UNIONE BANCARIA E BASILEA 3 RISK & SUPERVISION 2016

IT, Model & Conduct Risk

Aree di sovrapposizione e possibili approcci metodologici

Roma, 21 Giugno 2016

UBI Banca

Agenda

Rischio Operativo

- **Principali componenti**
- **Principali aree di sovrapposizione** *(IT, Model & Conduct Risk)*
- **Possibili evoluzioni dei framework per la gestione del Rischio Operativo**

Principali componenti del Rischio Operativo

Rischio Operativo

È il rischio di perdite derivanti dalla inadeguatezza o dalla disfunzione di processi, risorse umane e sistemi interni, oppure da eventi esogeni, ivi compreso il rischio giuridico

Rischio Operativo

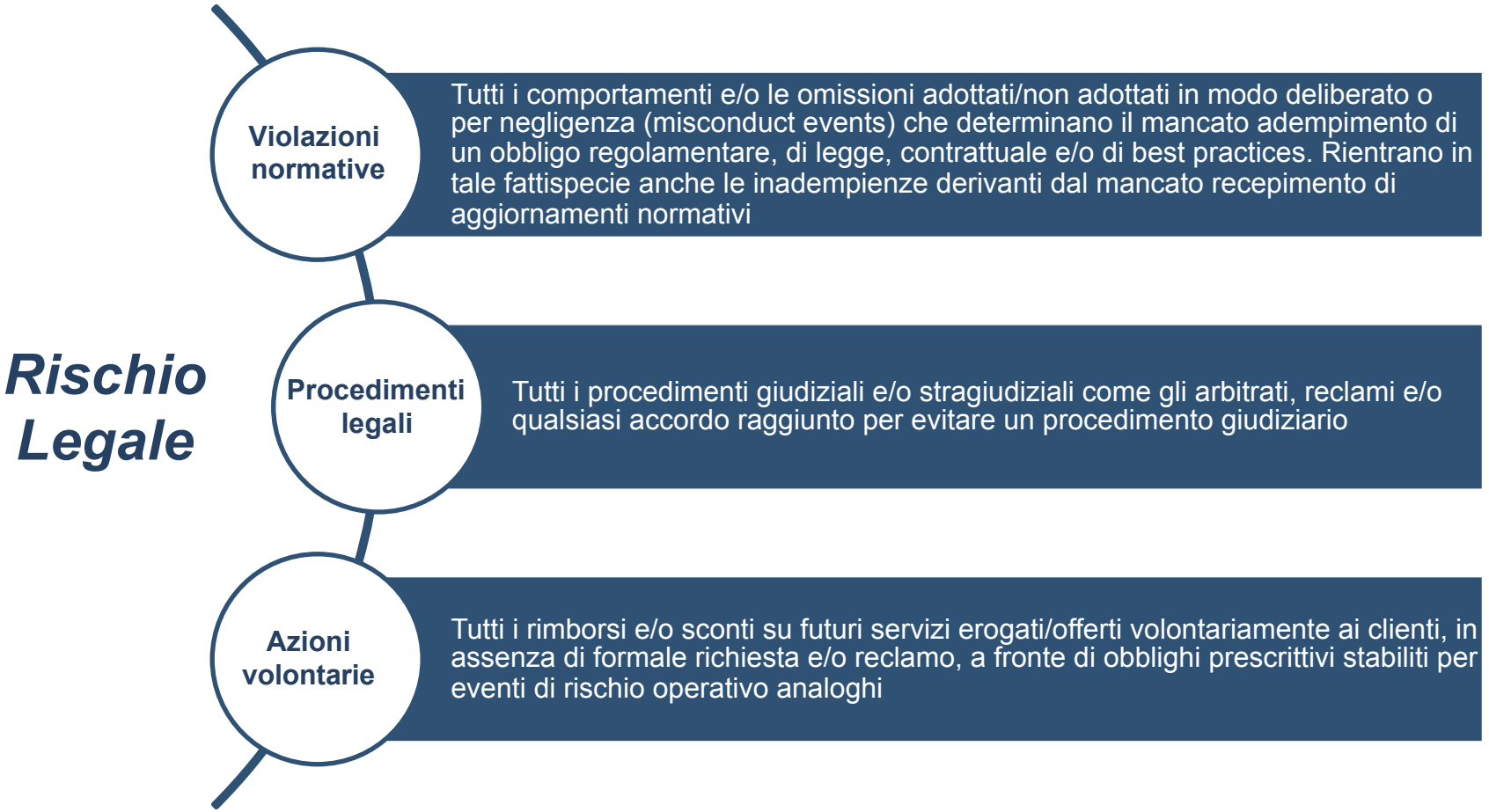
- **Rischio Legale**: Perdite e/o costi aggiuntivi causati da violazioni normative (Rischio di non conformità), procedimenti legali o azioni volontarie assunte per evitare il manifestarsi di un rischio legale (compresi quelli derivanti da misconduct events)
- **Rischio IT**: Perdite e/o costi aggiuntivi causati dall'inadeguatezza e/o malfunzionamenti dei sistemi IT
- **Rischio Modello**: Perdite e/o costi aggiuntivi causati dai modelli utilizzati nei processi decisionali
- **Rischio Credito**: Perdite e/o costi aggiuntivi causati da un rischio operativo in fase di collocamento di un prodotto creditizio e/o nell'ambito del processo del credito
- **Rischio Mercato**: Perdite e/o costi aggiuntivi causati da un rischio operativo nell'ambito delle transazioni finanziarie

