



**MONTE
DEI PASCHI
DI SIENA**
BANCA DAL 1472

Il ruolo della Compliance bancaria nel rischio geopolitico

Dott. Ettore Carneade

Chief Compliance Executive Gruppo Montepaschi

Siena, 10 giugno 2026

Cos'è il rischio geopolitico



Il rischio geopolitico è **un fattore sistemico**, non facilmente classificabile come rischio idiosincratico o puramente sistemico, che richiede **lettura integrata e capacità anticipatoria**.

Una definizione operativa di rischio geopolitico

- Nella normativa bancaria europea (es. CRD) non esiste una definizione autonoma di rischio geopolitico
- Le Autorità di Vigilanza (BCE, EBA) lo trattano come fattore di rischio trasversale (trigger)
- Non è un rischio “stand-alone”, ma un evento esterno che innesca o amplifica i rischi tradizionali

Eventi geopolitici rilevanti

- Conflitti e guerre → impatti su asset, infrastrutture, continuità operativa
- Tensioni politiche e sanzioni → limitazioni a transazioni, liquidità, accesso ai mercati
- Instabilità macroeconomica → shock su prezzi, inflazione, frammentazione dei mercati
- Innovazione tecnologica → AI, Stablecoin, Euro Digitale, Terre Rare, Outsourcing

Canali di trasmissione sui rischi bancari

- Rischio di credito → deterioramento della qualità degli attivi
- Rischio di mercato → volatilità, spread, correzioni brusche
- Rischio di liquidità → stress sui funding e sui mercati valutari
- Rischio operativo → interruzioni, cyber risk, crisi delle sedi locali

Come la Vigilanza lo rende “operativo”

- ICAAP / ILAAP
- Stress test
- SREP e Pillar 2 Requirement (P2R)

Compliance e rischio geopolitico: evoluzione del ruolo



In tale contesto la **Compliance** agisce come **funzione “sentinella”** intervenendo nei processi quando si formano e presidiando la conformità secondo un approccio compliance by design

- **Design dei presidi e Governance**
 - lettura critica della corretta composizione del RAF
 - Definizione di framework e di indicatori che permettano di seguire nel tempo la robustezza della prevenzione e
 - Definizione di processi per tradurre scenari globali in impatti operativi
 - Coordinamento cross-funzionale con Risk, IT e Business
- **Alerting normativo e radar anticipativo**
 - Monitoraggio evoluzioni regolamentari PSD3/PSR (Payment Services Regulation), DSA (Digital Services Act), DMA (Digital Markets Act) come riflesso di dinamiche geopolitiche
 - Contributo per «tone of the top» del board
 - Early warning e supporto al management,
 - Dialogo con Autorità e anticipazione vigilanza
- **Rischi sanzionatori e reputazionali**
 - Sanzioni internazionali e frammentazione normativa
 - Exposure a controparti e filiere geopolitiche critiche
 - Controlli antifrode, nuovi attori e data sharing
- **Ruolo proattivo per il business**
 - Traduzione degli scenari geopolitici in opportunità (nuovi corridoi commerciali, mercati)
 - Supporto a scelte di posizionamento geografico e settoriale e sviluppo di modelli resilienti e compliance-by-design
 - Supporto a posizionamento strategico e competitività

Casi applicativi e rischi geopolitici emergenti

- **Magnifica Humanitas**
 - «[...] diventa decisivo ciò che chiamiamo accountability: la possibilità di identificare chi deve «rendere conto» delle decisioni, motivarle, controllarle e, quando necessario, contrastarle e rimediare ai danni che ne derivano» (Punto 105)
 - «[...] esiste spesso uno squilibrio tra la velocità dello sviluppo tecnologico e il ritmo con cui maturano consapevolezza, norme, controlli e istituzioni capaci di governarne gli effetti». (Punto 106)
- **Caso Claude Mythos**
 - Modello AI capace di individuare vulnerabilità in pochi minuti
 - accesso limitato a player tecnologici e banche non europee → Europa esclusa da test (Project Glasswing)
 - Technology gap e asimmetria difensiva (banche USA testano difese avanzate mentre banche UE resterebbero senza accesso diretto)
 - Accelerazione cyber risk
 - Reazione BCE: Riunione d'urgenza e pressione su banche
- **Aumento spesa militare e legislazioni nazionali**
 - Legge 220/2021 Misure per contrastare il finanziamento delle imprese produttrici di mine antipersona, di munizioni e submunizioni a grappolo
 - Dual use
- **Big Tech & Pagamenti (Payment Services Regulation – art. 88)**
 - Ingresso nuovi attori tecnologici ai dispositivi mobili di pagamento
 - Rischi: dipendenza da big tech e perdita sovranità tecnologica
- **Trattamento dei dati**
 - GDPR al suo primo decennio
 - AI Act
 - Digital Services Act e Digital Markets Act



Conclusioni

Compliance: da conformità a visione

- Rischio geopolitico – tecnologico: dipendenza da fornitori extra-UE e perdita sovranità digitale
- Rischio operativo: incapacità di adeguare tempestivamente controlli e sicurezza
- Rischio reputazionale: breach legati a vulnerabilità note ma non testabili (es. Mythos)
- Priorità: early warning, cooperazione, presidio del rischio di asimmetria tecnologica

La Compliance è chiamata a evolvere profondamente da Funzione di Controllo a... Funzione di Intelligence!



Grazie per l'attenzione

