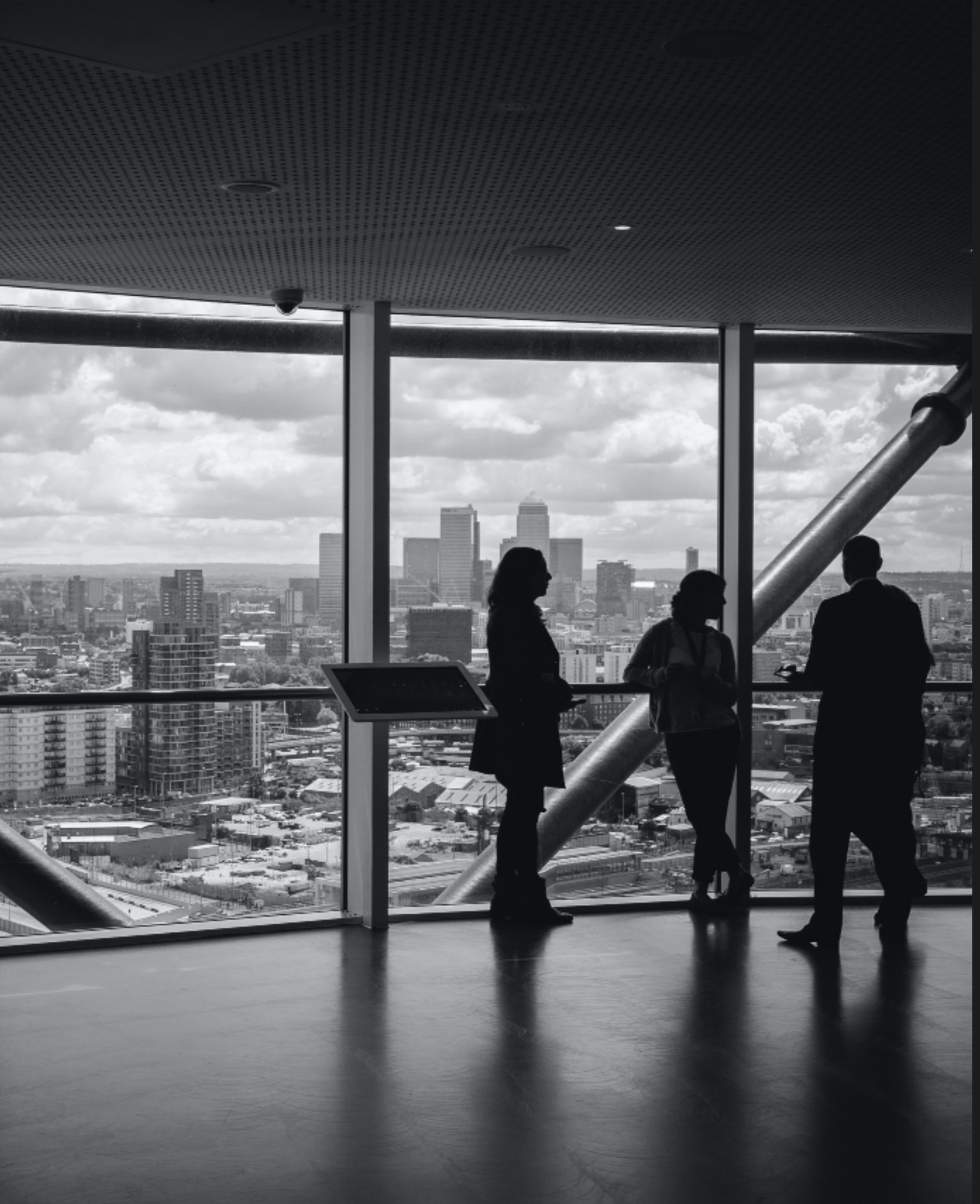


DB non solo diritto bancario

leggi l'articolo nel sito www.dirittobancario.it

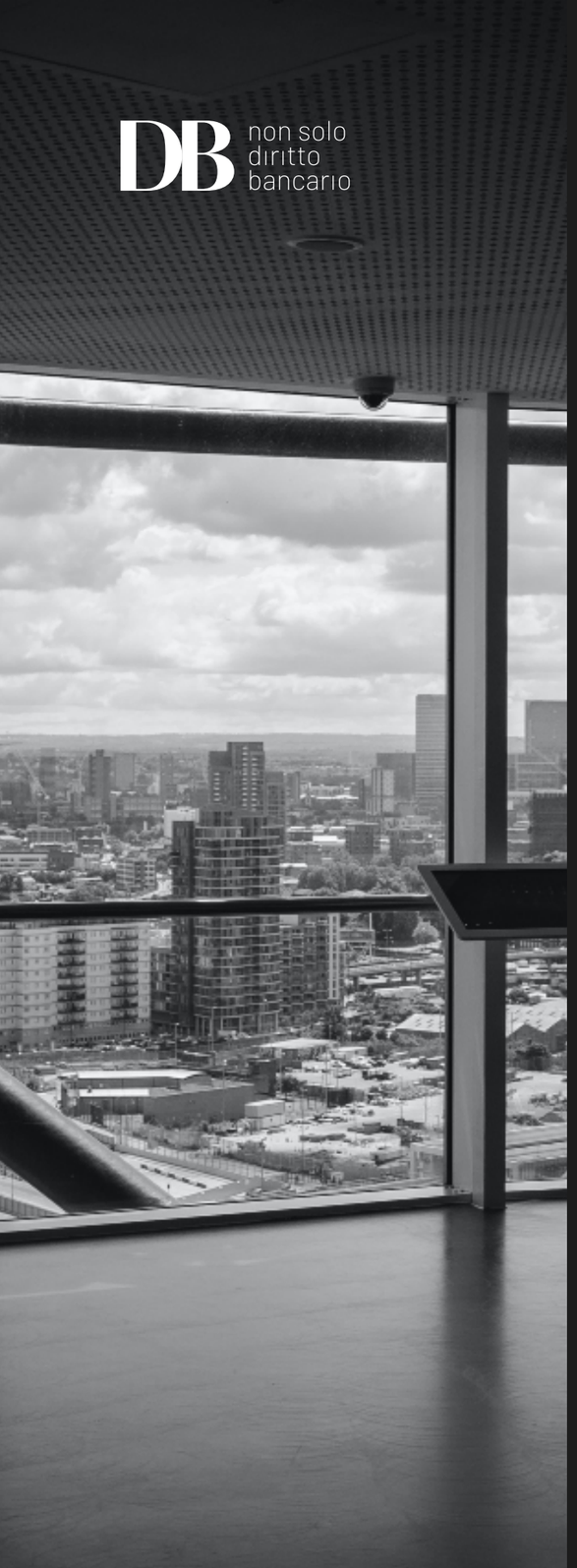
ATTUALITÀ

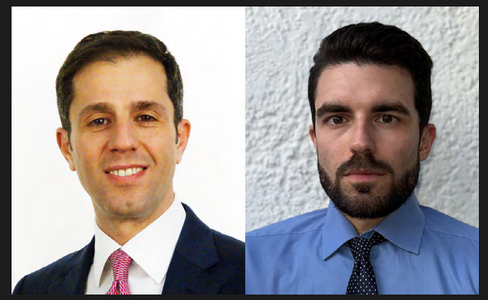
RDARR: aggregazione e reporting dei dati di rischio nell' industria bancaria

Recenti evoluzioni normative e principali ambiti di intervento

5 maggio 2025

Fabio Luca Crepaldi, Partner, Deloitte Risk Advisory
Fernando Montuori, Manager, Deloitte Risk Advisory





