MONTE DEI PASCHI DI SIENA
BANCA DAL 1472

I RISCHI OPERATIVI NEL NUOVO QUADRO REGOLAMENTARE
Esperienza del Gruppo MPS

Luigi Saputo
Head of Operational Risk Management

SUPERVISION RISKS & PROFITABILITY

Milano, 09 giugno 20206

1

Il passaggio dai metodi interni alla nuova regolamentazione

1. Adattare un processo già strutturato basato sui modelli interni
2. Tassonomie a più livelli - La verifica ed aggiornamento degli alberi decisionali
3. Definizione degli attributi di classificazione
4. Business Indicator – Rafforzamento relazioni tra le Funzioni Aziendali nel RAF

2

Conservazione delle componenti qualitative del modello nelle prassi operative

1. Lo studio della frequenza di accadimento
2. L'analisi dei rischi operativi nei processi aziendali
3. Raccolta e sviluppo Giudizi Esperti – Analisi di scenario e gli stress interni
4. Case study sugli scenari: Non solo Cybersecurity ma anche la Tecnologia a supporto delle Frodi

3

Come sta cambiando l'analisi del rischio operativo nel dialogo con la Vigilanza

1. Nuove frontiere del Rischio Operativo, la Resilienza Operativa e Innovazione Digitale
2. Incidenti – Gli Impatti Economici non limitati alle perdite contabilizzate
3. Processi di Digitalizzazione – Investimenti progettuali e rischi di business

1.1 Adattare un processo già strutturato basato sui modelli interni

Tutte le Componenti del modello di misurazione interna sono state evolute per adeguare la gestione dei rischi operativi al nuovo contesto regolamentare.

La **Loss Data Collection** è un processo in gran parte automatizzato che consente di censire gli eventi di rischio operativo, classificarli per tipologia e fattore di rischio e seguirne gli sviluppi contabili. Il processo ha reso disponibili oltre 20 anni di serie storiche.

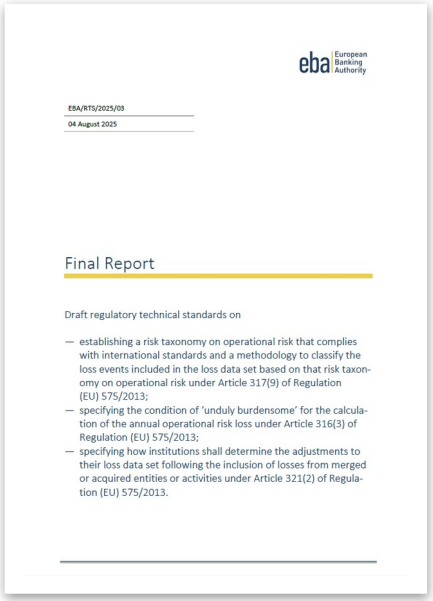
Il Risk Assessment dei processi aziendali consente di valutare i **fattori di contesto e di controllo** con il coinvolgimento del *Middle Management.* L'autovalutazione sulla qualità dei presidi posti in essere per la gestione e il controllo dei rischi consente di identificare aree di intervento e ridurre la frequenza di accadimento.

Contribuzione ed utilizzo delle informazioni di Sistema fornite **dall'Osservatorio DIPO** (Database Italiano delle Perdite Operative).
Il sistema offre la possibilità di identificare e studiare fenomeni idiosincratici di rara frequenza e di alto impatto non presenti nelle serie storiche interne.

L'elaborazione degli scenari avviene ipotizzando accadimenti in un contesto macroeconomico di riferimento al quale si aggiungono **l'evoluzione negativa di eventi noti e lo sviluppo di eventi non noti** elaborati anche con la raccolta di Giudizi Esperti (*Top Management).*

1.2 Tassonomie a più livelli - La verifica ed aggiornamento degli alberi decisionali

Il Gruppo MPS ha adottato fin dalla realizzazione del modello AMA una metodologia di identificazione delle Fonti Informative e di studio dei fenomeni che consente di mappare gli Eventi di Rischio Operativo in tassonomie su più livelli, integrati in un continuo percorso di verifica e miglioramento della raccolta dei dati di perdita. In quanto parte di un modello interno, la metodologia è stata sottoposta nel continuo anche a verifiche della convalida interna e oggetto di Audit.


