

APPROFONDIMENTI

Gestione fornitori non-ICT: nuove linee guida EBA e rapporti con DORA

Due diligence e contratti nella gestione delle
terze parti non ICT

Ottobre 2026

Alessandro Ferrari, Partner, Head of Technology Sector, DLA Piper



Alessandro Ferrari, Partner, Head of Technology Sector, DLA Piper

> **Alessandro Ferrari**

Alessandro Ferrari è Partner del dipartimento Intellectual Property & Technology e dirige il Sector Technology in Italia e si occupa principalmente di diritto applicato alla tecnologia, assistendo i clienti in questioni transactional, advisory and IT litigation. Ha esperienza nella redazione e negoziazione di accordi strategici e cross-border di outsourcing di processi aziendali e di altri contratti commerciali, IT e relativi alla proprietà intellettuale in diversi settori e in diverse geografie. Ha inoltre esperienza nella consulenza su tutti gli aspetti del processo di sourcing/approvvigionamento, compreso lo sviluppo della struttura dell'accordo, la negoziazione e l'assistenza ai clienti nell'implementazione e nelle strategie di integrazione, nella governance e nei performance management regimes.

Le linee guida EBA/GL/2026/09, pubblicate il 18 settembre 2026 dall'Autorità bancaria europea, ridefiniscono la gestione dei rischi legati ai fornitori di servizi non ICT. Gli orientamenti disciplinano la selezione dei prestatori, i contratti e il controllo del rapporto sino alla sua cessazione. Il loro ambito supera la tradizionale esternalizzazione, come già avviene con DORA per i servizi ICT. La revisione serve anche a coordinare la disciplina EBA con quest'ultimo regolamento, applicabile dal 17 gennaio 2025 alla resilienza operativa digitale. Le linee guida si concentrano sui servizi non ICT, lasciando a DORA quelli relativi alle tecnologie dell'informazione e della comunicazione, e chiedono alla banca di valutare complessivamente le proprie dipendenze dai fornitori.¹

Il coordinamento risponde a un'esigenza concreta. Uno stesso processo può dipendere dal lavoro di un operatore esterno, da una piattaforma e da servizi affidati a subfornitori. Alle diverse prestazioni possono applicarsi requisiti differenti, mentre la continuità del processo dipende dal loro funzionamento congiunto. Se il servizio sostiene una funzione essenziale o importante, di seguito FEI, occorre coordinare anche i presidi rafforzati previsti dai due quadri.

Il contributo esamina il contenuto delle linee guida, con particolare attenzione alla *due diligence* pre-contrattuale e alle clausole contrattuali. Il confronto con DORA chiarisce quali presidi siano comuni, quali richiedano adattamenti e come coordinarli nei contratti misti, che comprendono componenti ICT e non ICT. Al 28 settembre 2026 le linee guida sono definitive ma non ancora applicabili: l'analisi ne considera il contenuto in vista dell'adeguamento.²

1. Il nuovo perimetro della gestione del rischio di terze parti

Le linee guida sono orientamenti di vigilanza adottati ai sensi dell'articolo 16 del regolamento istitutivo dell'EBA. Autorità competenti e istituzioni finanziarie devono compiere ogni sforzo per conformarsi; le autorità comunicano la propria conformità o intenzione di conformarsi, motivando l'eventuale sco-

¹ EBA, Guidelines on the sound management of third-party risk regarding non-ICT services, EBA/GL/2026/09, 18 settembre 2026 («GL»), §§ 5-7 e 17. Testo e comunicato ufficiali: <https://www.eba.europa.eu/activities/single-rulebook/regulatory-activities/internal-governance/guidelines-third-party-risk-management>. Regolamento (UE) 2022/2554 («DORA»), artt. 3, 28-30 e 64: <https://eur-lex.europa.eu/eli/reg/2022/2554/oj/ita>.

² Scheda EBA cit., stato al 28 settembre 2026. Pubblicazione, applicazione e sostituzione degli orientamenti del 2019 sono momenti distinti.

stamento. Questa natura giuridica le distingue da DORA e dai suoi regolamenti delegati, direttamente applicabili. La conformità alle linee guida rileva quindi nella vigilanza sull'organizzazione, sulla gestione dei rischi e sul mantenimento dei requisiti autorizzativi.³

L'intervento riguarda i servizi non ICT che sostengono una o più funzioni su base ricorrente o continuativa. La nozione di funzione comprende processi, servizi, attività e loro parti. L'*outsourcing* costituisce un sottoinsieme: si ha quando il terzo svolge una funzione che sarebbe altrimenti esercitata dall'ente. Anche quando il rapporto non configura un'esternalizzazione, occorre quindi verificarne l'inclusione nel nuovo perimetro. Sono inclusi i rapporti infragruppo, pur con gli adattamenti consentiti dalla disciplina.⁴

Gli orientamenti del 2019 già richiedevano di gestire i rischi dei terzi non qualificabili come outsourcer. Il nuovo testo estende però requisiti specifici a rapporti ulteriori. L'adeguamento deve quindi partire dal censimento dei servizi acquistati: limitarsi al registro storico delle esternalizzazioni può lasciare fuori rapporti ora rilevanti.

