Allianz

Allianz Bank
Financial Advisors

Supervision, risks and profitability 2026

Rischio ICT oltre l'operativo: integrare senza duplicare

Milano, 10 giugno 2026

Regole del gioco chiare hanno nel tempo condotto a framework consolidati…

Variabile target

Eventi scatenanti

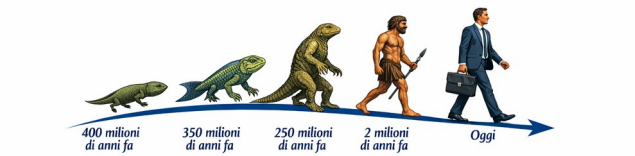
Per **rischio operativo** si intende il rischio di subire **perdite** derivanti **dall'inadeguatezza o dalla disfunzione di procedure, risorse umane e sistemi interni, oppure da eventi esogeni**. Rientrano in tale tipologia, tra l'altro, le perdite derivanti da frodi, errori umani, interruzioni dell'operatività, indisponibilità dei sistemi, inadempienze contrattuali, catastrofi naturali. Nel rischio operativo è compreso il rischio legale, mentre non sono inclusi quelli strategici e di reputazione *

IDENTIFICAZIONE	MISURAZIONE	GESTIONE
dipo database italiano perdite operative		RAF
RISK SELF ASSESSMENT		ACCETTAZIONE / MITIGAZIONE
KRI		MITIGATION / COPERTURA

** Banca d'Italia, Circolare n. 263*

… contribuendo alla creazione dell'attuale Enterprise Risk Governance.

Pillar	Rischio	Quantificabile	Rilevante	RISCHI TRASVERSALI: ESG	RISCHI TRASVERSALI: Geo-Politico
I	Rischio di Credito	✓	✓	✓	✓
	Rischio di Controparte	✓			
	Rischio di CVA	✓			
	Rischio Operativo	✓	✓	✓	✓
	Rischio di Mercato	✓			
	Rischio di Regolamento	✓			
II	Rischio di Liquidità		✓	✓	✓
	Rischio di Leva Finanziaria eccessiva	✓	✓		
	Rischio di Concentrazione single name	✓	✓	✓	
	Rischio di Concentrazione settoriale				
	Rischio Residuo	✓	✓		✓
	Rischio di Tasso interesse IRRBB	✓	✓		✓
	Rischio di differenziali creditizi CSRBB	✓			
	Rischio derivante da cartolarizzazioni	✓			
	Rischio Strategico	✓	✓	✓	
	Rischio Reputazionale		✓	✓	✓
	Rischio IT		✓	✓	✓
	…				



Schema esemplificativo a soli fini illustrativi, sulla base della definizione Rischi ex Circolare 285 e di talune prassi operative adottate dalla Banca

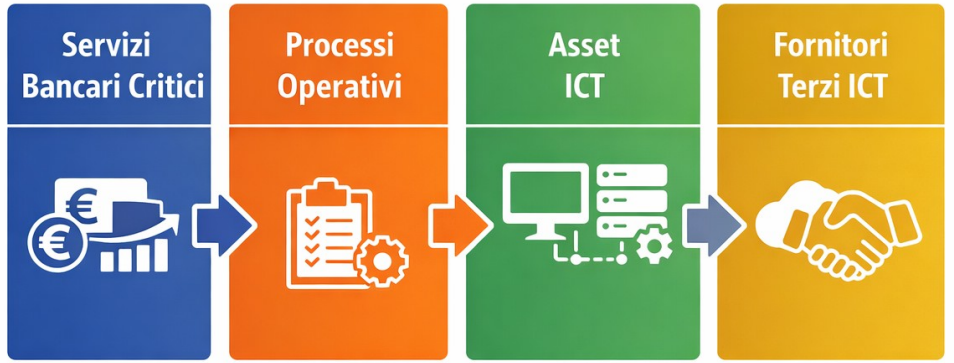
Nuove normative e nuove tecnologie hanno consolidato la presenza del nuovo rischio ICT

Pillar	Rischio
I	Rischio di Credito
	Rischio di Controparte
	Rischio di CVA
	Rischio Operativo
	Rischio di Mercato
	Rischio di Regolamento
II	Rischio di Liquidità
	Rischio di Leva Finanziaria eccessiva
	Rischio di Concentrazione single name
	Rischio di Concentrazione settoriale
	Rischio Residuo
	Rischio di Tasso interesse IRRBB
	Rischio di differenziali creditizi CSRBB
	Rischio derivante da cartolarizzazioni
	Rischio Strategico
	Rischio Reputazionale
	Rischio IT
	…

Rischio ICT

- *Confidenzialità, integrità, disponibilità*
- *…*
- *Qualità del dato*
- *Rischio Progetto ICT*
  - *Rischio di Execution*
  - *Rischio Cyber*
  - *Rischio …*
  - *Rischio Compliance*
- *Rischio AI*
  - *Rischio di Data Protection*
  - *Rischio Legale*
  - *…*
  - *Rischio Etico*
- *… (e.g. Rischio Cyber)*
- *Rischio Terze Parti ICT*
  - *Rischio Credito*
  - *Rischio Concentrazione*
  - *…*
  - *Rischio di Vendor Lock-in*

… spesso declinato su diversi livelli della value chain e per diverse finalità gestionali e regolamentari.