eba European Banking Authority

EBA/RTS/2025/03

04 August 2025

Final Report

Draft regulatory technical standards on

— establishing a risk taxonomy on operational risk that complies with international standards and a methodology to classify the loss events included in the loss data set based on that risk taxonomy on operational risk under Article 317(9) of Regulation (EU) 575/2013;
— specifying the condition of 'unduly burdensome' for the calculation of the annual operational risk loss under Article 316(3) of Regulation (EU) 575/2013;
— specifying how institutions shall determine the adjustments to their loss data set following the inclusion of losses from merged or acquired entities or activities under Article 321(2) of Regulation (EU) 575/2013.

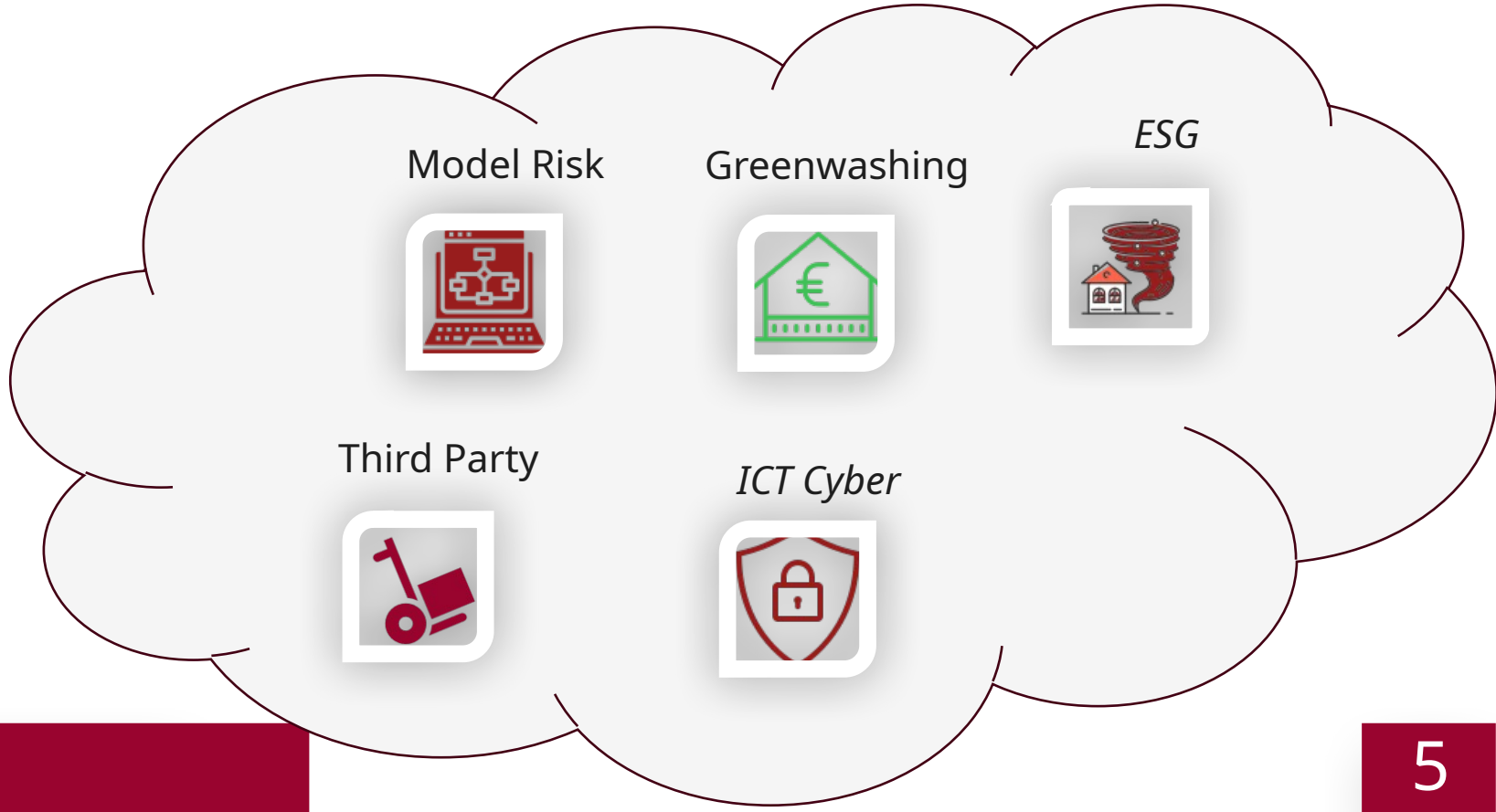
A seguito dell'adozione della tassonomia a due livelli (EBA/RTS/2025/03) è stato deciso di non perdere i livelli di maggior dettaglio assicurati delle tassonomie in uso e di utilizzare più alberi decisionali, attivando quindi un *parallel running.*

