DB non solo diritto bancario

leggi l'articolo nel sito www.dirittobancario.it

APPROFONDIMENTI

Dalle linee guida sull'outsourcing al third-party risk

La metamorfosi EBA nell'era DORA

Aprile 2026

Savino Casamassima, Partner, Qubit Law Firm & Partners

Savino Casamassima, Partner, Qubit Law Firm & Partners

Savino Casamassima

Savino Casamassima è un Avvocato del Foro di Milano. Ha una significativa esperienza presso studi legali italiani ed internazionali a Milano e Londra ed ha ricoperto funzioni apicali in ambito sia legale che compliance presso banche internazionali e società operanti nel mondo dei servizi bancari e fintech. Già membro di Consigli di Amministrazione ed Organismi di Vigilanza 231 presso banche ed intermediari finanziari internazionali.

1. Premessa

1.1 *Il documento di consultazione e il quadro evolutivo*

Con la pubblicazione, l'8 luglio 2025, del documento di consultazione EBA/CP/2025/12 (Draft Guidelines on the sound management of third-party risk), l'Autorità Bancaria Europea ha avviato un processo di ridefinizione organica del framework regolamentare in materia di rischio da terze parti. Tale processo riguarda il ricorso a soggetti terzi da parte degli intermediari finanziari vigilati, al di fuori del perimetro ICT già presidiato da DORA. Chiusa la fase consultiva l'8 ottobre 2025 e acquisite le osservazioni formulate dagli stakeholders anche nel corso dell'udienza pubblica virtuale del 5 settembre 2025, la versione definitiva delle nuove Linee Guida — la cui adozione è prevista **nel corso del primo semestre 2026 — è destinata a sostituire integralmente le vigenti *EBA Guidelines on outsourcing arrangements* del 2019** (EBA/GL/2019/02), costruendo un regime di più ampia portata per la gestione di tutti gli accordi con terze parti che esulano dalla sfera ICT.

1.2 *L'architettura regolatoria post-DORA: dal sistema dualistico alle nuove Guidelines*

Le nuove Guidelines si inseriscono in un'architettura regolatoria che ha conosciuto una profonda trasformazione nel corso degli ultimi anni. L'entrata in vigore, il 17 gennaio 2025, del Regolamento (UE) 2022/2554 (DORA) ha introdotto un regime specifico, vincolante e direttamente applicabile per la gestione del rischio ICT da terze parti, sottraendo gli accordi aventi ad oggetto servizi ICT al perimetro delle Guidelines del 2019 e assoggettandoli a un corpus normativo strutturalmente diverso: un Regolamento europeo, corredato da una serie articolata di Regulatory Technical Standards (RTS) e Implementing Technical Standards (ITS) elaborati dalle Autorità europee di vigilanza (EBA, EIOPA, ESMA) e adottati dalla Commissione con forza normativa vincolante — tra cui, in particolare, il Regolamento Delegato (UE) 2024/1773 del 13 marzo 2024 (relativo alla politica sugli accordi contrattuali per l'utilizzo di servizi TIC a supporto di funzioni essenziali o importanti) e il Regolamento Delegato (UE) 2025/532 del 24 marzo 2025 (relativo al subappalto di servizi TIC a supporto di funzioni essenziali o importanti). Il risultato, dopo l'entrata in vigore di DORA, è stato un sistema dualistico: rigore sistematico per il rischio ICT, regime pre-esistente del 2019 per tutto il resto. **Le nuove Guidelines si propongono di colmare questa asimmetria**.

