
DORA e la nuova architettura della resilienza operativa

Controllo, continuità e scelta tecnologica.

aruba.it

RES

Il Digital Operational Resilience Act (DORA) è uno dei pilastri della strategia dell'Unione Europea per rafforzare la solidità del sistema finanziario nell'era digitale. Il Regolamento (UE) 2022/2554 introduce un quadro armonizzato per la gestione del rischio ICT, con l'obiettivo di prevenire, gestire e recuperare da incidenti tecnologici che potrebbero compromettere la stabilità dei mercati.

Nel nuovo contesto regolatorio europeo, integrità dei dati, sicurezza e fiducia non sono più caratteristiche accessorie dell'infrastruttura digitale, ma assumono il ruolo di elementi strutturali dell'architettura operativa delle organizzazioni finanziarie. In altre parole, la compliance va inserita sin dal design e non aggiunta in corsa o alla fine come mero accessorio, rappresenta un'occasione strategica per evolvere l'intera organizzazione verso modelli più robusti, agili e sicuri.

La resilienza operativa richiesta dal DORA implica, infatti, un approccio di **"compliance by design"**, in cui i requisiti normativi vengono integrati fin dalle prime scelte architettureali e operative. Questo principio si traduce in un modello di "end-to-end integrity", nel quale fiducia e sicurezza devono essere incorporate lungo l'intero stack digitale, dai data center fisici fino alle interazioni digitali più remote.

Questo paper analizza gli elementi operativi chiave del DORA e propone linee guida concrete per supportare banche, assicurazioni e infrastrutture di mercato finanziario (FMI) nella costruzione di una resilienza digitale reale, non soltanto dichiarata.

Molte organizzazioni si proclamano "resilienti", concretamente poche lo dimostrano nei fatti sotto stress operativo o sotto audit. Per costruire davvero un'organizzazione resiliente servono scelte concrete e approcci integrati. Prendiamo l'esempio di interruzioni recenti su hyperscaler globali: interi ecosistemi fermi per ore, con impatti a catena. Il DORA non è solo normativa. Cambia il paradigma: l'infrastruttura digitale ora è al cuore della stabilità finanziaria, nella gestione del rischio IT, della cybersecurity e della continuità operativa. Negli ultimi dieci anni il settore ha scommesso su cloud e big provider globali: benefici enormi in scalabilità e innovazione, ma anche rischi sistemici. La dipendenza da pochi vendor, infatti, crea concentrazioni pericolose.

Il DORA affronta proprio questo rafforzando il quadro di resilienza operativa ICT che:

- **entra in un quadro di vigilanza armonizzato UE;**
- **diventa responsabilità diretta del board;**
- **estende il controllo alla supply chain digitale.**

Non basta più la conformità formale, fatta di policy o procedure sulla carta. La resilienza operativa è il risultato di un lavoro strutturato, che coinvolge persone, processi, tecnologie e governance ben prima che un incidente si verifichi.

La vera domanda è: **l'organizzazione garantisce continuità, controllabilità e resilienza digitale?**

Qui il DORA cambia paradigma: non si tratta più di un tema puramente tecnico, ma di governance, sovranità digitale e stabilità finanziaria.

La resilienza operativa non riguarda soltanto la gestione degli incidenti o la conformità normativa. Sempre più spesso implica la capacità delle organizzazioni di mantenere controllo sulle proprie scelte tecnologiche nel tempo.

La gestione del rischio digitale, il rischio di concentrazione dei fornitori e le decisioni architetturali sull'infrastruttura sono quindi strettamente collegati a un tema più ampio: la capacità delle imprese di **controllare strategicamente il proprio ecosistema tecnologico senza perdere governance su dati, infrastrutture e opzioni future.**

Sommario

01	Fondamenti e pilastri della resilienza operativa	5
02	A chi si applica DORA	7
03	Timeline dell'applicabilità e dell'evoluzione regolatoria	8
04	Il ruolo delle persone e delle competenze	9
05	Toolkit pratico: requisiti contrattuali operativi	10
06	Gestione e monitoraggio dei fornitori ICT e roadmap resilienza operativa	12
07	Estensione del rischio digitale: il ruolo della brand protection	13
08	Il rischio di concentrazione: una variabile sistemica spesso sottovalutata	15
09	Aruba e la resilienza operativa nel contesto DORA	17
10	La nuova valuta della fiducia finanziaria	19
11	Conclusioni e azioni prioritarie	21

CAPITOLO 01

Fondamenta e pilastri della resilienza operativa

Il DORA introduce un quadro normativo armonizzato per la gestione del rischio ICT che coinvolge migliaia di entità finanziarie europee e i rispettivi fornitori di tecnologie dell'informazione e della comunicazione (TIC).