Fabio Luca Crepaldi, Partner, Deloitte Risk Advisory

Fernando Montuori, Manager, Deloitte Risk Advisory

Fabio Luca Crepaldi

Fabio Crepaldi è esperto di risk management nell'ambito delle istituzioni finanziarie. E' docente di risk management in diversi master, tra cui SDA Bocconi e MIB Trieste. Nel corso della sua carriera Fabio Crepaldi si è occupato di una serie di questioni regolamentari e di gestione del rischio, con particolare attenzione al rischio di credito e alle operazioni di credito. Tra le altre cose, Fabio ha maturato una forte competenza su requisiti regolamentari, risk governance e risk modelling, con particolare attenzione ai modelli di rischio di credito, ai sistemi di rating interni ed alla loro integrazione nelle operazioni di credito. Inoltre, ha maturato una significativa esperienza in ambito data governance e information technology.

1. Le regulatory expectations

La crisi finanziaria iniziata nel 2007 ha messo in luce significative carenze nelle capacità delle banche di aggregare in maniera efficace i dati e di generare report di rischio tempestivi e accurati al fine di prendere decisioni informate in tempi rapidi.

In risposta a queste problematiche, il Comitato di Basilea per la Vigilanza Bancaria (di seguito anche BCBS) ha pubblicato nel 2013 il documento "*BCBS239 - Principles for effective risk data aggregation and risk reporting*", con l'obiettivo di rafforzare le pratiche di gestione ed aggregazione dei dati di rischio. In particolare, il documento declina 14 principi a cui le Banche devono ispirarsi nella definizione dei propri processi e strumenti di aggregazione e reporting dei dati di rischio, articolate in 4 macro-sezioni:

- *infrastruttura e governo societario*,
- *capacità di aggregazione dei dati di rischio*,
- *prassi di reportistica in materia di rischio*,
- *strumenti e cooperazione delle autorità di vigilanza*.

Nonostante la rilevanza data al tema dai Regulator, l'implementazione di tali principi da parte degli enti bancari è stata spesso lenta, disomogenea e poco efficace, con carenze strutturali nella qualità e tracciabilità dei dati, nella governance del dato, e nell'integrazione tra i diversi sistemi informativi, come evidenziato - tra l'altro - all'interno dei report della Banca Centrale Europea "*Aggregate result of SREP letter*" del Febbraio 2022, e "*Supervisory Data: ECB Management Report and Data Quality matters*" del Giugno 2023[1].

A fronte di tali considerazioni, la BCE ha emanato a maggio 2024, una "*Guide on effective risk data aggregation and reporting*" (di seguito "Guida RDARR") in cui dettaglia e rafforza le attese di Vigilanza sulla

1 Tra le principali evidenze riscontrate si riportano criticità a carico della completezza dei dati rappresentati nei report di rischio legate all'inadeguatezza dei servizi di *Software/IT vendors*, errori operativi impattanti sulla corretta implementazione delle regole di validazione per la reportistica regolamentare EBA e la non precisa identificazione delle *root causes* sottostanti le criticità sulla *data quality* individuate.

vedi l'articolo online

tematica per le Banche dell'area Euro, inserendola tra le *Supervisory Priorities* per il 2023/2025.

In particolare, la Guida RDARR è articolata in sette macro-ambiti di intervento:

- **Responsabilità degli Organi di Gestione**: vengono definite le attese circa la responsabilità relative alla definizione, implementazione e monitoraggio dell'attuazione del framework RDARR in capo agli organi di gestione della banca, che devono peraltro possedere competenze adeguate. Tra l'altro viene specificata la possibilità di identificare uno o più membri dell'organo di gestione (es. Consiglio di Amministrazione) come diretti responsabili della messa a terra del Framework RDARR, a diretto riporto dell'organo stesso, che ne mantiene la responsabilità ultima;