Il paragrafo 33 esclude dal perimetro, tra l'altro, la revisione legale, determinate infrastrutture finanziarie, le informazioni di mercato, le operazioni finanziarie tra controparti e l'acquisto di beni e utenze. Sono esclusi anche servizi privi di un impatto materiale sull'esposizione ai rischi o sulla resilienza operativa. Gli esempi di prestazioni professionali e amministrative indicati da EBA devono essere letti alla luce di questo criterio. Un parere occasionale e la gestione continuativa di un processo operativo significativo presentano presupposti differenti, anche se acquistati da soggetti appartenenti alla stessa categoria professionale.^[5]

L'esclusione dei servizi finanziari regolamentati riguarda quelli che devono per legge essere prestati da un'altra entità finanziaria regolata dal diritto dell'Unione. La sola qualità di soggetto vigilato del prestatore non esclude ogni sua prestazione. Le esclusioni, inoltre, non dispensano dalla gestione generale dei rischi e dalle altre discipline applicabili.

³ Regolamento (UE) n. 1093/2010, art. 16; GL, §§ 1-6: <https://eur-lex.europa.eu/eli/reg/2010/1093/oj/ita>.

⁴ GL, §§ 17 e 23-32. EBA/GL/2019/02, §§ 12 e 26-33, nella sezione storica della scheda EBA citata.

I destinatari delle linee guida, elencati ai paragrafi 8-15, non coincidono con quelli DORA: mancano, in generale, le imprese di assicurazione.⁵

2. La rilevanza delle funzioni e la responsabilità della banca

La distinzione tra servizi ICT e non ICT individua il quadro pertinente; la valutazione della funzione sostenuta determina l'intensità di molti presidi. Secondo le linee guida, una funzione è essenziale o importante quando una sua interruzione o esecuzione difettosa comprometterebbe materialmente la performance finanziaria, la solidità o continuità delle attività, oppure il rispetto delle condizioni autorizzative e degli obblighi della normativa finanziaria. Occorre motivare il giudizio con riferimento alla situazione della banca e agli effetti del malfunzionamento.⁶

Le attività operative delle funzioni di controllo interno affidate a terzi sono considerate FEI, salvo che la valutazione escluda un impatto negativo sull'efficacia dei controlli in caso di mancata o inadeguata esecuzione. Il paragrafo 36 qualifica automaticamente come FEI le funzioni delle attività bancarie, dei servizi di pagamento o dell'emissione di token collegati ad attività quando il loro svolgimento richiederebbe un'autorizzazione. Per gli enti soggetti alla disciplina di risoluzione, il paragrafo 37 considera FEI anche le funzioni necessarie alle linee di business principali o alle funzioni critiche, salvo che la loro mancata o inadeguata esecuzione non ne comprometta materialmente la continuità operativa.

Occorre prima verificare se il servizio sia incluso nel perimetro EBA e poi se la funzione sostenuta sia essenziale o importante. Un servizio può rientrare nelle linee guida senza sostenere una FEI, con applicazione dei presidi di base secondo proporzionalità. Né il trattamento di dati personali, né l'importo del corrispettivo determinano da soli la classificazione: anche un servizio poco costoso può essere difficilmente sostituibile.

Nei rapporti misti occorre collegare ogni servizio alla funzione. Se lavorazione operativa e piattaforma sostengono entrambe una FEI, per ciascuna vanno verificati i requisiti rafforzati pertinenti. Un contratto unitario non rende essenziale ogni prestazione marginale; una separazione formale non può occul-

⁵ GL, §§ 8-15 e 33, nota 41.

⁶ GL, § 17 e §§ 34-37; DORA, art. 3, punto 22, e art. 31.

tare dipendenze materiali.

Il ricorso al prestatore non trasferisce le responsabilità dell'organo di gestione della banca. I paragrafi 38-50 richiedono strategia, politica e processi che consentano di comprendere i rischi e intervenire in caso di prestazioni inadeguate. EBA ammette strategie integrate o separate e il coordinamento delle policy con quelle adottate in ambito DORA, mantenendo riconoscibili le differenze. La banca deve comunque conservare competenze e risorse sufficienti per gestire e controllare gli affidamenti, come richiesto dal paragrafo 43.⁷

L'affidamento deve fondarsi su informazioni adeguate e prevedere responsabilità e misure per correggere le carenze. Ciò vale anche per i fornitori del gruppo.

3. L'analisi precontrattuale richiesta dalle linee guida

Il paragrafo 68 articola la fase precontrattuale in valutazione della criticità, verifica delle condizioni di vigilanza, analisi dei rischi, *due diligence* sul prestatore e individuazione dei conflitti di interesse. Sono verifiche collegate, con oggetti differenti. L'analisi del rischio riguarda ciò che l'affidamento comporta per la banca; la *due diligence* accerta se il prestatore sia adatto a eseguire quel servizio. Un fornitore finanziariamente solido può comunque proporre un modello che renda il servizio non trasferibile o impedisca controlli adeguati.⁸

Una prima verifica riguarda la legittimazione a svolgere l'attività. Per le funzioni relative alle attività e ai servizi regolamentati individuati dal paragrafo 69, quando sia necessaria un'autorizzazione o registrazione, il prestatore deve possederla oppure essere altrimenti abilitato dal quadro nazionale pertinente. Per le funzioni bancarie, di pagamento o di emissione dei token richiamati dal paragrafo 70, affidate a un prestatore di un paese terzo e soggette ad autorizzazione o registrazione nello Stato membro della banca, occorrono anche autorizzazione o registrazione e vigilanza locale, oltre a un adeguato accordo di cooperazione tra autorità. Queste condizioni dipendono dalla natura dell'attività: non costituiscono un obbligo generale di autorizzazione per ogni fornitore non ICT.