ANALISI GESTIONALI			ANALISI «REGOLAMENTARI»
Analisi		Perimetro	
ICT Risk Assessment	⟷	Asset ICT	Riesame del quadro per la gestione dei rischi informatici
Project Risk Assessment	⟷	Progetto ICT	ICT Risk Questionnaire
Third Party ICT Risk	⟷	Fornitore - Asset ICT	Questionario Fintech
AI Risk	⟷	Use case / Asset ICT	Relazione sull'analisi dei rischi operativi e di sicurezza nei servizi di pagamento
			Valutazione dei rischi di esternalizzazione
			…

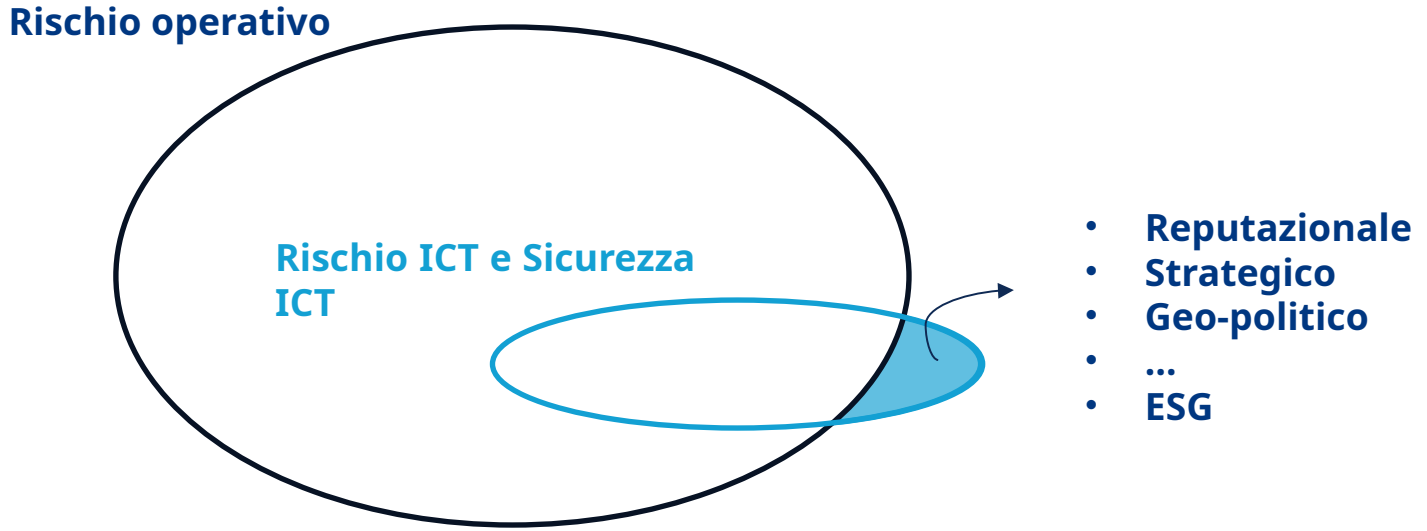
Il rischio ICT possiede elementi propri non soltanto del rischio operativo:

Circ. 285

«**rischio informatico (IT)**»: il **rischio di perdite** corrente o potenziale dovuto all'inadeguatezza o al guasto di hardware e software di infrastrutture tecniche suscettibile di compromettere la disponibilità, l'integrità, l'accessibilità e la sicurezza di tali infrastrutture e dei dati.

DORA

«**rischi informatici**»: qualunque circostanza ragionevolmente identificabile in relazione all'uso dei sistemi informatici e di rete che, qualora si concretizzi, può compromettere la sicurezza dei sistemi informatici e di rete, di eventuali strumenti o processi dipendenti dalle tecnologie, di operazioni e processi, oppure della fornitura dei servizi causando **effetti avversi** nell'ambiente digitale o fisico;



…il giudizio finale può condividere la scala di valutazione con il rischio operativo, ma non necessariamente il significato!

Governance	Terze Parti	Sicurezza ICT	…	Continuity
Strategia di resilienza	Flussi informativi	Gestione accessi	…	B.I.A.
Organizzazione ICT	Gestione concentrazioni	Gestione vulnerabilità	…	Piani di crisi
…	…	…	…	….
Framework di controllo	Risk assessment	Classificazione dei dati	…	Testing

- Aspetti generali (eg audit)
- Confidenzialità
- Integrità
- Disponibilità
- Sicurezza
- …
- Gestione dei cambiamenti
- Esternalizzazioni
- AI / Cloud

Efficacia dei controlli

Rischio potenziale	Alta	Medio-Alta	Medio-Bassa	Bassa
Basso	1	2	2	3
Medio-Basso	2	2	3	4
Medio Alto	3	3	4	4
Alto	3	4	4	4

Pur in un contesto di **regole e logiche condivise con il rischio operativo**, la valutazione di rischio informatico «residuo» racchiude in sé elementi propri anche di altri rischi di secondo pilastro. Così come avviene per i c.d. rischi trasversali, questi elementi devono essere separati e correttamente allocati ai rischi di riferimento per evitare «*double counting*» regolamentari

DORA è in produzione, le nuove priorità sono chiare. Quindi è tutto consolidato?

A valle Riesame, continuo fine tuning del «Quadro» per la gestione del rischio ICT:

- Rafforzamento della value-chain (sub-forniture)
- Rafforzamento framework concentrazione
- Consolidamento KRIs e *continuous assessment*
- Rapporti con terze parti
- Audit terze parti
- ….

Macro-«Quadro» per la gestione dei rischi: corretta allocazione di «parte» del rischio ICT all'interno della mappa dei rischi

Grazie per l’attenzione