UBI Banca

Principali componenti del Rischio Operativo

Rischio Legale

È il rischio di incorrere in perdite e/o sostenere costi aggiuntivi a causa di violazioni normative, procedimenti legali o azioni volontarie assunte per evitare il manifestarsi di un rischio legale



Principali componenti del Rischio Operativo

Rischio Legale

Tutti i comportamenti e/o le omissioni adottati/non adottati in modo deliberato o per negligenza che determinano l'insorgenza di un rischio legale sono definiti ***"Conduct Risk"***

Alcuni esempi

- Vendita fraudolenta di prodotti
- Cross-selling aggressivo di prodotti a clienti Retail
- Limitazione al cambiamento di prodotti finanziari durante la loro vita residua
- Inadeguatezza dei canali distributivi che potrebbe favorire l'insorgenza di conflitti d'interesse
- Rinnovo automatico di prodotti e/o introduzione di penali di uscita/recesso
- …

Possibile approccio metodologico

La quantificazione del *Conduct Risk* deve essere effettuata sulla base degli esiti delle attività di monitoraggio del rischio storico e potenziale

Alcuni esempi di Key Risk Indicator (KRI):

- Sanzioni per pratiche misconduct applicate dalle autorità
- Sanzioni per pratiche misconduct applicate a Istituzioni terze
- Numero di reclami contro e/o relativi impatti economici
- …