- **Perimetro di applicazione:** viene specificato che il Framework RDARR deve considerare tutte le *legal entities* di gruppo, i rischi a cui sono esposti, le linee di business e processi di reporting maggiormente rilevanti, coprendo l'intero ciclo di vita dei dati in analisi, ed includendo – oltre alla reportistica di rischio interna - la reportistica contabile, i *supervisory reports* (ad es. FINREP e COREP, Pillar III reports, EBA Stress Test reports) ed i modelli interni di risk management (ad es. modelli IRB ed IFRS9). Infine, si specifica la necessità di identificare puntualmente i *Key Risk Indicators* interni (ad es. *Risk Appetite Indicators*) ed i *Critical Data Elements* a cui si riferiscono[2];

- **Framework di Data Governance:** la guida ribadisce la necessità di normare in *policy* interne soggette a revisione periodica i presidi di Data Governance della Banca. Tra l'altro la guida richiede l'identificazione:

    - di una funzione centrale di Data Governance incaricata di definire le policy e i processi per la gestione della qualità dei dati, supervisionarne l'implementazione a livello di gruppo, monitorare e valutare la qualità dei dati nel tempo e partecipare ai processi di cambiamento che impattano significativamente su RDARR, come fusioni, acquisizioni, esternalizzazioni, nuovi prodotti o aggiornamenti IT;

2 Nella Guida sono definiti "*critical data elements*" tutte le componenti dei dati utilizzate per il calcolo dei KRIs, che hanno un impatto diretto significativo sul valore dell'indicatore o sui processi tecnici di calcolo o di reporting.

    - dei *Data Owners* e la declinazione delle loro responsabilità. In particolare *i Data owners* hanno il compito di garantire accuratezza, integrità, completezza e tempestività dei Critical Data Elements, contribuire alla definizione dei controlli, monitorarne la qualità e intervenire in caso di carenze lungo tutta la filiera di elaborazione del dato;

    - della funzione di controllo di secondo livello, indipendente dalle unità operative, che assicuri il corretto funzionamento dei processi attraverso valutazioni periodiche delle capacità RDARR dell'intera organizzazione, coprendo tutti le componenti del processo – inclusi infrastrutture IT, data lineage, tassonomie, outsourcing e nuove iniziative tecnologiche;

    - della funzione di audit interno, terza linea di difesa, che ha il compito di svolgere revisioni indipendenti periodiche sul funzionamento della funzione di validazione, sull'intero framework di data governance, sulle capacità RDARR e sulla qualità dei dati utilizzati nella quantificazione dei rischi;

- **Architettura dati integrata:** viene ripresa la necessarietà di disporre di un'architettura dati integrata a livello di gruppo, in grado di aggregare tempestivamente i dati anche per produrre viste non standard (cd. ad hoc reporting). Le banche devono, inoltre, disporre di una *data taxonomy* omogenea ed univoca, nonché di soluzioni per il *data lineage,* ovvero di una mappatura del ciclo di elaborazione del dato lungo tutto il processo, dalla acquisizione dei dati elementari al reporting finale;

- **Standard di Data Quality:** il framework di Data Quality deve essere disciplinato a livello di Gruppo, garantendo completezza ed efficacia dei controlli rispetto alle dimensioni di accuratezza, integrità, completezza e tempestività dei dati. Le banche devono monitorate la qualità dei Critical Data Elements mediante l'utilizzo di opportuni indicatori e mantenere un registro delle criticità rilevate, con individuazione delle *root causes*, valutazione degli impatti, tempistiche di *remediation* ed *escalation* per la loro risoluzione;

- **Tempestività della reportistica sul rischio:** la produzione del reporting di rischio deve avvenire con tempistiche coerenti con le caratteristiche del rischio e le esigenze gestionali anche in situazioni di stress (es. reporting infragiornaliero per crisi di liquidità);

vedi l'articolo online

- **Programmi di attuazione:** è richiesto che ogni Banca definisca programmi di rafforzamento delle proprie capacità RDARR con una chiara identificazione degli obiettivi e delle tempistiche di completamento, sostenuti da governance progettuale e risorse adeguate.

