DB non solo diritto bancario

leggi l'articolo nel sito www.dirittobancario.it

APPROFONDIMENTI

La gestione del rischio terze parti alla luce delle nuove EBA Guidelines

Impatti attesi sui modelli operativi

Gennaio 2026

Gianfranco Tessitore, Senior Partner, Deloitte Advisory
Gabriele Manganaro, Senior Manager, Deloitte Advisory

Gianfranco Tessitore, Senior Partner, Deloitte Advisory

Gabriele Manganaro, Senior Manager, Deloitte Advisory

Gianfranco Tessitore
Ha oltre 20 anni di esperienza nel settore bancario e assicurativo a fianco dei principali player di sistema ricoprendo ruoli manageriali in progetti di advisory inerenti gli ambiti Governance, Risk & Regulatory Strategy and Advisory, Business and Controls Transformation, Operational Resilience-DORA, Recovery & Resolution, GRC platforms and RegTech solutions.

Gabriele Manganaro
Ha maturato circa 10 anni di esperienza nel settore bancario e assicurativo in ambito Risk & Regulatory Transformation presso i principali player di sistema, supportandoli in progetti di advisory inerenti la Governance, l'analisi strategica e organizzativa e il disegno di soluzioni di business, organizzative e di risk management.

1. Premessa

Le novità introdotte dal **Regolamento DORA** sulla resilienza operativa digitale (Regolamento UE 2022/2554), tra le quali si sono rivelate di particolare rilevanza ed impatto le aspettative sulla gestione delle terze parti che erogano servizi ICT, hanno rappresentato un punto di svolta a partire dal quale le **Autorità di Supervisione Europee** (cd. "ESAs", che comprendono – oltre l'EBA – anche EIOPA ed ESMA) hanno avviato un percorso strutturato finalizzato a raggiungere obiettivi di rafforzamento e **convergenza della regolamentazione europea** nel settore finanziario su diversi temi. Nell'ambito di tale percorso, che ci si attende essere ampio e di respiro pluriennale, è partita una razionalizzazione ed armonizzazione del complessivo framework regolamentare sulla gestione del rischio derivante da terze parti.

Le nuove "***EBA Guidelines on the sound management of third-party risk***" (EBA/CP/2025/12) rispondono esattamente a questa **finalità**: uniformare la regolamentazione vigente rispetto alle nuove disposizioni previste dal DORA, garantendo uno stretto allineamento tra i due quadri normativi e rafforzando i presidi per la gestione di un rischio sempre più complesso e di rilevanza strategica per la sostenibilità dei modelli di business degli operatori di mercato, come più volte dimostratoci dagli eventi verificatisi negli ultimi anni sia a livello globale che locale.

Le nuove EBA GL, oltre al superamento delle vigenti "*EBA Guidelines on outsourcing arrangements*" (EBA/GL/2019/02), si pongono alcuni obiettivi di rilievo:

- **allargare** il **perimetro soggettivo di applicazione**, andando oltre i soli enti creditizi e imprese di investimento, IP e IMEL e coinvolgendo la maggior parte dei cd. «enti finanziari», (soggetti vigilati per i quali l'EBA ha carattere vincolante e non vigilati per i quali le linee guida assumono valore di best practices o raccomandazioni). Il tutto con la finalità anche di garantire il cd. *level playing field*, obiettivo che vedremo essere complesso in assenza di perimetri oggettivi all'ambito di applicazione della disciplina;
- **estendere** in maniera sostanziale il **perimetro oggettivo di applicazione**: non si parlerà più esclusivamente di servizi esternalizzati (cd. "*Outsourcing arrangements*"), ma di "***Third-Party Arrangements***" (cd. TPA) a tutto tondo;

vedi l'articolo online

- **rafforzare** la **gestione** del **rischio derivante dai fornitori terzi** estendendo la disciplina anche i **servizi non ICT**, non rientranti nel perimetro disciplinato dal DORA (che copre i servizi ICT incluso il cloud), che saranno pertanto regolati dalle nuove EBA GL, garantendo allineamento tra i due quadri normativi.