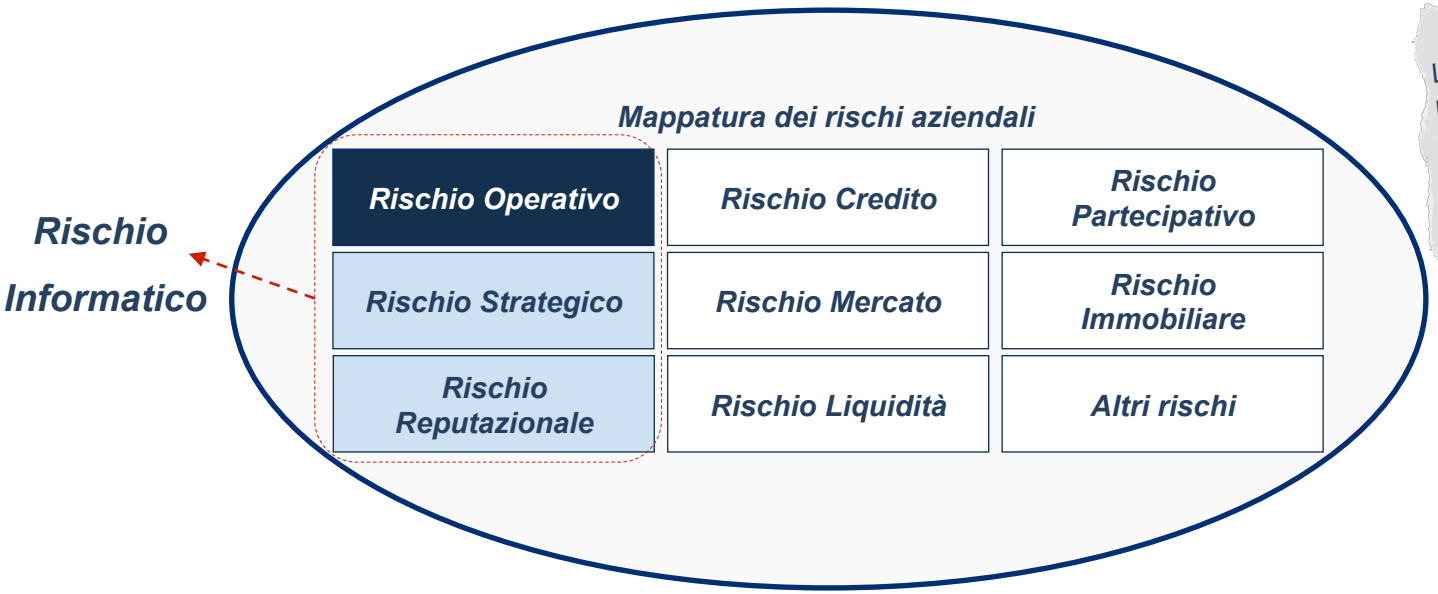
In linea con quanto definito nel documento EBA "Guidelines on common procedures and methodologies for the supervisory review and evaluation process (SREP)", un framework di Operational Risk Management efficace deve prevedere un sistema di KRI che consenta di identificare e valutare ex ante gli impatti derivanti dai possibili misconduct events

UBI Banca

Principali componenti del Rischio Operativo

Rischio IT

È il rischio di incorrere in perdite economiche, di reputazione e di quote di mercato in relazione all'utilizzo di tecnologia dell'informazione e della comunicazione



Le politiche di governo dei rischi IT, devono essere definite nel più ampio quadro di riferimento del Risk Appetite Framework (RAF)

Avere una gestione efficace dei rischi informatici significa individuare il grado di protezione che si intende predisporre per salvaguardare l'**integrità**, la **riservatezza** e la **disponibilità** dei dati in relazione ad un livello di rischio prefissato

Principali componenti del Rischio Operativo

Rischio IT

L'analisi del rischio informatico costituisce uno strumento a garanzia dell'efficacia e dell'efficienza delle misure di protezione delle risorse ICT e permette di graduare le misure di mitigazione nei vari ambienti in funzione del profilo di rischio predefinito

Obiettivi dell'analisi del rischio IT

Definizione di un indicatore di rischio per ciascuna Risorsa Informatica

Definizione di KRI che siano espressione di:

- probabilità di accadimento delle minacce
- danno economico conseguente al loro accadimento

Definizione di un sistema strutturato per il monitoraggio del profilo di rischio

Rilevazione sistematica dell'andamento dei KRI in modo da garantire:

- un continuo monitoraggio dell'andamento del profilo di rischio
- il rispetto del Risk Appetite Framework e delle Policy di Sicurezza
- l'identificazione di azioni di contenimento del rischio coerenti alle strategie di gestione dello stesso

Definizione di presidi di sicurezza in relazione al rischio

Definizione, per ciascuna risorsa informatica, di presidi di sicurezza differenziati in funzione di:

- livello di criticità
- tipologia di dati gestiti/custoditi
- grado di accessibilità

Oltre al monitoraggio degli indicatori di rischio sopra citati, devono essere previsti specifici controlli di secondo livello sugli ambiti Cyber Crime e IT Outsourcing

UBI Banca

Principali componenti del Rischio Operativo

Rischio Modello

È il rischio di incorrere in perdite e/o sostenere costi aggiuntivi a causa dei modelli utilizzati nei processi decisionali

Alcuni esempi

- Mancata e/o inadeguata verifica dell'idoneità dei modelli utilizzati per la valutazione degli strumenti finanziari e/o per il pricing dei prodotti
- Mancata e/o inadeguata verifica dell'adeguatezza dei modelli rispetto alle correnti condizioni di mercato
- Errate valutazioni mark-to-market e di misurazione del rischio a causa di errori effettuati nella registrazione delle operazioni nei sistemi di trading
- …