Il Gruppo ha valutato come sostenibile lo sforzo di riprocessare gli eventi di rischio operativo attraverso un nuovo albero decisionale sviluppato sugli RTS.

1.3 Definizione degli attributi di classificazione

Risulta, invece, più gravoso il compito di associare agli eventi di rischio i nuovi attributi. Seppure il documento finale degli RTS abbia chiarito diversi ambiti di incertezza l'attività di ricostruzione presenta un impegno significativo.

L'utilizzo di una tassonomia di Fattori di Rischio associati agli Event Type può agevolare l'assegnazione di alcune categorie. Attualmente sono in corso di verifica ed aggiornamento le associazioni Fattore di Rischio – Evento di Rischio al fine di ottimizzare il processo di ricostruzione degli attributi senza ripetere l'analisi di dettaglio su eventi di rischio ormai esauriti nella manifestazione contabile.



1.4 Business Indicator – Rafforzamento relazioni tra le Funzioni Aziendali nel RAF

La nuova regolamentazione ha portato un significativo cambiamento nella determinazione dei Requisiti Patrimoniali a Fronte dei Rischi Operativi, che crescono più velocemente all'aumentare % del valore Business, mentre possono ridursi in una fase di ristagno economico anche in presenza di una crescita delle Perdite Operative.

Fino al 2024 i risultati del modello AMA sono stati acquisiti dalle Funzioni Aziendali con la fiducia dovuta ad un modello validato, ma con la distanza di chi non riscontra nel risultato del modello una spiegazione lineare con il contesto che sta vivendo.

Anche se dal 2025 il calcolo del Requisito è passato alla Funzione Bilancio, nel RAF è comunque la Funzione di Risk Management a effettuare le misurazioni ei Requisiti in relazione al profilo di rischio. Per fare questo è coinvolta in modo più continuo nello sviluppo degli scenari e partecipa attivamente alla costruzione del Business Indicator di piano, ricevendo le informazioni dalla Pianificazione e fornendo le attese di perdita derivanti dagli eventi operativi.

Nel processo ICAAP sono inoltre effettuate delle prove di stress che prevedono anche contributi dei rischi operativi per effetti indiretti in grado influenzare l'andamento del Business (ad esempio perdita di fiducia a seguito di gravi eventi operativi classificati come Misconduct), che pur producendo un requisito a fronte dei rischi operativi potenzialmente in diminuzione implicano la manifestazione di effetti su altri ambiti di rischio.

Stress indotto su altre tipologie di rischio

Nello sviluppo degli scenari di rischio, oltre alle descrizioni degli accadimenti attesi dal modificato contesto esterno, sono state introdotte descrizioni di impatti indiretti relativi a eventi di rischio operativo in grado di produrre una limitata manifestazione economica (perdita contabile) ma un'ampia risonanza mediatica. Ad esempio scenari di incidenti operativi, o di sicurezza, e difficoltà nella realizzazione dei progetti di trasformazione digitale sono forniti come input per lo sviluppo di volumi e redditività degli Asset ma anche per i rischi di liquidità.

