

Laurea Triennale
in
Economia and Management

**La quantificazione dei rischi operativi in banche e
assicurazioni**

Relatore

Prof. Salvatore Forte

Candidato

Davide Emanuele
Ianniello

Anno Accademico 2024/2025

Indice

| | |
|---|-----------|
| I.Introduzione | 3 |
| II.Rischi Operativi | 5 |
| Definizione di Rischio Operativo | 5 |
| Cosa caratterizza il Rischio Operativo e quante tipologie si hanno | 10 |
| Perché è importante la gestione dei rischi operativi nelle banche e nelle compagnie assicurative | 16 |
| III.Metodi di Quantificazione dei Rischi Operativi | 20 |
| Basic Indicator Approach | 25 |
| Standardised Approach: Applicazione Pratica | 26 |
| Advanced Measurement Approach | 32 |
| Analisi di Scenario e Stress Testing | 42 |
| IV.Limiti e Criticità nel quantificare i Rischi Operativi | 44 |
| Limiti e criticità dei modelli che vengono utilizzati | 44 |
| Fattori che possono influenzare la precisione nelle stime | 50 |
| V.Strategie di Gestione e Mitigazione del Rischio Operativo | 56 |
| Gestione Proattiva | 56 |
| Controlli Interni nella Gestione del Rischio e il Ruolo della Compliance | 65 |
| Il Fallimento della Barings Bank: Un caso esemplare di Rischio Operativo | 69 |
| VI.Quadro Normativo | 75 |
| Sfondo Normativo e regolamentare di riferimento per la gestione dei rischi operativi in banche e assicurazioni. | 75 |
| Conclusioni | 82 |
| Riferimenti Bibliografici | 84 |

I. Introduzione

Nel panorama sempre più complesso e dinamico del settore finanziario, la gestione dei rischi operativi rappresenta una sfida cruciale per banche e assicurazioni. L'evoluzione delle normative, l'incremento delle minacce cyber e l'aumento delle aspettative da parte degli stakeholder rendono indispensabile un approccio rigoroso e sistematico alla quantificazione e alla gestione di tali rischi. La capacità di identificare, misurare e mitigare efficacemente i rischi operativi non solo preserva la stabilità e l'integrità delle istituzioni finanziarie, ma contribuisce anche a mantenere la fiducia del mercato e la solidità del sistema economico globale.

Questa tesi si propone di esplorare in modo approfondito il tema della quantificazione dei rischi operativi in banche e assicurazioni, offrendo una panoramica dettagliata delle diverse tipologie di rischio, dei metodi di quantificazione utilizzati, delle criticità associate a tali metodi e delle strategie di gestione e mitigazione. Il lavoro si articola in cinque capitoli, ciascuno dei quali affronta un aspetto specifico del problema.

Nel primo capitolo, **Rischi operativi**, verrà offerta una classificazione esaustiva delle diverse forme di rischio operativo. Verranno analizzate le principali categorie, come il rischio di frode interna ed esterna, il rischio di fallimento dei sistemi e dei processi, e il rischio legale e di conformità, ponendo l'accento sulle peculiarità che caratterizzano ciascun tipo di rischio.

Il secondo capitolo, **Metodi di quantificazione dei rischi operativi**, esaminerà i principali approcci metodologici impiegati nel settore finanziario. Saranno analizzati il Basic Indicator Approach, lo Standardised Approach, l'Advanced Measurement Approach e lo stress testing. Ogni metodo verrà descritto nei suoi dettagli tecnici e confrontato in termini di efficacia, complessità e applicabilità pratica.

Nel terzo capitolo, **Limiti e criticità nel quantificare i rischi operativi**, si discuteranno le principali difficoltà e i limiti inerenti alla quantificazione dei rischi operativi. Verranno esaminati i problemi legati alla disponibilità e qualità dei dati, alla modellizzazione del rischio e all'incertezza intrinseca dei modelli. Questo capitolo metterà in evidenza come tali criticità possano influenzare la precisione e l'affidabilità delle stime del rischio.

Il quarto capitolo, **Strategie di gestione e mitigazione del rischio operativo con il ruolo della compliance**, esplorerà le diverse strategie e pratiche per la gestione e la mitigazione dei rischi operativi. Particolare attenzione sarà dedicata al ruolo della funzione di compliance e verrà presentato un caso studio sulla crisi della Barings Bank, un esempio emblematico di fallimento della gestione del rischio operativo.

Infine, il quinto capitolo, **Quadro normativo di riferimento per la gestione dei rischi operativi in banche e assicurazioni**, fornirà una panoramica delle principali normative e regolamentazioni che disciplinano la gestione dei rischi operativi nel settore finanziario. Verranno analizzate le direttive internazionali, come Basilea III, e le normative specifiche per il settore assicurativo, evidenziando le implicazioni per le istituzioni finanziarie.

Questo lavoro mira a fornire una comprensione approfondita e articolata della quantificazione dei rischi operativi, un tema di fondamentale importanza per garantire la resilienza e la sostenibilità delle banche e delle assicurazioni in un contesto economico sempre più sfidante.

II. Rischi Operativi

Definizione di Rischio Operativo

“You cannot swim for new horizons until you have courage to lose sight of the shore.”¹

Negli attuali contesti ambientali sempre più dinamici, le varie aziende si trovano a doversi rapportare ad una molteplicità di rischi che gravano sui processi decisionali, il tutto per poter salvaguardare la propria operatività. Data l'incertezza del mondo finanziario, abbiamo potuto notare nel corso del tempo come sia cresciuta la domanda di risk management da parte degli stakeholder, ragion per cui il tema del risk management sta riscontrando sempre un interesse maggiore.

L'evoluzione a cui assistiamo prevede anche l'introduzione di metodologie e tecniche per poter individuare e valutare i rischi in modo da poterli mitigare. Il Codice di Autodisciplina della Borsa Italiana² ha sottolineato l'importanza del sistema dei controlli interni evidenziando il ruolo con il processo proprio di identificazione e gestione dei rischi. Con l'edizione risalente al 2011, il Codice prevede che le società quotate debbano dotarsi di un sistema di gestione dei rischi.

Possiamo, anzi è doveroso, citare in questo contesto l'importanza dell'art.2428 c.c. in materia di Relazione sulla Gestione, in quanto prevede che tra le tante informazioni che deve contenere, la relazione sulla gestione deve fornire “...una descrizione dei principali rischi ed incertezze a cui la società è esposta...”.³

Ma per rischio cosa intendiamo?

In finanza, il rischio si riferisce al grado di incertezza e alla potenziale perdita finanziaria inerente ad una determinata decisione di investimento. Con l'aumento dei rischi di investimento, gli investitori cercano rendimenti molto più elevati per poter sentirsi “ricompensati” per l'assunzione di tali rischi. L'accezione di rischio in finanza si può riscontrare anche negli studi sulla valutazione d'azienda e creazione del valore, in quanto il concetto di rischio lo vediamo associato alla variabilità dei flussi economici e finanziari che si considerano in un'ottica valutativa.

Secondo una prospettiva economico-aziendale si tende a ritenere il rischio come la possibilità di danno economico legato ad un dato evento futuro di

¹ William Faulkner.

² Il Codice di Autodisciplina delle società quotate è stato redatto nel 1999 e rivisitato nel 2003; contiene raccomandazioni che costituiscono un modello di “best practice” per il buon funzionamento delle società quotate.

³ Si nota che tutte le società di capitali sono tenute a predisporre la relazione sulla gestione in base a quanto ordina l'art.2428 c.c., indipendentemente dal fatto che redigano il bilancio in conformità ai principi contabili internazionali (IAS/IFRS).

manifestazione incerta che può comportare una variazione positiva o negativa rispetto a quanto prestabilito.

Nel concetto di rischio non tendiamo a considerare, invece, quegli eventi che non hanno il carattere di incertezza che invece contraddistingue l'evento rischioso.

Proseguendo il nostro discorso in merito, possiamo asserire che il rischio prevede la compresenza di due componenti: il manifestarsi aleatorio degli eventi e l'incapacità dell'uomo di poter prevedere i mutamenti. Queste componenti sono strettamente interconnesse: la capacità di poter prevedere dei mutamenti è strettamente connessa alle caratteristiche dei processi di cambiamento, che sia relativo alla frequenza con cui si manifestano i cambiamenti o relativo al numero delle variabili che si prendono in considerazione.

Il rischio è **dinamico**: tende a modificarsi nel corso del tempo a causa di fattori esterni ed interni che concorrono nella determinazione di nuovi rischi o il termine di altri. Con lo scorrere del tempo, dunque, il livello di esposizione di un'azienda rispetto ad un singolo fattore di rischio e rispetto a quello che nel complesso grava su di essa, è destinato a mutare.

Un altro tratto caratterizzante del rischio è la sua **sistematicità**: all'interno della realtà aziendale ci possono essere molte realtà esposte al rischio e la caratteristica della sistematicità sta nel fatto che tra le varie realtà vi sono dei legami che intrecciano i rischi specifici in un complesso unitario. I rischi specifici come rischio di credito e rischio di liquidità nell'insieme concorrono a determinare il rischio complessivo, con la differenza che i rischi specifici possono essere eliminati, mentre il rischio complessivo non è eliminabile, quanto più può essere ridotto.

La gestione del rischio possiamo definirla in prima battuta come quel processo attraverso il quale si misura o si stima il rischio e successivamente si sviluppano delle iniziative e strategie per poterlo gestire entro i limiti. Della gestione del rischio se ne occupano le imprese di grandi dimensioni così come anche le piccole imprese.

Nelle aziende di piccole dimensioni l'attività di risk management si sviluppa secondo modelli non formalizzati; assistiamo all'imprenditore che direttamente è coinvolto nella gestione dei rischi. E' con il crescere delle dimensioni che il risk management si articola e si sviluppa per delega e per vari livelli organizzativi. Di solito al vertice l'attenzione si concentra su rischi che riguardano il profilo strategico dell'azienda, a livello di funzione si focalizzano su quei fattori di rischio che potrebbero impattare sulle attività che rientrano nell'area funzionale e ai livelli esecutivi si lavora sui rischi legati allo svolgimento di attività e operazioni elementari. Nonostante questa suddivisione, però, si deve sempre mantenere una visione globale e non bisogna vedere il risk management come un processo divisionale. Ricordiamo che anche avendo diversi livelli operativi, ci possono essere fattori di rischio che possono avere un impatto negativo sulla reputazione, sulla sopravvivenza dell'azienda.

All'interno del sistema di risk management possiamo individuare tre elementi distintivi e caratteristici:

- **Attori:** sono i soggetti che nei vari livelli sono impegnati nelle varie attività di identificazione, di valutazione e trattamento dei rischi;
- **Processo:** si articola in tre tipiche fasi. La fase di identificazione vuole identificare i rischi che possono impattare negativamente sull'economicità della gestione; la fase di valutazione vuole attribuire un giudizio al rischio, un certo livello di probabilità di accadimento e l'intensità dell'impatto data la sua manifestazione; la fase di trattamento, l'ultima, consiste nell'individuare il piano e le azioni da dover adottare per contenere e ridurre il rischio;
- **Tecniche e Strumenti:** vengono utilizzati dagli attori per uno svolgimento efficace del processo e sono tutti quegli elementi che supportano gli attori nelle varie fasi del processo come workshop, modelli probabilistici e contratti derivati.

Aspetto importante da toccare è in primo luogo la classificazione delle varie tipologie di rischio. Esistono una molteplicità di tipologie di rischio ed è importante farne una rassegna di quelli più rilevanti in ambito finanziario per poi soffermarci su uno in particolare. La profondità del concetto di rischio e quanto sia intrinseco e necessario, non solo per i mercati e per i soggetti che li caratterizzano ma in generale per l'intero assetto finanziario, deve farci comprendere quanto sia vitale una giusta comprensione e un giusto approccio al concetto di rischio per potersi coprire in casi spiacevoli. Secondo gli studiosi McNeil, Frey ed Embrechts⁴ possiamo distinguere i seguenti rischi:

- **Rischio di mercato:** consiste nella variazione di valore di una posizione finanziaria o di un portafoglio a causa di un cambiamento di variabili importanti del mercato da cui i sottostanti del portafoglio dipendono. Esempi di queste variabili importanti possono essere i prezzi delle obbligazioni, materie prime, tassi di cambio⁵. Per coprirsi da questi rischi è solito ricorrere agli strumenti finanziari derivati che ci permettono di neutralizzare le fluttuazioni del mercato. Il rischio di mercato si articola in tre tipologie di rischio: rischio di cambio, rischio di tasso di interesse e rischio di prezzo.
- **Rischio operativo:** viene definito come il rischio di subire delle perdite a causa di procedure inadeguate interne, errori commessi dal personale. Questa è una definizione "positiva" utilizzata anche dalla *Solvency II*

⁴ Cfr. McNeil, Frey & Embrechts, *Quantitative Risk Management*, Princeton, Princeton University Press (2015).

⁵ Cfr. <https://www.borsaitaliana.it/borsa/glossario/rischio-di-mercato.html>.

Framework e che risulta molto diversa da quella “negativa” che ritroviamo negli accordi di Basilea I. Negli accordi di Basilea I il rischio operativo veniva visto come qualsiasi rischio non classificabile come rischio di mercato o di credito.

- **Model Risk:** si intende la perdita potenziale a cui può andare incontro una società conseguentemente a decisioni prese da output prodotti tramite modelli interni, a causa di errori di sviluppo o di utilizzo di tali modelli.
- **Rischio di Liquidità:** si intende come il rischio che un’entità non riesca a far fronte ai propri impegni di pagamento quando giungono a scadenza. Di base una società è in grado di fronteggiare le proprie uscite di cassa in disparati modi. Un esempio, mediante i flussi di cassa in entrata, le attività prontamente liquidabili oppure la capacità di ottenere credito, anche se le attività prontamente liquidabili potrebbero avere problemi non legati esclusivamente alla società; problemi non legati alla società si possono avere quando magari sui mercati si registrano delle tensioni che ne rendono difficoltosa la vendita e in questa circostanza il rischio di liquidità è legato alle condizioni di liquidità del mercato.
- **Underwriting risk:** importante in ambito assicurativo. Può imbattersi in questo rischio il sottoscrittore in merito ad un eventuale perdita a causa di un’insufficienza dei premi a coprire sia i sinistri che le spese.
- **Rischio di credito:** è il rischio che il creditore non sia in grado di onorare le proprie obbligazioni.

Con la crescita delle attività bancarie che va a pesarsi distintamente in rapporto alla specializzazione di ognuna, le Istituzioni hanno indirizzato la loro concentrazione non solo esclusivamente sui noti rischi di credito e di mercato, ma su una “nuova” tipologia di rischio, il rischio operativo.

Prima di entrare nel dettaglio circa questo rischio occorre definire i fattori che hanno dato maggiore consapevolezza dell’esistenza di questo rischio intrinseco oramai:

- **L’aumento dimensionale delle banche**, che iniziava a contare ampliamenti sia organizzativi che di business offerti ai propri clienti;
- **Operazioni di fusione e acquisizione tra banche**, che inglobano anche fusioni tra sistemi operativi e informativi differenti, e questo aumenta la probabilità di disfunzioni;
- **Investimenti tecnologici bancari;**
- **Sviluppo di canali informatici ed elettronici**, come *e-banking* che non ha fatto altro che incrementare il rischio di frodi esterne e di criminalità.