Possibile approccio metodologico

- La valutazione di tale tipologia di rischiosità rientra nel quadro più generale delle analisi effettuate in fase di progettazione di nuovi prodotti/servizi e/o modifica di quelli esistenti
- Lo scopo è quello di identificare eventuali rischi operativi in modo da definire opportune garanzie contrattuali e/o interventi di mitigazione

Sono escluse le perdite sostenute a causa di sottovalutazioni dei requisiti patrimoniali calcolati utilizzando modelli interni sottoposti all'approvazione delle Autorità di Vigilanza

Un framework di Operational Risk Management efficace deve prevedere un sistema di valutazione dei rischi operativi potenziali capace di prevenire e/o mitigare l'accadimento di eventi che potrebbero compromettere il raggiungimento degli obiettivi aziendali

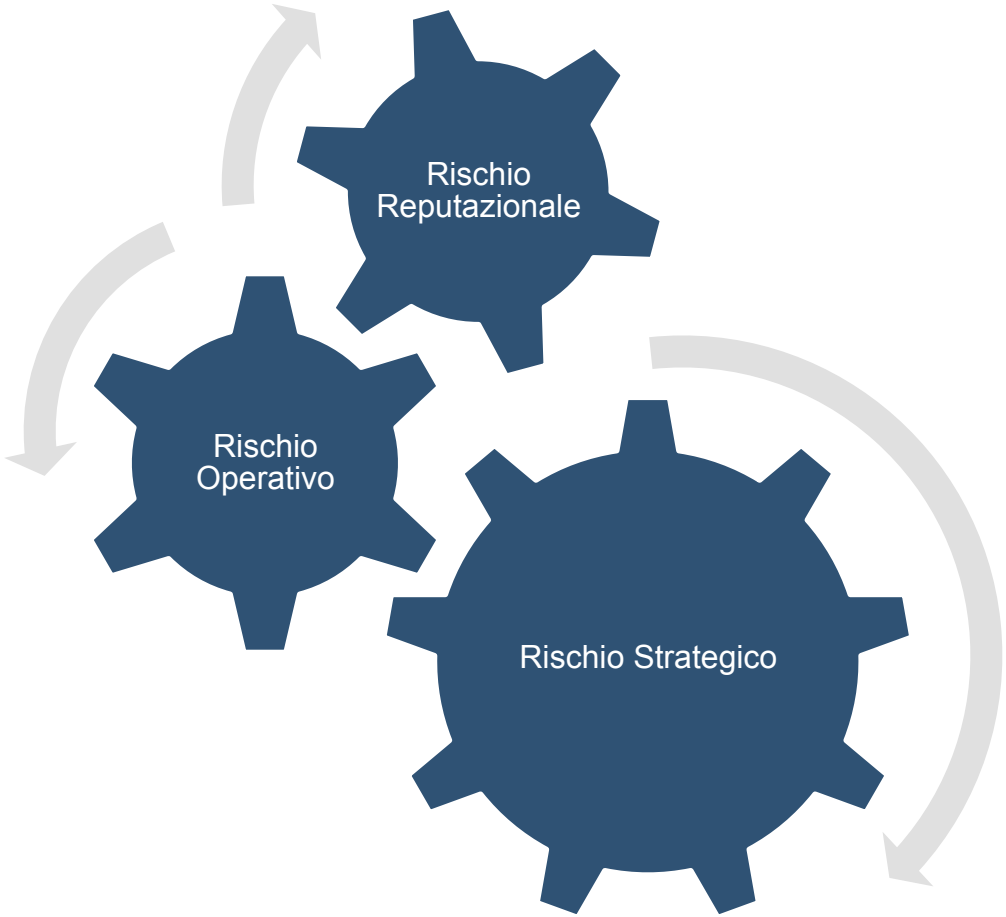
UBI Banca

Principali componenti del Rischio Operativo

Rischio Operativo e correlazioni

Sono esclusi dalla definizione di Rischio Operativo il rischio Reputazionale e quello Strategico