1

Il passaggio dai metodi interni alla nuova regolamentazione

1. Adattare un processo già strutturato basato sui modelli interni
2. Tassonomie a più livelli - La verifica ed aggiornamento degli alberi decisionali
3. Definizione degli attributi di classificazione
4. Business Indicator – Rafforzamento relazioni tra le Funzioni Aziendali nel RAF

2

Conservazione delle componenti qualitative del modello nelle prassi operative

1. Lo studio della frequenza di accadimento
2. L'analisi dei rischi operativi nei processi aziendali
3. Raccolta e sviluppo Giudizi Esperti – Analisi di scenario e gli stress interni
4. Case study sugli scenari: Non solo Cybersecurity ma anche la Tecnologia a supporto delle Frodi

3

Come sta cambiando l'analisi del rischio operativo nel dialogo con la Vigilanza

1. Nuove frontiere del Rischio Operativo, la Resilienza Operativa e Innovazione Digitale
2. Incidenti – Gli Impatti Economici non limitati alle perdite contabilizzate
3. Processi di Digitalizzazione – Investimenti progettuali e rischi di business

2.1 Lo studio della frequenza di accadimento

Il modello di misurazione Regolamentare basato su componenti economiche che formano il Business Indicator non viene influenzato dalla frequenza degli eventi di rischio operativo. Sotto il profilo di contenimento delle Perdite Future e di detection di nuovi fattori di rischio emergenti, il Gruppo MPS ha mantenuto in essere un processo di analisi nel continuo degli eventi e di verifica della robustezza dei presidi di controllo posti all'interno dei processi aziendali.

Seppure il requisito abbia concentrato le segnalazioni sulla Perdita Contabilizzata in un periodo, la raccolta degli eventi di rischio viene sviluppata anche su accadimenti che non hanno ancora generato la perdita e per i quali la **Data di Accadimento/Rilevazione presenta una informazione importate** per lo studio dei fattori di rischio

Attraverso lo studio della distribuzione degli eventi, metodo di analisi ereditato dal modello interno mantenuto nei processi di gestione del rischio operativo, vengono intercettate **dinamiche inattese delle manifestazioni di rischio**

Nuove dinamiche possono evidenziare esigenze di aggiornamento delle tassonomie e/o associazioni di nuovi fattori di rischio nei Processi Aziendali in cui si manifestano gli eventi

Le azioni correttive che portano al rafforzamento processi attivano il successivo monitoraggio sulla loro efficacia

Raccolta periodica delle informazioni necessarie a valutare e monitorare i fattori di contesto operativo e di controllo. Autovalutazione fatta con il coinvolgimento del Middle Management in qualità di «process owner» o «utilizzatore» dei processi.

2.2 L’analisi dei rischi operativi nei processi aziendali

Nel Quadro di Gestione del Rischio Operativo (art. 323) viene chiesto alle Banche di mantenere un adeguato sistema di valutazione delle esposizioni al rischio e tenere traccia dei dati pertinenti, non limitati ai dati sulle perdite.

FUNZIONI AZIENDALI COINVOLTE

Tutti i Process Owner, Middle Manager (indipendentemente dalla storia delle perdite generate dal processo di riferimento).

Rappresentanti degli Attori di Processo (identificati nei presidi Territoriali a maggiore operatività e con più elevato valore del Business in gestione).

I FATTORI DI CONTESTO E DI CONTROLLO

Permette di fare una ricognizione periodica, sistematicamente aggiornata, sui rischi operativi presenti in tutti i processi aziendali, che comprende :

- la valutazione qualitativa dei presidi posti in essere a fronte di ciascun fattore di rischio;
- la segnalazione, in caso di presidio non ottimale, contribuendo alla definizione di un intervento migliorativo della qualità della gestione.

PRINCIPALI VANTAGGI

- Partecipazione dei rappresentanti di tutte le Business Lines alle valutazioni del rischio operativo
- Miglioramento del processo di analisi degli eventuali rischi da mitigare (es. modifiche ai processi/sistemi, rafforzamento competenze con attività formativa)
- Supporto all’organizzazione aziendale per la classificazione dei Processi e il collegamento ai rischi
- Arricchimento delle Fonti di Identificazione degli eventi di rischio e delle tassonomie

Esempio: Analisi eventi connessi al Model Risk

Data Management (7.4)

Model Implementation and Use (7.5)

Model Methodology (4.8)

2.3 Raccolta e sviluppo Giudizi Esperti – Analisi di scenario e gli stress interni

Gli scenari di Stress Firm-Wide approvati dal CdA nell'ambito dello Stress Test Programme 2026 forniscono componenti idiosincratiche non legate al contesto macroeconomico ma riconosciute come fattori di rischio per capitale e liquidità in un orizzonte pluriennale.