⁷ GL, §§ 26-30 e 38-50, in particolare §§ 38, 41 e 49; DORA, artt. 5 e 28; regolamento delegato 2024/1773, artt. 3-4.

⁸ GL, §§ 68-73 e 77-82; per le attività regolamentate, §§ 69-70 e disposizioni settoriali richiamate.

La valutazione dei rischi deve considerare l'impatto sulla capacità della banca di rispettare la normativa, controllare il servizio e proteggere i clienti. I paragrafi 71-76 includono rischi operativi, legali, reputazionali e di concentrazione. Richiedono attenzione alla possibile crescita del servizio senza revisione dell'accordo, alla sostituibilità del prestatore, alla possibilità di riportare la funzione all'interno della banca e alla protezione dei dati. La sostituibilità va esaminata sul piano contrattuale e pratico, considerando tempi, costi e ostacoli alla continuità.

La concentrazione può derivare da più forniture dipendenti dallo stesso gruppo o da una catena comune. La valutazione considera anche i rischi aggregati. Per gli enti significativi rileva anche il rischio che divenga necessario sostenere finanziariamente un prestatore in difficoltà o assumerne le attività. Nella subfornitura a supporto di FEI va valutato se catene lunghe e complesse ostacolano il controllo della banca o la vigilanza delle autorità.⁹

La *due diligence*, disciplinata dai paragrafi 77-82, considera modello di business, struttura proprietaria e organizzativa, solidità finanziaria, capacità operativa e tecnica ed esperienza del prestatore. Il dettaglio deve essere proporzionato alla rilevanza della funzione. Per le FEI occorre accertare, tra l'altro, reputazione, competenze, risorse, controlli interni, gestione dei rischi, dipendenze geografiche, piani di continuità e possibilità effettiva di svolgere audit. Vanno considerate le subforniture previste e le autorizzazioni necessarie.

Quando il servizio comporta il trattamento di dati personali o riservati, il paragrafo 81 richiede misure tecniche e organizzative adeguate. Il fatto che la prestazione sia non ICT non riduce il rilievo della sicurezza: accessi ai documenti, trasferimenti, conservazione e disponibilità delle informazioni possono essere determinanti anche in attività prevalentemente umane. Il paragrafo 82 considera inoltre coerenza con valori e codice di condotta dell'ente e, per i prestatori di paesi terzi e ove pertinente i loro subfornitori, profili etici, sociali, ambientali e di rispetto dei diritti umani.

Le verifiche precontrattuali dovrebbero distinguere rischi accettabili, carenze rimediabili e ostacoli all'affidamento. Le carenze rimediabili dovrebbero tradursi in impegni verificabili, con tempi, respon-

⁹ GL, §§ 74-76 e 79-80; DORA, art. 29.

sabilità e, se necessario, condizioni da soddisfare prima dell'avvio del servizio. Il contratto deve poi preservare le capacità accertate e consentire il controllo sulle loro modifiche.

4. Le differenze nella due diligence rispetto al quadro DORA

La struttura dell'analisi EBA è vicina a quella dell'articolo 28, paragrafo 4, DORA. Anche quest'ultimo richiede di classificare la funzione, verificare le condizioni di vigilanza, analizzare i rischi, accertare l'idoneità del prestatore e individuare i conflitti di interesse. Il confronto completo deve includere il regolamento delegato 2024/1773, relativo alla politica per i servizi ICT a supporto di FEI, e il regolamento delegato 2025/532 sulla subfornitura. Anche questi atti concorrono a definire la due diligence ICT.¹⁰

La differenza più netta riguarda gli accertamenti specificamente tecnologici. L'articolo 28, paragrafo 5, DORA consente di stipulare contratti soltanto con fornitori che soddisfino standard appropriati di sicurezza delle informazioni. Per i servizi a supporto di FEI richiede di prendere in debita considerazione gli standard di qualità più aggiornati ed elevati. L'articolo 6 del regolamento 2024/1773 aggiunge la capacità di seguire gli sviluppi tecnologici, individuare le pratiche avanzate di sicurezza ICT e attuarle ove opportuno. Questo porta a verificare capacità e controlli differenti da quelli necessari, ad esempio, per una lavorazione documentale manuale.

La distinzione non coincide però con una separazione tra *due diligence* tecnica e *due diligence* aziendale. Il medesimo articolo 6 considera reputazione, risorse finanziarie e umane, organizzazione, controlli interni, autorizzazioni, continuità e possibilità di audit. Comprende anche condotta etica, diritti umani, tutela ambientale e condizioni di lavoro. Questi profili sono quindi comuni, con adattamenti, ai due quadri.