Il processo di individuazione di una definizione contemplata e condivisa del rischio operativo non è stato semplice, consci del fatto che da una prima riesamina veniva considerato come un semplice rischio residuale rispetto ai

classici rischi di credito e di mercato. La stessa Banca d'Italia includeva i rischi operativi all'interno della categoria "altri rischi", così come l'Associazione Bancaria Italiana sosteneva che il rischio operativo era tutto ciò che non poteva essere definito come rischio di credito e di mercato. Sarà solamente con gli Accordi di Basilea II che avremo una definizione acclamata e riconosciuta:

"Il rischio di subire perdite derivanti dall'inadeguatezza o dalla disfunzione di procedure, risorse umane e sistemi interni, oppure da eventi esogeni. Nel rischio operativo è compreso il rischio legale⁶, mentre non sono inclusi quelli strategici⁷ e di reputazione⁸".⁹

ART.101 Direttiva 2009/139/CE

Da come possiamo evincere leggendo la circolare n.263, il tratto distintivo e caratterizzante dei rischi operativi è che, salvo strategie di mitigazione, non possono essere evitati, si distinguono dagli altri rischi a cui possono essere esposte banche e assicurazioni per il fatto che non sono conseguenza di operazioni rischiose che puntano ad un ottenimento di profitto maggiore, ma derivano dalla normale e quotidiana gestione operativa.

Il rischio operativo viene incluso in quelli che sono i **rischi puri**¹⁰, cioè quei rischi che possono generare esclusivamente risultati negativi.

Un'altra classificazione relativa al rischio operativo riguarda anche il suo collocamento nella categoria di **rischi assicurabili**: prima di Basilea II, veniva gestito prettamente tramite politiche di accantonamento, quindi relegandolo all'intermediario, o tramite il ricorso alle assicurazioni effettuando dei trasferimenti in capo a terzi.

Un ultimo elemento distintivo è il non diretto legame tra l'esposizione al rischio operativo, la dimensione dell'intermediario e il volume delle operazioni: non accade frequentemente che le banche di maggiori dimensioni presentino esposizioni maggiori rispetto a quelle di minori dimensioni, per cui si tiene conto molto anche delle caratteristiche qualitative.

⁶ "Il rischio legale include varie fattispecie di violazioni di norme, comportamenti illeciti, ricorso a schemi negoziali non conformi agli ordinamenti che possono causare perdite patrimoniali per l'intermediario" (Banca d'Italia).

⁷ Il rischio strategico è legato a tutti gli eventi che potrebbero minare la posizione competitiva dell'azienda nel mercato in cui si trova, minacciando il conseguimento degli obiettivi stabiliti.

⁸ "Il rischio reputazionale è il rischio attuale o prospettico di flessione degli utili o del capitale derivante da una percezione negativa dell'immagine dell'azienda da parte di clienti, controparti, azionisti, investitori o autorità di vigilanza" (Banca d'Italia).

⁹ Il motivo per il quale si escludono il rischio strategico e il rischio reputazionale è dovuto dalla necessità di gestione e monitoraggio solamente sui rischi i cui modelli di misurazione risultavano più robusti. (V. Rao, A. Dev, *Operational Risk: Some Issues in Basel II AMA Implementation in US Financial Institution*, in E. Davis, "The Advanced Measurement Approach to operational Risk", Risk Books, London, 2006).

¹⁰ Per un più chiaro approfondimento sulla differenza tra rischi speculativi e rischi puri, cfr. William Arthur C., "Attitudes toward Speculative Risks as an Indicator of Attitudes toward Pure Risks", The Journal of Risk and Insurance, 1966.

Cosa caratterizza il Rischio Operativo e quante tipologie si hanno

Per poter delinearare le attività di gestione dei rischi operativi è di primaria importanza che tutte le informazioni che caratterizzano un rischio operativo siano adeguatamente strutturate e ben classificate; il framework di partenza si basa su una catena dalla seguente struttura.



Specificando questa tripartizione:

- **Causa/e:** si fa riferimento al complesso di circostanze che portano al verificarsi dell'evento di rischio;
- **Evento:** è il registrarsi dell'accadimento congiuntamente allo scostamento tra l'esito atteso dal risultato effettivo. Lo scostamento che si registra può essere dovuto ad un'inadeguatezza, alle risorse umane, o circostanze di origine esterna;
- **Effetto/i:** s'intende l'impatto che l'evento ha sull'organizzazione. Possiamo distinguere due tipologie di effetti:
 - **Effetto diretto:** quello che ha un impatto diretto sul Conto Economico;
 - **Effetto indiretto:** può essere di natura finanziaria o non finanziaria, e non impatta direttamente sul Conto Economico.

Gli aspetti che caratterizzano qualsiasi evento di perdita sono:

- **Risk Factor:** la categoria delle cause che portano al registrarsi dell'evento dannoso;
- **Event Type:** la categoria degli eventi associati all'evento rischioso;
- **Loss Effect:** la categoria degli effetti a cui l'evento è associato.

Per quanto concerne i risk factor occorre precisare che il rischio operativo si registra per quattro cause differenti:

- **People:** il rischio operativo può aversi a causa delle risorse umane a causa di dipendenti carenti o una mancanza letterale di questi ultimi. Sono casi in cui il personale non ha le conoscenze adeguate per far fronte ad una situazione, o differentemente non si ha una quantità adeguata di dipendenti in certi periodi particolari e delicati. Gestire questo fattore di rischio significa lavorare sul fattore umano come formazione del personale, garantire un'alta fidelizzazione dei dipendenti.
- **Processes:** si lega a difficoltà conseguenti ad una non corretta determinazione delle procedure interne, ad un sistema di controlli interni inefficiente.¹¹
- **Systems:** è connesso ai problemi che si possono avere relativamente ai sistemi informativi e tecnologici. Le aziende si affidano sempre più a software per gestire la loro attività e spesso questi possono essere obsoleti, inadeguati, o includiamo anche la possibilità che i sistemi non siano competitivi come quelli di un competitore.
- **External Events:** in molti casi il rischio operativo lo possiamo ricondurre all'esterno dell'azienda. Le cause possono essere le più disparate, dai disastri naturali come terremoti, incendi, o situazioni politiche e militari.

Con Basilea II si registra anche una classificazione delle varie tipologie di eventi che possono generare delle perdite operative. Seguentemente alla classificazione delle cause è evidente il necessario seguito della classificazione delle sette classi di Event Types:

¹¹ A questo fattore di rischio abbiamo una radicalizzazione di altri quattro rischi:

- **Model Risk:** è il rischio di errore dovuto a inadeguatezze nei modelli di misurazione e di valutazione del rischio. Un'attenzione insufficiente al Model Risk può portare a perdite finanziari notevoli;
- **Transaction Risk:** è il rischio di errore dovuto a errori di contabilizzazione, registrazione e documentazione delle transazioni;
- **Security Risk:** è il rischio legato a violazioni della sicurezza informatica a causa di sistemi di controlli interni carenti o non sicuri;
- **Settlement Risk:** è un tipo di rischio di controparte legato anche al Default Risk, nonché alle differenze temporali tra le parti. E' la possibilità che una o più parti non riesca a consegnare secondo i termini di un contratto nel tempo concordato. E' chiamato anche rischio di consegna o "Herstatt Risk".



- **Internal Fraud:** gli atti di frode che sono commessi internamente in un'organizzazione e che vanno a ledere il suo interesse. Le perdite possono essere un effetto collaterale dell'intenzione di commettere atti di frode, dall'appropriazione indebita di beni, da una qualsiasi azione di falsificazione, dalle tangenti.¹²
- **External Fraud:** le frodi esterne sono invece delle attività commesse da terzi. Esempi di pratiche frequenti di frode esterna possono essere: furto, frode di assegni e violazione della sicurezza del sistema mediante hacking¹³ o reperimento di informazioni riservate.¹⁴
- **Employment practices & work-place safety:** le aziende di ogni dimensione e forma devono seguire le leggi conformi. Ci sono alcuni settori che hanno norme specifiche circa la sicurezza sul posto di lavoro, sebbene la maggior parte delle aziende debba aderire come minimo a: Leggi di base sulla sicurezza¹⁵, politiche di assunzione eque e non discriminatorie, Regole di compensazione come il salario minimo. Creare situazioni di conflitto con questi regolamenti espone l'azienda a dei rischi sia operativi che finanziari.
- **Clients, products & business practice:** spesso può capitare che non si riesca a mantenere le promesse fatte a causa di circostanze non intenzionali derivanti da pratiche negligenti. Le violazioni della privacy, l'uso errato di informazioni riservate, la manipolazione del mercato sono pratiche molto comuni che portano le aziende ad affrontare cause legali.

¹² L'Association of Certified Fraud Examiners ha stimato che le frodi interne sono costate alle aziende 3,6 miliardi di dollari nel 2022. Notiamo che questo totale rappresenta solamente i casi noti.

¹³ Molte aziende stanno creando data lake nel cloud per ridurre al minimo le interruzioni dovute all'esilio di dati. I Data Lake si possono descrivere come un luogo destinato all'archiviazione, analisi e correlazione di dati strutturati e non strutturati (da quelli relativi al CRM ai post delle pagine social). Il tratto distintivo è di poter consentire il recupero e l'organizzazione dei dati in rapporto al tipo di analisi che si vuole andare a fare.

¹⁴ IBM stima che il costo medio di una violazione dei dati sia di 4,45 milioni di dollari.

¹⁵ Come i regolamenti OSHA.

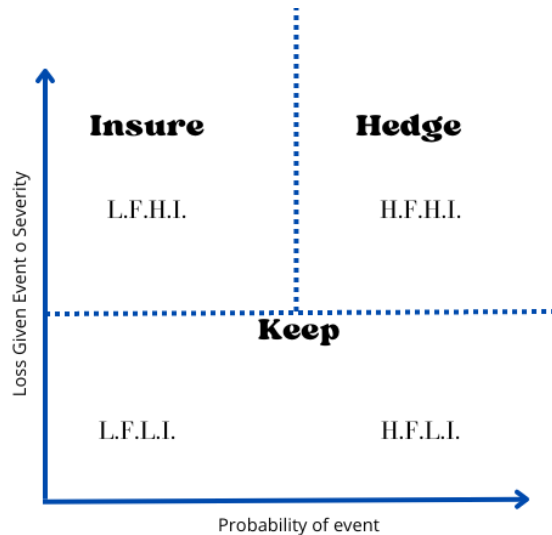
- **Damage to physical assets:** si subiscono perdite a causa disastri naturali o altri eventi come atti di terrorismo e vandalismo.
- **Business disruption and systems failures:** sono perdite legate all'interruzione della continuità aziendale, a guasti del sistema, interruzione delle telecomunicazioni.
- **Execution, delivery & process management:** il fallimento nella gestione della consegna delle transazioni o dei processi è un rischio operative che può portare perdite.

Avendo approfondito la molteplicità di Event Types che si possono categorizzare, a posteriori è possibile individuare 4 macrogeneri di eventi:

1. **L.F.L.I. (*Low Frequency and Low Impact Events*):** sono quegli eventi con una bassa probabilità di accadimento e basso impatto;
2. **H.F.L.I. (*High Frequency and Low Impact Events*):** sono quegli eventi con alta probabilità di accadimento e con basso impatto;
3. **L.F.H.I. (*Low Frequency and High Impact Events*):** sono quegli eventi con bassa probabilità di accadimento e alto impatto;
4. **H.F.H.I. (*High Frequency and High Impact Events*):** sono quegli eventi con alta probabilità di accadimento e alto impatto.

Per ciascuno di questi eventi vi sono modalità di gestione differenti:

- I. **Keep (*nel caso di Low Frequency and Low Impact e di High Frequency and Low Impact*):** la banca potrà essere in grado di decidere di mantenere questa tipologia di esposizione andando ad evitare i costi di un trasferimento o legati alla copertura di quest'ultima. Si andrà a coprire l'*expected loss* con delle riserve opportune, mentre l'*unexpected loss* attingendo dal capitale disponibile della banca.
- II. **Insure (*nel caso di Low Frequency and High Impact*):** per questa tipologia di evento si predilige ricorrere ai contratti assicurativi. Ricorrendo a quest'ultimo la banca, con un pagamento di un premio, effettua un trasferimento ad una società specializzata (specificamente una compagnia di assicurazione), gli impatti finanziari ed economici data l'insorgenza del rischio operativo. Il compito della compagnia sarà quello di rivalere l'assicurato del danno nei limiti della polizza.
- III. **Hedge (*nel caso di High Frequency and High Impact*):** in questo caso siamo davanti a dei rischi che non conciliano con la capacità di assorbimento delle perdite della banca, per cui la strategia di hedging prevede politiche di riduzione del rischio con investimenti tecnologici e nel fattore umano.



Dunque, è possibile generalizzare le perdite operative in due sezioni:¹⁶

- I. *Predictable Loss*: sono categorizzabili come perdite ad alta frequenza e a basso impatto. Sono le perdite che la banca non può evitare data la loro presenza nella quotidiana attività aziendale.
- II. *Not Predictable Loss*: sono invece le perdite a bassa frequenza ma ad alto impatto, di natura patologica e con effetti collaterali economici rilevanti e in grado di mettere a rischio quella che è la sana continuità aziendale. Sono queste perdite oggetto di hedging e di trasferimento di rischi operativi.

Un'ultima attribuzione è relativa alle Business Line: l'autorità regolamentale ha elencato otto linee di business nelle quali si possono generare gli eventi di rischio operativo.¹⁷

¹⁶ G. BIRINDELLI, P. FERRETTI, *Il rischio operativo nelle banche italiane. Modelli, gestione e Disclosure*, Roma, Bancaria Editrice, 2009, pag. 181.

¹⁷ E' a discrezione delle banche l'eventuale scelta di raccolta dati di perdita su una classificazione più dettagliata circa gli Event Type e Business Line. L'eventuale scelta sarebbe comprovata da un desiderio di miglior identificazione e gestione di ogni singolo aspetto critico.

| Business Unit | Level 1 | Level 2 | Activity Groups |
|--------------------|-------------------------------------|-----------------------------------|---|
| INVESTMENT BANKING | Corporate Finance | Corporate Finance | Mergers and Acquisitions, Underwriting, Privatisations, Securitisation, Research, Debt (Government, High Yield) Equity, Syndications, IPO, Secondary Private Placements |
| | | Municipal/Government Finance | |
| | | Merchant Banking | |
| | | Advisory Services | |
| | Trading & Sales | Sales | Fixed Income, equity, foreign exchanges, commodities, credit, funding, own position securities, lending and repos, brokerage, debt, prime brokerage |
| | | Market Making | |
| | | Proprietary Positions | |
| BANKING | Retail Banking | Treasury | Retail lending and deposits, banking services, trust and estates |
| | | Retail Banking | |
| | | Private Banking ² | |
| | Commercial Banking | Card Services | Merchant/Commercial/Corporate cards, private labels and retail |
| | | Commercial Banking | Project finance, real estate, export finance, trade finance, factoring, leasing, lends, guarantees, bills of exchange |
| | Payment and Settlement ³ | External Clients | Payments and collections, funds transfer, clearing and settlement |
| | Agency Services | Custody | Escrow, Depository Receipts, Securities lending (Customers) Corporate actions |
| Corporate Agency | | Issuer and paying agents | |
| Corporate Trust | | | |
| OTHERS | Asset Management | Discretionary Fund Management | Pooled, segregated, retail, institutional, closed, open, private equity |
| | | Non-Discretionary Fund Management | Pooled, segregated, retail, institutional, closed, open |
| | Retail Brokerage | Retail Brokerage | Execution and full service |

18

L'introduzione delle Linee di Business è giustificata dalla gestione del rischio operativo che si vuole adottare coinvolgendo tutte le risorse della struttura organizzativa. Con Basilea II e Basilea III si pone l'attenzione su una gestione molto dinamica del rischio e della liquidità, ragion per cui le banche hanno dovuto predisporre una governance e una struttura di dati adeguata.¹⁹

Affinché vi sia una buona gestione del rischio operativo è necessario che una buona base sia definita da una governance strutturata e solida. Il Comitato di Basilea, per questo fattore, ha evidenziato un modello basato su tre linee di difesa:

- i. *Gestione delle linee di Business*²⁰: nota anche come gestione operativa è una funzione che possiede e gestisce il rischio stesso. E' la prima linea di difesa che i responsabili operativi devono possedere. Questo rende quest'ultimi responsabili dell'implementazione di azioni che vogliono correggere carenze. Il processo insito nella gestione operativa, e che approfondiremo successivamente, comprende l'identificazione del rischio, la valutazione del rischio, il controllo dei rischi e la mitigazione dei rischi, andando a verificare che le attività siano in linea con gli obiettivi.
- ii. *Una funzione indipendente di gestione del rischio operativo aziendale*: la seconda linea di difesa include una funzione di gestione del rischio

¹⁸ COMITATO DI BASILEA PER LA VIGILANZA BANCARIA, *Convergenza Internazionale della misurazione del capitale e dei coefficienti patrimoniali*.