vedi l'articolo online

1.3 *Il perimetro soggettivo: nuove entità e confronto con DORA*

La perimetrazione soggettiva delle nuove Guidelines merita un'attenzione specifica, anche in relazione al confronto con DORA. Le nuove Guidelines si applicano agli enti creditizi, agli istituti di pagamento e agli istituti di moneta elettronica già inclusi nel perimetro del 2019, nonché ad alcune nuove categorie: specifiche imprese di investimento (quelle che non soddisfano le condizioni per qualificarsi come piccole e non interconnesse ai sensi del Regolamento IFR, Reg. UE 2019/2033), gli emittenti di asset-referenced tokens (ART) ai sensi del Regolamento MiCAR (Reg. UE 2023/1114 del 31 maggio 2023) e i creditori ipotecari non bancari ai sensi della Direttiva 2014/17/UE. L'ambito soggettivo rimane tuttavia più ristretto rispetto a quello di DORA, che copre un perimetro significativamente più ampio di entità finanziarie, di cui alle oltre venti categorie indicate all'art. 2 del Regolamento — tra cui imprese di assicurazione, controparti centrali, depositari centrali di titoli, gestori di fondi, prestatori di servizi per le cripto-attività — e introduce, per i fornitori ICT designati come critici (Critical ICT Third-Party Service Providers, CTPP), un regime di supervisione diretta da parte delle ESAs senza equivalente nel perimetro non-ICT. Il confronto evidenzia come l'architettura complessiva sia ancora in divenire: l'EBA ha rilevato che un progressivo allineamento del perimetro soggettivo delle nuove Guidelines a quello di DORA sarà oggetto di valutazione nel medio termine, confermando la direzione di marcia verso un framework di third-party risk genuinamente universale.

2. Dal confronto con le Guidelines 2019: la mappa delle discontinuità

L'analisi comparativa tra le Guidelines del 2019 e il documento di consultazione EBA/CP/2025/12 consente di identificare sei assi di discontinuità strutturale che, insieme, definiscono la portata della evoluzione regolamentare in atto.

2.1 *L'ambito oggettivo: dal contratto di outsourcing al Third-Party Arrangement*

Le Guidelines del 2019 adottavano una definizione tecnico-giuridica di «outsourcing» inteso come affidamento continuativo a un prestatore esterno di attività o funzioni che altrimenti sarebbero svolte internamente dall'ente: una nozione selettiva, che escludeva dal perimetro applicativo una vasta gamma di accordi con terze parti non qualificabili come outsourcing in senso stretto, pur generando rischi operativi, reputazionali e di continuità del tutto analoghi. Contratti di fornitura di servizi non continuativi, accordi di collaborazione operativa, partnership commerciali con componenti di servizio, strutture intra-gruppo atipiche: tutti questi accordi restavano al di fuori del perimetro regolamentare. Le nuove Guidelines adottano invece il concetto di Third-Party Arrangement (TPA): qualsiasi accordo contrattuale mediante il quale un soggetto esterno — incluse le entità intra-gruppo — fornisce o supporta funzioni dell'entità finanziaria, a prescindere dalla qualificazione formale dell'accordo. La distinzione, da sempre problematica nell'applicazione pratica delle Guidelines del 2019, tra outsourcing e altre forme di ricorso a terzi viene così superata. Rimane ferma, e strutturale, l'eccezione per gli accordi aventi ad oggetto servizi ICT: questi restano esclusivamente riservati al regime DORA.

2.2 *L'ambito soggettivo: verso un progressivo allineamento*

Come illustrato in premessa, il perimetro di applicazione si estende a nuove categorie di entità finanziarie, segnalando l'intenzione del regolatore di allineare progressivamente le Guidelines al perimetro più ampio già definito da DORA per il dominio ICT. La direzione è chiara anche se il percorso è ancora parziale.

2.3 *L'approccio lifecycle: governance strutturata del ciclo di vita*

Le Guidelines del 2019 regolamentavano i momenti principali del rapporto con il fornitore — due diligence preventiva, requisiti contrattuali, monitoraggio, uscita — senza tuttavia organizzare questi obblighi in un percorso formale e sequenziale. Le nuove Guidelines introducono un approccio lifecycle articolato in **sette fasi identificabili nella struttura del documento:** valutazione preliminare del rischio, due diligence, negoziazione contrattuale, gestione delle sub-esternalizzazioni, monitoraggio continuativo, pianificazione dell'uscita e cessazione effettiva del rapporto. Ciascuna fase è presidiata da obblighi procedurali e sostanziali graduati in funzione della criticità dell'accordo. L'approccio lifecycle non è una mera riorganizzazione formale: impone alle entità di investire nella governance dell'intero ciclo di vita di ogni TPA rilevante, non soltanto nei momenti di ingresso e di crisi, e richiede una capacità organizzativa e documentale strutturalmente più sofisticata rispetto al passato.