In questo contesto, il presente contributo si propone di analizzare i **principali elementi di novità** e gli **impatti attesi** sui modelli operativi, sui processi di governance e sulle scelte organizzative delle istituzioni finanziarie, offrendo agli operatori una vista olistica sul tema e una **chiave di lettura pratica** per orientarsi nella nuova disciplina e per poter attivare consapevolmente e tempestivamente il percorso di adeguamento ai nuovi standard.

2. Timeline regolamentare e impatti sulla normativa vigente

L'**8 luglio 2025** l'Autorità Bancaria Europea (EBA) ha avviato una consultazione pubblica finalizzata a definire le **nuove linee guida sulla gestione del rischio di terze parti**, con l'obiettivo di rafforzare la governance e la resilienza operativa nel sistema finanziario europeo in tale ambito sulla scia del percorso avviato dal DORA. **In continuità con il DORA**, ma con un perimetro più ampio, il nuovo framework regolamentare supera la tradizionale focalizzazione sull'outsourcing e introduce un approccio olistico per la gestione delle dipendenze da fornitori esterni, ICT e non-ICT. Per gli operatori finanziari, si apre dunque una fase di profonda revisione dei modelli di governance, dei processi e dei presidi di controllo ma soprattutto si attiva un percorso che porrà sotto la lente di ingrandimento tutta la gestione delle terze parti, incluso il perimetro non disciplinato dal DORA e dalle precedenti linee guida sull'outsourcing.

Il **processo di consultazione si è concluso lo scorso 8 ottobre 2025**, ed ha visto una partecipazione ampia degli operatori di mercato che hanno indirizzato verso l'Autorità numerosi quesiti ("Q&A") finalizzati a meglio comprendere alcune "aree grigie", anche e soprattutto alla luce dell'esperienza applicativa maturata nel percorso di adeguamento al DORA, percorso tra l'altro ancora lontano dal potersi considerare completato. Tra i principali temi sottoposti all'Autorità ci sono:

- Definizione di "ICT Service", ai fini della chiara distinzione tra servizi coperti da DORA e servizi non ICT soggetti alle nuove linee guida EBA;
- Eccessiva estensione del perimetro, con il rischio che anche forniture a basso rischio o irrilevanti per la resilienza siano incluse;
- Incertezza su "funzioni critiche o importanti". La definizione andrebbe allineata pienamente con DORA e chiarita nei criteri applicativi;
- Gestione intra-gruppo: richiesta di linee guida specifiche su obblighi e registrazione dei fornitori interni e sulle modalità di gestione consolidata del rischio terze parti.

In attesa dei riscontri formali ai quesiti posti, la pubblicazione delle nuove **linee guida EBA in versione finale dovrebbe avvenire entro aprile 2026**, salvo slittamenti al momento non prevedibili.

A partire dalla pubblicazione delle nuove linee guida, sarà previsto un *"grace period"* di adeguamento per consentire agli operatori di garantire la piena conformità ai nuovi standard regolamentari. In attesa di comprendere le tempistiche ufficiali, EBA ha già precisato che ci sarà un ***"grace period"* di due anni per l'adeguamento degli standard contrattuali** e del **nuovo Registro Terze Parti** (sui cui dettagli torneremo).