Per i paesi terzi, EBA considera stabilità politica, sicurezza, diritto applicabile, protezione dei dati e conseguenze dell'insolvenza. DORA, nell'articolo 29 e nel regolamento 2024/1773, affronta temi analoghi; quest'ultimo menziona anche embarghi e sanzioni. Per le attività non ICT regolamentate rilevano inoltre le condizioni dei paragrafi 69-70 EBA. Le verifiche dipendono quindi da prestazione e localizza-

¹⁰ DORA, art. 28(4)-(5); regolamento delegato (UE) 2024/1773, artt. 5-7: https://eur-lex.europa.eu/eli/reg_del/2024/1773/oj/ita. Profili etici e sociali: art. 6(1)(f) e GL, § 82.

zione, con molti elementi comuni.

Il regolamento 2024/1773 individua anche le evidenze utilizzabili nella selezione: audit, valutazioni indipendenti, relazioni interne, certificazioni e altre informazioni. Può essere necessario combinarle per ottenere garanzie adeguate, verificandone la pertinenza. La stessa impostazione può essere adottata operativamente nella due diligence EBA.

Per la subfornitura ICT a supporto di FEI, l'articolo 3 del regolamento 2025/532 specifica ulteriormente le verifiche sulla capacità del contraente principale di selezionare e valutare i subfornitori e monitorarne i rischi. Le linee guida EBA richiedono a loro volta di considerare la catena, ma il regolamento delegato approfondisce il contesto tecnologico e le capacità necessarie a controllarlo. Anche la due diligence della banca deve quindi comprendere come il fornitore eserciti il controllo sui soggetti dei quali si avvale.¹¹

In pratica, una banca può usare una base comune di informazioni societarie, finanziarie e organizzative, completata da verifiche specifiche. Per un servizio operativo contano, secondo i casi, capacità produttiva, competenze, segregazione dei compiti, controllo degli errori e sostituzione del personale. Per una piattaforma assumono rilievo architettura, gestione degli accessi, vulnerabilità, ripristino e dipendenze tecnologiche. Nei servizi misti occorre poi un giudizio sul funzionamento congiunto: l'idoneità del personale non dimostra che possa operare durante un'interruzione della piattaforma, né un buon piano di ripristino garantisce lo smaltimento delle pratiche arretrate.

5. Il contenuto del contratto secondo le linee guida EBA

I paragrafi 83-86 distinguono una base contrattuale applicabile agli accordi compresi nel perimetro e un livello aggiuntivo per quelli a supporto di FEI. Il contratto deve attribuire chiaramente diritti e obblighi e descrivere in modo completo i servizi. Deve indicare i luoghi di esecuzione e le condizioni per modificarli, compreso l'obbligo di comunicazione, oltre alla legge applicabile e ai luoghi di trattamento e conservazione dei dati. Sono richieste disposizioni sulla protezione dei dati, sui livelli di servizio, sulla

¹¹ Regolamento delegato (UE) 2025/532, art. 3: https://eur-lex.europa.eu/eli/reg_del/2025/532/oj/ita. GL, §§ 75 e 79-80.

cooperazione con le autorità e sui diritti di cessazione e relativi preavvisi.¹²

La tutela comprende disponibilità, autenticità, integrità e riservatezza dei dati. Per quelli appartenenti all'ente devono essere garantiti accesso, recupero e restituzione in caso di insolvenza, risoluzione o cessazione dell'attività del prestatore, oppure di cessazione del contratto. Il paragrafo 86 richiede che il fornitore sia contrattualmente tenuto a rispettare gli obblighi di protezione dei dati applicabili alla banca, inclusi il segreto bancario e la tutela dei dati personali. È opportuno identificare le informazioni da restituire, comprese le evidenze dei controlli e lo stato delle lavorazioni, evitando che l'accessibilità dipenda da dispute sulla proprietà del dato.

Per gli enti soggetti alla direttiva 2013/36/UE (CRD), il paragrafo 84(j) richiede un riferimento ai poteri dell'autorità di risoluzione, in particolare agli articoli 68 e 71 della direttiva 2014/59/UE (BRRD), e una descrizione delle obbligazioni sostanziali ai sensi dell'articolo 68. La clausola deve rendere riconoscibili tali obblighi, compresi quelli di pagamento, e coordinare i diritti di cessazione con i limiti previsti dalla BRRD in caso di misure di prevenzione o gestione della crisi.

Per le FEI, il paragrafo 85 richiede obiettivi quantitativi e/o qualitativi precisi, tali da consentire monitoraggio e interventi correttivi tempestivi. Si aggiungono obblighi di comunicazione degli sviluppi che possano incidere materialmente sulla prestazione, sull'osservanza della legge e sui livelli concordati. Il contratto deve inoltre regolare l'eventuale copertura assicurativa richiesta, l'attuazione e verifica dei piani di emergenza, i diritti di controllo e la transizione in uscita. La previsione assicurativa richiede di precisare se il prestatore debba assicurarsi e, in tal caso, quale copertura: non impone indistintamente una polizza di contenuto predeterminato.

Gli accordi sui livelli di servizio (SLA) devono misurare la prestazione acquistata. Per la lavorazione di pratiche possono riguardare tempi, errori, arretrati e capacità di assorbire picchi. La disponibilità del portale documentale non dimostra l'efficienza del servizio operativo, né il numero di pratiche completate esclude perdite di dati. Le metriche sono scelte negoziali da ricavare dalla valutazione dei rischi.