¹⁹ La definizione tardiva dei dati computabili al rischio operativo ha rallentato e limitato notevolmente la gestione di quest'ultimo prima di Basilea III, richiedendo il suo apporto con estrema urgenza.

²⁰ Questo giustifica l'importanza della loro categorizzazione.

affinché si monitori l'adozione di pratiche di gestione del rischio e si assista all'operato dei responsabili nella definizione delle "esposizioni target", riportando poi i dati connessi.

- iii. *L'indipendenza del revisore del framework adottato dalla banca:* con la terza linea di difesa si marca l'importanza dell'audit interno. Lo scopo dell'audit è fornire delle informazioni sulla gestione del rischio, i controlli interni e l'efficacia della governance.

Un'attenta conoscenza del rischio e del flusso informativo necessario per la gestione e prevenzione di quest'ultimo è alla base di una ottimale gestione del rischio operativo.

Perché è importante la gestione dei rischi operativi nelle banche e nelle compagnie assicurative

La gestione dei rischi operativi è un'attività fondamentale per le banche e le compagnie assicurative come abbiamo visto, lo è per diversi fattori in particolar modo:

1. *Preservazione della reputazione:* le banche e le compagnie assicurative intrattengono rapporti di profonda dipendenza con la fiducia dei propri clienti. Un danno reputazionale con errori operativi rilevanti, furto di dati o un'interruzione dei servizi, avrebbe un impatto enorme. Una gestione efficace dei rischi operativi aiuta dunque a evitare situazioni spiacevoli del genere preservando i rapporti di fiducia.
2. *Minimizzazione delle perdite finanziarie:* gli errori operativi possono causare delle significative perdite finanziarie. Queste perdite possono derivare da frodi, errori umani, eventi esterni e una gestione efficace che identifica, valuta e mitiga questi rischi in maniera tempestiva permette di ridurre le probabilità di perdite impreviste. Il principio 7 del documento emesso dal Comitato di Basilea nel Febbraio del 2003 enuncia proprio testuali parole: "Le banche dovrebbero predisporre piani di emergenza e di continuità operativa per assicurare la prosecuzione dell'attività e minimizzare le perdite in caso di gravi disfunzioni operative". Le banche, infatti, dovrebbero periodicamente esaminare i piani di continuità operativa ed emergenziali sottoponendoli anche a dei test periodici valutandone l'applicabilità e la validità in situazioni di minaccia all'operatività della banca.

3. *Conformità normativa*: le istituzioni sono soggette ad una serie di regolamenti e normative come il Basel Committee on Banking Supervision che ha emesso delle linee guida tassative con Basel II e Basel III richiedendo alle banche di tenere conto dei rischi operativi nei loro calcoli di capitale. È proprio la gestione dei rischi operativi che aiuta le banche e le compagnie assicurative a rimanere conformi a tali normative.
4. *Continuità Operativa*: eventi imprevisti come interruzioni di sistema, attacchi informatici possono causare gravi e improvvise interruzioni di operazioni quotidiane bancarie e assicurative. Una gestione dei rischi operativi efficace e scrupolosa include anche la pianificazione della continuità operativa assicurando che in circostanze imprevedibili siano in grado di ripristinare il regolare funzionamento il più rapidamente possibile.
5. *Miglioramento dell'efficienza*: l'identificazione e la gestione dei rischi operativi permette di garantire un incremento dell'efficienza operativa. Questi processi possono includere l'ottimizzazione dei processi, un'allocazione efficiente delle risorse e riduzione degli sprechi. È chiaro che un'efficienza che tende al miglioramento con una gestione dei rischi ben strutturata può garantire una maggiore redditività complessiva.

Consegue che, poiché il sistema bancario e assicurativo svolgono un ruolo molto rilevante in qualsiasi contesto economico globale e nazionale, gli effetti collaterali di una cattiva gestione del rischio sono di vasta portata.²¹ Naturalmente anche nella piccola realtà bancaria si riversano i danni in quanto se un istituto di credito è in difficoltà può andare ad agire sulla riduzione o l'interruzione dei prestiti andando ad influire sulla disponibilità di fondi e sulla crescita economica che si rallenterebbe.

Per comprendere al meglio quanto e perché sia importante la gestione del rischio possiamo citare e analizzare uno studio sulla gestione del rischio globale avanzato da Accenture in cui si afferma che il 77% dei risk manager si mostravano preoccupati per i rischi operativi e finanziari che stanno emergendo sempre più rapidamente; non a caso quello che si definisce abitualmente come "*risk landscape*"²² sta assumendo sempre più connotati frenetici, dinamici e complessi.

²¹ Si pensi alla crisi finanziaria del 2007-2008.

²² Per "*risk landscape*" la metafora di "panorama del rischio" è molto forte in quanto cattura l'idea di dover navigare intorno ai rischi e alle insidie tra dove si trova istantaneamente l'impresa e dove si spera di essere nel futuro.

Di seguito si riporta una rappresentazione di “panorama di rischio”.



Un recente studio sui rischi di Accenture ha posto una grande attenzione sulla varietà di rischi che si devono fronteggiare tenendo conto della grande interconnessione tra di loro: vi sono tra questi dei “rischi leader” cioè che sono aggravati di molto dai grandi rischi presenti dovunque, tra questi vediamo per l’appunto il rischio operativo. Accenture riporta un grafico in cui si possono osservare i rischi aggravati dai rischi operativi nella fattispecie.

Rischi aggravati dai rischi operativi



È dall'interconnessione che comprendiamo quanto sia essenziale gestire il rischio operativo, per evitare che si possa innescare un effetto domino dal quale non ci si può più tirare indietro. L'incapacità di tenere il passo con la natura mutevole del rischio espone sempre più le aziende a maggiori livelli di minacce e vulnerabilità: prepararsi ai rischi interconnessi può gettare le basi per la resilienza e la crescita del business.

III. Metodi di Quantificazione dei Rischi Operativi

Con Basilea II la disciplina ha avuto la possibilità di definire un trattamento prudenziale del rischio operativo ad hoc con tre differenti metodologie di quantificazione: metodo base (*Basic Indicator Approach-BIA*), metodo standardizzato (*Standardised Approach- SA*) e i metodi avanzati (*Advanced Measurement Approaches-AMA*)²³.

Queste metodologie mirano tutte alla definizione del capitale regolamentare da dover allocare per fronteggiare i rischi operativi; inoltre, si contraddistinguono per un grado crescente di complessità a cui si lega un maggiore necessità di disporre di un data set attendibile e adeguato circa le perdite operative. Naturalmente il ricorso ai metodi avanzati per il calcolo del requisito patrimoniale è subordinato all'autorizzazione della Banca d'Italia post valutazione dei requisiti tecnico-organizzativi e di controllo interno.

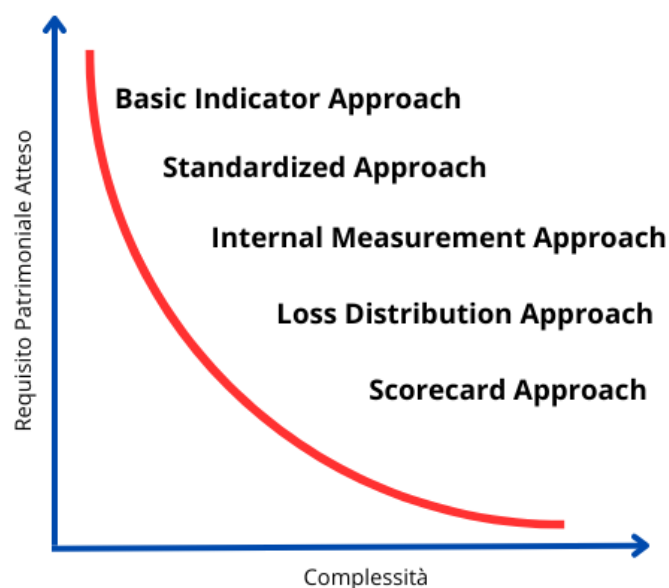


Figura 1: Ammontare di capitale da dover allocare al variare dei metodi scelti.

Le banche sono in una posizione che permette loro di poter adottare il metodo più adatto in base alla loro realtà dimensionale e operativa, sebbene il desiderio dell'autorità regolamentare sia che le banche possano adottare dei modelli sempre più all'avanguardia circa la sensibilità del rischio. Proprio per poter avere un maggior ricorso ai modelli avanzati, l'Accordo di Basilea dà la

²³ I tre principali dei metodi avanzati sono: l'Internal Measurement Approach-IMA, il Loss Distribution Approach-LDA e lo Scorecard Approach.

possibilità di poter far applicare i metodi standardizzati ad una parte delle attività svolte e per la restante parte i metodi AMA.²⁴

Sommariamente nel metodo base il requisito patrimoniale viene calcolato applicando al margine di intermediazione un coefficiente. Nel metodo standardizzato per comprendere il capitale da dover allocare, si vede l'applicazione di diversi coefficienti al margine di intermediazione²⁵ per ogni linea di business in cui è possibile dividere l'attività aziendale. Negli AMA invece l'ammontare del requisito patrimoniale viene calcolato dalla banca mediante dei modelli che si basano su dati di perdita operativa e altri fattori di valutazione.

L'approccio che risulta più stimolante specie dal punto di vista statistico è proprio quello avanzato: offre il vantaggio di poter avere una misurazione precisa dell'esposizione al rischio operativo data la loro peculiarità nell'essere costruiti ad hoc per ogni singola realtà bancaria. Per la costruzione di un efficace modello, la banca deve considerare i dati interni di perdita operativa, dati esterni e analisi di scenario.

La rilevante importanza dei dati interni di perdita operativa è dovuta al fatto che sono indispensabili per la costruzione di un sistema che rilevi e quantifichi i rischi operativi. La banca fissa le soglie minime di perdita, al di sotto di quest'ultime non si vanno a considerare le perdite. Queste soglie fissate dalla banca sono definite singolarmente e differentemente per ciascuna classe di rischio non escludendo rilevanti eventi operativi e non creando stime distorte con dati poco attendibili. Inoltre, per conferire robustezza al processo di stima, è necessario dotarsi di un dataset di perdite interne per un range temporale di minimo cinque anni: può capitare che i dati interni non siano ingenti numericamente, ragion per cui è indispensabile il ricorso ad un dataset con dati esterni e di scenario.

Le fonti da cui si attinge per i dati esterni di perdite operative sono fornite da un insieme di banche e altri intermediari come DIPO (Database Italiano Perdite Operative)²⁶, oppure di mercato, quindi reperibili da archivi reperiti da fornitori del settore.

²⁴ Il Comitato si augura che le banche si muovano dall'approccio più semplice in direzione di uno più avanzato in rapporto alla crescita dei sistemi di misurazione e gestione del rischio. Se una banca decide di optare per un approccio più avanzato, successivamente non sarà autorizzata a regredire con un approccio più semplice. È invece consentito poter adottare degli approcci diversi in base a ciascuna delle linee di business.

²⁵ Il margine di intermediazione (MINTM) è una voce presente nel bilancio di una società bancaria, specificatamente nel conto economico. È composta dalla somma algebrica di interessi attivi e passivi (margine d'interesse, MINT), rettifiche nette su crediti (margine d'interesse rettificato MINTR), dividendi e altri proventi, ricavi netti per servizi, profitti e perdite da operazioni finanziarie, altri proventi netti di gestione (margine d'intermediazione).

In parole povere, il margine di intermediazione indica il valore che una banca è riuscita ad ottenere dalla sua attività principale, quella legata alla mediazione tra domanda e offerta di credito.

Una banca solida deve essere capace, quindi, di maturare un margine da questa attività di intermediazione, ovvero dalla differenza tra gli interessi attivi e quelli passivi del periodo considerato.

È determinato secondo i principi IFRS/IAS definiti dall'International Accounting Standards Board (IASB).

²⁶ DIPO è un'attività interbancaria lanciata nel 2003 e progettata per supportare lo sviluppo della gestione del rischio operativo e creare una metodologia per raccogliere e scambiare informazioni sulle perdite operative subite dai membri. Le attività consistono principalmente nella gestione e mantenimento del database italiano delle perdite

Per quanto concerne i dati di scenario, cioè eventi operativi “estremi” che potrebbero plausibilmente verificarsi, sono frutto di un processo interno che tiene conto della grandezza del business della banca e del contesto socioeconomico in cui è collocata²⁷.

Una volta rilevati i dati esterni e di scenario bisogna incorporarli nel modello con delle metodologie ad hoc. I dati che verranno utilizzati per la costruzione del modello preposto alla gestione dei rischi operativi sono:

- **Perdite interne;**
- **Perdite esterne al di sopra di una soglia derivanti da database come DIPO e dati pubblici;**
- **Perdite prospettive superiori alla soglia derivate da analisi di scenario.**

L’approccio a cui si ricorre per poter “modellare le perdite” è l’approccio attuariale: si prevede un’analisi separata di frequency²⁸ e la severity²⁹.

La distribuzione di severity sta ad indicare la densità di probabilità del singolo impatto monetario che può derivare da un evento operativo. La distribuzione viene divisa in due parti: **body** che viene modellizzato basandosi sulle perdite interne alla banca, **tail o coda superiore**, cioè le perdite che sono superiori alla soglia u ³⁰ che viene strutturata in modo distinto così da dare più rilievo alle perdite estreme andando quindi ad attingere ai dati di scenario e perdite delle altre banche.

È un modo di approcciarsi molto comune nella gestione del rischio dato che molto spesso per modellizzare le perdite si ricorre alla distribuzione lognormale, Weibull, l’esponenziale andando però a sottostimare le perdite nella coda destra della distribuzione, impattando infine su una sottostima del capitale totale.

- La distribuzione lognormale** descrive una variabile causale x il cui logaritmo, $\log x$, è normalmente distribuito con media μ e deviazione standard σ ;
- La distribuzione esponenziale**, che ha funzione di densità $f(x)=\lambda e^{-\lambda x}$ e funzione di ripartizione $F(x)=1-e^{-\lambda x}$, e la cui forma dipende dal parametro λ che è il reciproco della media della distribuzione;
- La distribuzione Weibull**, che ha una funzione di densità $f(x)=\frac{\alpha}{\beta^\alpha} x^{\alpha-1} e^{-(x/\beta)^\alpha}$.

operative (DIPO), un database che dal gennaio 2003 raccoglie informazioni su ogni singolo evento generatore di una perdita per rischio operativo subito dalle banche aderenti. Da dicembre 2011 DIPO è entrata a far parte di ABIServizi S.p.A.