vedi l'articolo online

2.4 *Il Registro delle Informazioni (ROI): armonizzazione con DORA*

Le Guidelines del 2019 richiedevano il mantenimento di un registro degli accordi di esternalizzazione, con informazioni dettagliate per le funzioni critiche o importanti (CIF), ma senza un formato armonizzato con altri regimi regolamentari. Le nuove Guidelines prevedono un ROI i cui data point sono progettati per essere coerenti con quelli già richiesti da DORA per gli accordi ICT: **è espressamente ammessa la tenuta di un unico registro integrato per accordi ICT e non-ICT**, e per i TPA non-CIF i requisiti informativi sono calibrati in modo proporzionale, così da evitare oneri sproporzionati. La coerenza con DORA non è solo tecnica: è il segno più tangibile del disegno regolamentare di convergenza.

2.5 *La definizione armonizzata di funzione critica o importante (CIF)*

Le Guidelines del 2019 adottavano una definizione propria di CIF, non pienamente allineata a quella di DORA, con conseguenti incertezze interpretative per le entità soggette a entrambi i regimi, costrette a classificare i propri accordi con criteri parzialmente divergenti. **Le nuove Guidelines adottano la medesima definizione di CIF già introdotta da DORA** all'articolo 3, paragrafo 22: la funzione la cui interruzione o svolgimento difettoso potrebbe materialmente pregiudicare la conformità regolamentare, la performance finanziaria o la continuità operativa dell'entità. Un criterio classificatorio unico per l'intero portafoglio di accordi — ICT e non-ICT — è il presupposto indispensabile per la costruzione di un framework integrato di third-party risk.

2.6 *I requisiti contrattuali e le strategie di uscita*

Le Guidelines del 2019 prescrivevano per i TPA-CIF un insieme di clausole obbligatorie — diritti di audit, cooperazione con il regolatore, continuità del servizio, controllo delle sub-esternalizzazioni — che la prassi aveva ormai consolidato. Le nuove Guidelines introducono obblighi aggiuntivi di rilievo: l'obbligo per il fornitore di partecipare attivamente ai test del Business Continuity Plan (BCP) dell'entità, simulando scenari di interruzione del servizio; requisiti più analitici per la gestione della catena di sub-esternalizzazione di funzioni CIF, con obbligo di approvazione preventiva; strategie di uscita da documentare ex ante, sin dalla fase di negoziazione, con l'identificazione delle soluzioni alternative di sourcing. Quest'ultimo profilo riflette una lezione precisa dell'esperienza applicativa: molte entità si sono trovate in posizione di lock-in verso fornitori strategici, prive di opzioni di uscita genuinamente praticabili, non per una scelta consapevole ma per assenza di pianificazione anticipata.

3. La grammatica del cambiamento: DORA come lente interpretativa

Le discontinuità appena descritte riflettono una trasformazione più profonda del paradigma regolamentare europeo in materia di rischio da terze parti, che il Regolamento DORA ha catalizzato attraverso il suo lungo percorso di elaborazione e di prima attuazione.

3.1 *Le origini sistemiche e le innovazioni strutturali di DORA*

Il percorso verso DORA affonda le radici nel riconoscimento, maturato nel secondo decennio del secolo, che il rischio ICT da terze parti aveva assunto una dimensione sistemica nel settore finanziario. La progressiva concentrazione del mercato dei servizi cloud — con un numero limitato di grandi operatori da cui dipende l'operatività di una quota rilevante delle istituzioni finanziarie europee — rendeva strutturalmente inadeguati i meccanismi di vigilanza indiretta: il regolatore sorveglia la banca, la banca sorveglia il fornitore. In questo schema, la capacità di influenza sul fornitore dipendeva integralmente dal peso contrattuale del singolo ente, non dall'autorità regolatoria. Incidenti di ampia portata a infrastrutture ICT condivise e la pandemia da Covid-19 — che aveva messo sotto pressione le catene di fornitura operative di centinaia di intermediari simultaneamente — avevano offerto al legislatore europeo prove empiriche di questa inadeguatezza sistemica.