2. Lo stato dell'arte

A valle del rilascio della Guida sopra citata, la BCE ha avviato una *targeted review* circa lo stato dell'implementazione dei programmi RDARR su un ampio campione di banche europee. Le risultanze di tale review, sintetizzate in una pubblicazione di febbraio 2025, hanno evidenziato rilevanti criticità in particolare in tre aree di intervento chiave:

- **Governance interna:** In molti enti bancari, il Consiglio di Amministrazione non ha assegnato priorità sufficiente al tema RDARR, limitandosi a un approccio formale e non strategico. Le responsabilità relative alla qualità e all'aggregazione dei dati risultano poco chiare o frammentate, spesso senza una funzione indipendente di controllo, e le attività di *gap analysis* periodiche rispetto ai principi BCBS 239 e alle *Guidelines ECB* sono assenti, datate o prive di connessione con piani di azione strutturati. Inoltre, con riferimento ai programmi di attuazione delle iniziative RDARR, le *milestones* di implementazione non sono generalmente vincolanti e il perimetro di applicazione è spesso ristretto e non copre tutte le entità o linee di business rilevanti;

- **Infrastruttura dati e architettura IT:** numerose banche presentano infrastrutture IT obsolete, basate su sistemi frammentati e rigidi, che ostacolano l'aggregazione efficiente dei dati di rischio, specialmente in contesti di crisi, con architetture dati non pienamente integrate a livello di gruppo e che non permettono una tracciabilità *end-to-end* del *data lineage*. Inoltre, sono spesso assenti tassonomie comuni, processi automatici per la gestione dei dati e una chiara assegnazione della *data ownership*, compromettendo l'affidabilità e la tempestività delle informazioni disponibili per la gestione dei rischi e il reporting regolamentare;

- **Accuratezza e integrità della reportistica:** La reportistica di rischio è ancora fortemente condizionata da interventi manuali, processi non automatizzati e attività di *end user computing* che aumentano notevolmente il rischio di errore e la perdita di coerenza tra le fonti dati. Inoltre, i controlli sulla qualità dei dati sono spesso inefficaci, non sistematici e non sufficientemente integrati nei processi aziendali, e le azioni di rimedio spesso consistono in correzioni ex-post delle anomalie anziché in azioni strutturali e pervasive. Un altro aspetto particolarmente rilevante è la sostanziale incompletezza della governance dei report regolamentari e gestionali, con una copertura parziale dei documenti critici e con rilevanza materiale, anche quando richiesti dagli organi di vigilanza.

Parallelamente, Banca d'Italia ha avviato nel corso del 2023 un'indagine su un campione di *Significant Institutions* e *Less Significant Institutions* italiane, allo scopo di acquisire informazioni di dettaglio circa i processi e le prassi di aggregazione e reportistica dei dati di rischio adottati, le cui evidenze sono stati incluse all'interno del documento prodotto del 2024 "*Indagine su risk data aggregation e risk reporting*". In particolare, tra gli aspetti positivi rilevati è stata evidenziato come nella maggior parte dei casi le architetture IT delle banche in analisi risultano in grado di supportare una buona granularità dei dati, e i sistemi IT sono generalmente inclusi nei piani di *business continuity*. Inoltre, le capacità di aggregazione dei dati di rischio si dimostrano essere solide, con una buona copertura delle fonti informative e un'adeguata gestione delle soglie di materialità. Tuttavia, in linea con quanto evidenziato nella *targeted review* BCE, tra le principali aree di criticità si rilevano carenze nelle modalità di attribuzione di ruoli e responsabilità nell'attuazione dei Framework di Data Governance, una non efficace individuazione dei requisiti di *data quality,* la scarsità di processi di validazione indipendenti su RDARR, presidi non sufficienti sul *data lineage* e una non diffusa applicazione dei requisiti di accuratezza dei dati inclusi nei report di rischio.