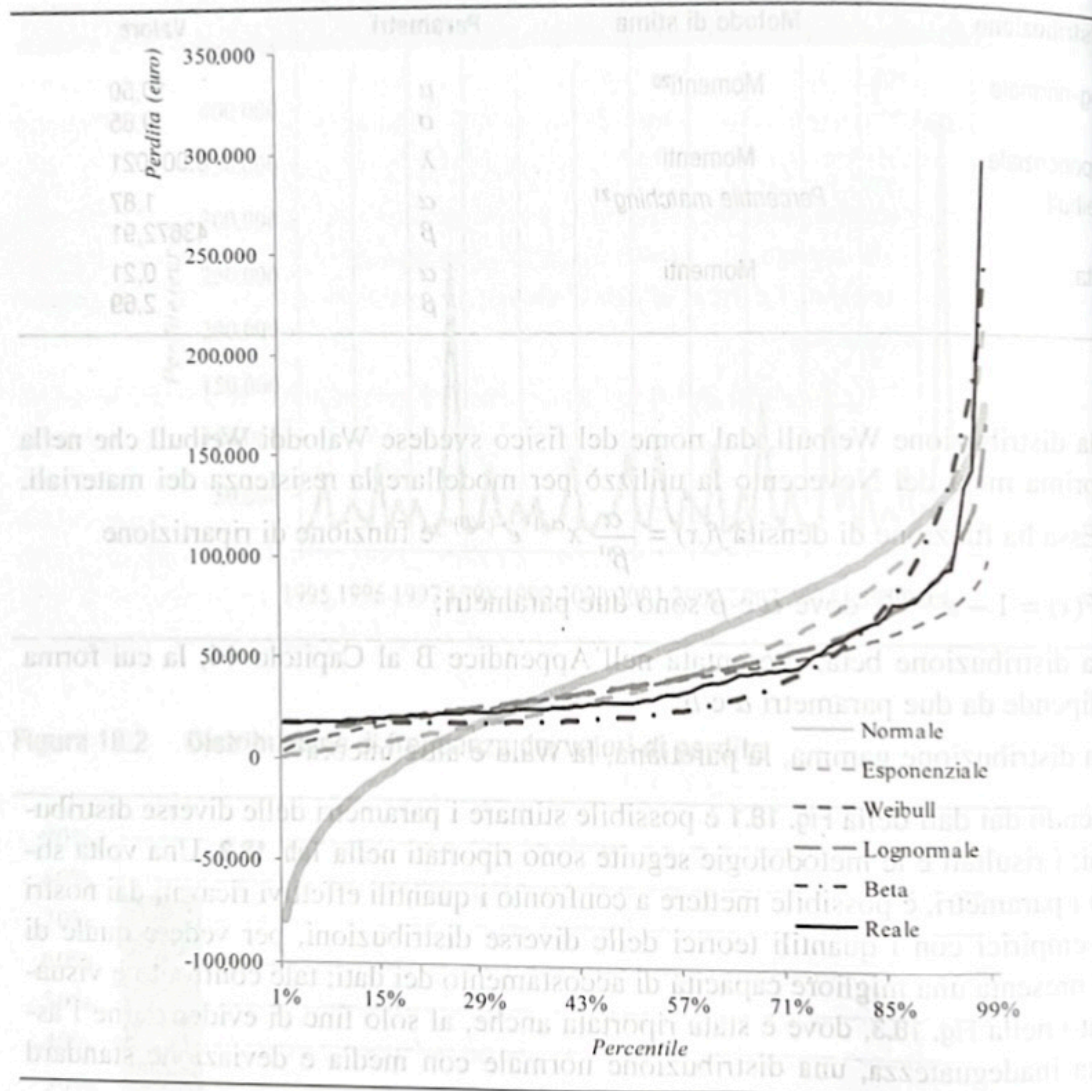
²⁷ Si deve tenere conto, infatti, che questo processo generatore di dati coinvolge esperti interni o esterni che si vanno a confrontare con gli altri dati di cui si dispone per poterne valutare l’affidabilità.

²⁸ Si analizza la frequenza di accadimento di un evento in particolare.

²⁹ Si analizza la distribuzione dell’impatto monetario che ha un singolo evento operativo.

³⁰ Il valore u viene fissato dal management della banca. Rammentiamo che oltre a questo valore si considerano gli importi che appartengono alla coda.

Figura 18.3 Percentili empirici e percentili generati con alcune distribuzioni teoriche



Come si può evincere le distribuzioni Weibull e lognormale mostrano una buona capacità di accostamento alla curva dei dati reali, difatti la qualità dell'approssimazione risulta più precisa in corrispondenza dell'estremo destro della curva, dunque nella zona degli eventi di perdita più gravi e rari. Distintamente la distribuzione esponenziale dispone di una capacità di accostamento più limitata in corrispondenza dei valori bassi o medi, per cui risulta in grado di descrivere in maniera più soddisfacente il comportamento dei valori di perdita più elevati.

L'unico difetto di questo approccio sta nel fatto che basandosi su dati esterni e di scenario che sono superiori alla soglia implica che non si dispone di dati esterni nella scelta di una soglia inferiore.

La distribuzione di severity di ogni singola perdita interna sarà formata dalla misurazione di due distribuzioni: di body e tail.

$$f(x) = \begin{cases} \omega \cdot f_{body}^*(x) & \text{per } x \leq u \\ (1 - \omega) \cdot f_{tail}^*(x) & \text{per } x > u \end{cases}$$

Formula in cui:

- $f_{body}^*(x) = f_{body}(x)/F_{body}(u)$ è la distribuzione del body troncata ai valori inferiori alla soglia u ;
- $f_{tail}^*(x) = f_{tail}(x)/[1-F_{tail}(u)]$ è la distribuzione della tail troncata ai valori superiori alla soglia u ;
- $\omega = F_{body}(u)$ invece è il peso del body della distribuzione.

Per quanto concerne la distribuzione di frequency, invece, è indicata come la distribuzione di probabilità del numero di perdite operative che si registrano nell'arco di un anno. La si va a stimare basandosi sulle sole perdite interne dato che riflettono più autenticamente le caratteristiche della banca.

Tutte le classi di rischio vengono modellizzate sulla base di una Poisson con una densità:

$$f_{Pois}(k; \lambda) = \frac{\lambda^k e^{-\lambda}}{k!}$$

dove il parametro $\lambda > 0$ viene stimato con lo stimatore dei momenti sulla base del numero di perdite annue n_i , con $i = 1, \dots, M$, dove M è il numero di anni per cui si hanno a disposizione dati riguardanti le perdite interne.

Assunta la totale indipendenza delle due distribuzioni, otteniamo la stima del capitale a rischio mediante un processo di convoluzione delle distribuzioni con l'algoritmo Monte Carlo³¹. Ogni simulazione di perdita aggregata annua si ottiene nel seguente modo:

$$S = \sum_{i=1}^N s_i + s'$$

Qui:

- N è il numero di perdite che viene simulato dalla distribuzione di frequency;
- S_i è l'importo di ogni singola perdita al di sopra di una soglia;
- S' è la media empirica delle perdite aggregate annue al di sotto della soglia.

Dato che si ottiene la distribuzione aggregata annua di perdite per ogni Event Type, è possibile desumere e quantificare delle stime del capitale a rischio, specie in queste voci:

- **VaR (Value at Risk):** è definito dalla Banca d'Italia come il 99.9% della distribuzione empirica e rappresenta il capitale che bisogna allocare per un event type;

³¹ "La simulazione Monte Carlo prevede un insieme di risultati basati su una gamma stimata di valori rispetto a un insieme di valori di input fissi. In altre parole, una simulazione Monte Carlo crea un modello di possibili risultati sfruttando una distribuzione di probabilità, come una distribuzione uniforme o normale, per qualsiasi variabile che abbia un'incertezza intrinseca. Ricalcola quindi i risultati ancora e ancora, utilizzando ogni volta una serie diversa di numeri casuali compresi tra il valore minimo e quello massimo. Fornisce dei vantaggi rispetto ai modelli predittivi con degli input fissi, come la capacità di condurre un'analisi di sensibilità o calcolare la correlazione degli input." Cfr <https://www.ibm.com/it-it/topics/monte-carlo-simulation>.

- **EL (Expected Loss):** è il valore medio della distribuzione rappresentando le perdite attese per l'anno seguente, ma non è possibile utilizzarlo come indicatore per il capitale da allocare.

Può risultare interessante citare dei dati empirici sul rischio operativo rilevati da un vasto numero di banche mondiali durante una survey internazionale condotta dal Comitato di Basilea tra 89 banche appartenenti a 19 Paesi Europei, Nord e Sud America, Asia e Australia. A queste banche è stato chiesto di fornire dei dati sulle perdite operative registrate over 10.000€ nel 2001 articolandole nei rispettivi Event Type e Business Line.

Complessivamente sono stati rilevati 47.269 eventi di perdita e perdite totali per 7,8 miliardi di euro.³²

Basic Indicator Approach

Il primo e più semplice approccio prevede che il requisito patrimoniale sia commisurato al MID³³, nonché margine di intermediazione della banca; quest'ultimo lo si può intendere come un indicatore di dimensione "puro" che non fornisce delle indicazioni relative alla qualità dei ricavi aziendali, e quindi nemmeno sulla rischiosità dei processi operativi.

Il margine di intermediazione viene moltiplicato per un coefficiente di rischio, α , che è stato fissato al 15% dal Comitato di Basilea. La scelta di questo percentile è stata adottata sulla base di dati forniti al Comitato da un numero limitato di banche che nel 2000 disponevano già di un sistema di misurazione del rischio operativo.³⁴

Tale coefficiente viene applicato al valore medio degli ultimi tre anni del margine di intermediazione per poter ottenere il requisito patrimoniale k_{RO} relativo al rischio operativo.

$$K_{RO} = \alpha \cdot \frac{\sum_{i=1}^3 \max(0, MID_{t-i})}{N}$$

Con N che rappresenta il numero di anni in cui il MID è risultato positivo, tra gli ultimi tre anni.

Tuttavia, questo approccio non lo si considera come quello più indicato e preciso, ma esattamente il contrario. La prima perplessità nasce proprio in merito alla scelta del MID: da un lato, si riconosce che il MID non sia la misura più adeguata a poter esprimere l'ampiezza dell'operatività bancaria, e dall'altro lato, sorgono altre perplessità circa la relazione tra l'ammontare di

³² Cfr. Basel Committee on Banking Supervision (2003b).

³³ Come è stato anticipato prima, il MID deve essere al lordo dei costi operativi e delle rettifiche di valore (un esempio sono gli interessi legali contabilizzati su crediti non-performing). Da questo devono essere esclusi dei profitti eventuali o perdite che derivano dalla cessione di titoli del portafoglio immobilizzato e altri risultati di natura straordinaria.

³⁴ Il primo Quantitative Impact Study (QIS) circa il rischio operativo, ha sottolineato che in media le banche allocavano il 15% del capitale economico di cui disponevano (cioè il 12% del capitale regolamentare) alla classe del rischio operativo. È opportuno ricordare che inizialmente il Comitato desiderava richiedere un requisito più pesante e che furono proprio i risultati del QIS a distoglierlo da questa richiesta.

questo indicatore e l'esposizione effettiva al rischio operativo. Nello specifico, è doveroso ricordare che il registrarsi di rischi catastrofali non ha alcuna relazione con l'ampiezza del margine in questione.

Distintamente è stato dimostrato come un volume maggiore del MID dia la possibilità di poter attenuare l'impatto causato dalle perdite operative, specie quelle che registrano più severità.

In conclusione, di questa esamina circa l'approccio dell'indicatore base possiamo individuare due tratti tipici e distintivi:

- a. **La facilità di calcolo e l'agevole reperibilità dei dati;**
- b. **L'inadeguatezza nel considerare la differente rischiosità operativa nelle differenti attività che svolge quotidianamente una banca.**

E' chiaro che questo approccio sia maggiormente indicato nell'adozione in realtà minori, data la complessità ridotta dei sistemi di misurazione che caratterizzano le banche di minore dimensione.

Standardised Approach

Il secondo approccio, nonchè lo Standardised Approach, è sostanzialmente un'evoluzione del Basic Indicator Approach con l'obiettivo di poter far diventare il modello più articolato in rapporto alle differenti aree operative bancarie. Questo è un approccio molto più complesso e raffinato rispetto al precedente: in primo luogo, adottando dei coefficienti che sono predeterminati dalle autorità di vigilanza si va a limitare la capacità di poter rappresentare in maniera autentica il profilo di rischio delle banche.

Questo approccio prevede che il requisito patrimoniale sia misurato in maniera distinta, quindi, per le principali linee di attività andando a moltiplicare il loro MID per un coefficiente specifico di rischiosità, β_i , che è differente per le singole Business Line.³⁵

I coefficienti β_i esprimono, come nel caso del coefficiente alfa, una misura della relazione che c'è tra il volume di operatività legato alle diverse aree operative e il rischio connesso al registrarsi delle perdite. Il β_i funge da proxy per le relazioni, a livello di settore intero, tra le perdite per rischi operativi storicamente riscontrate in una determinata linea e il livello aggregato di reddito lordo per quella stessa linea.³⁶

I coefficienti, in conclusione dunque, rispecchiano il rapporto tra le perdite storicamente registrate dalla realtà bancaria nelle diverse linee e il relativo margine d'intermediazione.

³⁵ Cogliendo il diverso grado di rischiosità per Business Line, conduce ad un requisito patrimoniale maggiore per le banche che operano in settori di fatto più rischiosi.

³⁶ Cfr. <https://www.bis.org/bcbs/cp3fullit.pdf>

Riportiamo di seguito le business line con i relativi coefficienti beta nell'approccio standardizzato in esame.

Figura 2 Linee di business e coefficienti regolamentari

| Linea operativa | Fattori β |
|--|-----------------|
| Corporate finance (β_1) | 18% |
| Negoziazioni e vendite (β_2) | 18% |
| Retail banking (β_3) | 12% |
| Commercial banking (β_4) | 15% |
| Pagamenti e regolamenti (β_5) | 18% |
| Gestioni fiduciarie (β_6) | 15% |
| Asset management (β_7) | 12% |
| Intermediazione al dettaglio (β_8) | 12% |

Inoltre, è ammesso che il MID di una business line sia negativo uno o più anni, a patto che il risultato complessivo della banca sia positivo. Nel caso in cui così non fosse, nella stima della media relativa ai tre anni, quest'ultimo viene posto pari a 0. La logica sottesa al seguente approccio prevede che le banche che operano su aree di attività più rischiose nella chiave del rischio operativo, debbano detenere un patrimonio maggiore dinanzi a tale esposizione.

La formula del calcolo del requisito patrimoniale relativo al rischio operativo mediante l'approccio standardizzato è come segue:

$$k_{RO} = \sum_{i=1}^3 \frac{\text{Max}(\sum_{j=1}^8 \beta \cdot \text{MID}_{j,t-i}, 0)}{3}$$

E' possibile desumere che la scelta di calcolare il requisito patrimoniale della banca come una sommatoria di quelli relativi alle singole linee di business ipotizza una correlazione perfetta tra le diverse tipologie di eventi di perdita. Nel pratico si suppone che le perdite operative delle differenti business line non si compensino manifestandosi in istanti temporali differenti, ma che avvengano congiuntamente: infatti alla banca è diretta la richiesta di dotarsi patrimonialmente in maniera sufficiente per coprire il totale delle perdite che derivano da eventi di matrice diversa.