¹² GL, §§ 83-86; per gli enti CRD, § 84(j); per l'assicurazione, § 85(c).

Molti requisiti trovano corrispondenza nell'articolo 30 DORA: descrizione del servizio, localizzazione, protezione dei dati, SLA, cooperazione, audit e transizione. DORA aggiunge però prescrizioni ICT puntuali. Già tra le clausole di base figurano l'assistenza per incidenti connessi al servizio senza costi aggiuntivi oppure a costo stabilito ex ante e le condizioni di partecipazione ai programmi di sensibilizzazione e formazione. Per i servizi a supporto di FEI sono richieste misure, strumenti e politiche di sicurezza ICT, oltre alla partecipazione e piena cooperazione ai test avanzati di penetrazione basati su minacce, i TLPT, quando applicabili. Le clausole EBA non hanno un equivalente puntuale di questi obblighi.¹³

Nei rapporti misti, un allegato DORA può offrire una base per molte tutele richieste anche dalle linee guida EBA. Occorre però verificarne il contenuto e l'applicabilità alle prestazioni non ICT: una clausola riferita ai soli servizi ICT non si estende automaticamente alla componente operativa. L'estensione convenzionale delle tutele all'intero servizio richiede una scelta esplicita e proporzionata.

Massimali, penali e costi di migrazione vanno valutati anche nel loro effetto combinato. Un credito di servizio o una riduzione del corrispettivo previsti come unico rimedio non dovrebbe impedire misure correttive o cessazione richieste dalla disciplina. Tali esigenze non implicano, di per sé, responsabilità illimitata o migrazione gratuita.

6. I diritti di accesso e audit

Per le FEI, le linee guida richiedono ampi diritti di accesso a sedi, informazioni e documenti rilevanti, nonché di ispezione e audit, a favore della banca, degli incaricati e delle autorità. Per le altre funzioni, il paragrafo 99 richiede di valutare in base al rischio l'inclusione di tali diritti, considerando anche la crescita del servizio e gli effetti sulla continuità. Restano le garanzie contrattuali per le verifiche dell'audit interno e, per gli enti CRD, il richiamo ai poteri informativi e investigativi delle autorità, previsti dai paragrafi 96-97 anche fuori dalle FEI.¹⁴

¹³ DORA, art. 30(2)(f) e (i), art. 30(3)(c)-(d) e artt. 26-27; GL, §§ 84-85. SLA, rimedi economici e struttura degli allegati descritti sono proposte negoziali.

¹⁴ GL, §§ 96-107, specie §§ 96-99 e 102-104; DORA, art. 30(3)(e); regolamento 2024/1773, art. 8.

L'EBA ammette audit congiunti tra clienti, certificazioni e relazioni di audit. Per i servizi a supporto di FEI, la banca deve valutarne adeguatezza e sufficienza e non può affidarsi esclusivamente a certificazioni e relazioni nel tempo. Il paragrafo 104 richiede condizioni sul contenuto, sull'aggiornamento e sulla qualità delle evidenze, mantenendo la possibilità contrattuale di chiedere un ragionevole ampliamento dell'ambito delle certificazioni o relazioni e di svolgere audit individuali.

Anche su questo terreno la convergenza con DORA è ampia. L'articolo 30 e l'articolo 8 del regolamento 2024/1773 contemplano accesso, ispezioni, audit e forme alternative di verifica, con le relative condizioni. In entrambi i quadri il contratto deve rendere il diritto esercitabile, coordinandolo con riservatezza, sicurezza e tutela degli altri clienti.

Preavvisi e regole di sicurezza non devono impedire controlli necessari o urgenti. Nei rapporti misti, un programma coordinato può coprire procedure operative e sistemi, verificando anche come le anomalie tecnologiche siano prese in carico dal personale.

7. Il controllo della subfornitura e i rimedi contrattuali

Le linee guida dedicano i paragrafi 87-95 al subappalto di funzioni essenziali o importanti o di loro parti materiali. Il contratto deve chiarire se sia consentito e a quali condizioni. Il prestatore deve monitorare le prestazioni subaffidate e i rischi geografici, riferire alla banca e assicurare la continuità lungo la catena. Sono richiesti obblighi di monitoraggio e reporting nei rapporti a valle e diritti di accesso, ispezione e audit per la banca e le autorità. L'attenzione deve concentrarsi, in particolare, sui subfornitori che sostengono effettivamente il servizio non ICT rilevante.¹⁵

Il prestatore deve comunicare tempestivamente nuovi subappalti e modifiche materiali, consentendo alla banca di valutarne l'effetto. Il contratto prevede un termine ragionevole per approvare od opporsi. L'attuazione segue l'approvazione o la mancata opposizione entro quel termine. Quando il rischio eccede la tolleranza dell'ente, quest'ultimo si oppone e chiede modifiche prima che la nuova configurazione divenga operativa. La qualità dell'informazione ricevuta è quindi essenziale: una comunicazione che

¹⁵ GL, §§ 87-94, specie § 89 per la catena e §§ 90-93 per preavviso e opposizione.

identifichi soltanto il nuovo nominativo, senza descrivere attività, località e dipendenze, può non consentire la valutazione richiesta.

