ANNUAL
FUNZIONI AZIENDALI DI CONTROLLO
INCERTEZZA E CONTROLLI: DA ANTITESI A SINTESI
10, 11 e 12 NOVEMBRE 2020

COVID-19 e operational risk management: (prime) lessons learned

Veruska ORIO
Resp. Operational, Reputational e Cyber Risk, Intesa Sanpaolo

Di cosa ci siamo occupati?

Business Continuity	Collaborazione con l'Unità di Emergenza per l'attivazione del piano di continuità operativa e per la successiva (rapida) definizione delle ulteriori azioni da intraprendere con il progredire dell'epidemia
Loss Data Collection e Analisi di Scenario	Raccolta degli extra-costi connessi alla pandemia e delle informazioni utili al processo di analisi di scenario e di valutazione degli impatti di medio/lungo termine sul capitale
Interazione con il Business	Comprensione delle modifiche al modello operativo e al processo di trasformazione digitale e supporto alle scelte strategiche e operative dell'Unità di Emergenza
Profilo di rischio	Analisi delle variazioni nel profilo di rischio operativo alla luce della pandemia, della risposta alla pandemia e del diverso modello operativo
Interazione con il Supervisore	Supporto agli incontri dell'Unità di Emergenza con il Supervisore; predisposizione delle risposte a data e info request veicolate dal JST

Business Continuity

Il Modello Organizzativo di Gestione delle Crisi disegnato in passato sotto la spinta della normativa in materia ed evoluto negli anni seguenti è ben consolidato e ha visto il **coinvolgimento diretto del Chief Risk Officer nei lavori dell'Unità di Emergenza**

- *Attivazione di un'Unità di Emergenza dedicata alla gestione dello scenario pandemico*
- *Attuazione tempestiva delle misure incluse nel piano di emergenza*
- *Disponibilità di siti alternativi, adozione dello smart-working, backup delle risorse chiave, turni fisici per garantire la continuità dei servizi*
- *Test effettuati (es. Vulnerability Assessment e Penetration Test) sull'infrastruttura IT per far fronte all'aumento degli accessi remoti e degli attacchi informatici*
- *Verifiche sulla necessità per i fornitori/outsourcer di accedere ai nostri locali al fine di fornire il servizio in base ai contratti esistenti*
- *Interruzione di trasferte e viaggi, ad eccezione di quelli richiesti da situazioni aziendali critiche*

Loss data collection e analisi di scenario

I processi tradizionali di valutazione del rischio operativo sono ormai maturi e **sono in grado di raccogliere informazioni in maniera omogenea**, anche in caso di eventi di impatto ampio ed esteso. Serve però un ruolo di indirizzo forte da parte della funzione di Operational Risk Management (soprattutto con riferimento al tipo di «effetto» da raccogliere)

- *Attivazione della raccolta nel continuo delle perdite operative dovute alla pandemia (extra costi per igienizzanti, DPI, ecc.) e inclusione nel dataset di calcolo del capitale*
- *Monitoraggio Costi Operativi*
- *Creazione di uno scenario di rischio per stimare gli impatti futuri (Come valutare tali impatti? Con un workshop tra più funzioni o tramite valutazioni disgiunte?)*

Interazione con il Business

L'interazione con il Business si è evoluta rispetto alle occasioni di incontro periodiche già codificate (processi di assessment annuali, avvio nuovi prodotti/servizi/esternalizzazioni). La funzione di Operational Risk Management ha messo a disposizione il proprio know-how per disegnare un modello decisionale ad hoc e assegnare una priorità di intervento in caso di accadimento di scenari di rischio differenti

- *Valutazione delle possibili conseguenze della rivisitazione delle modalità di lavoro e dei processi aziendali (es. offerta servizi a distanza, industrializzazione processi in precedenza manuali)*
- *Sviluppo cd. «contagion risk model», per una valutazione autonoma dell'evoluzione del numero dei contagi e la conseguente individuazione di contromisure correlate ai livelli di rischio atteso*
- *Definizione delle priorità e delle modalità di intervento in caso di accadimento di scenari di rischio differenti*

Analisi del profilo di rischio

	Effetti immediati	Effetti emergenti	Effetti di lungo termine
Business Continuity Risk	Estensione lavoro da remoto (aumento remote collaboration/ acquisto laptop) Accelerazione del processo di trasformazione digitale	Spossatezza da lavoro in remoto/burn-out Aumento capacità dell'infrastruttura VPN Rivisitazione di processi/controlli	Sostenibilità del modello di business Revisione priorità e progetti strategici
IT Risk			
Cyber Risk	Crescita minacce cyber (es. social engineering, malware/ phishing)	Aumento attacchi cyber (es. DDoS) Parziale consapevolezza di dipendenti e clienti	?
Third Party Risk	Potenziali problemi di continuità operativa per certi fornitori	Difficoltà a sostenere lavoro da remoto	Potenziale riduzione nel numero di outsourcer/fornitori