Le implicazioni non finiscono qui. La pubblicazione delle nuove GL implicherà quantomeno:

- l'**abrogazione delle *"EBA Guidelines on outsourcing arrangements"*** (EBA/GL/2019/02) che verranno pertanto superate, o per meglio dire "inglobate" nella nuova disciplina;
- il **recepimento delle nuove EBA GL all'interno del quadro regolamentare nazionale**. Come già avvenne, per le *EBA GL on outsourcing*, la **Circolare di Banca d'Italia n. 285/13** dovrà riflettere i nuovi aggiornamenti (integralmente, o quasi, in considerazione dell'intervento atteso della Vigilanza volto all'integrazione del DORA nelle Disposizioni di Vigilanza, il quale potrebbe influenzare il contenuto e i tempi dell'aggiornamento complessivo;
- **interventi normativi**, nella stessa direzione, **delle altre Autorità di Supervisione Europee**, che già hanno collaborato sinergicamente nel processo di stesura del framework regolamentare DORA e che rifletteranno questi sviluppi all'interno **della normativa di settore.** A riguardo, **ESMA** ha già pubblicato lo scorso 12 giugno 2025 i *"Principles on third-party risks supervision"*. **EIOPA**

invece ha dichiarato, nel proprio "*Annual Work Programme 2026*", che nel Q1 2027 è prevista la revisione dei requisiti in ambito outsourcing, seguendo il percorso già settato da EBA per il contesto bancario.

Ci sono inoltre già stati, o sono attesi, **ulteriori interventi anche da parte dell'Autorità di Vigilanza** nonché delle principali istituzioni finanziarie deputate all'emanazione delle cd. *soft law*, tutti finalizzati ad alzare il livello di maturità del sistema rispetto ai rischi che comporta il ricorso a fornitori esterni:

- ECB Guide on outsourcing cloud services to cloud service providers (luglio 2025) chiarisce le aspettative ECB sul rispetto dei requisiti DORA e fornisce buone prassi per la gestione dei rischi di outsourcing, in particolare per l'uso di servizi cloud di terzi da parte delle banche vigilate. ECB ha inoltre recentemente lanciato un "*Resilience Stress Test on Geopolitical Risks*", nell'ambito del quale è prevista anche la verifica della tenuta dei presidi in ambito outsourcing/terze parti.
- BCBS "*Principles for the sound management of third- party risk*" (dicembre 2025) stabiliscono una base comune e coerente per banche e Autorità di Vigilanza nella gestione dei rischi derivanti da accordi con fornitori terzi di servizi, introducendo un framework strutturato dedicato al rischio terze parti.
- FSB "*Enhancing Third-Party Risk Management and Oversight. A toolkit for financial institutions and financial authorities*" (dicembre 2023) per armonizzare la gestione e la supervisione del rischio di terze parti, riducendo la frammentazione regolamentare e i costi di compliance e favorendo il coordinamento tra autorità, intermediari e fornitori.

In questo articolato contesto regolamentare ciò che è certo è che **le Autorità hanno avviato un percorso di armonizzazione della normativa a livello europeo e nazionale che**, date le modalità di intervento scelte (non a livello centralizzato di ESAs ma a livello di singole Autorità settoriali)**, avrà inevitabilmente un respiro pluriennale**. Gran parte del merito va dato al Regolamento DORA che ha senza dubbio gettato le fondamenta di un **percorso di gestione olistica della resilienza operativa del sistema finanziario** nel quale la gestione delle terze parti gioca un ruolo di primo piano.

3. Principali novità e impatti attesi sui modelli operativi

Analizziamo ora le novità più significative che introducono le nuove EBA GL per la gestione del rischio terze parti.

3.1 *Principali novità*

3.1.1. Estensione del Perimetro di Applicazione (soggettivo e oggettivo)

Le nuove EBA GL hanno esteso il novero dei soggetti obbligati destinatari della disciplina **(perimetro soggettivo di applicazione)** includendo anche:

- le imprese di investimento non classificate come "piccole e non interconnesse" ai sensi dell'art. 12, par. 1, del Regolamento UE 2019/2033 (IFR – Investment Firms Regulation);
- gli emittenti di asset-referenced tokens (ARTs) soggetti al Regolamento UE 2023/1114 (MICAR);
- i creditori come definiti dall'art. 4, par. 2 della Direttiva 2014/17/UE (MCD – Mortgage Credit Directive), quando sono enti finanziari.