L'obiettivo è superare la frammentazione delle normative nazionali e stabilire un approccio comune alla resilienza operativa digitale.

Si tratta di rafforzare le misure di sicurezza informatica e, in una lettura più ampia, di costruire un modello di gestione del rischio capace di prevenire, gestire e ripristinare rapidamente le funzioni operative critiche anche in presenza di perturbazioni gravi.

1 ICT RISK MANAGEMENT

Le entità finanziarie devono adottare un framework strutturato di gestione del rischio ICT, sotto la responsabilità ultima dell'organo di gestione. Il modello deve includere l'identificazione degli asset critici, la definizione delle strategie di resilienza e processi di monitoraggio continuo dell'infrastruttura digitale.

3 RESILIENCE TESTING

Il DORA introduce programmi di test periodici obbligatori per verificare la capacità delle organizzazioni di resistere a scenari di stress operativo. Per alcune entità finanziarie di maggiore rilevanza è previsto, con cadenza triennale, il Threat-Led Penetration Testing (TLPT) condotto secondo il framework europeo TIBER-EU.

2 INCIDENT REPORTING

Gli incidenti informatici devono essere gestiti attraverso procedure di classificazione e reporting basate sull'impatto dell'incidente e sulla criticità dei servizi interessati. Gli eventi classificati come gravi devono essere notificati tempestivamente alle Autorità di Vigilanza secondo criteri armonizzati a livello europeo.

4 THIRD-PARTY RISK MANAGEMENT (TPRM)

La resilienza operativa non riguarda più soltanto i sistemi interni, ma l'intera catena di fornitura digitale. Il DORA richiede quindi una gestione strutturata del rischio associato ai fornitori ICT, introducendo strumenti di monitoraggio, requisiti contrattuali specifici e poteri di supervisione diretta sulle infrastrutture tecnologiche critiche.

Il framework DORA si fonda su alcuni pilastri principali che definiscono l'architettura della resilienza operativa nel settore finanziario europeo.

CAPITOLO 02

A chi si applica DORA

Il DORA si applica a un ampio spettro di soggetti del sistema finanziario europeo e dei fornitori tecnologici che ne supportano le attività operative.

Il Regolamento agisce come *lex specialis* rispetto alla Direttiva NIS2: per gli ambiti coperti dal DORA, le entità finanziarie applicano il quadro previsto dal Regolamento, evitando sovrapposizioni normative.

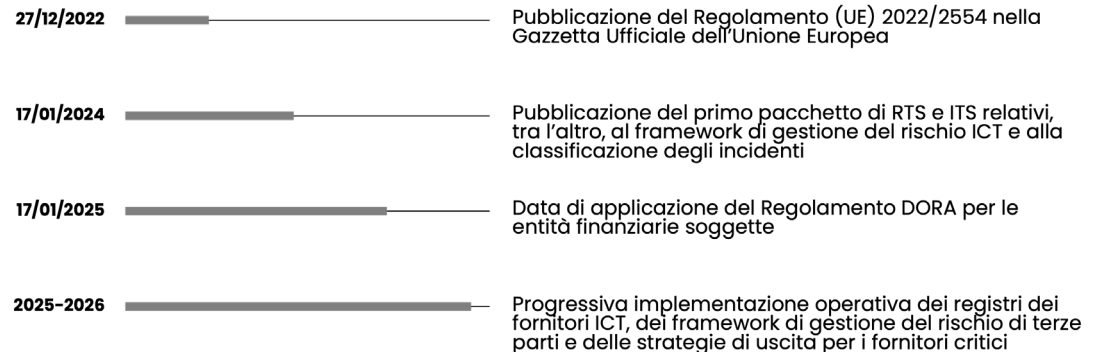
L'obiettivo è creare un quadro di resilienza operativa coerente per l'intero ecosistema, includendo sia le entità regolamentate sia i fornitori ICT che supportano funzioni essenziali o importanti.