Questi diritti sono largamente analoghi a quelli del regolamento delegato DORA 2025/532. L'articolo 4 disciplina condizioni del subappalto, monitoraggio, reporting, continuità e accesso; l'articolo 5 prevede preavviso delle modifiche sostanziali, approvazione o opposizione e richiesta di modifiche. L'opposizione della banca non è quindi una novità esclusiva EBA. Anche i nuovi subappalti ICT rientrano nei controlli: il considerando 8 ne richiama il processo di approvazione e il considerando 11 l'informazione preventiva. L'articolo 5 va letto insieme a questi considerando e agli articoli 4 e 6, che, come i paragrafi 90-93 EBA, assoggettano a controllo anche i nuovi affidamenti.¹⁶

Una differenza puntuale riguarda l'oggetto della cessazione. Al paragrafo 95 EBA chiede che il contratto principale assicuri la possibilità di risolvere l'accordo tra prestatore e subfornitore nelle ipotesi indicate di subaffidamento non consentito, introdotto nonostante l'opposizione o attuato anticipatamente senza approvazione. L'articolo 6 del regolamento 2025/532, letto con l'articolo 4, paragrafo 1, lettera I), riguarda invece la cessazione del rapporto tra entità finanziaria e fornitore ICT. Restano, nel quadro EBA, i separati diritti sul contratto principale previsti dal paragrafo 108.¹⁷

Il testo EBA non attribuisce per ciò solo alla banca un potere diretto di risolvere un contratto del quale non è parte. La sua attuazione richiede che il contraente principale disponga dei diritti necessari verso il subfornitore e che il contratto con la banca regoli le conseguenze dell'evento. Una soluzione negoziale consiste nel prevedere la rimozione o sostituzione del subfornitore quando necessaria, con tempi, cooperazione e misure di continuità, mantenendo i pertinenti diritti di uscita dal rapporto principale. La concreta struttura dipende dalla legge applicabile e dalla catena contrattuale.

Nei servizi misti si può coordinare la procedura, identificando prestazioni subaffidate e requisiti da trasferire a valle. Cambiare un operatore o un'infrastruttura digitale può richiedere informazioni differenti. Se la modifica incide su entrambe le componenti, la banca deve valutarne l'effetto complessivo.

¹⁶ Regolamento 2025/532, considerando 8 e 11 e artt. 4-6, testo definitivamente adottato.

¹⁷ GL, §§ 95 e 108-109; regolamento 2025/532, artt. 4(1)(I) e 6. L'attuazione del rimedio EBA sul subcontratto dipende dalla struttura negoziale e dalla legge applicabile.

8. Continuità operativa e uscita dal rapporto

La disciplina EBA collega la continuità della banca alla capacità dei fornitori di sostenere le FEI. I paragrafi 54-55 richiedono piani appropriati, mantenuti e testati periodicamente, con coinvolgimento dei prestatori quando opportuno. L'analisi degli impatti deve considerare interruzioni gravi, processi di supporto, dipendenze e sostituibilità. Il contratto, ai sensi del paragrafo 85, deve a sua volta imporre al prestatore di attuare e verificare i propri piani di emergenza.¹⁸

Per una prestazione non ICT le misure possono riguardare sedi alternative, personale sostitutivo, trasferimento delle istruzioni di lavoro e recupero degli arretrati. Queste soluzioni devono essere compatibili con gli accessi ai sistemi e con la disponibilità dei dati. Nel caso misto, il ripristino della piattaforma può lasciare irrisolto l'arretrato operativo, mentre il trasferimento del personale può fallire se la sede alternativa non dispone degli accessi necessari. Una prova coordinata dovrebbe quindi verificare se la banca torni a ricevere il risultato atteso nei tempi sostenibili per la funzione.

L'uscita è un percorso distinto dal ripristino presso lo stesso fornitore. I paragrafi 114-116 richiedono, per le FEI, una strategia documentata e piani realistici, fattibili e basati su scenari plausibili. I piani devono individuare alternative, responsabilità, risorse, criteri di successo e indicatori che possano attivare l'uscita. Il paragrafo 115 richiede che i piani siano sufficientemente testati, ove appropriato. Il contratto deve rendere possibile la transizione e il trasferimento del servizio, con un periodo adeguato durante il quale il prestatore continua a operare e assiste il passaggio.¹⁹

DORA prevede presidi analoghi; l'articolo 10 del regolamento 2024/1773 richiede revisione e test periodici dei piani di uscita. Sul piano operativo cambia ciò che va trasferito: procedure, fascicoli e conoscenze per il servizio operativo; dati, configurazioni e diritti di migrazione per la tecnologia. Attività, tempi e costi devono essere definiti. L'assistenza agli incidenti ICT senza costi aggiuntivi o a costo predeterminato non implica la gratuità della migrazione.

¹⁸ GL, §§ 54-55 e 85(d); DORA, art. 30(3)(c). Le prove coordinate descritte sono proposte operative.

¹⁹ GL, §§ 85(f), 108-109 e 114-116; DORA, artt. 28(7)-(8) e 30(3)(f); regolamento 2024/1773, art. 10.