INTESA SANPAOLO

Interazione con il Supervisore

Nonostante l'apparente allentamento della pressione regolamentare legata alla proroga concessa su alcune scadenze istituzionali (es. EBA Stress Test), **l'interazione con il supervisore si è intensificata** e si è concretizzata in meeting settimanali con l'Unità di Emergenza, domande spot e richieste di report da produrre su base periodica funzionali a stimare l'impatto del Covid sia sui processi interni (es. incidenti) sia sui comportamenti dei clienti

JST REQUEST ON IT AND IT SECURITY: assurance sulle modifiche nei processi e nei controlli, modifiche all'infrastruttura IT/alle modalità di accesso ai sistemi, comunicazione con i dipendenti in lavoro da remoto, andamento delle frodi interne/esterne, andamento dei reclami

SSM COVID-19 REPORTING PACKAGE (Operational Continuity Template): effettiva «possibilità» di lavorare da remoto; funzionalità del sistema informativo (pagamenti)/degli ATM; % di apertura delle filiali; andamento dei reclami

Che cosa abbiamo capito?

BUSINESS CONTINUITY

- E’ impossibile prevenire qualunque tipo di rischio... Val la pena fare piani partendo dal presupposto che qualche rischio si verificherà
- E’ opportuno estendere il dominio delle soluzioni di continuità alla luce delle nuove possibilità offerte dalla tecnologia e della rinnovata fiducia nelle persone
- E’ imprescindibile investire ancora in «awareness» di clienti e dipendenti e rafforzare la «readiness» dei processi (anche comunicativi)

INTERAZIONE CON IL BUSINESS

- Nella funzione di Operational Risk Management è opportuno rafforzare skill e capability per interagire con il business...
- ... ed è necessario sviluppare strumenti (semplici, da utilizzare «a chiamata») a supporto dei processi decisionali del Top Management, così da dare piena attuazione alle scelte in logica «risk-driven»

Che cosa abbiamo capito?

PROCESSI DI OPERATIONAL RISK MANAGEMENT e ANALISI DEL PROFILO DI RISCHIO

- I tempi dei tradizionali processi di operational risk management (fortemente manuali) potrebbero essere incompatibili con le crescenti esigenze di tempestività nell'analisi e fruizione di dati e informazioni o nella identificazione e valutazione di nuovi rischi, soprattutto in situazioni non ordinarie
- E' opportuno investire di più sul consolidamento di tool e metodologie che si focalizzino sull'analisi dei rischi associati a modifiche apportate ai processi, ai sistemi e ai controlli

INTERAZIONE CON IL SUPERVISORE

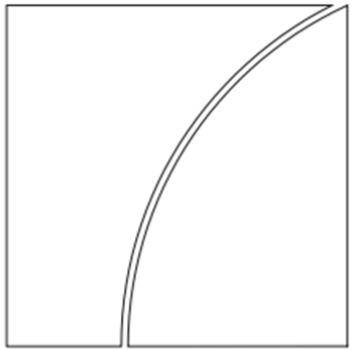
- Permane una forte focalizzazione sulla «financial resilience»...
- ... Ma si fa strada la consapevolezza che la «operational resilience» è una condizione necessaria (ma non sufficiente) per garantirla
- E' tempo di valorizzare il ruolo dell'Operational Risk Management come funzione di controllo di secondo livello

Che cosa abbiamo capito?

Basel Committee on Banking Supervision

Consultative Document

Principles for operational resilience



August 2020

Issued for comment by 6 November 2020

- Until recently, some of the most predominant operational risks that banks faced resulted from vulnerabilities related to the rapid adoption of and increased dependency on technology infrastructure for the provision of financial services and intermediation, as well as the sector's growing reliance on technology-based services provided by third parties. The Covid-19 pandemic has exacerbated these operational risks and increased economic and business uncertainty
- Further work is necessary to **strengthen banks' ability to absorb operational risk-related events**, which could cause significant operational failures or wide-scale disruptions in financial markets
- **Operational resilience is an outcome that benefits from the effective management of operational risk**

Conclusioni

- **La complessità del rischio operativo continua a crescere**, in ragione delle evoluzioni di contesto interno ed esterno e sotto la spinta della regolamentazione
- Il concetto di operational resilience sarà probabilmente uno dei cardini su cui fare la differenza e uno dei punti chiave dell'interazione con il Supervisore

- **E' necessario che i tradizionali processi di gestione del rischio operativo divengano meno generici e più dinamici**
- **Quattro le aree di evoluzione principali**
  i. ruolo di funzione di secondo livello
  ii. analisi e segnalazione dei rischi in tempo reale
  iii. aggiornamento degli skill nella funzione
  iv. crucialità dei rischi di change management e legati alle nuove tecnologie e rinnovata attenzione ai rischi connessi al fattore umano

INTESA SANPAOLO

Grazie!

DISCLAIMER!
Le opinioni espresse in questo documento sono esclusivamente dell'autore e non rappresentano necessariamente prassi o regole in essere nel Gruppo Intesa Sanpaolo

VERUSKA ORIO
Resp. Operational, Reputational & Cyber Risk
Intesa Sanpaolo
veruska.orio@intesasanpaolo.com