CATEGORIA	ESEMPI SOGGETTI INCLUSI	REQUISITI SPECIFICI
ENTITÀ FINANZIARIE	Banche, assicurazioni, istituti di moneta elettronica, piattaforme di crowdfunding, operatori di crypto-asset (CASP)	Implementazione completa o semplificata del framework DORA e responsabilità diretta del Board sulla resilienza operativa ICT
FORNITORI ICT	Cloud provider, operatori di data center, servizi fiduciari, software provider	Possibile designazione come fornitori ICT critici e assoggettamento alla vigilanza diretta delle Autorità Europee di Vigilanza

CAPITOLO 03

Timeline dell'applicabilità e dell'evoluzione regolatoria

L'adeguamento al DORA richiede un percorso progressivo che tiene conto non solo del testo del Regolamento, ma anche delle norme tecniche di regolamentazione e di attuazione (RTS e ITS) sviluppate dalle Autorità Europee di Vigilanza.



CAPITOLO 04

Il ruolo delle persone e delle competenze

Spesso si tende a leggere questi obblighi di compliance esclusivamente in chiave tecnologica, dimenticando che la resilienza digitale si costruisce anche con le persone, in almeno tre direzioni.

- **Mentalità e cultura organizzativa orientate alla resilienza:** definire con chiarezza ruoli, responsabilità e procedure, ma anche allenare l'organizzazione ad agire con consapevolezza e velocità quando si verificano eventi inattesi.
- **Diffusione della consapevolezza a tutti i livelli aziendali:** ogni individuo, non solo gli specialisti IT o gli addetti alla cybersecurity, è parte integrante del sistema di sicurezza.
- **Competenze specifiche per gestire e valorizzare la tecnologia:** non solo skill tecnici, ma anche capacità di governance, comunicazione, gestione del rischio e incident response.

Per CIO e CISO è importante costruire un percorso che tenga insieme strumenti innovativi e sviluppo delle competenze, per una solida cultura aziendale orientata alla sicurezza. **Per il Regolamento DORA è fondamentale e necessaria la formazione a tutti i livelli.**

Responsabilità e conseguenze della non conformità

La conformità alle prescrizioni del Regolamento DORA non può essere semplicemente vista dal punto di vista dei suoi aspetti regolatori, tecnici o contrattuali, ma deve riguardare l'intera governance dell'organizzazione.

Il Regolamento stabilisce chiaramente che l'organo di gestione detiene la responsabilità ultima per la gestione del rischio ICT e per la resilienza operativa dell'organizzazione.

La conformità non può quindi essere delegata esclusivamente alle funzioni tecniche o di sicurezza informatica, ma deve essere guidata nei processi di governo e supervisione strategica.

CAPITOLO 05

Toolkit pratico: requisiti contrattuali e operativi

La gestione dei fornitori ICT deve basarsi su una mappatura del rischio coerente con il framework DORA, che parte dall'identificazione delle funzioni di business supportate da servizi importanti distinguendo in particolare le funzioni essenziali o importanti dalle altre attività operative.

Per i servizi che supportano tali funzioni, il Regolamento richiede l'inclusione nei contratti con i fornitori ICT di specifiche clausole che garantiscano trasparenza, controllabilità e resilienza operativa.

I contratti relativi a funzioni essenziali o importanti devono includere almeno i seguenti elementi.

1

DIRITTI DI AUDIT E ISPEZIONE

Diritti di audit e di accesso alle informazioni che consentano all'entità finanziaria e alle autorità competenti di verificare il rispetto dei requisiti di resilienza operativa.

2

STRATEGIE DI USCITA (EXIT STRATEGIES)

Piani di uscita e di transizione che consentano la migrazione dei servizi e dei dati verso un altro fornitore o verso soluzioni interne senza compromettere la continuità delle funzioni critiche.

3

NOTIFICA DEGLI INCIDENTI

Obblighi contrattuali di notifica tempestiva degli incidenti ICT rilevanti, in linea con i requisiti di reporting previsti dal DORA.

