Durata dell’incidente**: la persistenza nel tempo dell’interruzione o del malfunzionamento è un indicatore chiave;
3. **Distribuzione geografica**: l’estensione territoriale dell’impatto viene valutata in relazione alle operazioni dell’entità;
4. **Perdite di dati**: qualsiasi compromissione dell’integrità, disponibilità, riservatezza o autenticità dei dati, anche una sola violazione di dati sensibili;
5. **Criticità dei servizi interessati**: l’impatto sulle funzioni essenziali o importanti dell’entità finanziaria;
6. **Impatto economico**: le perdite effettive o potenziali, inclusi i costi diretti e indiretti dell’incidente.

Nella DORA compliance, questi criteri devono essere applicati in modo combinato, e il superamento anche di una sola soglia può determinare la classificazione come incidente *major*. Le organizzazioni stanno implementando sistemi di *scoring* automatizzati che valutano in tempo reale gli incidenti rispetto a questi criteri, consentendo decisioni rapide sulla necessità di segnalazione.

Gestione del rischio di terze parti: il nodo critico della DORA compliance

Forse l’aspetto più dirompente della DORA compliance riguarda il Capo V sulla gestione del rischio derivante dai fornitori terzi di servizi ICT. Il regolamento introduce un regime di *oversight* che impatta in modo particolare sui fornitori di servizi *cloud*, che vengono ora sottoposti a un framework di vigilanza diretta da parte delle autorità europee.

Obblighi contrattuali secondo l’articolo 30

Per le financial entities, questo si traduce in obblighi contrattuali stringenti. L’articolo 30 del regolamento DORA richiede che gli accordi con i fornitori ICT includano clausole dettagliate che coprono:

- Descrizione chiara e completa di tutte le funzioni e i servizi ICT da prestare;
- Luoghi di elaborazione e conservazione dei dati, con obbligo di notifica preventiva di eventuali cambiamenti;
- Disposizioni in materia di disponibilità, autenticità, integrità e riservatezza dei dati;
- Garanzie di accesso, ripristino e restituzione dei dati in formato accessibile;
- Livelli di servizio concordati con obiettivi quantitativi e qualitativi precisi;
- Termini di preavviso e obblighi di segnalazione;
- Diritti di accesso, ispezione e audit, inclusi quelli delle autorità competenti;
- Strategie di uscita (*exit strategy*) con periodo di transizione obbligatorio.

Il punto più delicato della DORA compliance riguarda i diritti di accesso, ispezione e audit che l’entità finanziaria deve potersi riservare, incluso il diritto delle autorità competenti di condurre ispezioni dirette presso i locali del fornitore.

Questo ha generato tensioni significative nelle negoziazioni contrattuali, soprattutto con i grandi *provider cloud* internazionali abituati a modelli contrattuali standardizzati. Giganti tecnologici come Google Cloud e Microsoft hanno dovuto adattare i propri termini contrattuali per rispondere ai requisiti della DORA compliance, offrendo *mappature* specifiche dell’articolo 30 e documentazione di supporto per i clienti del settore finanziario.

Il registro dei contratti e la valutazione del rischio di concentrazione

Il registro dei contratti con fornitori terzi di servizi ICT, previsto dall'articolo 28, è diventato uno strumento di governance essenziale nella DORA compliance. Le Autorità di Vigilanza Europee hanno pubblicato gli *Implementing Technical Standards* (ITS) che definiscono i modelli standard per questo registro.

Le entità finanziarie devono documentare:

- Identificazione dei fornitori di servizi ICT e delle entità che partecipano agli accordi contrattuali;
- Informazioni relative all'identificazione delle funzioni esternalizzate;
- Informazioni sulla catena di fornitura dei servizi ICT;
- Informazioni sulla valutazione dei servizi ICT offerti;
- Cronologia di eventi rilevanti, come interruzioni o incidenti;
- Misure di controllo e monitoraggio delle *performance* e della sicurezza;
- Informazioni sulla conformità normativa;
- Dettagli sui piani di *exit* e strategie di transizione.