"APPLICAZIONE PRATICA"

REQUISITO PATRIMONIALE COMPLESSIVO: UTILIZZO DELLO STANDARDISED APPROACH E DEL BASIC INDICATOR APPROACH

Per comprendere nello specifico il processo di calcolo del requisito patrimoniale complessivo di una banca utilizzando lo Standardised Approach ed il Basic Indicator Approach, illustreremo ed esamineremo di seguito i passaggi di due esempi pratici.

STANDARDISED APPROACH (I CASO)

Per quanto concerne il primo esempio pratico, suddividiamo il nostro operando in cinque fasi distinte per garantire chiarezza e precisione nel calcolo.

Nella prima fase, si procederà alla determinazione del margine di intermediazione per ciascuna Business Line per ogni anno considerato.

MID per Linee di Business (in milioni di euro)

| Business line | Anno t-2 | Anno t-1 | Anno t |
|------------------------|-----------------|-----------------|---------------|
| Corporate finance | 1500 | 1600 | 1550 |
| Trading and sales | 2000 | 1800 | 2100 |
| Retail Banking | 3000 | 3200 | 3100 |
| Commercial banking | 2500 | 2400 | 2300 |
| Payment and settlement | 1000 | 1200 | 1100 |
| Agency services | 800 | 850 | 900 |
| Asset management | 700 | 750 | 800 |
| Retail brokerage | 500 | 450 | 550 |

Nella seconda fase procederemo con l'applicazione dei coefficienti regolamentari specifici (β_i) ai margini di intermediazione annuali di ogni Business Line. In tal modo andremo a determinare il requisito patrimoniale per ciascun anno.

| Business line | Coefficiente | Requisito Patrimoniale Anno t-2 | Requisito Patrimoniale Anno t-1 | Requisito Patrimoniale Anno t |
|------------------------|---------------------|--|--|--------------------------------------|
| Corporate finance | 18% | 270 | 288 | 279 |
| Trading and sales | 18% | 360 | 324 | 378 |
| Retail Banking | 12% | 360 | 384 | 372 |
| Commercial banking | 15% | 375 | 360 | 345 |
| Payment and settlement | 18% | 180 | 216 | 198 |
| Agency services | 15% | 120 | 128 | 135 |
| Asset management | 12% | 84 | 90 | 96 |

| | | | | |
|------------------|-----|----|----|----|
| Retail brokerage | 12% | 60 | 54 | 66 |
|------------------|-----|----|----|----|

Nella terza fase sommiamo i requisiti patrimoniali annuali per ottenere un totale complessivo per ciascun anno. Qualora tale somma risulti negativa, applichiamo una correzione impostandola a zero. Successivamente, nella quarta fase, determiniamo i requisiti patrimoniali per ciascuno dei tre anni, tenendo conto dell'eventuale correzione dei valori negativi, così facendo avremo una visione chiara dei requisiti patrimoniali su base triennale.

| Ann o | Somma Algebrica | Correzione Negativi | Valori | Requisiti Patrimoniali |
|----------|-----------------|------------------------|--------|---------------------------|
| t-2 | 1809 | 1809 | | 1809 |
| t-1 | 1844 | 1844 | | 1844 |
| t | 1869 | 1869 | | 1869 |

Per concludere, nella quinta fase andremo a calcolare il Requisito Patrimoniale Complessivo utilizzando la formula prevista dallo Standardised Approach. Questo avverrà sommando i requisiti patrimoniali dei tre anni e dividendo il risultato ottenuto per tre, al fine di ottenere una media annuale ponderata che rifletta accuratamente l'esposizione al rischio della banca.

$$k_{RO} = \sum_{i=1}^3 \frac{\text{Max}(\sum_{j=1}^8 \beta * MID_j, t - i, 0)}{3}$$

$$k_{RO} = 1840,5$$

Il risultato ottenuto rappresenta il capitale (in milioni di euro) che la banca deve mantenere a riserva per coprire il rischio operativo, secondo il metodo Standardised Approach.

BASIC INDICATOR APPROACH (II CASO)

Passiamo ora ad esaminare il secondo esempio pratico, che ci permetterà di comprendere il processo di calcolo del requisito patrimoniale complessivo utilizzando il Basic Indicator Approach.

Anche per questo approccio, è previsto che il requisito patrimoniale sia commisurato al MID, nonché margine di intermediazione della banca.

| Anno | MID |
|------|-------|
| t-2 | 12000 |
| t-1 | 12250 |
| t | 12400 |

A differenza dello Standardised Approach che prevede che il requisito patrimoniale sia misurato in maniera distinta per le principali linee di attività andando a moltiplicare il loro MID per un coefficiente specifico (β_i), nel metodo di base il margine di intermediazione viene moltiplicato per un coefficiente di rischio, α , fissato al 15% dal Comitato di Basilea.

Tale coefficiente viene applicato al valore medio degli ultimi tre anni del margine di intermediazione per poter ottenere il requisito patrimoniale complessivo relativo al rischio operativo.

| Media Triennale | Coefficiente α |
|-----------------|-----------------------|
| 12216,7 | 15% |

$$k_{RO} = \alpha * \frac{\sum_{i=1}^3 \max(0, MID_{t-i})}{N}$$

$$k_{RO} = 1832,5$$

È chiaro che questo approccio sia maggiormente indicato nell'adozione in realtà minori, data la complessità ridotta dei sistemi di misurazione che caratterizzano le banche di minore dimensione. Quest'approccio pecca di accuratezza in quanto non considera la differente rischiosità operativa nelle differenti attività che svolge quotidianamente una banca diversamente dallo Standardised Approach.

ANALISI COMPARATIVA

Si evidenzia una differenza tra i due risultati ottenuti, con lo Standardised Approach che richiede un requisito di capitale complessivo superiore al Basic Indicator Approach. Questo può indicare che il SA ha rilevato una maggiore esposizione al rischio nei dettagli delle attività della banca rispetto al BIA. Dal punto di vista regolamentare il SA può essere più vantaggioso poiché fornisce una valutazione più accurata e dettagliata dei rischi, potenzialmente migliorando la gestione del capitale della banca; tuttavia, lo stesso comporta anche costi e complessità aggiuntivi, in quanto richiede sistemi di gestione del rischio più avanzati e una raccolta di dati più granulare. La scelta tra i due approcci dipende dalle risorse disponibili e dalla struttura operativa della banca. Banche con portafogli di rischio complessi potrebbero trarre maggiori

benefici dall'implementazione del SA, mentre istituzioni meno complesse potrebbero preferire il BIA per la sua facilità di applicazione.

Sia nel metodo di base che in quello standardizzato, la base del calcolo, come abbiamo potuto constatare, è il margine d'intermediazione. Questo indicatore è espresso al lordo di quelle che possono essere eventuali rettifiche di valore, per cui tende ad assumere dei valori più elevati del normale per le banche che prestano a mercati più rischiosi, a tassi più alti, ma che d'altro canto operano anche con delle rettifiche di valore più consistenti.

Per queste in particolare con l'ultima formula citata si avrebbe un k_{RO} più elevato giustificato dalla qualità peggiore del portafoglio crediti, e non per un rischio operativo maggiore. Naturalmente questo non sarebbe corretto dato che i rischi connessi ad una peggiore qualità del credito vengono considerati già ai fini del calcolo del requisito patrimoniale obbligatorio attraverso dei meccanismi che non devono andare ad alterare la stima del rischio operativo. È proprio per queste ragioni che il Comitato di Basilea ha poi previsto che le singole autorità di vigilanza nazionali potessero inserire anche un *approccio standardizzato alternativo (ASA)*.

La possibilità di poter adottare questo approccio alternativo è stata condizionata dal fatto che riesca a dimostrare che attraverso l'impiego del metodo standard alcuni rischi possono risultare sovrastimati, e che sia in grado di assicurare una base migliore ricorrendo a tale metodo, come ad esempio evitando le duplicazioni nel calcolo dei rischi.

Il consenso per il ricorso a tale approccio è accordato su una base discrezionale dalle autorità di vigilanza e non è appoggiato l'impiego dell'ASA da parte di grandi banche diversificate che operano su mercati importanti.

La formula non muta notevolmente rispetto alla formula utilizzata nel metodo standardizzato: viene fuori da una sommatoria dei prodotti tra i coefficienti β che sono fissati dal Comitato di Basilea per ogni linea operativa. La differenza tra i due approcci sta nell'indicatore di esposizione da utilizzare nel calcolo del requisito patrimoniale per le linee di *Retail Banking e Commercial Banking*.

Nell'approccio alternativo queste linee operative possono utilizzare come indicatore di esposizione l'ammontare di prestiti e anticipazioni, moltiplicato per un fattore fisso e definito uguale al 0,035) al posto del reddito lordo. I beta restano invariati al 12% e 15%, oltre ad essere possibile l'aggregazione delle due linee utilizzando un Beta pari al 15%. Per quanto concerne le banche non sono in grado di poter disaggregare il loro MID nelle altre 6 Business Line, possono aggregare il MID totale per queste ricorrendo ad un Beta del 18%.

$$K_{ASA} = \sum_{i=1}^2 MI_i \cdot \beta_i + \sum_{i=3}^4 LA \cdot \beta_i \cdot m + \sum_{i=5}^8 MI_I \cdot \beta_i$$

Qui occorre precisare alcuni fattori presenti nella formula:

- *m*: Fattore fisso stabilito dal Comitato di Basilea, nonchè pari al valore di 0,035
- *LA*: la media sugli ultimi tre esercizi del totale dei prestiti e delle anticipazioni in essere delle linee operative Retail e Commercial (non ponderate per il rischio e al netto degli accantonamenti).

Advanced Measurement Approach

Il terzo e ultimo approccio è dato da una varietà di possibili metodologie che sono sviluppate all'interno delle banche³⁷, rispetto alle quali la normativa si limita a stabilire dei requisiti minimi da rispettare.

Si prevede che una banca che abbia sviluppato un modello per la misura del rischio e la determinazione del capitale economico sia in grado di poterne usufruire anche per la determinazione del requisito patrimoniale minimo obbligatorio, come già si registra per i rischi di mercato.

Il Comitato non impone alcun modello in particolare ma lascia ad ogni banca la flessibilità nell'elaborazione della metodologia da utilizzare, in modo da poterla rendere quanto più aderente alle differenti operatività e ai rispettivi profili di rischio.

Soddisfatti dei requisiti quantitativi e qualitativi, considerando sempre l'autorizzazione dell'organo di vigilanza, le banche potranno essere in grado di poter calcolare il capitale regolamentare richiesto per i rischi operativi con modelli di misurazione analitici in grado di esprimere al meglio l'assorbimento del capitale economico che è legato a questa tipologia di rischi, andando, inoltre, a rappresentare al meglio la rischiosità dell'attività svolta dalla banca. I modelli AMA hanno diversi vantaggi, tra questi quello di garantire una puntuale misurazione dell'esposizione al rischio operativo, dovuto proprio al fatto che vengono costruiti appositamente "*su misura*" per la singola banca; raccolgono una gamma molto vasta di metodologie con un'ampia caratterizzazione statistica e sensibilità verso il rischio, difatti la stima delle perdite operative si ha mediante l'analisi delle serie storiche³⁸.

³⁷ Si parla infatti di una pluralità di Advanced Measurement Approach.

³⁸ L'analisi delle serie storiche è una metodologia statistica che consiste nell'esaminare i dati storici per identificare modelli, tendenze o comportamenti passati al fine di fare previsioni o trarre conclusioni per il futuro. Questa analisi è ampiamente utilizzata in vari settori, inclusi l'economia, le scienze sociali, la finanza, la meteorologia e molti altri.

Vi sono, però, una serie di requisiti che una banca deve rispettare per poter adottare il proprio modello interno per il calcolo del requisito patrimoniale sul rischio operativo:

- i. Il consiglio di amministrazione e l'alta direzione della banca devono essere coinvolti nella supervisione del processo di gestione del rischio operativo;
- ii. La banca deve disporre di un'unità indipendente di controllo e monitoraggio del rischio;
- iii. Il sistema di misura del rischio deve essere integrato strettamente nel processo di gestione quotidiana del rischio della banca; la banca, quindi, deve disporre di un sistema di allocazione del capitale alle diverse Business line così da incentivare una riduzione del rischio;
- iv. La banca deve dimostrare che il modello interno che intende adottare sia in grado di cogliere adeguatamente gli eventi estremi, nonché la tail loss event: nel dettaglio la misura del rischio deve essere in una linea coerente con i parametri fissati per il metodo dei rating interni sul rischio di credito, quindi un livello di confidenza del 99,9% e un orizzonte temporale di un anno³⁹;
- v. Le valutazioni del rischio devono prendere in considerazione anche l'ambiente esterno e il sistema di controlli interni della banca, oltre ai dati interni ed esterni: variazioni di queste categorie devono essere captate dal modello; dunque, non può limitarsi solamente ad elaborare in modo meccanico i dati storici ma attuare un approccio "forward looking";

Rilevante citare che in un working paper del 2001, redatto in preparazione dell'accordo del 2004, il Comitato di Basilea menzionava tre possibili approcci avanzati a cui avrebbero potuto rifarsi i modelli interni delle banche⁴⁰:

- **Internal Measurement Approach (IMA),**
- **Scorecard Approach,**
- **Loss Distribution Approach (LDA).**

Con l'Internal Measurement Approach il capitale da allocare ad ogni linea operativa dipende dalla somma delle perdite attese e inattese, tant'è che si ipotizza una relazione lineare tra perdita attesa e perdita inattesa⁴¹.

L'IMA si articola nelle seguenti fasi:

- a. Anche qui si fa riferimento alle 8 Business Line ma, distintamente dall'approccio standard, l'autorità di vigilanza definisce nel dettaglio l'Event Type di perdita da considerare per ciascuna di esse.

³⁹ Sebbene il Comitato di Basilea abbia unificato il livello di confidenza e l'orizzonte temporale richiesti per la misura del rischio di credito e di quello operativo, continua ugualmente a richiedere dei parametri differenti in materia di rischio di mercato (un livello di confidenza al 99% e orizzonte temporale di 10 giorni lavorativi almeno).

⁴⁰ Non sono stati inclusi nella versione finale dell'accordo sebbene rappresentino un buon esempio di cosa le Autorità di Vigilanza si aspettino dalle banche.

⁴¹ La perdita attesa è la perdita media che ci si aspetta di subire a causa di eventi di rischio operativo nel corso del tempo, mentre la perdita inattesa è la parte della perdita che supera la perdita attesa rappresentando il rischio inaspettato o estremo. Ambedue le misure sono fondamentali per la gestione del rischio operativo e la valutazione del capitale necessario per la copertura da tale rischio. Inoltre, le istituzioni finanziarie e le compagnie assicurative le utilizzano spesso per valutare la robustezza del loro capitale e delle loro riserve dinanzi al rischio operativo.

- b. Per ciascuna combinazione, l'organo preposto alla vigilanza mira a identificare un indicatore di esposizione, **EI- Exposure Indicator**, che rappresenta un proxy dell'esposizione di ogni Business Line a ciascun Event Type.
- c. Per ogni combinazione Business Line/Event Type di evento di perdita, le banche misurano sulla base dei dati interni ed esterni la probabilità che un evento di perdita si possa verificare, cioè la **PE- Probability of Loss Event**), e l'entità della perdita successivamente al registrarsi di un evento, **LGE- Loss Given that Event**.
- d. Il prodotto di EI, PE e LGE viene utilizzato per calcolare l'Expected Loss.
- e. Le banche, confrontando anche i dati consortili, indicano il fattore gamma γ per ciascuna combinazione Business Line/Event Type. Il fattore gamma traduce la stima della perdita attesa in requisito patrimoniale e deve necessariamente tener conto delle perdite inattese, che devono essere ipotizzate in correlazione alle perdite attese. Il concetto di determinazione del fattore gamma deriva dall'applicazione dei modelli di misurazione simili a quelli utilizzati per il calcolo del VAR parametrico.