4

SUPPORTO ATTIVITÀ

Impegno del fornitore a supportare le attività di testing della resilienza operativa, inclusi i test di penetrazione basati sulle minacce (TLPT) quando richiesti dalle autorità di vigilanza.

5

TRASPARENZA DATI

Informazioni chiare sulla localizzazione dei dati, sui regimi giuridici applicabili e sulle misure di sicurezza adottate per proteggerli.

6

SERVICE LEVEL AGREEMENT

Definizione di livelli di servizio e parametri di continuità operativa (ad es. RTO e RPO) coerenti con i requisiti di resilienza delle funzioni supportate.

7

GESTIONE DEL SUB-OUTSOURCING

Condizioni chiare per il ricorso a subfornitori, inclusi obblighi di notifica, trasparenza e diritti di opposizione da parte dell'entità finanziaria.

8

PIANI DI EMERGENZA E SICUREZZA ICT

Obbligo di implementare, testare e mantenere piani operativi d'emergenza e misure di sicurezza adeguate.

CAPITOLO 06

Gestione e monitoraggio dei fornitori ICT e roadmap della resilienza operativa

Il DORA richiede alle entità finanziarie di mantenere un registro aggiornato degli accordi con i fornitori ICT che supportano le attività operative.

Questo registro rappresenta uno degli strumenti principali per la gestione del rischio di terze parti e per il monitoraggio della dipendenza da servizi tecnologici esterni.

Il registro deve consentire alle organizzazioni di identificare chiaramente:

- i fornitori coinvolti nella fornitura di servizi ICT;
- le funzioni aziendali supportate da tali servizi;
- la classificazione delle funzioni come essenziali o importanti;
- il profilo di rischio associato al fornitore;
- le condizioni di portabilità dei dati e le strategie di uscita.

Queste informazioni permettono alle istituzioni finanziarie e alle autorità di vigilanza di valutare il livello di concentrazione dei fornitori, la dipendenza da infrastrutture tecnologiche esterne e la capacità dell'organizzazione di mantenere la continuità operativa in caso di interruzione del servizio.

Roadmap della resilienza operativa

Le attività di testing previste dal DORA dovrebbero seguire un percorso progressivo di maturità, volto a rafforzare progressivamente la capacità dell'organizzazione di prevenire, rilevare e gestire incidenti ICT.

Un percorso tipico include:

- **vulnerability assessment**, per identificare vulnerabilità tecniche nei sistemi e nelle infrastrutture ICT;
- **gap analysis**, per valutare il livello di conformità rispetto ai requisiti di resilienza operativa;
- **test di scenario end-to-end**, per verificare la continuità delle funzioni critiche in condizioni di stress operativo.

Inoltre, con un percorso ad hoc, vengono pianificati in collaborazione con le Autorità competenti i **Threat-Led Penetration Testing (TLPT)**, test avanzati basati su scenari di minaccia reali condotti periodicamente per le entità finanziarie di maggiore rilevanza.

CAPITOLO 07

Estensione del rischio digitale: il ruolo della brand protection



Accanto alla gestione del rischio ICT interno e alla supervisione della supply chain tecnologica, emerge un ulteriore livello di esposizione spesso sottovalutato: quello legato all'ecosistema digitale esterno in cui operano brand, servizi e identità delle istituzioni e delle entità finanziarie.

Attacchi di phishing, typosquatting o altre applicazioni fraudolente o di impersonificazione del brand, generate dall'abuso di domini internet, rappresentano vettori di rischio in grado di compromettere la continuità operativa, la fiducia degli utenti e l'integrità dei servizi digitali, pur avendo origine al di fuori del perimetro infrastrutturale tradizionale.

In questo scenario, **la protezione proattiva del proprio brand assume un ruolo complementare ai framework di ICT Risk Management e Third-Party Risk Management:** pur non essendo esplicitamente prevista dal Regolamento DORA, la protezione del brand diventa quindi parte integrante di un modello di "end-to-end integrity", contribuendo a intercettare minacce che possono tradursi in incidenti operativi rilevanti.

Integrare strumenti di brand protection nei processi di gestione del rischio digitale consente alle organizzazioni di **rafforzare la propria postura di sicurezza** in modo proattivo, **migliorare le capacità di incident detection** e **ridurre l'esposizione a eventi** che, pur non originandosi da vulnerabilità interne, possono avere impatti significativi su clienti, operatività e compliance.