Un aspetto cruciale della DORA compliance è la valutazione del rischio di concentrazione, disciplinata dall'articolo 29. Le entità finanziarie devono analizzare se dipendono in modo eccessivo da un singolo fornitore o da un gruppo ristretto di fornitori, valutando i potenziali meccanismi di *lock-in* tecnologico e contrattuale. Questa analisi deve essere condotta sia a livello individuale sia, quando applicabile, su base consolidata.

La designazione dei fornitori

critici e il framework di vigilanza

Un elemento innovativo della DORA compliance è il framework di *oversight* sui fornitori terzi critici di servizi ICT (*Critical Third-Party Providers* – CTPP), disciplinato dagli articoli 31-44 del regolamento.

Le Autorità di Vigilanza Europee (EBA, EIOPA, ESMA) hanno la responsabilità di identificare e designare come critici quei fornitori di servizi ICT il cui malfunzionamento potrebbe avere impatti sistemici sul settore finanziario europeo. Il processo di designazione segue una roadmap precisa:

1. **Valutazioni di criticità**: le autorità conducono valutazioni basate su criteri quali l'importanza sistemica, il numero e la tipologia di entità finanziarie servite, la concentrazione di mercato
2. **Notifica ai fornitori**: entro luglio 2025 per la prima designazione, con un periodo di sei settimane durante il quale i fornitori possono presentare obiezioni motivate
3. **Designazione finale**: dopo la valutazione delle eventuali obiezioni, pubblicazione della lista dei CTPP
4. **Avvio della vigilanza**: i fornitori critici entrano nel perimetro di vigilanza diretta delle autorità europee

Una volta designati come critici, i fornitori ICT sono soggetti a un regime di vigilanza che include ispezioni generali e sul posto, richieste di informazioni, raccomandazioni e, in caso di inosservanza, sanzioni pecuniarie che possono raggiungere l'1% del fatturato mondiale medio giornaliero dell'anno precedente.

Questo aspetto della DORA compliance rappresenta un cambiamento significativo nel rapporto tra autorità di vigilanza finanziaria e fornitori tecnologici, tradizionalmente soggetti a regimi di supervisione diversi o inesistenti.

Framework di gestione degli incidenti ICT nella DORA compliance

Il framework di gestione degli incidenti ICT stabilito dal Capo III introduce tempistiche di notifica stringenti che hanno costretto molte organizzazioni a ripensare i propri processi di *incident response*. La classificazione degli incidenti come *major*, basata sui sei criteri precedentemente illustrati, richiede capacità di assessment rapido che non tutte le entità avevano sviluppato.

Tempistiche di segnalazione

Nell'ambito della DORA compliance, le tempistiche di segnalazione sono rigide:

- **Segnalazione iniziale**: entro 4 ore dalla classificazione dell'incidente, e comunque non oltre 24 ore dalla sua identificazione;
- **Relazione intermedia**: entro 72 ore dalla prima notifica, per aggiornare le informazioni disponibili;
- **Relazione finale**: entro un mese dalla risoluzione dell'incidente, contenente l'analisi delle cause, l'impatto finale e le misure correttive adottate.

Tutti i report devono essere trasmessi tramite i canali indicati dalle autorità di vigilanza competenti, in formato standardizzato secondo quanto previsto dagli ITS. In Italia, le entità finanziarie si rivolgono a Banca d'Italia per il settore bancario, IVASS per quello assicurativo, Consob per i mercati finanziari e COVIP per la previdenza complementare.

Cultura dell'apprendimento post-incident

Ma al di là degli aspetti procedurali della DORA compliance, c'è una dimensione più profonda che merita attenzione. Il regolamento spinge verso una cultura dell'apprendimento *post-*

incident che vada oltre la semplice *remediation* tecnica. I report intermedi e finali richiesti devono includere analisi delle cause radice, valutazioni dell'efficacia della risposta, e identificazione delle lezioni apprese.

Le organizzazioni più mature nella DORA compliance stanno adottando approcci strutturati di *post-incident review* che coinvolgono non solo i team tecnici ma anche il management, utilizzando framework consolidati come i *blameless postmortem* mutuati dall'ingegneria del software. L'obiettivo non è individuare responsabili, ma comprendere i fattori sistemici che hanno permesso l'incidente e migliorare la resilienza complessiva dell'organizzazione.