DORA ha risposto con tre innovazioni strutturali che hanno cambiato il quadro di riferimento. La prima è l'introduzione di un regime di supervisione diretta dei CTPP da parte delle ESAs: per la prima volta nella storia del diritto europeo della vigilanza finanziaria, un fornitore di servizi a enti vigilati è soggetto a controllo diretto dell'autorità, indipendentemente dall'ente cui presta i propri servizi. La seconda è l'approccio lifecycle integrale e formalizzato: non singoli obblighi di due diligence o requisiti contrattuali, ma una governance continua e documentata dell'intero rapporto con il fornitore ICT, dalla valutazione preliminare alla terminazione. La terza è l'armonizzazione degli strumenti a livello europeo: registro delle informazioni con data point uniformi, definizioni condivise, standard tecnici vincolanti emanati dalle ESAs e adottati dalla Commissione con forza di Regolamento Delegato — una base comune che sostituisce il mosaico di interpretazioni nazionali che aveva caratterizzato l'applicazione delle Guidelines del 2019.

3.2 *Il sistema a due velocità e la risposta dell'EBA*

L'entrata in applicazione di DORA ha tuttavia prodotto un effetto strutturale imprevisto nella sua pienezza: un sistema a due velocità. Gli accordi ICT, presidiati dal rigoroso framework DORA, erano assoggettati a obblighi di governance, documentazione e vigilanza di ben altro livello rispetto agli accordi non-ICT, rimasti sotto le Guidelines del 2019. L'asimmetria era sempre più difficile da giustificare sul piano della coerenza del sistema: il rischio operativo derivante dall'esternalizzazione di funzioni critiche a fornitori non-ICT — società di consulenza gestionale e strategica, studi legali, operatori logistici e di facilities management, provider di servizi HR e compliance — può essere altrettanto materiale di quello derivante da un fornitore cloud. In alcuni casi la situazione è persino più critica: i fornitori non-ICT tendono ad avere catene di fornitura più opache, strutture di governance meno sofisticate e una minore familiarità con le aspettative di vigilanza cui si erano ormai abituati i grandi operatori del settore ICT.

L'EBA ha dunque tratto dalla fase di attuazione di DORA — e dall'esperienza accumulata da migliaia di entità finanziarie impegnate nella gap analysis, nella revisione contrattuale e nella costruzione del ROI — le evidenze necessarie per progettare il nuovo framework non-ICT. Il risultato è visibile nella struttura del documento di consultazione: le nuove Guidelines sono modellate sulla grammatica concettuale di DORA, con gli adattamenti proporzionali dovuti alla diversa natura dei rischi e alla maggiore eterogeneità del mercato dei fornitori non-ICT. Il percorso di DORA ha anche chiarito un aspetto importante sul piano operativo: il Registro delle Informazioni — la cui trasmissione alla Banca d'Italia era stata richiesta con la Comunicazione al mercato del 23 dicembre 2024 (in materia di sicurezza ICT) — e il processo di autovalutazione approvato dall'organo di amministrazione entro il 30 aprile 2025 hanno dimostrato come la costruzione di un'infrastruttura documentale strutturata sia non solo realizzabile in tempi definiti, ma anche capace di migliorare la qualità della governance interna. È su questa esperienza che le nuove Guidelines poggiano la propria ambizione di estendere analoga disciplina al perimetro non-ICT.