La formula si presenta nel seguente modo:

$$K_{IMA} = \sum_i \sum_j [\gamma(i, j) \cdot EI(i, j) \cdot PE(i, j) \cdot LGE(i, j)]$$

Dove:

- $\gamma(i, j)$ = Percentuale fissa, proposta dalle banche e accettata dalle autorità di vigilanza, in base alla perdita attesa per ciascuna combinazione di *Business Line* e tipo di evento.
- $EI(i, j)$ = Livello dell'indicatore di esposizione per la *Business Line* *i*-esima e tipo di evento *j*-esimo.
- $PE(i, j)$ = Probabilità di un evento di perdita per la *Business Line* *i*-esima e tipo di evento *j*-esimo.
- $LGE(i, j)$ = Ammontare medio della perdita in caso di manifestazione dell'evento di perdita per la *Business Line* *i*-esima e tipo di evento *j*-esimo.

L'approccio Loss Distribution, differentemente dai precedenti, è in grado di riflettere meglio il rischio effettivo sopportato dalle banche. Si distingue dal precedente approccio dato che la stima delle perdite inattese avviene

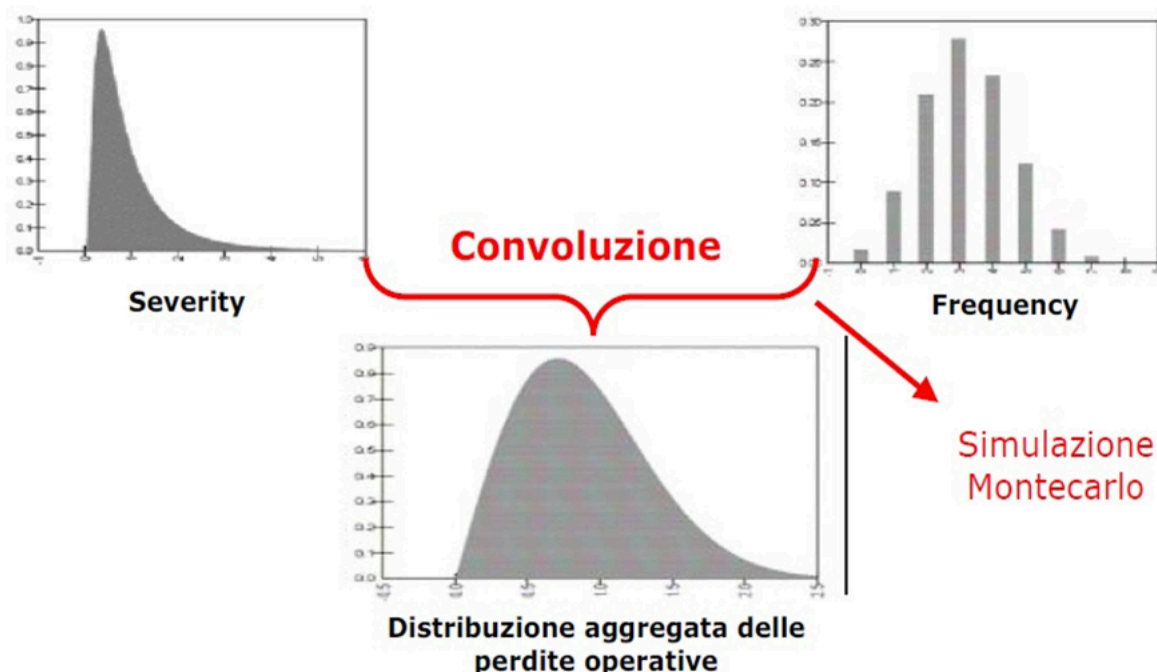
direttamente e non in maniera mediata, cioè con l'assunzione di ipotesi sull'eventuale relazione tra perdite attese e inattese con l'inserimento del fattore gamma.

Per ciascuna Business Line e per ciascun Event Type la banca deve:

- i. **Stimare due distribuzioni di probabilità:** la distribuzione della frequenza dell'evento di perdita (PE) in un orizzonte temporale di un anno, e la distribuzione dell'entità della perdita al verificarsi dell'evento (LGE).
- ii. **Costruire una distribuzione cumulata delle perdite sulla base delle due precedenti distribuzioni (PE e LGE).**
- iii. **Calcolare il VaR della distribuzione cumulata.**
- iv. **Sommare i VaR calcolati per ogni combinazione per poter ottenere il requisito patrimoniale a fronte del rischio operativo.**

La distribuzione aggregata finale di perdita ci permette di poter stimare l'ammontare di capitale che è necessario per poter coprire le perdite attese e inattese che derivano dai rischi operativi su un orizzonte temporale di un anno e con un livello di confidenza del 99,9% (CAR- Capital At Risk).

Figura 3: Loss Distribution Approach



Fonte: Cosma Simona (2007) – “La misurazione del rischio operative nelle banche”.

Per poter determinare la distribuzione aggregata il metodo indicato è il ricorso a delle tecniche di simulazione. Nell'analisi del rischio operativo il goal

principale è la determinazione della misura di capitale da dover allocare a ciascuna Business Unit per poter far fronte alle perdite inattese.

Questo processo non è nient'altro che la ricerca di modelli statistici che possano rappresentare al meglio le perdite che hanno impatti maggiori.

Il Comitato di Basilea ha dato la possibilità a coloro che utilizzano il LDA di poter usufruire di un requisito patrimoniale calcolato senza l'obbligo di rispettare un requisito di capitale minimo. Il metodo LDA, difatti, ha il vantaggio di una misurazione più puntuale e precisa dell'esposizione al rischio operativo.

Abbiamo poc'anzi introdotto gli approcci statistici che sono utilizzati nei metodi avanzati. Gli approcci statistici per quantificare il rischio operativo sono degli approcci che si scorgono tra le banche che stanno sviluppando dei metodi di misurazione del capitale distinti rispetto a quelli canonici, e che possono essere realizzati in due modi: *bottom-up* oppure *top-down*.

Gli approcci *top-down* sono caratterizzati dal fatto che il calcolo del valore dell'esposizione al rischio operativo sia eseguito da un ufficio centrale senza andar a coinvolgere le singole Business Line, e solo successivamente il calcolo lo si cerca di allocare a ciascun livello ricorrendo ad una proxy che ne stabilisca l'esposizione al rischio⁴².

Gli approcci, invece, *bottom-up* hanno come base l'analisi dei singoli processi di ogni unità operativa per poter identificare, classificare e infine valutare tutti i rischi a cui si è esposti. L'obiettivo di questo approccio è quello di procedere ad un mapping dei processi organizzativi, così da valutare il rischio insito in ogni area. Si procede, poi, approfondendo l'analisi dei rischi in aree più critiche e più d'impatto da un punto di vista strategico.

Con questo approccio si procede ad un'analisi *statistico-inferenziale* con l'obiettivo di poter individuare il requisito di capitale a livello dell'intera azienda e inoltre per le singole linee di attività.

I metodi *bottom-up* sono prediletti per l'allocazione del capitale in quanto si registra un elevato grado di soggettività nel processo, mentre i metodi *top-down* si prediligono nel periodo short quando non ci sono dati sufficienti per poter ricorrere al metodo *bottom-up* con un livello di confidenza elevato.

In ultimo abbiamo lo Scorecard Approach che nel calcolo del requisito patrimoniale impone alla banca diverse cose:

- Definire il capitale economico che deve far fronte al rischio operativo utilizzando metodi di stima simili a quelli già citati;
- Attribuire il capitale a ciascuna delle Business Unit sulla base del rispettivo profilo di rischio;

⁴² Esempi di proxy in questo caso sono dati contabili, dati di controllo di gestione oppure il valore di mercato dell'azienda.

- Individuare un numero di indicatori che siano in grado di esprimere tipi di rischio all'interno delle Business Line;
- Richiedere al personale di compilare periodicamente le scorecard così da usare i dati di perdita interna per poterli valutare;
- Sottoporre le scorecard ad una revisione e aggiustare il requisito patrimoniale richiesto rivedendo poi l'allocazione di quest'ultimo tra le diverse linee operative.

Avendo definito cosa impone alla banca è doveroso fissare i tratti distintivi dello Scorecard Approach successivamente all'averne individuato la definizione.

Lo scorecard approach, o approccio della scheda di valutazione, è una metodologia che viene utilizzata nelle istituzioni finanziarie per valutare e quantificare il rischio operativo all'interno di un'organizzazione.

Si articola in differenti fasi:

1. **Identificazione dei Fattori di Rischio:** la prima fase coinvolge l'identificazione dei fattori di rischio operativo che sono specifici per un'organizzazione, questi possono includere errori umani, frodi, problemi legali e regolamentari e altri eventi.
2. **Punteggio degli Indicatori di Rischio:** Identificati i fattori di rischio, si devono selezionare gli indicatori chiave di rischio (KRI, Key Risk Indicators, che approfondiremo successivamente) che possono essere misurati e monitorati nel tempo.
3. **Assegnazione dei Punteggi:** a ciascun indicatore di rischio viene assegnato un punteggio in base alla sua importanza e rilevanza per il rischio operativo complessivo dell'organizzazione. Un esempio da riportare, un indicatore di rischio che riguarda la frequenza degli incidenti può avere un punteggio più alto rispetto ad un indicatore meno critico.
4. **Calcolo dello Scorecard:** Il calcolo viene eseguito combinando i punteggi degli indicatori di rischio, sia con dei modelli statistici sia con modelli analitici. Il risultato sarà un punteggio che riflette il livello di rischio operativo dell'organizzazione in un dato periodo di tempo.
5. **Valutazione e Monitoraggio Continuo:** Creato la scorecard, lo si utilizza per valutare e monitorare il rischio operativo nel tempo.

Complessivamente i vantaggi della scorecard sono molteplici partendo dall'identificazione precoce dei rischi che aiuta ad identificare i potenziali rischi operativi in maniera precoce, ad una gestione proattiva del rischio che da' la possibilità di fornire una base per l'implementazione di azioni correttive e piani di mitigazione del rischio, oltre che rappresentare una valutazione oggettiva del rischio.

Per completare il discorso sui modelli AMA è necessario approfondire il sistema di misurazione dei rischi operativi, che per garantire affidabilità e solidità, è composto da quattro componenti principali:

- ⇒ Dati di perdita interni;
- ⇒ Dati di perdita esterni;
- ⇒ Dati generati da analisi di scenario;
- ⇒ Fattori del contesto operativo e del sistema dei controlli interni.

Il primo componente sono i **dati di perdita operativa interni**, che concorrono a determinare la base per la costruzione di un sistema di misurazione dei rischi operativi. L'holding period richiesto è con un minimo di cinque anni, o nel caso in cui si è in una fase di avvio dell'utilizzo degli AMA di tre anni, e si richiede di classificare tali anni in funzione delle otto Business Line e dei sette Event Type. Naturalmente non si vuole solamente censire l'importo delle perdite al lordo dei recuperi, ma i recuperi stessi, le date in cui si sono registrati gli eventi. Deve essere rispettata la completezza di dati sebbene l'intermediario debba individuare soglie minime di perdita⁴³ per comprendere da quale soglia a quale soglia indirizzarle alla raccolta dei dati interni.

Il processo di censimento e di classificazione di tutti gli eventi di rischio registrati con le rispettive perdite prende il nome di **Loss Data Collection, LDC**.

Il processo di Loss Data Collection nel rischio operativo è una fase cruciale della gestione del rischio operativo in cui un'organizzazione raccoglie, registra e analizza dati relativi alle perdite subite. Naturalmente questo è un processo che fornisce un quadro quanto più dettagliato delle perdite passate e ci permette di poter identificare le cause sottostanti.

La prima fase coinvolge l'identificazione delle fonti di dati da cui poter raccogliere informazioni sulle perdite: queste fonti includono report interni, registri di incidenti, reclami dei clienti, report di audit e altre fonti rilevanti⁴⁴.

⁴³ La definizione delle soglie dipende dalla gestione del rischio operativo che si prefissa di avere la realtà finanziaria ad oggetto. L'intermediario, però, deve comprovare che le soglie da lui individuate non escludono dei dati di perdita e che assicurano l'affidabilità e l'accuratezza (che devono essere sempre garantite) delle stime di rischio in ottica di perdite attese e inattese.

⁴⁴ Maggiori sono le fonti consultate e maggiore sarà la panoramica a disposizione per poter vantare di una raccolta quanto più esaustiva.

Si prosegue con la definizione dei tipi di perdite, una creazione di un Database per poter registrare tutte le informazioni sulle perdite⁴⁵.

Gli aspetti critici della LDC sono riconducibili ad una copertura limitata e ad una natura predittiva molto limitata e contenuta, tanto da richiedere l'affiancamento dei **dati di perdita esterni** a quelli interni.

Questa integrazione è indispensabile e necessaria specie per eventi *major*, o detti *Black Swan Events*⁴⁶, accrescendo il limite connesso alla scarsità dei dati disponibili.

Le principali fonti per dati esterni di perdite operative sono quelle fornite dall'insieme di banche e intermediari finanziari (abbiamo citato precedentemente l'Osservatorio DIPO a questo proposito), esempi ulteriori sono l'Operational Riskdata eXchange Association (ORX), Global Operational Loss Database (GOLD).

Il terzo elemento è l'**analisi di scenario** che insieme al quarto elemento, **i fattori di contesto operativo e del sistema di controllo interno**, rappresenta una valutazione di tipo qualitativo con l'integrazione poi della parte quantitativa per giungere all'Operational Var di cui parleremo successivamente.

Per poter valutare la propria esposizione agli eventi con una notevole gravità, la banca deve analizzare lo scenario basandosi in particolare su dei giudizi espressi da esperti.

I dati di scenario devono essere generati da un processo interno adeguato che deve considerare sia la dimensione del business bancario e sia il contesto socioeconomico in cui la banca è collocata.

Nel pratico l'analisi di scenario è caratterizzata da interviste ad esperti circa le varie Business Area e la gestione del rischio richiedendone giudizi su eventi dannosi gravi per cui la banca non dispone dati storici o comunque dati insufficienti.

Nel caso in cui non si disponga di dati, le segnalazioni esterne si integrano con le valutazioni di esperti così da poter ricostruire la distribuzione delle perdite mediante delle tecniche *Extreme Value Theory (EVT)*; nel caso di eventi molto rari, la stima delle cose estreme può avvenire con modelli **POT (Peaks Over Threshold)**, entrambi sono delle tipologie di modelli parametrici basati sulla Generalized Pareto Distribution.

Approfondiamo dunque questi due modelli poc'anzi citati partendo dall'EVT.

⁴⁵ Le informazioni possono essere relative alla struttura dati della perdita come: la data dell'evento, la descrizione dell'evento, il tipo di perdita, l'ammontare della perdita, cause e contromisure che sono state adottate.

⁴⁶ Ci si rifà alla "teoria del cigno nero". È una metafora che descrive un evento che si presenta come una sorpresa, ha un effetto importante; la teoria è stata sviluppata da Nassim Taleb per spiegare il ruolo sproporzionato di eventi di alto profilo che sono difficili da prevedere che vanno oltre normali aspettative. Cosa interessante da citare è che Taleb afferma che un evento di cigno nero dipende dall'osservatore ponendo questo esempio: quella che può essere una sorpresa del Cigno Nero per un tacchino, non lo è per il suo macellaio, ergo l'obiettivo dovrebbe essere "evitare di essere il tacchino" identificando le aree di vulnerabilità per poter rendere "bianchi i cigni neri".