Il regolamento richiede esplicitamente che le entità finanziarie conducano verifiche tecniche approfondite, che possono includere attività di *digital forensic*, collaudi sui sistemi colpiti, analisi dei registri di *log*, e valutazione delle debolezze organizzative o di processo che hanno favorito l'incidente. I risultati di queste analisi devono essere formalizzati in report interni e condivisi con gli organi di governance, in particolare con la funzione di gestione del rischio ICT, al fine di integrare le misure correttive nelle policy e procedure adottate.

Competenze e consapevolezza: il fattore umano nella DORA compliance

Un aspetto spesso sottovalutato nelle discussioni sulla DORA compliance riguarda i requisiti in termini di competenze e consapevolezza. L'articolo 9 del regolamento stabilisce che le entità finanziarie devono disporre di personale con competenze e conoscenze sufficienti nel campo ICT, e che il management deve possedere una comprensione adeguata dei rischi legati al digitale.

Nella pratica della DORA compliance, questo si traduce in

programmi di formazione articolati che devono raggiungere diversi livelli organizzativi. Non è sufficiente che i team tecnici conoscano le *best practice* di cybersecurity; è necessario che il *board* comprenda realmente le implicazioni strategiche delle scelte tecnologiche, che i *risk manager* sappiano dialogare efficacemente con i responsabili IT, e che le prime linee operative possano riconoscere e segnalare tempestivamente anomalie potenzialmente rilevanti.

Alcune financial entities stanno sperimentando approcci innovativi per la DORA compliance, come *simulation game* che mettono il management in scenari di crisi cyber realistici, costringendoli a prendere decisioni con informazioni parziali e sotto pressione temporale. Questi esercizi rivelano spesso gap significativi nella comprensione dei processi di *incident response* e nella capacità di coordinamento tra diverse funzioni aziendali.

Il regolamento non prescrive modalità specifiche di formazione, ma stabilisce il principio che le competenze devono essere proporzionate alla complessità, al profilo di rischio e alle dimensioni dell'entità finanziaria. Le organizzazioni più avanzate stanno implementando programmi di *cyber awareness* continui, che vanno oltre le tradizionali sessioni annuali di formazione obbligatoria, includendo simulazioni di *phishing*, newsletter periodiche su minacce emergenti, e meccanismi di *gamification* per mantenere alta l'attenzione del personale.

RTS e ITS: il completamento del quadro normativo DORA

Sebbene il Regolamento (UE) 2022/2554 sia direttamente applicabile dal 17 gennaio 2025, il quadro normativo della DORA compliance non è ancora del tutto completo. Il regolamento ha conferito alle Autorità di Vigilanza Europee (ESA) il mandato di elaborare *Regulatory Technical Standards*

(RTS) e *Implementing Technical Standards* (ITS) per specificare e armonizzare aspetti tecnici dell'implementazione.

Il 17 gennaio 2025, le ESA hanno pubblicato il primo set di RTS e ITS, attualmente al vaglio della Commissione Europea. Tra i documenti più rilevanti per la DORA compliance:

- **RTS sulla gestione del rischio ICT**: specifiche su politiche, procedure, protocolli e strumenti per la sicurezza ICT;
- **RTS sul TLPT**: criteri per identificare le entità tenute a condurre test guidati dalla minaccia, requisiti per i tester interni, metodologia e approccio per ogni fase del testing;
- **ITS sui modelli di segnalazione**: template standardizzati per la notifica degli incidenti ICT alle autorità competenti;
- **ITS sul registro dei contratti**: modelli standard per documentare gli accordi con fornitori terzi di servizi ICT;
- **Regolamento delegato (UE) 2024/1774**: che delinea le policy di *risk management* per l'identificazione e valutazione dei rischi ICT.

Le entità finanziarie impegnate nella DORA compliance devono monitorare costantemente l'evoluzione di questi standard tecnici, poiché introducono requisiti operativi specifici che vanno oltre i principi generali del regolamento. La procedura di approvazione degli RTS e ITS prevede che la Commissione Europea possa sollevare obiezioni entro tre mesi dalla ricezione; in assenza di obiezioni, gli standard sono considerati adottati.