CAPITOLO 08

Il rischio di concentrazione: una variabile sistemica spesso sottovalutata

In diversi confronti con istituzioni finanziarie emerge ancora una sottovalutazione del rischio di concentrazione tecnologica. Questo rischio viene spesso percepito come un tema puramente tecnico o infrastrutturale, mentre rappresenta in realtà una questione strategica di resilienza operativa.

Uno dei rischi osservati con crescente attenzione dalle Autorità Europee di Vigilanza non riguarda solo il singolo incidente informatico, ma il livello di concentrazione delle infrastrutture tecnologiche utilizzate dal settore finanziario. Quando un numero elevato di soggetti o istituzioni finanziarie dipende dalle stesse piattaforme o dagli stessi fornitori ICT, si crea una potenziale vulnerabilità sistemica.

In questo scenario:

- aumenta il rischio di impatti simultanei su più operatori finanziari;
- cresce la complessità delle attività di supervisione e vigilanza;
- si riduce la capacità effettiva di migrazione verso fornitori alternativi;
- aumenta l'esposizione a rischi operativi, infrastrutturali e geopolitici.

La **concentrazione tecnologica** è una tematica che va assolutamente presieduta, non può più essere considerato marginale a livello di governance. Se ignorato comporta un rischio troppo alto.

Per questo motivo il DORA introduce un meccanismo specifico per l'identificazione dei fornitori ICT critici, affidando alle Autorità Europee di Vigilanza il compito di monitorare i provider la cui operatività può avere impatti significativi sul funzionamento del sistema finanziario.

Per il board e il top management emerge quindi una domanda strategica:

Quanto è distribuito il nostro rischio digitale?

La resilienza operativa non riguarda soltanto la sicurezza informatica, ma la capacità dell'organizzazione di progettare un'architettura tecnologica resiliente, controllabile e verificabile. In questo contesto, la scelta delle infrastrutture tecnologiche diventa una decisione strategica. Non riguarda soltanto performance o scalabilità, ma anche il livello di controllo, auditabilità e resilienza operativa che un'organizzazione è in grado di garantire nel tempo.

Dal framework regolatorio all'architettura operativa

L'implementazione del DORA non dipende esclusivamente da policy e controlli interni, richiede anche scelte architetturali coerenti con i principi di resilienza operativa, controllabilità delle infrastrutture e gestione del rischio di terze parti.

In questo contesto, **la selezione dei fornitori ICT assume una rilevanza strategica**: non riguarda soltanto le prestazioni tecnologiche, ma anche la capacità del provider di supportare i requisiti di auditabilità, governance e resilienza richiesti dal quadro regolatorio europeo.

CAPITOLO 09

Aruba e la resilienza operativa nel contesto DORA

La scelta del fornitore ICT affianca alla consolidata valutazione tecnologia, una riflessione sulla governance del rischio.

Le istituzioni finanziarie devono essere in grado di dimostrare non solo la sicurezza dei propri sistemi, ma anche la trasparenza, l'auditabilità e la resilienza dell'intera supply chain digitale.

In questo scenario, **Aruba si propone come partner tecnologico europeo in grado di supportare organizzazioni che operano in contesti regolati**, contribuendo a ridurre la complessità operativa e a rafforzare la controllabilità delle infrastrutture ICT.

1. Infrastruttura digitale integrata

Aruba è uno dei principali operatori europei in grado di offrire una filiera di servizi digitali integrata che comprende:

- **data center proprietari** certificati, conformi alla normativa Rating 4 ANSI/TIA;
- **servizi cloud e infrastrutture** distribuite in regioni europee;
- **servizi di cybersecurity**;
- **servizi fiduciari** qualificati ai sensi del Regolamento eIDAS;
- **soluzioni di crittografia** in conformità PSD2;
- **connettività e interconnessioni**.

All'interno del Gruppo, le **Certification Authority Actalis** e **Aruba PEC** forniscono le fondamenta certificate che supportano i servizi fiduciari su cui Aruba eroga su larga scala servizi quali posta elettronica certificata (PEC), certificati e firme digitali.