Lo scenario idiosincratico dell'Operational Risk è determinato attraverso l'introduzione di perdite operative dovute ad evoluzioni negative di eventi noti e non noti, identificati anche sulla base dei giudizi esperti forniti con l'analisi di scenario effettuata al Top Management. Definito **l'intervallo di probabilità di accadimento** dello scenario di stress **inferiore al 5%,** vengono elaborati scenari ad hoc per ogni classe di rischio (Event Type).

Complessivamente sono stati applicati in fase di stress 24 scenari di perdite operative idiosincratiche. Alcuni scenari comportano, oltre alle perdite operative, impatti indiretti nel medio periodo derivanti dai rischi reputazionali.

Scenari di impatto estremo (rispetto alle serie storiche)

Alcuni esempi…

Event Type	Scenario
Frode Interna - ET1	
	Infedeltà Interna Compromissione Sistemi
	Infedeltà Interna Furto Dati
	Frode internal Banker
Frode Esterna - ET2	
	Furto dati Malware
	Attacco su Digital – Vulnerabilità zero day
Clienti, Prodotti e Prassi Operative - ET4	
	Variazione di giudizio su eventi noti
	Nuovi fenomeni Misconduct
	Greenwashing
Danni a beni materiali - ET5	
	Danni ad immobili - Incendio
	Danni ad immobili – Eventi Naturali
Interruzione dell'operatività e disfunzione dei sistemi - ET6	
	Incidente Operativo Change
	Incidente Operativo Run
Esecuzione, Consegna e Gestione dei Processi - ET7	
	Supply chain
Scenari specifici per il Cyber Risk	
	Impatti Diretti sul Gruppo di Cyber Risk Ransomware
	Impatti Indiretti sul Gruppo di Cyber Risk account dipendenti

Focus slide successiva

La produzione di scenari non è limitata allo Stress.

Lo studio dei fenomeni coinvolge gli esperti aziendali anche per elaborare scenari di eventi idiosincratici più probabili (Base).

2.4 Case study sugli scenari: Non solo Cybersecurity ma anche la Tecnologia a supporto delle Frodi

Le Minacce Tecnologiche e le relative implicazioni di Resilienza Operativa (incidenti di sicurezza o anche di tipo operativo) sono presenti in molti scenari valutati di rara frequenza ma di elevato impatto.

Un dipendente del Gruppo effettua estrazioni di dati della clientela costruendo un archivio personale di informazioni e dossier documentali, riuscendo ed esfiltrare i dati con l'utilizzo di un archivio personale in cloud. Solo dopo diverse settimane viene identificato l'anomalo accesso ai dati aziendali a seguito di un periodico controllo su diritti e autorizzazioni dell'utenza, che risultano più ampi di quelli strettamente necessari per le attività operative. Il dipendente è oggetto di indagini investigative dell'autorità giudiziaria per la presunta vendita delle informazioni. **La Banca subisce sanzioni per la violazione dei dati e contestazioni legali. Effetti reputazionali si osservano nell'abbandono della clientela, in particolare i grandi depositanti.**

Un'azienda del Gruppo è vittima di un attacco cyber di tipo social. I sistemi di difesa non hanno rilevato la presenza di un Malware installato inconsapevolmente da un utente, vittima di attacco social engineering (software latente). Dopo settimane dall'accadimento si manifestano malfunzionamenti nei sistemi di contabilità della Banca con mancata quadratura delle giornate contabili a causa della presenza di dati cifrati negli archivi. Un messaggio proveniente da un gruppo Hacker compare nei sistemi della Banca, fornendo come prova dati bancari esfiltrati con successo. Viene presentata la richiesta di un riscatto, con la minaccia di rendere pubblico l'accadimento in caso di mancato pagamento. La task force attivata per la ricerca delle cause dell'incidente conferma che i dati di contabilità sono stati cifrati ma che chiusure alla giornata precedente erano state eseguite correttamente. **La Banca è costretta a rendere pubblico l'accadimento e sospendere qualsiasi attività fino a conclusione delle procedure di sanificazione e ripristino.** Dopo la ripartenza la Banca non è in grado di identificare esattamente quali file e informazioni siano state esfiltrate e di quali clienti, tuttavia l'analisi dei flussi indica che i volumi di dati esfiltrati non siano significativi. Il gruppo Hacker aveva effettivamente esfiltrato dati aziendali e li pubblica, tra questi sono presenti dati personali e patrimoniali di personaggi di interesse pubblico. V**engono attivate procedure sanzionatorie dalle Autorità e si osserva la perdita di fiducia digitale sull'intero Gruppo. Oltre alla perdita della clientela, si osserva un numero crescente di richieste di**