9. La qualificazione dei servizi misti

Il coordinamento diventa più difficile quando un accordo comprende prestazioni operative e tecnologiche. Al paragrafo 32 EBA richiede alla banca di considerare tutti gli aspetti del servizio. Spetta alla banca valutare se l'impiego di servizi ICT, come definiti da DORA, sia materiale per l'erogazione e comporti l'applicazione di quel quadro. Non fissa soglie percentuali, né una regola di integrale applicazione di entrambi i regimi a ogni contratto misto.²⁰

I paragrafi 5 e 7 escludono dal perimetro EBA i servizi ICT disciplinati da DORA. Applicare il quadro pertinente a ciascuna prestazione autonomamente riconoscibile è una ricostruzione interpretativa coerente con questa distinzione, non una regola espressa di cumulo. La separazione deve riflettere prestazioni effettivamente distinguibili. Il criterio di materialità non può essere letto come un'esenzione generale per servizi che soddisfino autonomamente la definizione DORA.

Occorre distinguere l'uso di tecnologia dalla fornitura di un servizio ICT alla banca. Si immagini un incarico continuativo di controllo formale e preparazione di fascicoli creditizi, con decisione sul credito mantenuta dalla banca. Se il software organizza soltanto turni e risorse degli addetti, il suo uso non dimostra la presenza di un servizio ICT acquistato dalla banca. Occorre comunque verificare l'inclusione del servizio nel perimetro EBA e la rilevanza della funzione sostenuta.

Se il contratto comprende anche una piattaforma su cui la banca carica documenti, consulta archivi e segue le pratiche, possono emergere due prestazioni autonome: quella digitale da valutare ai fini DORA e quella operativa ai fini EBA. La prevalenza del costo del personale non esclude DORA. Vanno anche ricostruite le interdipendenze: un fermo del sistema può bloccare gli addetti, mentre la piattaforma può restare disponibile senza che le pratiche vengano completate.

L'accesso della banca alla piattaforma non è però un requisito della nozione di servizio ICT: anche un'elaborazione digitale continuativa con sola consegna dei risultati può essere un servizio ICT. Se il personale gestisce soltanto eccezioni al risultato automatizzato, occorre giustificare l'autonomia del

²⁰ GL, §§ 5-7 e 32; risposte alla consultazione, pp. 71-72. L'applicazione per prestazioni autonomamente identificabili è una ricostruzione interpretativa.

servizio non ICT. Denominazione del contratto e voci di prezzo non sono decisivi.

Per stabilire quali prestazioni ricadano nelle linee guida EBA occorre dunque chiarire quali siano servizi ICT ai sensi di DORA. È per questa ragione che rilevano le Q&A sul regolamento: lo stesso paragrafo 32 EBA richiama la Q&A DORA030. I due chiarimenti qui esaminati riguardano problemi diversi: la natura del servizio acquistato e la presenza di fornitori ICT nella catena di subfornitura.

La Q&A DORA030 della Commissione affronta il primo problema con riferimento ai servizi finanziari regolamentati che comprendono componenti ICT. Se il prestatore e il servizio finanziario sono regolamentati secondo il diritto dell'Unione, di uno Stato membro o di un paese terzo, il servizio ICT connesso a quello finanziario è considerato prevalentemente finanziario ed escluso dalla definizione di servizio ICT DORA. Restano invece inclusi i servizi ICT indipendenti da quello finanziario. Il chiarimento non consente quindi di escludere da DORA la tecnologia accessoria a qualsiasi servizio amministrativo. L'esclusione dalla nozione di servizio ICT lascia fermi gli altri obblighi DORA della banca e non determina automaticamente l'applicazione delle linee guida EBA: vanno verificate anche le esclusioni del paragrafo 33, già illustrate.²¹

Il secondo problema si pone quando il fornitore presta alla banca un servizio non ICT e utilizza, per eseguirlo, servizi ICT di un subfornitore. La Q&A congiunta delle autorità europee di vigilanza 2024_7089 chiarisce che questa circostanza, da sola, non impone di inserire nel registro DORA né il servizio acquistato dalla banca né i subfornitori ICT utilizzati dal prestatore. Restano applicabili gli obblighi previsti dalle altre discipline, comprese le linee guida EBA.

La stessa Q&A contempla però un'ipotesi ulteriore. La banca, nella propria valutazione del rischio, può rilevare che il servizio ICT del subfornitore sostiene una FEI, o sue parti materiali, in misura tale da poter essere riqualificato come equivalente a un servizio ICT fornito direttamente alla banca. In questo caso si applicano gli obblighi del capo V DORA sulla gestione dei rischi derivanti da terzi. Il solo coin-

²¹ GL, § 32, nota 40, e § 33. Commissione europea, Q&A DORA030, art. 3(21) DORA: https://www.eiopa.europa.eu/qa-regulation/questions-and-answers-database/dora030-2999_en.

volgimento di una FEI non basta: occorre anche valutare l'equivalenza fra fornitura indiretta e diretta.²²

Anche quando non si giunge a questa riqualificazione, la dipendenza tecnologica può dover essere censita secondo le linee guida EBA. Il paragrafo 58 richiede infatti di documentare nel registro EBA i subfornitori ICT che sostengono effettivamente i servizi non ICT forniti alla banca a supporto di FEI. Tale censimento rende visibili le dipendenze nella catena di fornitura; non comporta, da solo, l'applicazione di DORA. La banca deve quindi distinguere l'obbligo di conoscere e registrare la catena dalla valutazione che può rendere applicabile il capo V DORA.

