Banco Desio

Dalla frammentazione all'integrazione: l'evoluzione del Risk Management nei rischi non finanziari

Approccio metodologico e organizzativo di una banca Less Significant

Giugno 2026

L'EVOLUZIONE DEL FRAMEWORK DI GESTIONE DEI RISCHI NON FINANZIARI

APPROCCIO DI GESTIONE DEL GRUPPO BANCO DESIO

Evoluzione del Framework

2015

Framework unico di gestione rischi operativi, IT e prime valutazioni rischi terze parti

2018 - 2019

Creazione dei primi modelli verticali di valutazione del rischio IT e Terze parti

2022

Passaggio da BIA a TSA e modifica del framework di Rischio Operativo

2025

Adeguamenti a DORA e a CRR3

Evoluzione della Struttura organizzativa

2015

Nessuna Struttura organizzativa dedicata

2021

Creazione dell'Ufficio IT & Operational Risk in riporto al CRO

2025

Creazione di due uffici specialistici

ATTUALE MODELLO ORGANIZZATIVO ADOTTATO DAL GRUPPO BANCO DESIO

Nel 2025 il Gruppo ha introdotto una revisione organizzativa della Direzione Risk Management, con l'obiettivo di rafforzare la specializzazione senza compromettere il coordinamento.

In particolare:

- scorporo delle attività di **IT Risk e Rischi di Terze Parti** dai Rischi Operativi;
- creazione di **due uffici distinti e specialistici**;
- inserimento di **risorse con competenze verticali in ambito IT e sicurezza**.

Obiettivo: creare un'unità dedicata ai **rischi ICT emergenti**, in coerenza con la normativa DORA, rafforzando al contempo il **coordinamento con le Funzioni di controllo.**

	Ufficio IT Risk e Terze Parti	Ufficio ERM e Rischi Operativi
Rischi in perimetro	• Rischio Informatico e di Sicurezza • Rischio Terze Parti	• Rischio Operativo • Rischio Reputazionale • Rischio Strategico

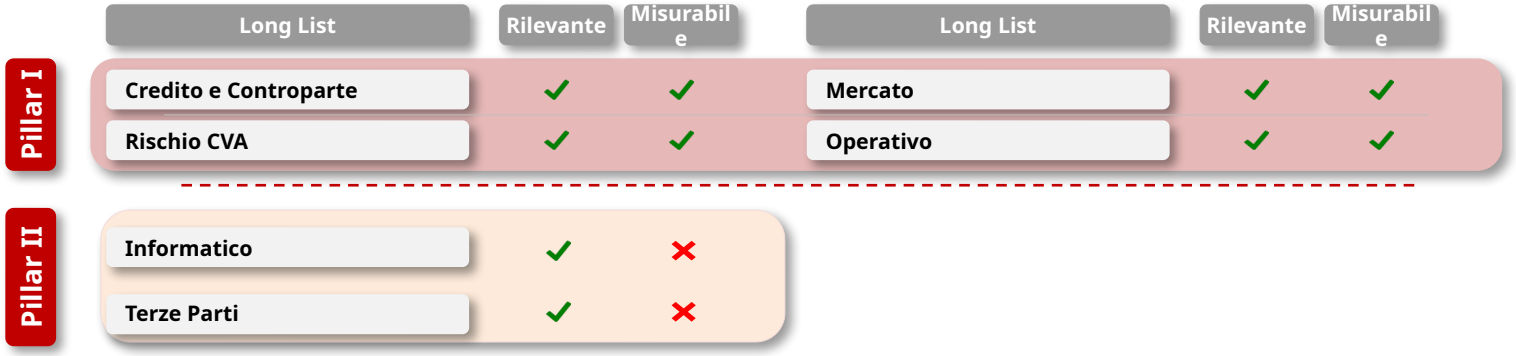
RISCHIO OPERATIVO E RISCHIO INFORMATICO

DEFINIZIONI E MAPPA DEI RISCHI

Rischio operativo: rischio di perdite derivanti dalla inadeguatezza o dalla disfunzione di processi, risorse umane e sistemi interni oppure da eventi esogeni, **ivi compresi,** tra l'altro, il rischio giuridico, il rischio di modello e il **rischio relativo alle tecnologie dell'informazione e della comunicazione (TIC**) ma non il rischio strategico e di reputazione.

Rischio informatico: il **rischio di perdite correlate a qualunque circostanza ragionevolmente identificabile legata all'uso della rete e dei sistemi informatici** che, qualora si concretizzi, potrebbe compromettere la sicurezza della rete e dei sistemi informatici, di eventuali strumenti o processi dipendenti dalle tecnologie, delle operazioni e dei processi, oppure della fornitura dei servizi, producendo effetti avversi nell'ambiente digitale o fisico.

Cfr. Regolamento UE 2024/1623



Rischio Informatico e Terze Parti giudicati «Rilevanti» con valutazione specifica dei presidi ma «Non Misurabili», il **Capitale interno è già compreso nel capitale interno del Rischio Operativo.**

RISCHIO OPERATIVO E RISCHIO INFORMATICO

INTERRELAZIONI NEL PROCESSO ICAAP

Nel 2025, in avvio del ciclo SREP, **Banca d'Italia ha richiesto alle banche di classe 2 di rafforzare l'informativa sui rischi operativi, con particolare riferimento ai rischi informatici.**

Nel Resoconto ICAAP sono quindi previsti **tre Capitoli distinti:**

- **Rischio Operativo**
- **Rischio Informatico**
- **Rischio Terze Parti**

Evoluzioni Principali:

- **rafforzamento della descrizione dei modelli di valutazione, monitoraggio e gestione**;
- inclusione di **scenari di stress di rischio operativo con componente IT**;
- integrazione, nello scenario macroeconomico, di **fattori di rischio legati a eventi IT e cyber**.

