

ATTUALITÀ

Il sistema di gestione del rischio operativo nel contesto della CRR3

Requisiti minimi dell'EBA e implicazioni per
gli istituti di credito

25 Settembre 2026

Michele Maugeri, Partner, KPMG
Francesco Russo, Senior Manager, KPMG



Michele Maugeri, Partner, KPMG
Francesco Russo, Senior Manager, KPMG

> **Michele Maugeri**

Michele Maugeri è Partner nell'area Regulatory & Risk Advisory di KPMG, con una esperienza pluriennale nell'ambito del Risk Management e della regolamentazione.

> **Francesco Russo**

Francesco Russo è Senior Manager nell'area Regulatory & Risk Advisory di KPMG con un'esperienza pluriennale nell'ambito del Risk Management e della regolamentazione.

1. Introduzione

Nell'ambito dell'implementazione della CRR3, l'EBA ha avviato nel mese di agosto una consultazione pubblica (EBA/CP/2026/18) finalizzata alla definizione di requisiti minimi armonizzati per la gestione del rischio operativo da parte degli istituti di credito, che si concluderà il 31 dicembre 2026.

Tramite tali requisiti e tenuto conto della natura, dei differenti canali di trasmissione e del grado di connessione e dipendenza dei sottesi fattori di rischio (es. condotta, processi, sistemi IT, terze parti), l'EBA delinea un impianto organico di governo, gestione e valutazione del rischio operativo che, oltre a garantire la conformità normativa alla CRR3, risulti integrato nelle strategie, nei processi e nell'operatività aziendale ordinaria.

L'impianto in oggetto deve risultare coerente con il più ampio framework regolamentare dell'EBA supportando l'applicazione di un approccio "risk-based" per finalità di vigilanza prudenziale, a tal fine coordinandosi con i requisiti normativi in materia di resilienza digitale (DORA), gestione dei rischi ESG e dei rischi delle terze parti.

Parallelamente, il principio di proporzionalità formalizzato nell'EBA/CP/2026/18 costituisce un elemento strutturale del nuovo impianto, determinando una diversa intensità, livello di sofisticazione e frequenza nell'adozione ed applicazione di specifici requisiti di governo, gestione e valutazione del rischio operativo in funzione della rilevanza dell'indicatore di attività degli enti vigilati utilizzato per il calcolo dei fondi propri (i.e. "Business Indicator – BI" inferiore, pari o maggiore di 750 milioni di euro).

2. Configurazione del sistema di gestione del rischio operativo

Nelle aspettative dell'EBA, la gestione del rischio operativo deve superare una impostazione prevalentemente "ex-post" tramite rilevazione degli eventi e delle perdite accadute a favore di un approccio che permetta di identificare e valutare in maniera maggiormente accurata vulnerabilità, carenze nei controlli interni e rischi emergenti in ottica predittiva, favorendo quindi un'adeguata e compiuta comprensione delle esposizioni attuali e potenziali al rischio.

Le componenti di tale approccio devono operare in maniera interrelata affinché la gestione del rischio

operativo abiliti il processo decisionale (es. strategie commerciali, sistema di controllo interno, uso della tecnologia, ricorso alle terze parti) e contribuisca al rafforzamento della resilienza operativa (es. mappatura di processi critici, quantificazione e monitoraggio di eventi di “disruption”), pure in accordo ad altre normative e orientamenti regolamentari sul presidio dei rischi non finanziari, come i principi BCBS e la regolamentazione DORA sulla resilienza digitale nel settore finanziario.

In relazione a ciò e nel rispetto del principio di proporzionalità, il sistema di gestione del rischio si articola nelle seguenti componenti principali:

- **Governance**, che attiene primariamente alla chiara definizione ed assegnazione di ruoli e responsabilità agli Organi aziendali, al Senior management e alle tre linee di difesa (incl. validazione interna) nell’implementazione, attuazione e supervisione degli obiettivi, dei processi e delle metodologie di gestione del rischio;
- **Processo di gestione**, che ricomprende l’insieme di politiche e procedure documentate tramite cui i rischi attuali e potenziali sono identificati, analizzati, controllati e mitigati su basi continue;
- **Sistema di valutazione**, che riguarda l’insieme di tassonomie, dati, indicatori, autovalutazioni, analisi delle cause, scenari e stress test, capace di combinare approcci “bottom-up” e “top-down” e di offrire una rappresentazione corrente e “forward-looking” del profilo di rischio.;
- **“Use-test” e reporting**, relativamente agli strumenti e alle modalità di rappresentazione tempestiva del profilo di rischio operativo agli appropriati livelli aziendali (sistema di reporting) nell’ottica di supportare il processo decisionale e un’efficace supervisione delle esposizioni correnti e prospettiche al rischio.