3. Prossimi passi e lessons learnt

Sulla base delle evidenze sopra richiamate e del dialogo che le singole Banche, nei prossimi anni i Regulator manterranno una elevata attenzione sulla tematica con l'obiettivo di portare il Sistema Bancario verso standard in linea con le attese sopra richiamate e sin qua, lungamente, disattese

Alla luce dell'esperienza pluriennale maturata da Deloitte con primari operatori bancari domestici ed Europei su progettualità in ambito RDARR, riportiamo a seguire alcune *lessons learned* al fine di garantire il successo delle iniziative intraprese:

- **Governance**: è fondamentale una chiara identificazione dei ruoli e delle responsabilità sottese

vedi l'articolo online

il framework RDARR, a partire dagli organi di gestione, passando per il Senior Management e poi via via fino ad arrivare ai Data Owner ed alle strutture responsabili della Data Governance e dell'architettura IT. Nelle fasi di disegno ed implementazione del framework su tutto il perimetro è preferibile una struttura progettuale accentrata con una chiara identificazione degli obiettivi, della pianificazione e di risorse quali-quantitavamente adeguate al raggiungimento degli obiettivi

- **Scope of work:** in considerazione della potenziale ampiezza, è necessario procedure ad una chiara identificazione del perimetro rilevante ai fini RDARR in termini di: i) Legal Entities; ii) Report e Modelli; iii) Key Risk iii) Critical Data Elements; iv) perimetro di risalita (fino al data capture); v) sistemi ed applicativi coinvolti. A proposito è opportuno definire regole il più possibile oggettive a supporto del dialogo con il Regulator; allo stesso tempo è consigliabile identificare un perimetro prioritario su cui avviare le attività, per poi procedere ad una progressiva estensione dei presidi nel tempo.

- **Formazione:** è necessario prevedere programmi di formazione al fine di consentire una conoscenza e cultura diffusa all'interno dell'organizzazione della rilevanza del tema, degli strumenti e dei presidi definiti. Inoltre, è necessario prevedere una formazione specifica per i diversi ruoli, a partire dal Board e dagli organi di controllo. In particolare, è necessario creare una commistione e contaminazione di competenze (business vs. data governance) sulle figure direttamente coinvolte