RISCHIO OPERATIVO E RISCHIO INFORMATICO

INTERRELAZIONI NEL RAF

L'approccio metodologico adottato dal Gruppo per l'implementazione del RAF prevede:

- **mappa dei rischi,** che include tutti i rischi rilevanti e ne descrive metodologie di misurazione e gestione
- **valutazione combinata quantitativa e qualitativa, basata su:** indicatori di primo livello indicatori di secondo livello Key Risk Indicators (KRI)

	Indicatori di primo livello (^)	**Indicatori di secondo livello**	**Key Risk Indicators**
Monitoraggio	*Trimestrale*	*Mensile*	*Mensile*
Reporting	*CDA*	*Comitato Gestionale Rischi*	*Comitato Gestionale Rischi*
Escalation	*AD/CDA (*)*	*AD/Comitato Gestionale Rischi*	*n.a.*
Operativo	✓ (^^)	✓	✓
Informatico	✓	✓	✓
Terze Parti	✗	✗	✗

(^) Alcuni indicatori sono comuni al Recovery Plan

(*) In caso di supero della soglia di Tolerance di uno degli indicatori in commune con il Piano di Recovery la Banca d'Italia deve essere informata.

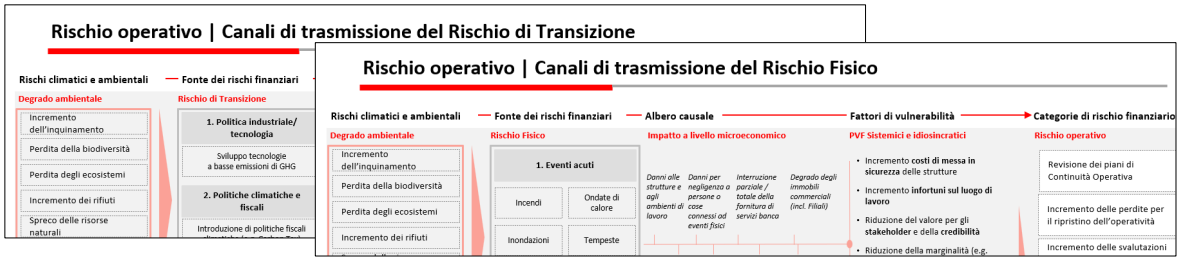
(^^) ***Solo gli indicatori di Rischio Operativo sono comuni con il Piano di Recovery, le perdite operative generate da rischi IT sono, tuttavia, incluse in questo indicatore*** .

LA FRAMMENTAZIONE DEL RISCHIO OPERATIVO OLTRE IL DORA

I RISCHI ESG

Il Gruppo Banco Desio **non ha previsto**, all'interno della mappa dei rischi di Gruppo, **l'identificazione dei Rischi ESG** (i.e. Fisico e di Transizione) ma ha integrato **i singoli rischi «Tradizionali».**

Per quanto riguarda il Rischio Operativo sono stati analizzati i **canali di trasmissione del Rischio Fisico e di Transizione** e identificate le potenziali categorie di **rischio finanziario**.



Dalle evidenze emerse **sono stati i criteri ESG nella valutazione del rischio operativo**:

- individuando **specifici Event Type riconducibili a fenomeni ESG** e monitorando le relative perdite operative connesse;
- effettuando **specifiche analisi** (accertamento e quantificazione – ove possibile) da inserire nel resoconto ICAAP;
- individuando specifici **indicatori di monitoraggio** inclusi nel **Tableau de Bord dei rischi.**

LA FRAMMENTAZIONE DEL RISCHIO OPERATIVO OLTRE IL DORA

ALTRI RISCHI

Oltre ai rischi tradizionalmente gestiti dalla Funzione Risk Management esistono **altre tipologie di rischi** che prevedono modelli **di gestione specifici** ma comunque **riconducibili nella macro-famiglia dei rischi operativi.**

	Mappa dei Rischi	ICAAP	RAF	Next Step
Riciclaggio e Finanziamento al Terrorismo	✓	• Presente Capitolo specifico, • descrizione qualitativa dei presidi organizzativi	• Presente Indicatore di RAF di primo livello; • Individuati KRI di monitoraggio	• Introduzione KRI di secondo livello
Rischio Sanction	✗	• Incluso nel capitolo del Rischio AML • Descrizione qualitativa dei presidi organizzativi	✗	• Inclusione nella mappa dei rischi; • Allo studio l'inclusione nel RAF di specifici indicatori.
Rischio Fiscale	✗	• Incluso nel capitolo del Rischio Compliance • Descrizione qualitativa dei presidi organizzativi	✗	✗

Eventuali **perdite operative** derivanti da tali rischi sono **già incluse nel modello di Loss Data Collection**, la valutazione dell'adeguatezza patrimoniale del Gruppo tiene conto **anche dei presidi organizzativi** in essere su tali rischi.

CONCLUSIONI

L'evoluzione del contesto esterno **rende necessario un adeguamento dei modelli di gestione dei rischi**, orientandoli verso un maggiore livello di specializzazione.

Tale esigenza **non rappresenta un elemento di novità** introdotto dal DORA..

La presenza di modelli distinti, gestiti da diverse strutture organizzative, **può generare sovrapposizioni e inefficienze nei presidi di controllo** (ad esempio tra rischio operativo e rischio informatico).

- Una chiara definizione del Risk Appetite Framework e una puntuale identificazione e valutazione dei rischi nell'ambito del processo ICAAP **consentono alla Banca di acquisire piena consapevolezza del proprio profilo di rischio** e dell'adeguatezza dei presidi in essere.