Questa integrazione verticale contribuisce a semplificare la gestione della supply chain ICT e può supportare le organizzazioni nella gestione del Third Party Risk Management (TPRM) richiesto dal DORA.

2. Auditabilità e collaborazione operativa

Il framework DORA richiede alle istituzioni finanziarie di poter dimostrare la controllabilità dei fornitori ICT e la capacità di effettuare verifiche tecniche e organizzative.

Aruba viene sottoposta in modo continuativo ad audit interni ed a verifiche di

terze parti indipendenti, ad opera di auditor qualificati e di organismi di certificazione accreditati. Inoltre, Aruba supporta processi di assessment, audit e verifiche ispettive condotte dai clienti e dalle autorità di vigilanza, favorendo un livello elevato di trasparenza operativa. Questo approccio consente alle organizzazioni di gestire con maggiore efficacia i requisiti di controllo previsti dai framework regolatori.

3. Flessibilità contrattuale per clienti Enterprise

Rispetto ai modelli contrattuali fortemente standardizzati di alcuni provider globali, **Aruba è in grado di soddisfare le esigenze di flessibilità contrattuale per clienti Enterprise**. I clienti possono richiedere clausole specifiche in funzione delle proprie esigenze operative, di compliance o di governance del rischio ICT. Questo approccio facilita la costruzione di accordi contrattuali allineati ai requisiti regolatori e alle specifiche esigenze di resilienza operativa.

4. Un unico interlocutore per infrastruttura e gestione operativa

Oltre ai servizi infrastrutturali, trust e cloud, **Aruba offre servizi di gestione operativa attraverso soluzioni di Managed Services**. Questo modello consente alle organizzazioni di ridurre la frammentazione della filiera tecnologica tra molteplici fornitori e di

mantenere un unico interlocutore per infrastruttura, piattaforme e gestione operativa. La semplificazione della supply chain ICT rappresenta un elemento rilevante nella gestione del rischio di terze parti.

5. Governance e infrastruttura europea

La struttura societaria e la natura giuridica del Gruppo Aruba, interamente soggetto al diritto dell'Unione Europea, garantiscono che il controllo strategico e decisionale dei servizi sia esercitato esclusivamente all'interno della giurisdizione europea.

Questo permette ad Aruba di garantire la localizzazione geografica e giuridica dei dati e il controllo esclusivo sulle loro operazioni di trattamento e conservazione grazie:

- al rispetto dell'applicazione dei requisiti necessari per i framework normativi europei di riferimento (GDPR, NIS2, DORA, ecc...);
- all'indipendenza da conflitti normativi con leggi extra-europee a effetto territoriale (es. US CLOUD Act, Patriot Act, Chinese Cybersecurity Law, ecc...);
- all'effettiva tutela, da parte delle autorità comunitarie, dei diritti degli utilizzatori dei servizi e utenti europei.

In un contesto in cui il tema della sovranità digitale assume crescente rilevanza nelle strategie tecnologiche, **la governance europea delle infrastrutture rappresenta un elemento distintivo** per molte organizzazioni regolamentate.

Un provider europeo è in grado di supportare le aziende non solo nella compliance normativa, ma anche nella costruzione di un modello di governance IT più autonomo e resiliente.

6. Solidità industriale

Aruba rappresenta oggi una delle principali infrastrutture digitali private europee. L'azienda ha ottenuto qualificazioni rilevanti nel mercato delle infrastrutture digitali e dei servizi cloud per contesti mission-critical e regolati.

La solidità economico-finanziaria del Gruppo e la crescita costante dell'organizzazione rappresentano elementi importanti per soggetti che devono garantire continuità operativa nel lungo periodo.



CAPITOLO 10

La nuova valuta della fiducia finanziaria

Il mercato finanziario digitale non misura più la fiducia soltanto in termini di solidità patrimoniale, ma sempre più spesso dipende dalla capacità delle organizzazioni di garantire continuità operativa, controllo delle infrastrutture tecnologiche e gestione trasparente del rischio digitale.