In merito alla governance, l’EBA enfatizza le responsabilità dell’Organo con funzione di gestione nell’approvazione del sistema di gestione del rischio operativo, nella definizione della propensione al rischio e nel monitoraggio dei relativi limiti rispetto al profilo di rischio assunto. Parallelamente, vengono attenzionati i ruoli indipendenti della seconda e terza linea di difesa, con specifico riferimento alla funzione di controllo dei rischi operativi, che sviluppa e supervisiona l’applicazione del sistema di gestione del

rischio, e alle funzioni di convalida e revisione interna che, per i propri ambiti di competenza, verificano la solidità, l’affidabilità e l’efficacia di detto sistema. Di rilievo risulta peraltro l’introduzione di meccanismi periodici di valutazione e revisione dell’efficacia del sistema di gestione del rischio operativo.

Circa il processo di gestione, l’EBA si focalizza sulla formalizzazione di politiche e procedure che sono diffuse ed applicate coinvolgendo le funzioni aziendali che gestiscono attività che possono causare eventi operativi o gli impatti degli eventi, favorendo di conseguenza la cultura, la comprensione e la consapevolezza sulle esposizioni al rischio rispetto agli obiettivi e ai limiti di rischio e sulle attività di controllo delle fonti, eventi e manifestazioni del rischio, anche al fine di orientare la definizione dei piani di rimedio (es. misure preventive e correttive di mitigazione, coperture assicurative).

Relativamente al sistema di valutazione, l’EBA attenziona gli approcci, le fonti dati e le tassonomie tramite cui identificare, classificare, analizzare e quantificare i rischi operativi affinché siano sviluppate capacità di gestione del rischio che integrino informazioni di natura consuntiva e prospettica. Il sistema di valutazione deve combinare approcci “bottom-up” e “top-down” di rilevazione dei rischi e una pluralità di strumenti e informazioni interne ed esterne sul profilo di rischio, come perdite consuntive, incidenti potenziali, valutazioni e indicatori di monitoraggio di rischi e controlli, analisi di scenario e stress-testing. Le risultanze del sistema di valutazione devono operare in maniera sufficientemente predittiva supportando la definizione e l’allocazione degli obiettivi e limiti di rischio, l’identificazione, la gestione e la quantificazione dei rischi emergenti (es. rischi ESG, rischi di modello connessi all’intelligenza artificiale, rischi geopolitici), la prioritizzazione dei piani di azione e la resilienza operativa.

Affinché le tre componenti possano operare in maniera sinergica ed efficace, la gestione del rischio operativo deve essere supportata da un appropriato **sistema di reporting** dei dati e dei fattori interni ed esterni sul rischio, nonché basarsi su informazioni accurate, trasparenti e tracciabili oggetto di appropriate **procedure di data quality** (es. riconciliazione contabile).

3. Principali novità per la gestione del rischio operativo

In relazione ai razionali, ai principi e alle aspettative dell’EBA, le novità emerse dalla consultazione pubblica non risiedono esclusivamente nell’introduzione di nuovi adempimenti sulla gestione del rischio operativo, evidenziandone una progressiva evoluzione verso un sistema maggiormente e struttural-

mente integrato nella gestione dei rischi e dell'operatività aziendale.