Sanzioni e meccanismi di enforcement della DORA compliance

Un aspetto che conferisce concretezza alla DORA compliance è

il regime sanzionatorio previsto dal regolamento. Le autorità competenti di ciascuno Stato membro hanno il potere di imporre sanzioni amministrative alle entità finanziarie che non rispettano gli obblighi del regolamento.

Sebbene DORA non specifichi importi sanzionatori fissi lasciando questa determinazione agli Stati membri, il regolamento stabilisce che le sanzioni devono essere effettive, proporzionate e dissuasive. Le autorità competenti possono:

- Richiedere alle entità finanziarie di adottare misure di sicurezza specifiche e di correggere vulnerabilità;
- Imporre la cessazione di determinati comportamenti;
- Sospendere l'esercizio di alcune attività;
- Richiedere la sostituzione di membri dell'organo di gestione;
- Applicare sanzioni pecuniarie amministrative.

Per i fornitori terzi critici di servizi ICT, il regolamento è più specifico: l'articolo 35 prevede che l'autorità di sorveglianza capofila possa imporre sanzioni fino all'1% del fatturato mondiale medio giornaliero dell'anno precedente in caso di inosservanza delle misure richieste.

Un elemento importante della DORA compliance è che le sanzioni non si applicano solo in caso di incidenti effettivi, ma anche per inadeguatezze nei framework preventivi, carenze nei test di resilienza, o mancato rispetto degli obblighi di segnalazione e documentazione. Questo sottolinea come il regolamento premi un approccio proattivo alla gestione del rischio piuttosto che reattivo agli incidenti.

DORA compliance e convergenza normativa: NIS2, GDPR, CER

Un aspetto cruciale nell'implementazione della DORA compliance

riguarda la necessità di coordinare gli adempimenti con altre normative europee che intersecano il dominio della sicurezza ICT. Le entità finanziarie si trovano oggi a dover gestire un ecosistema normativo complesso dove diversi regolamenti e direttive si sovrappongono parzialmente.

DORA e NIS2

La Direttiva NIS2 sulla sicurezza delle reti e dei sistemi informativi presenta numerosi punti di contatto con DORA, ma con un ambito di applicazione più ampio che include tutti i settori critici. Per le entità finanziarie che rientrano in entrambi i perimetri, è fondamentale comprendere come i requisiti si intersechino.

DORA, essendo un regolamento specifico per il settore finanziario, prevale sulla NIS2 per le entità finanziarie (*lex specialis*). Tuttavia, alcuni aspetti della NIS2 possono essere complementari, in particolare per quanto riguarda la cooperazione transfrontaliera e la condivisione di informazioni sulle minacce. Le organizzazioni più efficienti nella DORA compliance stanno adottando un approccio integrato che considera entrambi i framework normativi come parti di una strategia di sicurezza complessiva.

DORA e GDPR

Il rapporto tra DORA compliance e GDPR è particolarmente rilevante per quanto riguarda la gestione degli incidenti che coinvolgono dati personali. Un incidente ICT che comporti una violazione di dati personali (*data breach*) richiede adempimenti sia ai sensi di DORA sia ai sensi del GDPR.

Le tempistiche di notifica sono diverse: DORA prevede 4 ore per la notifica iniziale degli incidenti *major*, mentre il GDPR richiede 72 ore per la notifica delle violazioni di dati personali all’autorità di protezione dati. Inoltre, DORA richiede la notifica all’autorità di vigilanza finanziaria,

mentre il GDPR richiede la notifica al Garante per la Protezione dei Dati Personali.

Le organizzazioni impegnate nella DORA compliance devono predisporre procedure che gestiscano in parallelo entrambi gli obblighi di notifica, evitando duplicazioni inutili ma garantendo che tutte le autorità competenti ricevano le informazioni necessarie nei termini previsti. Molte entità stanno adattando le procedure di notifica dei *data breach* già esistenti per integrarle con i nuovi requisiti DORA.

DORA e Direttiva CER

La Direttiva sulla resilienza dei soggetti critici (CER) introduce obblighi di resilienza fisica e operativa per le entità considerate critiche, includendo potenzialmente anche entità del settore finanziario. La DORA compliance si concentra sulla resilienza operativa digitale, mentre la CER ha un approccio più ampio che include anche aspetti di sicurezza fisica.