Viene inoltre ampliato significativamente il **perimetro oggettivo di applicazione** della regolamentazione che non si limita più agli accordi di outsourcing (perimetro delle *EBA Guidelines on outsourcing arrangements*) e ai fornitori ICT (disciplinati dal DORA), ma include anche tutte forniture di servizi non ICT (con poche esclusioni, disciplinate nel Cap. 3, Comma 32, tra cui relative ai meri acquisti di beni, alle funzioni che devono essere obbligatoriamente da terzi, all'utilizzo delle infrastrutture di mercato, ai servizi bancari di corrispondenza alle utenze, come quelle elettriche e telefoniche).

Allo stesso tempo, viene preservato il ruolo del Regolamento DORA come "*lex specialis*" sulla normativa comunitaria e nazionale. Il DORA continuerà ad applicarsi al perimetro dei servizi ICT, le nuove EBA GL ne estendono i principi per garantire omogeneità di trattamento a tutti gli accordi con terze parti (TPA).

3.1.2. *Classificazione e Valutazione Preliminare*

Entrando nel dettaglio, le nuove EBA GL specificano che per ciascun rapporto con fornitore terzo sarà necessario **effettuare una valutazione preliminare** per determinarne **l'inclusione o meno nel perimetro di applicazione delle Linee Guida**, valutando la presenza di elementi di **ricorrenza/ continuità.**

Questa estensione comporta per molti operatori di mercato l'esigenza di un'**analisi** dello stato dell'arte **del proprio portafoglio fornitori** e di conseguenza una revisione approfondita secondo logiche che ne consentano la governabilità, la sostenibilità (sia rispetto alle strategie che al funzionamento del modello operativo) e il presidio efficace dei rischi sottesi.

Viene introdotto il concetto di **Third-Party Arrangement (TPA)**, definito come qualsiasi accordo tra un'istituzione finanziaria e un fornitore terzo per la fornitura di servizi o funzioni, compresi gli accordi infragruppo. Il TPA rappresenta pertanto l'elemento intorno al quale ruotano due componenti che vanno viste in modo integrato include:

- Tipologia di fornitura:
  - **Outsourcing**: qualsiasi accordo, di qualunque forma, tra un'entità finanziaria e un fornitore di servizi terzo, inclusi i fornitori di servizi terzi infragruppo, in base al quale il fornitore di servizi terzo svolge, su base ricorrente o continuativa, una funzione che altrimenti sarebbe svolta dall'entità finanziaria stessa;
  - **Non Outsourcing**: indica qualsiasi accordo, di qualunque forma, tra un'entità finanziaria e un fornitore di servizi terzo, inclusi i fornitori di servizi terzi infragruppo, per la prestazione di una o più funzioni a favore dell'entità finanziaria che non si configura come "Outsourcing";
- Tipologia di fornitore/oggetto della fornitura:
  - **Fornitori ICT**: fornitori di servizi informatici e di comunicazione;
  - **Fornitori non-ICT**: fornitori di servizi non informatici.

Questa valutazione e classificazione preliminare rappresenta la base per l'adozione di un **approccio proporzionale**: non tutti i TPA richiedono di adottare lo stesso livello di governance, ma i **presidi** devono essere **calibrati tenendo conto del livello di criticità della funzione supportata** dal fornitore ("*risk-based approach*") come meglio specificato nel successivo paragrafo. L'attuale limite è che l'individuazione e classificazione del perimetro di attività alle quali in concreto gli adempimenti andranno applicati, essendo demandata agli stessi soggetti obbligati, porta inevitabilmente a valutazioni discrezionali e disomogenee tra gli operatori di mercato, anche a parità di caratteristiche operative e settore di appartenenza e addirittura in caso di fornitori/forniture identiche. Il tutto tenendo presente che tali dati/informazioni devono poi essere riportate nel/i registro/i dedicati sulla base dei quali le Autorità di Vigilanza monitorano gli indicatori sui rischi sistemici, con conseguenti problemi di qualità dei dati stessi.