A tal fine, le principali novità ed elementi attenzionati dall'EBA sono riconducibili ai seguenti ambiti:

- **Strategia e governance**, in cui rientrano in particolare la definizione di un sistema di gestione di tutte le fonti e canali di trasmissione del rischio operativo (es. integrazione del rischio informativo), il setting e l'allocazione dell'appetito e dei limiti di rischio basati sull'indicatore di attività e metriche di perdita, e la revisione periodica dell'efficacia del sistema di gestione;
- **Identificazione e valutazione**, con riferimento allo sviluppo ed applicazione di approcci di identificazione, valutazione prospettica e quantificazione delle esposizioni al rischio, incorporando una visione sia strategica sia operativa delle minacce, controlli e vulnerabilità nei processi, scenari estremi e rischi emergenti. Tali approcci ricomprendono il processo di calcolo dei fondi propri sul rischio operativo ("Business Indicator component – BIC") e, ove applicabile, delle perdite storiche degli ultimi 10 anni;
- **Gestione dei dati**, in termini di disponibilità di svariate informazioni e fattori interni / esterni (es. perdite, "near miss", fonti causali, scenari, indicatori) che devono essere integrati e classificati secondo tassonomie¹ robuste per contribuire alla rappresentazione complessiva del profilo di rischio attuale e prospettico a supporto degli obiettivi di rischio, della gestione di rischi emergenti, dei piani di azione e della resilienza operativa. Procedure di data quality e riconciliazione contabile devono garantire l'accuratezza, la completezza e tracciabilità delle informazioni sul profilo di rischio operativo;
- **Utilizzo gestionale**, da intendersi come modalità di integrazione del sistema di gestione del rischio operativo nelle strategie aziendali, nei processi decisionali e nel quadro di resilienza operativa (es. mitigazioni, coperture assicurative, introduzione di nuovi prodotti, processi e sistemi, ricorso a terze parti, gestione dei processi critici). A tal fine, la gestione e la supervisione del rischio operativo devono essere supportati da un appropriato sistema di reporting (dati e fattori

interni e esterni sul rischio, obiettivi e limiti di rischio, controlli e mitigazioni);

- **Verifiche e controllo**, con riferimento al rafforzamento o introduzione di attività di verifica della conformità, validazione e revisione interna e indipendente del sistema di gestione del rischio nelle sue componenti di identificazione, valutazione e misurazione (es. fonti dati, procedure di data quality). In tale ambito, le funzioni di validazione e revisione interna assumono ruoli distinti ma complementari e coordinati nella conduzione delle proprie verifiche, assicurando un adeguato perimetro di controllo (es. attività di convalida proporzionata a variazioni nel contesto operativo e nel profilo di esposizione al rischio, review di audit focalizzate sulle esposizioni materiali al rischio), una rendicontazione tempestiva delle criticità riscontrate e il monitoraggio delle connesse azioni di rimedio.

4. Principio di proporzionalità e soglia del "Business Indicator" di 750 milioni di euro

La proporzionalità è un elemento strutturale del disegno regolamentare: tutti gli enti vigilati sono tenuti a disporre di un sistema di gestione del rischio operativo adeguato; per quelli con un "Business Indicator" inferiore a 750 milioni di euro, l'EBA prevede un alleggerimento mirato, in particolare tramite minore frequenza di riesami, reporting e minore granularità di dati, soglie di perdita e tassonomie.

La soglia, pertanto, non equivale ad un'esenzione, né consente l'adozione un sistema meramente formale di gestione del rischio operativo. Al contrario, essa mira a favorire un'applicazione proporzionata dei requisiti rispetto alla struttura degli enti.

¹ Il riferimento è alla classificazione degli eventi e degli attributi di rischio operativo formalizzati nel Regolamento Delegato (UE) 2026/1167 della Commissione del 28 maggio 2026.

Ambito del sistema di gestione del rischio operativo	Enti con Business Indicator ≥ 750 Mln/€	Enti con Business Indicator < 750 Mln/€
Review dell'efficacia del sistema di gestione del rischio	Almeno annuale	Almeno biennale
Appetito al rischio operativo	Business Indicator (e relative componenti) più limiti quantitativi basati sulle esposizioni al rischio	Almeno il Business Indicator (e relative componenti)
Dati e fattori interni / esterni sul rischio operativo	Set completo (perdite operative interne / esterne, "near miss", analisi di scenario, indicatori di rischio e controllo, Business Indicator, ecc.)	Set più contenuto che include le perdite operative di importo inferiore a 20.000 €
Tassonomia di rischio operativo	Coerenza con gli standard tecnici EBA (i.e. EBA/RTS/2025/03)	Raccomandata coerenza con gli standard tecnici EBA (i.e. EBA/RTS/2025/03) per le perdite di ogni importo
Sistema di reporting	Frequenza almeno trimestrale	Frequenza almeno annuale

L'appartenenza alla fascia sottosoglia non elimina la necessità di presidi più robusti quando il modello di business, l'uso di terze parti, la complessità tecnologica, la rilevanza dei processi critici o il profilo storico e prospettico di perdita lo richiedano.