1

Il passaggio dai metodi interni alla nuova regolamentazione

1. Adattare un processo già strutturato basato sui modelli interni
2. Tassonomie a più livelli - La verifica ed aggiornamento degli alberi decisionali
3. Definizione degli attributi di classificazione
4. Business Indicator – Rafforzamento relazioni tra le Funzioni Aziendali nel RAF

2

Conservazione delle componenti qualitative del modello nelle prassi operative

1. Lo studio della frequenza di accadimento
2. L'analisi dei rischi operativi nei processi aziendali
3. Raccolta e sviluppo Giudizi Esperti – Analisi di scenario e gli stress interni
4. Case study sugli scenari: Non solo Cybersecurity ma anche la Tecnologia a supporto delle Frodi

3

Come sta cambiando l'analisi del rischio operativo nel dialogo con la Vigilanza

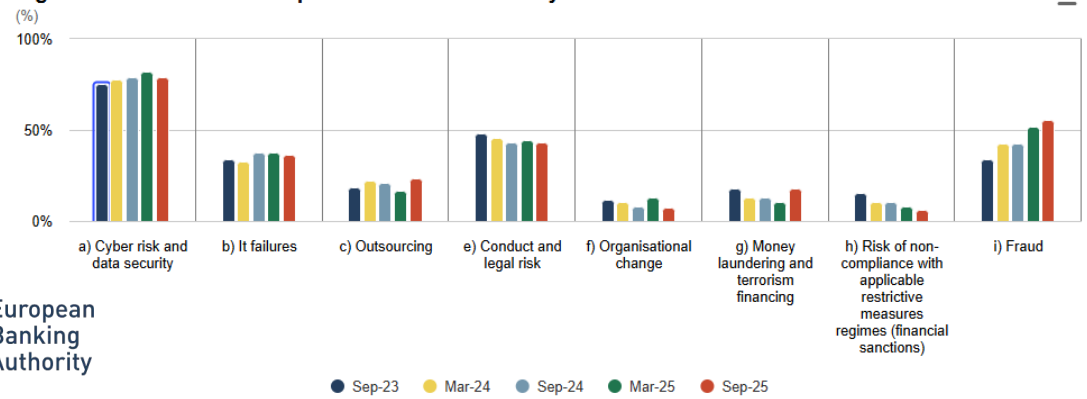
1. Nuove frontiere del Rischio Operativo, la Resilienza Operativa e Innovazione Digitale
2. Incidenti – Gli Impatti Economici non limitati alle perdite contabilizzate
3. Digitalizzazione – Rischi operativi connessi ai progetti e effetti su rischi di business

3.1 Nuove frontiere del Rischio Operativo, la Resilienza Operativa e Innovazione Digitale

Il Regolamento UE 2022/2554 (DORA) ha portato in evidenza una particolare tipologia di Rischio Operativo connesso alla Resilienza Operativa Digitale, tema ripreso nel 2025 dalla Vigilanza come priorità del piano, dedicando specifiche analisi anche all'interno del processo SREP. Nel Risk Assessment Questionnarie si Settembre 2025 le Banche confermano il Cyber Risk al primo posto per il rischio operativo.