Le entità finanziarie che rientrano in entrambi i perimetri devono integrare i requisiti di resilienza digitale di DORA con quelli più ampi di resilienza fisica e operativa della CER. Questo richiede un coordinamento tra diverse funzioni aziendali (IT, sicurezza fisica, *business continuity*, *risk management*) e la predisposizione di piani di resilienza integrati che considerino sia le minacce cyber sia quelle fisiche.

Prospettive evolutive: verso una resilienza adattiva nella DORA compliance

Guardando oltre l’immediato orizzonte della DORA compliance, emerge una domanda fondamentale: il regolamento riuscirà a

trasformare realmente la resilienza operativa del settore finanziario europeo, o rimarrà un ulteriore strato di adempimenti burocratici?

La risposta dipenderà in larga misura da come le organizzazioni sceglieranno di interpretare e implementare la DORA compliance. Se l'approccio sarà puramente difensivo e formalistico, il rischio è di creare sistemi di conformità rigidi che non si traducono in miglioramenti sostanziali della capacità di resistere a shock operativi. Se invece DORA verrà utilizzato come catalizzatore per ripensare in profondità la governance del rischio tecnologico, potrebbe effettivamente contribuire a costruire un sistema finanziario più robusto.

Il concetto di adaptive resilience

Un segnale interessante nella DORA compliance viene dall'attenzione crescente verso concetti come l'*adaptive resilience*: l'idea che i sistemi complessi non possano essere resi resilienti attraverso controlli statici, ma debbano sviluppare capacità dinamiche di *sensing*, *adaptation* e *learning*. In quest'ottica, i test di resilienza non sono momenti circoscritti di verifica, ma occasioni continue di apprendimento; le policy non sono documenti da aggiornare periodicamente, ma framework viventi che evolvono in risposta a nuove minacce e vulnerabilità; e la DORA compliance non è uno stato da raggiungere, ma un processo di miglioramento continuo.

Alcune organizzazioni all'avanguardia stanno sperimentando l'uso di *digital twin* e dati sintetici per condurre assessment continui delle infrastrutture, riducendo i tempi di valutazione e aumentando la confidenza nei risultati. Piattaforme automatizzate di emulazione delle minacce consentono di testare continuamente la resilienza dei sistemi senza impattare sugli ambienti di produzione, offrendo una risposta più dinamica alle minacce in evoluzione rispetto ai test triennali previsti dal regolamento.

L’evoluzione delle minacce e la necessità di agilità

Un aspetto critico della DORA compliance che emerge dalle discussioni tra esperti riguarda la rapidità con cui evolvono le minacce informatiche. Il white paper su DORA, LOTL e Threat Shifting evidenzia come le tecniche *Living Off the Land* (LOTL), che permettono agli attaccanti di utilizzare strumenti già presenti nei sistemi target, stiano rendendo le intrusioni sempre più rapide e difficili da rilevare.

In questo contesto, test di resilienza condotti ogni tre anni rischiano di diventare obsoleti molto rapidamente. La DORA compliance più efficace sarà quella che interpreta i requisiti minimi del regolamento come punto di partenza, non come punto di arrivo, implementando meccanismi di assessment e adattamento continui che permettano di mantenere un livello di preparazione adeguato rispetto a un panorama di minacce in costante evoluzione.

Il ruolo dell’intelligenza artificiale

L’intelligenza artificiale sta emergendo come elemento chiave sia nelle strategie di attacco sia in quelle di difesa. Le organizzazioni impegnate nella DORA compliance stanno esplorando l’uso dell’AI per migliorare la capacità di *detection* precoce delle anomalie, automatizzare le risposte agli incidenti, e ottimizzare l’allocazione delle risorse di sicurezza.

Tuttavia, l’AI introduce anche nuove sfide. Gli attaccanti utilizzano sistemi di intelligenza artificiale per automatizzare la ricognizione, personalizzare gli attacchi di *social engineering*, e identificare vulnerabilità più rapidamente. La DORA compliance del futuro dovrà necessariamente includere strategie specifiche per gestire i rischi legati all’AI, sia come vettore di attacco sia come

componente critica delle difese.