3.3 *I limiti strutturali della traslazione al perimetro non-ICT*

È essenziale, tuttavia, evidenziare con precisione i limiti di questa traslazione. **Le nuove Guidelines non replicano il regime di supervisione diretta dei CTPP**: non esiste una lista di «fornitori critici non-ICT» da sottoporre a vigilanza europea, né un'Autorità di Vigilanza designata con poteri di intervento continuativo nei confronti del fornitore. **Il regime applicabile ai fornitori non-ICT si articola su più livelli**, tutti attivabili su iniziativa dell'ente o dell'autorità, ma nessuno assimilabile a una relazione di supervisione proattiva e strutturata quale quella che DORA istituisce per i CTPP. **Il primo è contrattuale**: le nuove Guidelines impongono che i contratti con i TPA-CIF contengano clausole che garantiscano diritti di accesso, audit e cooperazione con l'autorità di vigilanza, rendendo l'adempimento del fornitore un obbligo negozialmente esigibile dall'ente vigilato. **Il secondo livello è di fonte legale primaria**: l'art. 54 TUB attribuisce a Banca d'Italia un potere ispettivo diretto — indipendente dal contenuto contrattuale — presso i soggetti ai quali le banche abbiano esternalizzato funzioni aziendali essenziali o importanti, con obbligo di esibizione di documenti e atti; l'art. 51, comma 1-quinquies TUB estende a tali soggetti gli obblighi di vigilanza informativa. **Il terzo livello è sanzionatorio**: l'art. 144, comma 1, TUB prevede l'applicazione di sanzioni amministrative pecuniarie direttamente nei confronti dei fornitori che violino tali obblighi. Banca d'Italia dispone pertanto, anche nel perimetro non-ICT, di una leva sanzionatoria amministrativa diretta nei confronti del fornitore, ancorché reattiva e circoscritta a specifiche violazioni degli obblighi di cooperazione ispettiva e informativa. È la struttura di questa leva — non la sua assenza — a distinguere il regime non-ICT dal framework DORA/CTPP. DORA costruisce una relazione di supervisione proattiva e continuativa con il fornitore, con obblighi operativi sostanziali, designazione formale e un'Autorità di Vigilanza dedicata, mentre il meccanismo TUB resta una leva ispettiva e sanzionatoria diretta, efficace ma non equivalente sul piano funzionale.

4. L'impatto operativo: sinergie, punti di attenzione e novità

Per gli intermediari italiani già impegnati nell'adeguamento a DORA, l'entrata in vigore delle nuove Guidelines rappresenta al tempo stesso un'opportunità concreta di efficientamento e un onere aggiuntivo di natura genuinamente nuova, che richiede investimenti specifici non interamente riducibili alle attività già svolte per il dominio ICT.

4.1 *Le sinergie con il framework DORA: l'infrastruttura riutilizzabile*

Sul piano delle sinergie, **il vantaggio più immediato riguarda l'infrastruttura del Registro delle Informazioni**. Le entità che hanno investito nella costruzione di un ROI DORA-compliant — con le relative piattaforme tecnologiche, i processi di raccolta e aggiornamento dei dati, i flussi di reportistica inter-

na e di segnalazione verso la Banca d'Italia — potranno estendere la stessa infrastruttura agli accordi non-ICT. L'armonizzazione dei data point tra i due regimi non è un esercizio astratto: è il presupposto che rende possibile la gestione integrata, riducendo i costi marginali di compliance per le entità che scelgono — come è fortemente consigliabile — di adottare un registro unico. **Il framework di governance del rischio terze parti costruito per DORA è una seconda area di sinergia rilevante**: la politica sul rischio da terze parti, il ruolo del Third-Party Risk Manager, i processi di escalation e di reportistica periodica al board, i criteri di classificazione della criticità possono essere adattati — non replicati identicamente, ma adattati — per coprire anche il perimetro non-ICT. La definizione armonizzata di CIF, in particolare, consente di applicare un processo classificatorio unico all'intero portafoglio di accordi, eliminando la duplicazione dei criteri valutativi che aveva caratterizzato il periodo di coesistenza tra le Guidelines del 2019 e DORA. Le metodologie di due diligence e i modelli di clausole contrattuali sviluppati per i fornitori ICT nel contesto DORA, infine, possono servire come base metodologica — da adattare ai profili di rischio tipici dei fornitori non-ICT — per i processi analoghi richiesti dalle nuove Guidelines.