Tale tecnica parte da una premessa secondo la quale l'interesse di un risk manager è concentrato sui valori estremi della distribuzione dei valori futuri, e nel dettaglio sulle grandi perdite. È importante quindi porre la massima attenzione per poter stimare in modo corretto la forma delle cose della distribuzione: ed è proprio in questo che ci aiuta la teoria statistica dei valori estremi.

Sebbene la distribuzione delle code estreme non sia conosciuta a priori, l'EVT constata che la distribuzione, nel caso in cui abbiamo un campione con un'ampiezza elevata, tende a convergere verso una distribuzione-limite con una forma funzionale: la Distribuzione di Pareto generalizzata.

Mediante questa constatazione, possiamo utilizzarla come appoggio per poter trovare analiticamente il VaR associato al livello di confidenza che si desidera. L'extreme Value Theory si basa sull'ipotesi che i rendimenti dei fattori di rischio siano i.i.d., cioè indipendenti e identicamente distribuiti⁴⁷; considera, inoltre, i rendimenti standardizzati, e_t , ottenuti dividendo i rendimenti r_t per una stima della loro volatilità.

$$e_t = \frac{r_t}{\sigma_t} \sim i. i. d.$$

Esistono due principali approcci alla stima delle distribuzioni dei valori estremi:

- i. L'approccio basato sui "picchi oltre una soglia" (*peaks over threshold, POT*);
- ii. L'approccio basato sui massimi a blocchi (*block maxima, BM*).

L'approccio POT si basa sull'osservazione secondo la quale, data una variabile casuale z , la distribuzione di probabilità cumulata delle perdite in eccesso $x=z-u$, rispetto ad una certa soglia superiore u , equivale a:

$$F_u(x) = pr [z \leq u+x | z > u]$$

Possiamo descriverla sotto delle condizioni generali con una distribuzione di Pareto generalizzata, per l'appunto. Questa distribuzione ha la seguente funzione di ripartizione:

$$G(x; \xi, \beta) = \begin{cases} 1 - \left(1 + \frac{\xi x}{\beta}\right)^{-\frac{1}{\xi}} & \text{se } \xi \neq 0 \\ 1 - e^{-\frac{x}{\beta}} & \text{se } \xi = 0 \end{cases}$$

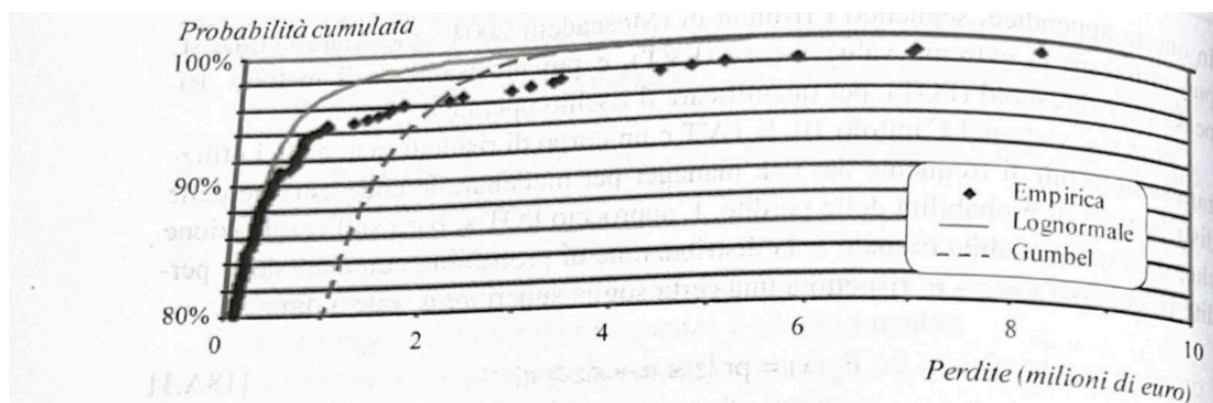
L'EVT risulta dunque molto efficace per poter trattare i dati relativi alle perdite operative; difatti, se si prova a modellare i dati tramite delle distribuzioni

⁴⁷ Sebbene sia noto che nel breve periodo questa ipotesi è violata dato che la varianza varia nel tempo.

standard, i risultati risultano totalmente insoddisfacenti quando si da' uno sguardo alle code estreme (cioè alla zona più di attenzione per un buon risk manager).

Di seguito si riporta un esempio dove le perdite di una businett unit, Corporate Finance, sono state interpolate con una distribuzione lognormale e con una Gumbel (che sarebbe un caso particolare della Generalized Extreme Value). Si nota che la probabilità associata alle perdite estreme risulta di molto sottostimata con il rischio di risultati poco soddisfacenti in ottica di misurazione e gestione del rischio operativo.

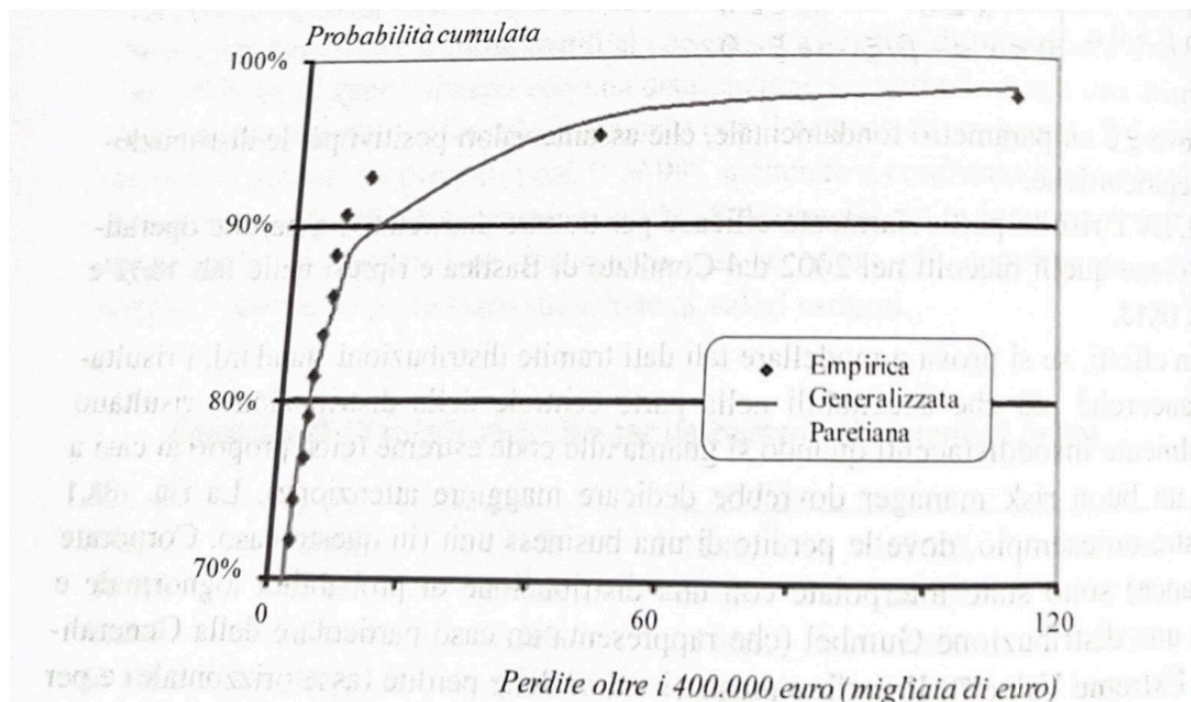
Figura 4 Perdite effettive e interpolate con le distribuzioni lognormale e Gumbel



Fonte: Moscadelli (2004)

Distintamente con il ricorso all'EVT può migliorare la qualità della stima. Successivamente alla fissazione di un u abbastanza elevato affinché l'equazione possa essere ritenuta valida, i valori di σ e ξ è possibile stimarli per massima verosimiglianza, così da poter inserire la funzione generalizzata paretiana che approssima al meglio la coda della distribuzione delle perdite.

Figura 5 Perdite in eccesso effettive e interpolate con una Generalised Pareto Distribution



Fonte: Moscadelli (2004)

Il caso della seconda immagine è quello della medesima linea di Business della precedente. E' evidente come con la seconda immagine si sia ottenuta una rappresentazione migliore dei casi estremi così da poter ricavare diverse misure di perdita inattesa.

E' proprio Moscadelli che in tale lavoro di confronto suggerisce "il median shortfall", cioè la mediana delle osservazioni che si trovano oltre la soglia u ; questo indicatore, distintamente dall'expected shortfall, ha il vantaggio di essere calcolabile anche quando la varianza della distribuzione dei valori sulla coda non è finita.

Infine, vi è l'approccio dei massimi a blocchi, **Block Maxima (BM)**, che prevede che la serie storica dei dati dei rendimenti standardizzati sia divisa in un numero M di sottocampioni ciascuno con una numerosità N abbastanza elevata, così da estrarre da ciascuno il suo valore massimo.

Per concludere possiamo constatare che in entrambe le varianti (POT e BM), l'EVT dà la possibilità di focalizzare attenzione sulle code, oltre a consentire un'analisi separata su ognuna di esse senza dover richiamare l'ipotesi di simmetria.

Analisi di Scenario e Stress Testing

I classici approcci di simulazioni come la simulazione storica e la simulazione Monte Carlo hanno l'obiettivo di generare un numero molto ampio di scenari così da poter approssimare l'intera distribuzione degli eventi possibili.

Un'alternativa è quella che si basa sulla stima degli effetti in ottica di perdite potenziali che sono connesse a eventi estremi.

In altri termini, il valore delle proprie posizioni viene rivalutato alle condizioni di scenari estremamente pessimistici determinandone la perdita.

Queste *prove di carico (stress test)* hanno in comune la logica dei modelli di simulazione dato che si basano su una rivalutazione in corrispondenza di circostanze simulate, anche se distintamente non replicano in modo del tutto realistico le possibili variazioni, ma le arbitrano in modo arbitrario assumendone le variazioni peggiori.

Le prove di stress sono uno strumento che ha l'obiettivo di identificare e gestire le situazioni che possono causare delle perdite straordinarie.

La costruzione degli scenari estremi può essere basata sui seguenti elementi:

- a. Sulla replica dei più forti shock di mercato che si sono registrati nel passato;
- b. Su misure di natura statistica;
- c. Su ipotesi completamente soggettive.

Il primo criterio è quello più diffuso; si basa su una rivalutazione delle proprie posizioni simulando degli shock nelle medesime proporzioni registratesi in passato.⁴⁸

Il secondo approccio è tipico delle tecniche di *factor push analysis (FPA)*, che lasciano il suggerimento di "spingere" i fattori di mercato verso la direzione più sfavorevole di un valore pari ad un certo N di volte la relativa deviazione standard, e di calcolare poi l'effetto combinato di tutte le variazioni avverse.

La FPA presenta il vantaggio di identificare il peggior evento possibile che genera la perdita più consistente così da permettere una più facile individuazione dei fattori più vulnerabili.

Il terzo approccio, invece, è stato in primo luogo adottato dal Derivatives Policy Group (DPG) che nell'anno 1995 ha reso pubblici degli esempi di ipotesi soggettive che possono guidare le prove di stress ed essere di aiuto alle singole istituzioni finanziarie nell'identificazione di casi di vulnerabilità nei confronti di variazioni di uno o più fattori di mercato.

Le prove di stress proposte dal DPG sono, però, unidimensionali: i fattori di mercato sono stressati singolarmente andando a non analizzarli congiuntamente e andando ad escludere un'eventuale correlazione tra i differenti fattori di mercato.

Alternativamente vi sono delle prove multidimensionali: si basano sulla simulazione congiunta di variazioni di più fattori di mercato.

⁴⁸ Esempi sono il crollo dei mercati azionari dell'ottobre 1987, del settembre 2001, ancora della crisi russa dell'agosto del 1998 e tanti ancora.

Indispensabile è dire che le prove di stress non devono essere una modalità di determinazione del VaR. Queste si fondano su delle ipotesi soggettive per quanto concerne la dimensione degli shock dei fattori di mercato, non permettono di poter effettivamente associare alla perdita una dimensione probabilistica, o un livello di confidenza; ragion per cui le prove di stress dovrebbero integrare un modello VaR piuttosto che sostituirlo.

L'integrazione è importante perché i modelli VaR sono fondati su dati storici recenti e non riescono a cogliere gli eventi estremi che si verificano con una frequenza limitata. Questo utilizzo complementare è, difatti, suggerito anche dagli stessi organi di vigilanza: è esplicitamente richiesto dal Comitato di Basilea alle banche che sono intenzionate ad adottare i propri modello interni di risk management per determinare il requisito patrimoniale obbligatorio.

IV. Limiti e Criticità nel quantificare i Rischi Operativi

Limiti e criticità dei modelli che vengono utilizzati

I modelli che abbiamo trattato in precedenza rappresentano certamente un corpus di tecniche utile e promettente. Tuttavia, la loro applicazione risulta limitata da una serie di ostacoli.

In particolare:

- Le basi di dati disponibili sono spesso molto limitate (s'intende in termini di numero di anni coperti e di variabili che è possibile avere nell'archivio) e di cattiva qualità, cioè non del tutto affidabili. Tale scarsità di dati è decisamente preoccupante, in quanto alcuni dei risultati teorici che vengono utilizzati per modellare le perdite operative (come, ad esempio, l'Extreme Value Theory) hanno un valore asintotico, cioè diventano del tutto affidabili solamente se sono applicati ad un campione significativo in termini di dimensione;
- E' problematico poter definire in maniera obiettiva e generica i control environment factors che sono utilizzati per poter rappresentare i fattori di rischio da cui, come abbiamo già visto, dipende il rischio operativo;

- Diventa molto complessa e incerta la stima del grado di correlazione e di dipendenza tra le categorie di perdite, data la difficoltà nel misurare formalmente la dipendenza delle diverse categorie di perdite operative dai fattori di rischio. Senza la stima del grado di correlazione non è possibile integrare in modo corretto le categorie di perdite e poter stimare il VaR della banca a fronte del rischio operativo.

Per poter ovviare a queste problematiche, e sempre in attesa di poter affinare le tecniche e i dati necessari per poter misurare il rischio in modo oggettivo, molte banche hanno introdotto dei sistemi di valutazione soggettiva della propria vulnerabilità alle perdite operative, sistemi che prendono il nome di **sistemi di self-assessment**.

I sistemi di self-assessment nel rischio operativo sono degli strumenti cruciali che consentono alle istituzioni finanziarie di poter identificare, valutare e gestire in maniera del tutto autonoma i propri rischi finanziari. Questi sistemi si basano sull'autovalutazione da parte di ciascuna singola unità operativa, che sono posizionate adeguatamente nel comprendere i rischi specifici che possono essere associati alla loro attività. Andremo ad affrontare nel dettaglio, nel prossimo capitolo, tali sistemi che attengono alla gestione del rischio proattiva.

Numerosi limiti e punti critici sono stati individuati anche post Accordo del 2004, che come ben sappiamo ha fornito i tre approcci principali per la quantificazione dei rischi operativi e per la determinazione dei requisiti patrimoniali corrispondenti.