L'EBA nell'Allegato 1 del documento di consultazione fornisce un elenco di attività esemplificativo e non esaustivo per supportare tale valutazione, ma la lista appare ancora generica e, pertanto, si auspica un concreto affinamento delle istruzioni a riguardo.

3.1.3. *Definizione di Critical or Important Functions (CIFs)*

Le nuove EBA GL mutuano il principio di proporzionalità basato sulla **classificazione delle funzioni aziendali** (funzione intesa come "qualunque processo, servizio o attività o parte di essi") con la finalità di prevedere presidi rafforzati per le funzioni classificate come "critiche" o "importanti". In linea con la definizione fornita dal Regolamento DORA, una funzione è considerata critica o importante se il suo mancato svolgimento può avere un impatto significativo sulla conformità normativa, sulla solidità finanziaria dell'istituto o sulla continuità operativa e qualità del servizio offerto ai clienti.

Una considerazione evidente è che il concetto di esternalizzazione rappresenta solo un sottoinsieme dell'accordo con terze parti oggetto di disciplina da parte delle nuove EBA GL.

Inoltre, in linea con quanto definito dalla direttiva **BRRD** ("*Bank Recovery and Resolution Directive*"), le funzioni essenziali per l'esecuzione delle "**critical functions**" e delle "**core business lines**" devono essere considerate come critiche. Questo passaggio è significativo perché:

- estende il concetto di criticità oltre la normale operatività (cd. *business as usual*) a situazioni di *recovery* o di *resolution*; richiedendo una valutazione basata su un modello integrato con il framework di recovery & resolution;

- pone una maggiore focus su tema della sostituibilità dei fornitori.

3.1.4. *Armonizzazione rispetto al Registro DORA e gestione degli accordi con TPSPs*

Come anticipato l'Autorità ha deciso di mutuare l'approccio operativo previsto dal Regolamento DORA su alcuni aspetti rilevanti che meritano coerenza e standardizzazione, tra cui:

- il superamento del Registro delle esternalizzazioni con previsione della possibilità di adottare un **Registro unico degli accordi con le terze parti,** per raccogliere informazioni coerenti **sia per i servizi ICT** (oggetto del cd. Registro delle informazioni DORA) **che non ICT**, con apposite segregazioni;
- l'adozione di una **Governance e di un processo di gestione degli accordi con Third-Party Service Providers ("TPSPs") per i servizi non ICT**, in linea con gli standard del DORA, prevedendo specifici passaggi per la valutazione e gestione del rischio lungo l'intero ciclo di vita degli accordi, incluso il rafforzamento dei presidi in capo alle funzioni di controllo, fino alla Funzione di Internal Audit anche per garantire un follow-up strutturato sulle criticità identificate.

3.2 *Impatti sui modelli operativi: quattro cantieri di lavoro sul percorso critico*

Entriamo nel cuore del processo di trasformazione. Le nuove EBA GL non richiedono un mero esercizio di compliance normativa: implicano **cambiamenti concreti e significativi in quattro aree chiave della gestione aziendale** e richiedono un approccio consapevole e proporzionale per fare in modo che il percorso di adeguamento non sia solo formale e di conseguenza un costo ma che dia un ritorno sull'investimento concretizzandosi in un effettivo rafforzamento della resilienza operativa, in un modello di gestione delle terze parti maggiormente efficace e compatibile con il modello di business e le strategie aziendali e che generi sinergie gestionali ed economiche.