4.2 *Le novità: il perimetro non-ICT come nuova frontiera regolamentare*

Il perimetro non-ICT, quindi, rappresenta una frontiera regolamentare che richiede un approccio genuinamente nuovo. **Il primo elemento aggiuntivo è la mappatura degli accordi non-ICT**: molte entità scopriranno di avere centinaia o migliaia di TPA che non sono mai stati assoggettati a un regime di gestione del rischio equivalente a quello cui sono sottoposti i contratti ICT. La costruzione di questo inventario — classificazione per criticità, identificazione del fornitore, verifica della conformità delle clausole contrattuali esistenti — costituirà da sola un progetto di compliance di significativa portata, che richiede il coinvolgimento coordinato di legal, procurement, risk management e business line. **L'esperienza DORA è utile come metodologia, ma il perimetro da mappare è strutturalmente diverso e, in molti casi, più ampio**.

Il secondo elemento aggiuntivo riguarda la negoziazione con i fornitori non-ICT. I grandi operatori cloud e i principali fornitori di servizi ICT sono ormai abituati — per effetto di DORA e di regimi analoghi in altri ordinamenti — ad accettare diritti di audit, clausole di continuità del servizio e obblighi di cooperazione con le autorità di vigilanza. Non lo sono, in generale ed a mero titolo esemplificativo, gli studi legali, le società di consulenza strategica, i fornitori di servizi HR, di sicurezza fisica o di facilities management: questi operatori non hanno mai avuto l'incentivo a sviluppare la capacità contrattuale e operativa necessaria per accettare e dare esecuzione a tali clausole. La negoziazione dei nuovi obblighi previsti dalle Guidelines — diritti di audit, partecipazione ai test BCP, strategie di uscita documentate — richiederà tempo, leverage contrattuale e, in molti casi, un approccio coordinato a livello di settore o di associazione di categoria, sul modello di quanto già sperimentato nell'ambito ICT.

Particolarmente sfidante appare l'obbligo di partecipazione del fornitore ai test del Business Continuity Plan dell'entità: si tratta di un requisito senza precedenti nel panorama non-ICT, che presuppone un livello di integrazione operativa tra ente finanziario e fornitore non sempre esistente o contrattualmente previsto. La sua attuazione richiederà non soltanto una rinegoziazione contrattuale sostanziale, ma la costruzione di processi congiunti di test e di documentazione degli esiti, in molti casi con fornitori che — a differenza dei grandi player ICT — non dispongono di procedure BCP strutturate.

È essenziale, tuttavia, evitare una lettura indiscriminata del perimetro applicativo. Le nuove Guidelines sono strutturalmente permeate dal principio di proporzionalità, che calibra l'intensità degli obblighi in funzione della criticità della funzione esternalizzata, della dimensione dell'ente e della complessità del rapporto: gli obblighi più onerosi — BCP testing congiunto, diritti di audit estesi, strategie di uscita ex ante documentate — si applicano precipuamente ai TPA-CIF, mentre per i TPA non qualificati come critici o importanti il framework prevede requisiti procedurali e informativi significativamente più leggeri. **La sfida operativa non è quindi di compliance universale sull'intero portafoglio di accordi non-ICT, ma di corretta classificazione iniziale**: un'adeguata mappatura che identifichi con precisione i TPA-CIF consente di concentrare gli investimenti di adeguamento dove il rischio è effettivo, evitando l'estensione indiscriminata dei processi più gravosi — e dei relativi costi di negoziazione con i fornitori — a rapporti che il framework stesso considera a bassa intensità regolamentare.