10. Come strutturare un contratto misto a supporto di una FEI

Accertata la presenza di componenti soggette ai due regimi, l'architettura contrattuale dovrebbe rendere riconoscibili gli obblighi e preservare la continuità del processo. Una soluzione è un accordo quadro con una disciplina comune e allegati che descrivano prestazioni, requisiti specifici e interdipendenze. È una proposta negoziale: le fonti non impongono questa struttura né, per il solo carattere misto del servizio, due contratti separati.

La parte comune può regolare reporting, modifiche, audit, cooperazione, continuità e uscita. Gli allegati descrivono componenti, funzione, SLA e requisiti specifici. La prevalenza tra documenti dovrebbe risolvere conflitti puntuali: far prevalere genericamente la disciplina più rigorosa può lasciare incerto quali prestazioni siano dovute e da chi.

Nel caso dei fascicoli creditizi, occorre verificare sia la capacità di lavorare le pratiche sia la disponibilità della piattaforma. Il contratto può combinare indicatori sulle componenti con misure del risultato complessivo, come il completamento dei fascicoli entro i tempi concordati.

La gestione delle modifiche (cd. *change management*) dovrebbe considerare anche il passaggio dall'attività umana a quella automatizzata. Se una lavorazione inizialmente non ICT viene sostituita da un'e-laborazione digitale continuativa, occorre riesaminare la qualificazione, la due diligence e le clausole

²² Autorità europee di vigilanza, Q&A 2024_7089, 8 agosto 2025: https://www.eba.europa.eu/single-rule-book-qa/qna/view/publicId/2024_7089. GL, § 58.

pertinenti prima di approvare la nuova configurazione. Non ogni aggiornamento organizzativo comporta tale effetto; il contratto dovrebbe però assicurare informazioni sufficienti sui cambiamenti che incidono su natura, rischi e controllo della prestazione.

Infine, la cessazione di una componente può rendere inutilizzabile l'altra. La banca può avere interesse a cambiare l'operatore mantenendo la piattaforma o a sostituire la tecnologia conservando il lavoro del prestatore. La negoziazione dovrebbe verificare la praticabilità delle due opzioni; il contratto deve poi regolare accessi, licenze, cooperazione, dati e assistenza necessari. Se la separazione non è realistica, il piano deve contemplare una transizione congiunta. I diritti di cessazione parziale, ove negoziati, vanno quindi collegati alla possibilità effettiva di continuare il servizio e agli effetti sul corrispettivo.

Se i fornitori sono due, contratti separati chiariscono le prestazioni, mentre resta alla banca il compito di gestirne le interdipendenze. Servono obblighi compatibili di cooperazione e transizione. La scelta tra uno e più prestatori deve quindi considerare concentrazione e capacità interna di coordinamento.

11. Monitoraggio e adeguamento dei rapporti esistenti

Le linee guida richiedono un monitoraggio proporzionato al rischio e continuativo per gli accordi a supporto di FEI. Le informazioni del prestatore, gli indicatori, gli audit e le verifiche di continuità devono aggiornare la valutazione iniziale e determinare azioni correttive quando emergano carenze. I paragrafi 58-67 disciplinano registro e documentazione, distinguendo FEI e altri rapporti. L'EBA consente un registro integrato con quello DORA e l'impiego del medesimo formato; questa possibilità non elimina le differenze nelle informazioni e negli adempimenti.²³

Per le FEI, il registro EBA riporta le valutazioni sulla sostituibilità e sulla reintegrazione, l'esistenza di un piano di uscita e, ove possibile, fornitori alternativi. Nei rapporti misti, contratto, singoli servizi e funzione sostenuta dovrebbero essere collegati nei registri, così da ricostruire le dipendenze e i controlli applicabili. I paragrafi 65-66 richiedono inoltre informative tempestive alle autorità sugli affidamenti di FEI programmati e sulle modifiche o eventi gravi rilevanti.

²³ GL, §§ 58-67 e 110-113, specie §§ 61 e 63; DORA, art. 28(3); regolamento di esecuzione (UE) 2024/2956: https://eur-lex.europa.eu/eli/reg_impl/2024/2956/oj/ita.

Attualmente il testo finale attende le traduzioni e non è ancora applicabile. Il paragrafo 18 ne prevede l'applicazione agli accordi conclusi, riesaminati o modificati dalla futura decorrenza. I paragrafi 19-20 richiedono il riesame degli accordi esistenti e, se entro due anni dall'applicazione non siano completati riesame e documentazione dei rapporti a supporto di FEI, una comunicazione all'autorità con le misure previste o una possibile strategia di uscita. Per gli altri rapporti, il paragrafo 21 consente il riesame e aggiornamento della documentazione in occasione del rinnovo.²⁴

L'adeguamento dovrebbe partire dalle differenze rispetto ai presidi esistenti. Nei servizi misti meritano priorità dipendenze non ricostruite, controlli non esercitabili e piani di uscita che presuppongono una separazione impossibile.

²⁴ GL, §§ 18-22; scheda EBA cit., stato al 28 settembre 2026. DORA, art. 64; regolamento 2025/532, art. 4(2).



DB non solo
diritto
bancario

A NEW DIGITAL EXPERIENCE

 **dirittobancario.it**