3.2.1 *Evoluzione della governance*

Dall'esperienza applicativa, derivante anche da quanto emerso dai programmi di adeguamento al DORA, nella maggior parte delle istituzioni finanziarie italiane la gestione del rischio terze parti è attualmente frammentata e destrutturata, non consentendo ai vertici aziendali di avere una visione integrata e olistica del rischio stesso. A riguardo le nuove EBA GL richiedono alcuni presidi chiave:

- **Chiara assegnazione di responsabilità interne**: deve essere designata una funzione responsabile della gestione del rischio di terze parti, con autorità e risorse adeguate al ruolo;
- **Supervisione efficace del Vertice aziendale**: il Board e i comitati competenti devono avere visibilità completa sulla gestione delle terze parti, con reporting regolare (almeno annuale);
- **Policy specifica in ambito**: deve essere adottata una politica formale per la gestione del rischio di terze parti che copra l'intero ciclo di vita degli accordi;
- **Integrazione nel complessivo risk framework aziendale**: la gestione del rischio terze parti deve essere integrata nel complessivo framework di risk management dell'entità.

Sul cantiere Governance la sfida principale per gli operatori di mercato sarà la revisione, possibilmente in ottica di semplificazione, del Modello di Governance in ambito, anche attraverso la convergenza e/o opportuni meccanismi di interazione e collaborazione tra i vari ruoli assegnati nel tempo a fronte delle singole e specifiche richieste regolamentari (Procurement Manager, Outsourcing Officer, Vendor Manager, TP Risk Manager, ecc.), mantenendo al contempo la necessaria segregazione tra le 3 linee di difesa aziendali. Questo implica ancora una volta:

- **Riordino dei ruoli e degli assetti organizzativi,** con la finalità di garantire la necessaria accountability con assegnazione di responsabilità precise a strutture organizzative e persone in grado di esercitarle con la dovuta consapevolezza;
- **Revisione dei processi decisionali** lungo tutte le fasi del ciclo di attività con chiara definizione dei processi approvativi e dei meccanismi di escalation in caso di necessità;

- **Investimento in competenze reali,** aspetto chiave per garantire una governance efficace delle terze parti e al contempo fare i conti non la sostenibilità del modello operativo, tenuto conto che non si ragiona a risorse infinite e che non si può pensare di rafforzare gli organici ad ogni richiesta regolamentare.

3.2.2. *Trasformazione e integrazione dei processi*

Le nuove EBA GL prescrivono un **processo strutturato in quattro fasi essenziali** che rappresentano l'intero ciclo di vita della relazione con il fornitore, i cui impatti operativi vanno valutati alla luce dell'estensione del perimetro oggettivo di applicazione:

- **Analisi pre-Contrattuale:** valutazione ex-ante del rischio del fornitore, con particolare attenzione al rischio di concentrazione, identificazione se la funzione è critica o importante, due diligence approfondita (e.g., reputazione, solidità finanziaria, capacità operativa, cybersecurity);
- **Fase Contrattuale**: stipula di un accordo contrattuale che preveda clausole specifiche più stringenti (e rafforzate in caso di servizi a supporto di funzioni critiche), SLA, KPI e metriche di performance, diritti di accesso, ispezione e audit e gestione di modifiche sostanziali al rapporto;
- **Monitoraggio Continuo**: monitoraggio della performance rispetto ai KPI; verifica della conformità contrattuale, identificazione di carenze e monitoraggio delle misure correttive, Audit periodici (almeno annuali per le CIFs);
- **Exit Strategy**: formalizzazione di un piano di uscita prima della firma del contratto, review periodica e test del piano (almeno annuale) e gestione dell'exit effettivo e dei diritti di recesso.

Sul cantiere processi la sfida principale per gli operatori sarà trovare il corretto bilanciamento tra standardizzazione dei processi e flessibilità che consenta di gestire le specificità in modo pragmatico. Ogni fornitore è diverso, ogni funzione ha caratteristiche ed esigenze specifiche. A riguardo le linee guida implicano un approccio coerente:

- calibrazione dei presidi operativi e di controllo in relazione al livello di criticità della funzione;
- template e checklist standardizzati;
- automazione, ove possibile, per ridurre l'effort manuale;
- iniziative di informazione e formazione continue e mirate finalizzate a garantire che tutti i soggetti coinvolti seguano il processo ufficiale.