Sfide operative nell'implementazione della DORA compliance

L'implementazione pratica della DORA compliance presenta sfide operative significative che vanno oltre gli aspetti puramente tecnici o normativi. Le organizzazioni si trovano ad affrontare questioni di allocazione delle risorse, gestione del cambiamento organizzativo, e bilanciamento tra innovazione e sicurezza.

Investimenti necessari

La **DORA compliance** richiede investimenti significativi in diverse aree:

- **Tecnologie avanzate di sicurezza**: sistemi di rilevamento delle intrusioni (IDS/IPS), soluzioni di crittografia, strumenti di monitoraggio continuo, piattaforme di *threat intelligence*
- **Formazione continua**: programmi strutturati per tutto il personale, dalle prime linee al *board*
- **Consulenze specialistiche**: per test di resilienza, *gap analysis*, implementazione di nuovi framework
- **Aggiornamento delle infrastrutture**: modernizzazione di sistemi *legacy*, implementazione di architetture *zero-trust*, miglioramento delle capacità di *backup* e *disaster recovery*

Per le entità finanziarie di dimensioni medio-piccole, questi investimenti possono rappresentare una sfida significativa. Tuttavia, il regolamento prevede un quadro semplificato per le microimprese (articolo 16), riconoscendo la necessità di proporzionalità negli adempimenti.

Gestione del cambiamento culturale

Uno degli aspetti più sottovalutati della DORA compliance riguarda la necessità di un profondo cambiamento culturale all'interno delle organizzazioni. La transizione da un approccio alla sicurezza ICT prevalentemente reattivo e focalizzato sulla conformità a un approccio proattivo e orientato alla resilienza richiede tempo e leadership forte.

Le organizzazioni che hanno maggiore successo nell'implementazione della DORA compliance sono quelle che hanno investito nella creazione di una cultura della sicurezza condivisa, dove ogni dipendente comprende il proprio ruolo nella protezione dell'organizzazione. Questo richiede comunicazione costante, esempi concreti dall'alto, e meccanismi di incentivazione che premino comportamenti virtuosi.

Conclusioni: la DORA compliance come opportunità strategica

Il settore finanziario europeo si trova oggi in una fase di transizione delicata. I prossimi mesi diranno se la DORA compliance avrà contribuito a creare organizzazioni realmente più resilienti, o se avrà semplicemente aggiunto complessità normativa senza benefici tangibili. La sfida è trasformare obblighi regolamentari in capacità organizzative autentiche, e in questo percorso, la differenza la faranno le scelte concrete di implementazione che ogni entità finanziaria sta facendo in queste settimane.

Le organizzazioni che interpreteranno la DORA compliance come mera *checklist* da completare rischiano di sprecare risorse significative senza ottenere miglioramenti sostanziali nella resilienza. Al contrario, quelle che vedranno in DORA un'opportunità per ripensare profondamente la propria governance del rischio tecnologico, per modernizzare

infrastrutture obsolete, e per sviluppare competenze critiche, si troveranno non solo conformi al regolamento ma anche meglio posizionate per competere in un mercato sempre più digitale e interconnesso.

La vera misura del successo della DORA compliance non sarà il numero di audit superati o di documenti prodotti, ma la capacità effettiva delle entità finanziarie europee di resistere, rispondere e riprendersi da eventi avversi che inevitabilmente si verificheranno. In questo senso, DORA rappresenta non tanto un punto di arrivo quanto un punto di partenza per un percorso di miglioramento continuo della resilienza operativa digitale del sistema finanziario europeo.

Risorse utili per approfondire la DORA compliance e l'implementazione pratica del regolamento:

Framework DORA e cybersecurity: analisi 7Layers

DORA come baluardo della cybersicurezza

White paper: DORA, LOTL e Threat Shifting

Testo ufficiale del Regolamento (UE) 2022/2554

Linee guida Banca d'Italia su DORA

European Banking Authority – DORA Resources

Condividi sui Social Network:
https://www.ictsecuritymagazine.com/articoli/dora-compliance/