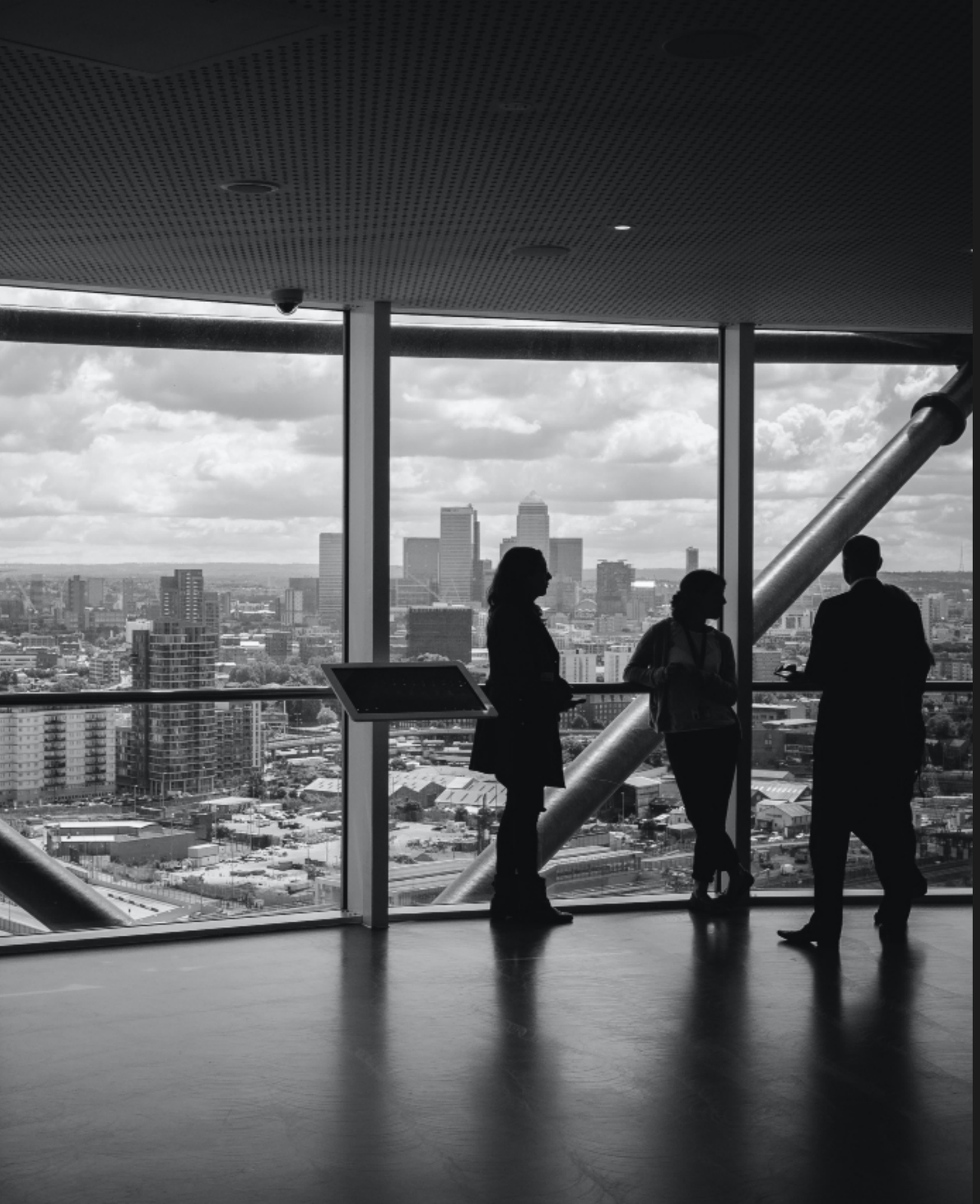
- **Data Owner:** in considerazione della centralità del ruolo del Data Owner e del fatto che tipicamente le figure incaricate di agire il ruolo hanno un background più legato ai processi di business e di controllo che ad aspetti di Data Governance, è fondamentale delimitare chiaramente il loro ruolo e relativo perimetro, fornendogli strumenti adeguati e definendo chiari ed efficaci modelli di collaborazione con le strutture di Data Governance - accentrate o federate - eventualmente delegando alcune attività a strutture operative dedicate (es. data stewards per la definizione e la manutenziome dei *data dictionaries* e del *data lineage*);

- **Data Governance:** è necessario assicurare che le policy e procedure di data Governance siano implementate in maniera efficace e consistente su tutto il perimetro rilevante, a proposito oltre a definire modelli di collaborazione efficaci con tutti gli attori coinvolti, è opportuno dotarsi di strumenti efficaci e per quanto possibile automatizzati per supportare le attività di Data Governance

- **Controlli di II livello**: possono essere accentrate su un'unica unità organizzativa o ripartite su varie unità in funzione delle specifiche competenze area di Controllo (ad. Esempio in area CRO, CFO o CIO), ma è in ogni caso necessario individuare una unica struttura indipendente quale struttura ultima responsabile dei controlli di secondo livello

- **Architettura tecnologica**: è necessario condurre specifiche analisi volte ad investigare la capacità di aggregazione in tempi adeguati di dati granulari che provengano da diverse aree applicative (es. credit risk, market risk, bilancio, reporting di Vigilanza) e diverse Società del gruppo. Inoltre, è necessario identificare le principali manualità ed End User Application e valutarne la rimozione. A proposito è chiave l'identificazione delle possibili aree di intervento e di analisi costi-benefici al fine di identificare e prioritizzare eventuali interventi di ammodernamento del parco applicativo

vedi l'articolo online



DB non solo diritto bancario

A NEW DIGITAL EXPERIENCE

dirittobancario.it