3.2.3. *Adeguamento dei contratti con terze parti e dei termini commerciali*

Uno dei cantieri di lavoro a maggiore impatto operativo è sicuramente quello della **revisione** degli **accordi contrattuali** con **i fornitori terzi** secondo i nuovi requisiti normativi che richiedono di valutare la **criticità** di **servizi non ICT** secondo regole precise (in particolare se non classificati come outsourcing) e di includere metriche di performance più precise, diritti di audit e accesso per l'entità e l'autorità di vigilanza, condizioni rigorose per il subappalto.

Come già avvenuto per DORA, tale intervento dovrà puntare ad adottare **modelli contrattuali chiari** e possibilmente standardizzati che prevedono contenuti minimi e soprattutto dovrà abilitare concretamente i processi di monitoraggio della relazione con i fornitori, aspetto imprescindibile per rafforzare la governance e il controllo complessivo. Questo obiettivo sappiamo bene essere tutt'altro che privo di ostacoli e compromessi, e il percorso di adeguamento dei contratti ai fini DORA (ancora in corso per molti operatori) è solo l'ultima delle esperienze che lo confermano.

Un ulteriore elemento di complessità sta nella **rinegoziazione dei contratti già in essere**. Molti fornitori "storici" non accetteranno facilmente, soprattutto a parità di condizioni economiche, nuove clausole, in particolare quelle relative ai diritti di audit e accesso. Per questo, anche considerata l'esperienza DORA, servirà:

- prioritizzare adeguatamente i contratti da rinegoziare (CIFs first);
- predisporre più strategie di negoziazione, che siano tra loro alternative in quanto calibrate in funzione della tipologia e criticità del servizio/fornitore;
- prevedere chiare soluzioni di *contingency* in caso di difficoltà a raggiungere ad un accordo con

il fornitore;

- gestire il rischio di interruzione del servizio il periodo transitorio per l'adeguamento;
- valutare una razionalizzazione/ottimizzazione del portafoglio fornitori e forniture, con l'obiettivo di semplificare e conseguire sia sinergie operative (per una maggiore sostenibilità e fluidità del modello operativo di gestione) che *saving* di costo (aspetto senza dubbio che può abilitare gli investimenti necessari per un percorso di reale trasformazione).

3.2.4. *Adozione/integrazione di strumenti e tecnologie a supporto*

Le nuove EBA GL sul rischio terze parti abiliterebbero ad un'evoluzione significativa degli strumenti a supporto del processo di **Third Party Risk Management**. In particolare:

- **Registro Unificato:** EBA concede la possibilità di adottare un registro unico degli accordi contrattuali con terze parti per servizi ICT e non ICT. Il registro unico dovrà tracciare tutti gli accordi con fornitori terzi, seguendo un tracciato di informazioni standardizzate minime (incluse informazioni e dati aggiuntivi per le CIFs) e dovrà essere allineato alle logiche e i requisiti previsti dal "Registro delle informazioni DORA", garantendo la conservazione dei dati per almeno cinque anni e la loro disponibilità in formati processabili per le Autorità di Vigilanza;
- **Strumenti di Monitoraggio continuo dei fornitori**, che consentano di rafforzare la capacità dell'ente di verificare in modo efficace lo svolgimento del rapporto con la terza parte e di agire tempestivamente in caso di problemi (monitoraggio performance rispetto ai KPI, rilevazione tempestiva di anomalie o carenze, gestione escalation di situazioni critiche e reporting efficace a supporto del management);
- **Adozione/Integrazione di sistemi e tecnologie** a supporto dei diversi attori aziendali coinvolti nel processo tra cui in primis procurement, vendor management, risk management, compliance e internal audit (e.g., piattaforme di sourcing integrate con piattaforme GRC per la gestione di registro, processo TPM, controlli, reporting), funzionali a garantire la disponibilità di un patrimonio informativo completo, di qualità e tempestivamente aggiornato, evitando duplicazioni e disallineamenti delle basi dati.