5. Conclusioni

In considerazione degli elementi sopra esposti, l'impatto concreto del nuovo impianto non sarà in ogni caso uniforme, in quanto dovrà essere valutato alla luce del principio di proporzionalità e del diverso grado di maturità dei presidi di gestione del rischio operativo già in essere, infatti:

- per gli enti vigilati che dispongono di sistemi più maturi anche in considerazione dei requisiti dei previgenti metodi avanzati sul rischio operativo, una parte significativa delle novità potrebbe tradursi nel rafforzamento, affinamento o formalizzazione di presidi già esistenti. Le direttrici di intervento potrebbero dunque riguardare la completezza degli approcci "bottom-up" e "top-down" e dei dati utilizzati per l'identificazione, valutazione predittiva e gestione del rischio (es. tassonomie, controlli e scenari, rischi emergenti), nonché l'estensione degli ambiti di verifica dell'affidabilità e solidità del sistema di gestione del rischio operativo (es. efficacia del sistema, procedure di data quality, perimetro delle verifiche di convalida interna);
- per gli altri enti vigilati, l'adeguamento potrebbe invece richiedere interventi più significativi o sostanziali su ruoli e responsabilità, processi, disponibilità e qualità dei dati, nonché sui meccanismi di reporting e valutazione del rischio. In tal caso, le direttrici di intervento abbracciano, tra l'altro, la configurazione e allocazione dell'appetito al rischio, lo sviluppo di metodologie strutturate e interdipendenti sui diversi requisiti di gestione del rischio (es. integrazione del rischio IT, analisi di processi, rischi potenziali e controlli, analisi di scenario e stress-testing, configurazione del sistema di reporting), incluse le tassonomie di classificazione e le procedure di data quality.

In definitiva, l'impianto proposto dall'EBA rafforza la concezione del rischio operativo quale dimensione trasversale dell'operatività aziendale, la cui gestione non può essere ricondotta alla sola rilevazione e verifica "ex-post" degli eventi e degli esiti dei controlli interni, ma deve concorrere alla comprensione delle vulnerabilità, dei rischi emergenti e dell'evoluzione del profilo di rischio corrente e potenziale così da supportare il processo decisionale, secondo un modello maggiormente dinamico, predittivo e quindi focalizzato sulla rappresentazione "forward-looking" del profilo di rischio (es. indicatori, analisi delle cause, conseguenze del rischio, scenari di rischio).

Peraltro, l'impatto del nuovo impianto andrà verificato anche in funzione degli elementi che l'EBA attenziona nell'ambito della consultazione, con particolare riferimento a:

- calibrazione della frequenza minima di riesame del sistema di gestione del rischio operativo;
- strumenti di valutazione delle esposizioni al rischio operativo (es. mappatura dei processi, valutazione di rischi e controlli, analisi di scenario);
- ruolo e responsabilità delle funzioni di validazione e revisione interna e relativi processi di verifica indipendente dei dati e del sistema di gestione del rischio operativo;
- procedure di data quality delle informazioni sul profilo di rischio operativo (es. riconciliazione contabile dei dati).

Con riserva di ritornare sugli argomenti esposti una volta che le norme tecniche dell'EBA saranno finalizzate ed emanate, sarà in ogni caso la capacità degli enti vigilati di tradurre tale evoluzione regolamentare in approcci robusti, integrati e proporzionati al proprio modello di business a determinare l'effettiva efficacia del sistema di gestione del rischio operativo, pure considerando le attuali prassi e il livello di sofisticazione già qualificanti la gestione del rischio in parola a livello aziendale.

DB non solo
diritto
bancario

A NEW DIGITAL EXPERIENCE

 **dirittobancario.it**