I punteggi SREP insoddisfacenti registrati per il rischio operativo e i risultati dell'attività di vigilanza negli ambiti della resilienza cibernetica e della gestione dell'esternalizzazione confermano le carenze negli assetti operativi delle banche e la necessità di compiere progressi nell'azione correttiva. Nel quadro dello SREP 2024 il rischio operativo ha continuato a essere l'area con il peggiore punteggio medio, riconducibile principalmente a elementi relativi alle tecnologie dell'informazione e della

Figure 48: Main drivers of operational risk as seen by banks



Source: EBA Risk Assessment Questionnaire

https://www.bankingsupervision.europa.eu/framework/priorities/html/ssm.supervisory_priorities202412~6f69ad032f.it.html
https://www.eba.europa.eu/publications-and-media/publications/risk-assessment-report-december-2025

3.2 Incidenti – Gli Impatti Economici non limitati alle perdite contabilizzate

Le implicazioni economiche della Resilienza Operativa sono state affrontate a partire dal Cyber Stress Test del 2024. Lo schema di valutazione degli impatti non viene applicato solo per la valutazione degli incidenti ma viene anche utilizzato per sviluppare una o più ipotesi per ogni scenario si stress operativo.

IMPATTI P&L COSTI DIRETTI OPERATING LOSSES

Gestione dell'evento idiosincratico	• Maggiori costi di engagement staff • Costi di ripristino sistemi (es. costi variabili outsourcer) • Costo perizia tecnica e forense • Costi interventi IT • Maggior costo personale interno • Costo Data Breach • Attivazione monitoraggi stampa e social • Costo della Comunicazione alla clientela
Contestazioni della clientela (passive)	• Accantonamenti / Indennizzi (Cause) • Accantonamenti / Esborsi (Stragiudiziale) • Rimborsi e ristori prestazioni pagate e non godute • Costi / spese legali
Possibili multe e sanzioni	• Multe da Autorità di Vigilanza (e.g. Sanzioni GDPR) • Eventuali altre sanzioni regolamentari
(Recuperi Assicurativi)	Indennizzi attesi da Assicurazioni Attive

ALTRI IMPATTI P&L (non Op. Losses)

- Investimenti per soluzioni di Ripristino Operatività
- Legale esterno (cause e contestazioni attive)
- Spese di consulenza
- Costi di revisione processi aziendali

ONERI INDIRETTI REPUTAZIONALI / STRATEGICI (Mancati guadagni e Perdita di Business)

- Mancati incassi per blocco delle transazioni
- Variazione % Volumi Raccolta (Stock)
- Variazione % Volumi Impieghi (Flusso)
- Variazione Commissioni o Interessi (Sconti per Retention)

3.3 Digitalizzazione – Rischi operativi connessi ai progetti e effetti su rischi di business

Come illustrato, tra le priorità della Vigilanza è stato posto un particolare focus ai processi di digitalizzazione ed agli impatti delle nuove tecnologie sullo sviluppo del Business. Temi affrontati dal Gruppo in specifiche attività di Vigilanza.

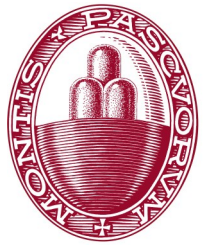
LA DIGITALIZZAZIONE ALLA BASE DEI PIANI STRATEGICI

La rilevanza della Digitalizzazione nei progetti di Piano del Gruppo ha portato all'adozione di un modello per il calcolo di un requisito patrimoniale di secondo pilastro rappresentativo del rischio strategico. Il rischio viene misurato rilevando criticità e mitigazioni di 16 fattori di rischio connessi alla realizzazione progettuale

LE MINACCE DERIVANTI DALLE NUOVE TECNOLOGIE

Il passaggio alla digitalizzazione è ormai obbligatorio per mantenere un adeguato livello di concorrenza tra le Banche. La Digitalizzazione espone le Banche a rischi di mancato raggiungimento degli obiettivi e a minacce relative alla difesa di processi, sistemi e dei clienti utilizzatori.

Il recente sfruttamento delle tecnologie AI per identificare e potenzialmente sfruttare vulnerabilità delle Banche o costruire attacchi di tipo social personalizzati sui Target interni ed esterni alle organizzazioni ha attirato l'attenzione della Vigilanza, preoccupata per i potenziali effetti sulla sicurezza e stabilità del Sistema. In questi giorni le Banche stanno tenendo incontri di approfondimento per mappare le prassi in uso ed i piani di azione che possono essere adottati per stare al passo con queste nuove minacce


MONTE DEI PASCHI DI SIENA
BANCA DAL 1472