4.3 *Tre profili di rischio trasversale*

Tre ulteriori punti di attenzione meritano una segnalazione esplicita. Il primo è il **rischio di concentrazione nel dominio non-ICT**, spesso sottovalutato: un'analisi rigorosa del portafoglio TPA può rivelare dipendenze sistemiche da pochi fornitori di servizi professionali — advisor strategici, studi legali di

riferimento, società di revisione — del tutto comparabili, in termini di impatto operativo, alle concentrazioni già mappate per il settore ICT. **Il secondo riguarda la gestione del periodo transitorio**: il documento di consultazione prevede disposizioni transitorie che offriranno un'opportunità di adeguamento progressivo, ma che richiedono un piano di lavoro strutturato fin dall'entrata in vigore delle nuove Guidelines, per evitare di gestire simultaneamente il completamento dell'adeguamento e la revisione periodica già dovuta per DORA. **Il terzo profilo riguarda la risoluzione della «fascia grigia» degli accordi ibridi**: accordi di business process outsourcing con componenti ICT rilevanti, contratti di consulenza che includono accesso a sistemi e dati dell'ente, partnership operative complesse. Questi accordi — rimasti in un'area di ambiguità classificatoria nel periodo di coesistenza tra le Guidelines 2019 e DORA — dovranno ora essere definitivamente ricondotti al regime ICT (DORA) o al regime non-ICT (nuove Guidelines), con le relative conseguenze contrattuali e di processo. La corretta delimitazione del perimetro rappresenta, in questo senso, la prima e più critica delle attività di adeguamento.

5. Conclusioni

Il percorso che conduce dalle Guidelines EBA sull'outsourcing del 2019 al documento di consultazione EBA/CP/2025/12 non è una semplice revisione tecnica: è l'espressione di una trasformazione paradigmatica nel modo in cui il diritto europeo della vigilanza finanziaria concepisce il rischio da terze parti. **Da fattispecie giuridica circoscritta — l'outsourcing, con la sua definizione tecnica e le sue condizioni applicative — a concetto operativo omnicomprensivo — il third-party risk, inteso come il rischio derivante dall'intera rete di accordi che connettono l'entità finanziaria al suo ecosistema di fornitori** — il framework regolamentare ha percorso in poco più di un lustro una distanza concettuale considerevole.

DORA ha funzionato da acceleratore e da modello. Ha dimostrato che un approccio lifecycle integrale, strumenti armonizzati e standard tecnici vincolanti a livello europeo non sono soltanto possibili ma efficaci nel presidiare rischi che il precedente quadro regolamentare faticava a governare. Le nuove Guidelines trasferiscono quella grammatica al dominio non-ICT, con gli adattamenti proporzionali dovuti alla maggiore eterogeneità del mercato dei fornitori e alla diversa struttura dei rischi. L'architettura che ne risulta — DORA per il rischio ICT da terze parti, nuove Guidelines per il rischio non-ICT — costituisce la **prima risposta genuinamente organica al problema della dipendenza strutturale delle entità finanziarie dall'ecosistema esterno di fornitura**. Le due componenti del sistema sono progettate per essere coerenti, non sovrapposte: **perimetri soggettivi convergenti, definizioni armonizzate, registri integrabili**.

Per gli intermediari italiani, la finalizzazione delle nuove Guidelines segna l'avvio di un percorso di adeguamento che conviene anticipare. Le sinergie con i processi DORA già costruiti sono reali e significative, ma sfruttarle pienamente richiede un **approccio integrato alla governance del rischio terze parti**, non la replica di compartimenti regolamentari separati. **Le principali novità** — la mappatura del perimetro non-ICT, la negoziazione con fornitori non avvezzi alle clausole di vigilanza, l'obbligo di BCP testing esteso al dominio non-ICT, la risoluzione degli accordi ibridi ICT/non-ICT — **richiedono investimenti specifici e pianificazione anticipata, non riducibili all'esperienza DORA già maturata**.

Per i professionisti del diritto bancario e della compliance, questa fase rappresenta una straordinaria opportunità di contributo sostanziale. La costruzione di framework integrati di third-party risk management, capaci di incorporare la complessità della doppia regolazione DORA e nuove Guidelines in architetture operative coerenti e proporzionate, richiede una competenza trasversale — legale, operativa, tecnologica — che è la cifra distintiva del professionista di valore nell'ecosistema regolamentare contemporaneo. Il perimetro si è espanso: la responsabilità professionale con esso.

DB non solo diritto bancario

A NEW DIGITAL EXPERIENCE

dirittobancario.it