Elementi come la continuità operativa dimostrabile, controllo sui dati, gestione del rischio di concentrazione e auditabilità delle infrastrutture diventano componenti essenziali della fiducia nel sistema finanziario. Le istituzioni o entità finanziarie che interpreteranno il DORA non solo come un obbligo regolatorio, ma come un'opportunità per rafforzare la propria resilienza operativa, potranno consolidare il proprio posizionamento nei confronti di clienti, investitori, autorità di vigilanza e partner internazionali. La resilienza operativa diventa quindi un elemento sempre più rilevante della competitività nel mercato finanziario digitale, uno strumento di governance capace di sostenere la stabilità e l'affidabilità delle organizzazioni in un contesto tecnologico sempre più complesso.

È su questo terreno che **partner tecnologici con esperienza, metodo e visione possono fare la differenza**, aiutando le aziende a trasformare un obbligo normativo in un vantaggio competitivo.

CONCLUSIONI

Azioni prioritarie

L'entrata in vigore del DORA segna il passaggio da un approccio formale alla compliance a un modello di resilienza operativa dimostrabile.

Sottovalutare il ruolo dell'organo di gestione o ignorare la complessità della supply chain ICT espone le organizzazioni a rischi sanzionatori, ma – ben più gravi - di integrità operativa e reputazionale.

Le istituzioni o entità finanziarie che sapranno dimostrare il pieno controllo della propria infrastruttura oltre a registrare piena conformità, rafforzeranno anche la propria competitività.

Le aziende che sapranno selezionare partner capaci di integrare sicurezza, gestione del rischio, supporto operativo e cultura della sovranità digitale saranno quelle più pronte ad affrontare il futuro.

Nella nuova normalità della sicurezza informatica, non basta avere gli strumenti: bisogna saperli utilizzare in modo efficace, responsabile e orientato agli obiettivi di business.

Gap Analysis Strategica

Validare l'allineamento dei framework ICT esistenti ai nuovi Regulatory Technical Standards (RTS).

Blindatura Contrattuale

Aggiornare gli accordi con i fornitori ICT, introducendo clausole che garantiscano trasparenza, auditabilità e strategie di uscita effettivamente attuabili.

Gestione del rischio nella supply chain ICT

Ridurre il rischio di concentrazione attraverso una gestione strutturata della supply chain ICT e una valutazione approfondita dei fornitori tecnologici.
La conformità normativa sta evolvendo rapidamente da semplice obbligo regolatorio a fattore strutturale di competitività.

Quando la fiducia è incorporata nell'architettura tecnologica le organizzazioni possono innovare più velocemente, entrare in nuovi mercati con maggiore sicurezza e dimostrare alle autorità di vigilanza la solidità dei propri modelli operativi.

Il Regolamento DORA rappresenta un passaggio fondamentale: la resilienza operativa abbandona le vesti di puro requisito di conformità, diventa componente essenziale della capacità delle istituzioni finanziarie di evolvere in modo sicuro nel mercato digitale.

È fondamentale costruire relazioni solide e strategiche con provider in grado di affiancare le imprese non solo sul piano tecnico, ma anche su quello consulenziale, operativo e di governance.

Le scelte architetturelle che le organizzazioni compiono oggi, nella gestione delle infrastrutture, dei dati e dei fornitori tecnologici, determineranno il grado di libertà con cui potranno evolvere domani.

La resilienza operativa e la gestione del rischio di concentrazione diventano quindi parte di una questione più ampia: preservare la capacità di scelta tecnologica nel lungo periodo.

About Aruba

Aruba, fondata nel 1994, è il Cloud Champion italiano e uno dei principali provider europei di infrastrutture e piattaforme digitali basate su asset proprietari. L'azienda progetta e gestisce l'intero stack tecnologico: dalla progettazione e costruzione di data center alle piattaforme cloud, dai servizi di trust e security alla connettività e alle soluzioni software che supportano strategie digitali e applicazioni basate su AI.

Con capitale interamente italiano, Aruba conta 16 milioni di utenti attivi sulle proprie piattaforme provenienti da oltre 100 nazioni e gestisce una infrastruttura distribuita su 8 data center in Europa, che ospita oltre 2,7 milioni di domini, 10 milioni di caselle e-mail, 9 milioni di caselle PEC e migliaia di infrastrutture IT di clienti.



Copyright © Aruba. All rights reserved.

Disclaimer: This content is provided for general information purposes and is not intended to be used in place of consultation with our professional advisors.

aruba.it