La vera sfida per rafforzare concretamente la governance del rischio terze parti consisterà dunque nel **far convergere ed integrare processi, strumenti e tecnologie evitando "doppi binari"** (DORA/non DORA, Terze parti ICT/non ICT, a supporto di CIFs/non CIFs, Outsourcing/non Outsourcing, …) che portano inevitabilmente ad inefficienze e complessità di gestione.

4. Conclusioni

Le nuove EBA GL sulla gestione del rischio terze parti, oltre a oltre a **cambiare il paradigma passando da "outsourcing" a "gestione del rischio di terze parti"**, introducono diversi elementi di novità che implicano impatti significativi sui profili di Governance e sui modelli operativi degli operatori finanziari.

Come è stato per DORA sulla componente relativa ai servizi ICT, gli impatti non riguarderanno i soli destinatari diretti della disciplina ma anche gli stessi fornitori, alcuni dei quali come sappiamo sono tutt'altro che abituati a fronteggiare molti degli standard applicati tipicamente agli intermediari finanziari vigilati (cooperazione con le autorità competenti, diritti di accesso, audit, risoluzione, solo per citarne alcuni).

Restano senza dubbio ancora aperti, e in alcuni casi scoperti, alcuni punti chiave per pervenire ad un quadro regolamentare organico, su cui si auspica (almeno in parte) un riscontro concreto delle Autorità nella versione definitiva, tra cui in primis i seguenti:

- Eccessiva discrezionalità nell'individuazione e classificazione del perimetro di attività alle quali in concreto gli adempimenti andranno applicati, tema demandato agli stessi soggetti obbligati, che porta inevitabilmente a valutazioni discrezionali e disomogenee tra gli operatori di mercato con conseguenti impatti non solo sulle prassi gestionali dei singoli operatori ma anche sui dati/informazioni utilizzate dalle Autorità di Vigilanza per monitorare gli indicatori sui rischi sistemici;
- Obiettivo di garantire il cd. *level playing field* per tutti gli intermediari vigilati (settori bancario, finanziario e assicurativo) al momento ancora lontano e che richiederebbe interventi normativi a livello di ESAs e non iniziative singole delle autorità settoriali, tra l'altro temporalmente sfasate;

- Assenza di previsioni finalizzate a costruire un meccanismo di oversight dei fornitori critici, percorso avviato dal DORA sui fornitori critici ICT (CTPPs), che consentirebbe un ulteriore passo in avanti nell'armonizzazione delle regole e dei controlli per tutti gli attori in ambito finanziario.

Gli operatori che hanno approcciato il **DORA** in modo serio e pragmatico avranno senza dubbio una **base solida su cui costruire la propria aderenza alle nuove EBA GL**. Tuttavia, l'estensione dei requisiti ai servizi non-ICT richiederà inevitabilmente un adattamento/ripensamento dei modelli operativi che non è da sottovalutare e soprattutto non può essere liquidato con un semplice *"abbiamo già fatto tutto per DORA"*.

Inutile dire che **il momento di agire è adesso**. La finestra temporale per allinearsi alle nuove aspettative regolamentari e di vigilanza sarà comunque limitata e ci sono diverse aree di intervento sulle quali si può già iniziare a lavorare senza attendere le linee guida definitive.

Come ci insegna l'esperienza applicativa, gli operatori che approcceranno strategicamente ***("beyond compliance")***, e tempestivamente il tema avranno vantaggi significativi (in termini di ritorno sugli investimenti, mitigazione del rischio e fiducia degli stakeholders) e continueranno il percorso di rafforzamento del proprio livello di resilienza operativa avviato concretamente con DORA, aspetto diventato imprescindibile per la sostenibilità e competitività di un'organizzazione moderna nell'attuale e futuro scenario di mercato.

vedi l'articolo online