Considerate le forti correlazioni esistenti tra tali forme di rischiosità, un Framework di Operational Risk Management efficace non può prescindere dall'analisi di tali rischi



Principali componenti del Rischio Operativo

Rischio Strategico

È il rischio di errata/inadeguata definizione degli obiettivi aziendali, delle strategie con cui si vogliono perseguire e/o di intempestivi adeguamenti dei processi decisionali alle evoluzioni del contesto operativo

Fattori chiave	Gestione efficace dei fattori chiave
Chiarezza di obiettivi, ruoli e responsabilità	• Gli obiettivi strategici aziendali devono essere chiaramente comunicati a ciascun dipendente • Ciascun dipendente deve conoscere in modo chiaro quale sarà il suo contributo per il raggiungimento degli obiettivi
Efficiente allocazione delle risorse	• Consapevolezza dei fattori chiave che consentono la massimizzazione delle performance • Implementazione di indicatori che consentano di avere un monitoraggio continuo delle performance • Processi organizzativi che prevedano la riallocazione delle risorse nei casi di scostamento dai risultati attesi
Gestione di fattori inattesi	• Monitoraggio dell'evoluzione del contesto operativo (nuove tecnologie IT, aggiornamenti normativi, ecc.) e dei mercati di riferimento (nuovi canali distributivi, evoluzione dei bisogni della clientela, ecc.) • Sviluppare capacità di reagire in modo da rispondere con rapidità ai cambiamenti esterni e/o eventi critici

Se non gestito correttamente, il Rischio Strategico potrebbe rappresentare la principale fonte di Rischio Operativo

Un framework di Operational Risk Management efficace deve prevedere un sistema di KRI che consenta l'identificazione ex-ante di eventuali fattori di criticità che potrebbero compromettere il raggiungimento degli obiettivi aziendali prefissati

UBI Banca

Principali componenti del Rischio Operativo

Rischio Reputazionale

È il rischio di flessione degli utili o del capitale derivante da una percezione negativa dell'immagine della banca da parte di clienti, controparti, azionisti della banca, investitori o Autorità di Vigilanza

Valutazione del grado di esposizione

La valutazione del grado di esposizione molto spesso è effettuata tramite il monitoraggio di una serie di indicatori differenziati per ciascun ambito di attività

Gestione e pianificazione delle risorse patrimoniali

- andamento dei coefficienti di solvibilità (Core Tier 1, Tier 1 e Total Capital)
- andamento della leva finanziaria
- …

Comportamento del personale dipendente

- Andamento del numero provvedimenti disciplinari verso i dipendenti
- andamento del numero di licenziamenti per giusta causa o giustificato motivo
- …

Altri indicatori quantitativi

- andamento del numero di reclami ricevuti
- Andamento dell'indice di customer satisfaction
- …

In conseguenza di un Rischio Operativo c'è sempre un Rischio Reputazionale

Un framework di Operational Risk Management efficace deve prevedere un sistema di KRI strettamente correlato con gli indicatori monitorati nell'ambito dei Rischi Reputazionali

UBI Banca

Principali aree di sovrapposizione *(IT, Model & Conduct Risk)*

Di seguito si riporta un possibile approccio metodologico per l'individuazione delle aree di sovrapposizione dei Rischi informatici, di modello e dei «miscoduct events»

Possibili evoluzioni dei framework per la gestione del Rischio Operativo

In considerazione delle evoluzioni normative in corso, tenendo conto delle considerazioni espresse nelle slide precedenti, è possibile prevedere che gli attuali framework metodologici possano evolvere secondo le seguenti direttrici

- **Potenziamento dei sistemi di identificazione e valutazione ex ante dei rischi potenziali basati su KRI sempre più strutturati**
- **Utilizzo delle analisi ex ante dei rischi potenziali per finalità gestionali e per la valutazione del rischio a fini di Pillar II e SREP**
- **Superamento delle tecniche di misurazione del capitale regolamentare per i rischi operativi basati su modelli interni di tipo stocastici**

Grazie

Domenico Pepe

@ domenico.pepe@ubibanca.it

+39 340 650 77 93

UBI Banca