Una prima critica parte dalla considerazione che il rischio operativo, distintamente dal rischio di mercato e dal rischio di credito, è un rischio tipicamente idiosincratICO⁴⁹, e non sistemico. Un ribasso generalizzato dei mercati azionari o obbligazionari può condurre a delle perdite rilevanti per un numero ingente di istituzioni finanziarie, mettendo così a repentaglio la stabilità dell'intero sistema; allo stesso modo, un aumento dei tassi di default delle imprese che è connesso al deteriorarsi del ciclo economico colpisce l'intero settore bancario, andandone a pregiudicare l'equilibrio.

Al contrario, nella circostanza del rischio operativo le perdite sono riconducibili a fattori specifici di una singola banca, fattori come infedeltà dei dipendenti, responsabilità legale verso terzi e così via, e non vanno dunque a contagiare le altre istituzioni.

⁴⁹ Per rischio idiosincratICO, o anche rischio specifico, s'intende un tipo di rischio che riguarda esclusivamente un singolo individuo, azienda o asset piuttosto che l'intero mercato o settore. Il rischio idiosincratICO non presenta alcuna correlazione con i movimenti generali del mercato, per cui mentre il mercato può scendere o salire, il rischio idiosincratICO può comportare variazioni positive o negative indipendentemente dalla tendenza di mercato. Fortunatamente, però, dispone di un grande vantaggio: può essere ridotto o eliminato attraverso la diversificazione. Molto utili per poter coprire specifici rischi idiosincratICI sono i derivati, come opzioni e futures, o anche l'acquisto di polizze assicurative per poter coprire eventi che rappresentano rischi idiosincratICI, come polizze contro interruzioni operative o perdite da frode.

Ne consegue che il rischio operativo mette a repentaglio la sopravvivenza dei singoli intermediari, ma non la stabilità complessiva del sistema: poiché è quest'ultima che rappresenta il bene che gli organi di vigilanza sono interessati a tutelare, molti critici non hanno ben compreso il motivo per il quale sia necessario imporre uno schema di requisiti patrimoniali sul rischio operativo.

Una seconda critica è stata avanzata dall'International Swaps and Derivatives Association (ISDA), si fonda sull'enorme difficoltà che si affronta nel voler misurare in modo adeguato e oggettivo questa tipologia di rischio. Siamo ben consapevoli del fatto che lo stato di avanzamento dei modelli sia ancora molto arretrato, al punto che il Comitato di Basilea nel 2004 non ha saputo indicare i contenuti di un modello avanzato, e si è dovuto limitare a dover prescrivere una serie di requisiti minimi molto generici. Ne consegue, dunque, che il requisito associato a tale rischio potrebbe essere poco preciso e scarsamente efficace.

Una terza critica riguarda le possibili conseguenze negative di un requisito patrimoniale a fronte del rischio operativo. Difatti, se il management della banca ritiene che tale rischio sia già coperto mediante un'apposita porzione di patrimonio minimo regolamentare, potrebbe dedicare una minore attenzione alle innovazioni di processo che hanno l'obiettivo di ridurlo e renderlo meno pericoloso.

La quarta critica riguarda l'approccio dell'indicatore base e l'approccio standard, che, come abbiamo approfondito nei capitoli precedenti, commisurano la copertura patrimoniale al margine d'intermediazione della banca. Questa base di calcolo risulta decisamente imprecisa: non vi è motivo alcuno per cui una banca con un margine d'intermediazione più elevato sia anche caratterizzata da un grado di rischio operativo maggiore.

Differentemente, è possibile che una banca sia più redditizia grazie ad un sistema gestionale molto più efficiente e responsabile, che genera dei rischi operativi minori: il paradosso vuole che ad una simile banca venga imposto, nell'approccio dell'indicatore base e in quello standardizzato, un requisito patrimoniale più elevato.

Inoltre, la scelta di commisurare il requisito patrimoniale alle dimensioni della banca non sembra aver alcun fondamento empirico.

Nomi noti come Shi, Samad-Khan e Medapa hanno mostrato come la variabilità delle perdite connesse al rischio operativo sia solo in minima parte spiegata da variabili dimensionali come il totale dell'attivo, i ricavi complessivi o il numero di dipendenti.

La scelta del margine d'intermediazione come base di riferimento fa sì che i requisiti patrimoniali sul rischio operativo, distintamente rispetto a quanto accade per il rischio di credito e di mercato, non incentivino le banche a ridurre i rischi in essere.

Una banca che desideri risparmiare patrimonio può, ponendo un esempio, diminuire il proprio requisito patrimoniale sul rischio di credito prestando a clienti con Probability of Default più basse o richiedendo delle maggiori

garanzie: in maniera analoga, la banca può ridimensionare il capitale regolamentare sui rischi di mercato, per esempio, riducendo la duration dei titoli obbligazionari in portafoglio.

Al contrario, nel caso degli approcci dell'indicatore base e standardizzato l'unico modo per ridurre il requisito patrimoniale sul rischio operativo è ridurre il margine d'intermediazione della banca, cioè produrre meno e guadagnare di meno.

Più con una visione generale, gli approcci dell'indicatore base e standardizzato sono stati ampiamente criticati, specialmente da parte delle associazioni di categoria delle banche, per la loro logica top-down che calcola il requisito patrimoniale partendo dal margine d'intermediazione della banca intera o di un'intera business line. Questo approccio è ritenuto poco soddisfacente perché non dà alcun incentivo alle banche nel migliorare il proprio sistema di controllo interno, non fornisce alcuna indicazione per quanto concerne le cause del rischio operativo e di conseguenza non supporta le azioni di contenimento del rischio, non è di aiuto per le banche nell'identificazione di eventuali politiche di trasferimento a terzi del rischio insito in determinati processi aziendali.

Oltre alle critiche che sono state esplicitate ampiamente dalla comunità finanziaria, la normativa in materia di rischi operativi suscita altre perplessità.

In primo luogo, il livello di confidenza del 99,9% prescritto negli approcci avanzati risulta essere molto elevato: tale livello corrisponde ad una probabilità d'insolvenza dell'1 per mille, e naturalmente ci si chiede se sia mai esistita un'impresa sopravvissuta per mille anni effettivi.

Si potrebbe anche obiettare che un livello di confidenza analogo è richiesto anche per il rischio di credito, sebbene vi siano due differenze rilevanti che rendono un caso a sé quello del rischio operativo:

- i. Mentre il rischio di credito ha una natura sistematica, il rischio operativo è prevalentemente idiosincratice; questo comporta che, mentre nel caso del rischio di credito un livello di confidenza elevato corrisponde alla necessità di evitare fenomeni di contagio e di dissesto generalizzato, nel caso del rischio operativo anche un livello di confidenza più basso potrebbe risultare accettabile e adattabile con la stabilità complessiva del sistema bancario;
- ii. Con la scelta di adottare un livello di confidenza del 99,9% nel caso del rischio operativo, significa includere, tra gli eventi che è indispensabile coprire con capitale degli azionisti, anche le catastrofi naturali la cui probabilità di accadimento è estremamente limitata e le cui conseguenze, in termini di perdite e di capitale richiesto per fronteggiarle, sono particolarmente rilevanti (*eventi low frequency high impact, LFHI*). Difatti una banca è difficilmente in grado di poter coprire questo tipo di evento attingendo dal capitale proprio, mentre sembra essere molto più

conveniente il ricorso a forme di copertura assicurativa: i rischi di natura catastrofica sono difatti ampiamente diversificabili e dunque attraenti per le imprese di assicurazione.

In secondo luogo, è molto discutibile il fatto che il requisito patrimoniale complessivo debba essere calcolato come la somma dei requisiti patrimoniali relativi a linee di business diverse. Questa regola (che ha valenza per l'approccio standardizzato e, in assenza di stime rigorose e affidabili delle correzioni, anche per gli approcci avanzati) elimina qualsivoglia incentivo alla diversificazione produttiva.

Difatti in assenza di stime che sono relative alle correlazioni sarebbe più corretto calcolare il requisito patrimoniale complessivo ipotizzando che le diverse business line siano indipendenti e non perfettamente correlate.

A posteriori a tale dibattito possiamo visionare dei dati per comprendere effettivamente quali sono gli approcci più utilizzati dalle banche.

L'European Banking Authority mette a disposizione il resoconto circa l'utilizzo delle differenti metodologie di calcolo dei requisiti patrimoniali per far fronte al rischio operativo, utilizzate dalle banche e dagli intermediari finanziari europei.

- **BIA:** Utilizzato da circa il 20% delle banche europee, principalmente istituti di credito di dimensioni ridotte.
- **SA:** Adottato da circa il 50% delle banche, questo metodo offre un buon compromesso tra semplicità e accuratezza.
- **AMA:** Utilizzato dal 30% delle banche, prevalentemente grandi istituti con operazioni internazionali e infrastrutture sufficientemente robuste per supportare modelli complessi.
- **Stress Testing:** Integrato in vari gradi nei modelli delle banche, con un'attenzione crescente in seguito alle crisi finanziarie recenti, che hanno evidenziato l'importanza di una gestione proattiva del rischio operativo.

Le scelte tra questi approcci dipendono dalla dimensione della banca, dalla complessità operativa, e dalle risorse disponibili per sviluppare e mantenere modelli di rischio. Le regolamentazioni attuali favoriscono un approccio più sofisticato per le banche più grandi, mentre permettono approcci più semplici per istituti più piccoli, bilanciando la necessità di robustezza del capitale con la capacità operativa delle banche stesse.

Possiamo fare un confronto decennale con i valori che l'EBA⁵⁰ pubblicò e diffuse ben 10 anni fa, nel 2013, per comprendere come il trend sia potuto mutare.

| | | IT | GB | DE |
|--|-----|--------|--------|--------|
| Percentuale del numero banche | BIA | 88,20% | 65,70% | 96,77% |
| | SA | 5,41% | 32,30% | 2,35% |
| | AMA | 6,39% | 1,50% | 0,94% |
| Percentuale di requisito patrimoniale calcolato | BIA | 34,94% | 17,90% | 43,92% |
| | SA | 20,31% | 63,10% | 19,24% |
| | AMA | 44,76% | 19,00% | 36,84% |

Fonte: European Banking Authority

È possibile notare che la metodologia più utilizzata nel lontano 2013 fosse quella Basic, considerando però non tanto il numero delle banche come misura di riferimento, ma l'ammontare complessivo del requisito patrimoniale che veniva richiesto per ciascuna nazione, ed è possibile osservare come la situazione tende a modificarsi.

In Italia l'88,20% delle istituzioni bancarie di dimensione ridotta che ricorrevano alla metodologia BIA rappresentano il 34,94% in termini di requisito patrimoniale operativo nazionale calcolato.

Il complesso dei valori che sono stati riportati risalenti a circa un decennio fa è rappresentativo del fatto che l'utilizzo dei diversi approcci sia grossomodo equilibrato, nonostante si possa notare le difficoltà delle piccole banche nell'utilizzo degli approcci avanzati a causa delle loro caratteristiche.

⁵⁰ L'Autorità Bancaria Europea (EBA) è un'agenzia indipendente dell'UE istituita nel 2011. La sua missione principale è quella di assicurare un livello elevato di regolamentazione e supervisione principale in tutta l'Unione Europea, al fine di garantire l'integrità, l'efficienza e il funzionamento ordinato del settore bancario. I principali compiti che svolge sono numerosi:

- Sviluppo di Norme Regolamentari: l'EBA elabora standard tecnici di regolamentazione (RTS) e standard tecnici di attuazione (ITS) che diventano giuridicamente vincolanti dopo l'adozione da parte della Commissione Europea. Tali standard coprono diversi aspetti della regolamentazione bancaria, tra cui i requisiti patrimoniali, la gestione del rischio e la trasparenza;
- Promozione dell'Uniformità delle prassi di vigilanza: l'EBA lavora per armonizzare le pratiche di vigilanza tra le autorità nazionali di vigilanza bancaria;
- Monitoraggio dei Rischi e Vulnerabilità del Settore Bancario: l'EBA conduce diverse valutazioni periodiche sui rischi e le vulnerabilità del settore bancario, pubblicando relazioni come il Risk Assessment Report e conducendo degli stress test su base regolare.

Fattori che possono influenzare la precisione nelle stime

Per poter comprendere al meglio quali sono i fattori che possono influenzare le stime e la loro precisione, bisogna approfondire il discorso delle strutture di dipendenza e delle correlazioni tra gli eventi di rischio, che come ben sappiamo concorrono alla formazione delle stime.

Mediante gli approcci AMA, le banche calcolano e determinano il requisito patrimoniale per far fronte al rischio operativo, come l'ammontare delle perdite che si possono registrare in un anno con un dato livello di confidenza del 99.9%.

Siamo consci del fatto che le perdite operative di un'istituzione bancaria scaturiscono da eventi di perdita molto etero variegati tra di loro, che si registrano in aree distinte di attività, e dunque l'ammontare totale che comprende queste perdite bisogna calcolarlo mediante un modello che sia in grado di considerare tutte le varie categorie e sottocategorie che lo compongono.

Il metodo più idoneo è quello basato sull'approccio LDA, che deve essere in condizioni favorevoli per calcolare le distribuzioni di perdita aggregata tenendo in considerazione le stime precedenti delle distribuzioni di frequenza e di impatto, nelle più disparate combinazioni di "Event Type" e "Business Line", per poi combinarle in una stima della distribuzione di perdita operativa totale per l'intero contesto della banca.

È un aspetto molto complicato quello inerente al processo di comprensione accurata dei gradi di dipendenza tra le perdite nelle varie classi di rischio. Difatti, se si ipotizza che esista una correlazione perfetta tra le perdite delle differenti aree di attività, si può pensare che, se si registra un evento negativo in un'area, dunque un altro evento si realizzerà in un'altra area. Distintamente, se le perdite sono indipendenti, si può asserire che eventi pregiudizievoli non si registrino in modo simultaneo in più Business Line.

Il contesto normativo, difatti, riconosce la possibilità di considerare eventuali correlazioni che possano esistere tra le perdite di natura operativa delle

differenti business line e event type. Per poter applicare tale possibilità, la banca deve dimostrare all'Autorità di Vigilanza che le metodologie utilizzate per stimare la correlazione sono robuste e in grado di riflettere l'incertezza che talvolta può caratterizzare queste stime nei periodi di stress.

Come abbiamo visto in precedenza l'applicazione della LDA ci permette di poter quantificare il rischio operativo basandosi sui dati di perdita interni identificati, e non a caso è uno dei metodi più utilizzati.

La distribuzione di perdita operativa complessiva in un'istituzione bancaria per un determinato periodo di tempo (convenzionalmente un anno) si articola in tre passaggi:

1. **Primo step:** Caratterizzare la distribuzione di impatto e di frequenza delle perdite per ciascuna unità che si considera, dunque si vanno a combinare le aree di attività con ciascun Event Type;
2. **Secondo step:** Si deriva la distribuzione aggregata delle perdite per ogni unità di misura;
3. **Terzo step:** Si combinano tutte le distribuzioni di perdita di tutte le unità che si considerano, per giungere poi ad una stima della distribuzione perdita totale della banca, o comunque alla determinazione di determinati quantili della distribuzione.

Per poter determinare e calcolare il quantile che viene richiesto nella distribuzione di perdita totale annuale vi è un metodo che consiste nel sommare i singoli quantili stimati per ciascuna distribuzione di perdita di unità assumendo una perfetta correlazione tra le varie distribuzioni.

Per ovviare a questo passaggio, spesso la banca può introdurre dei modelli che esplicitano le correlazioni da dover inglobare all'interno della metodologia LDA. Sebbene vi siano differenti modi, i principali ne sono tre:

- **1° Metodo:** in questo metodo si considera una dipendenza direttamente sulla distribuzione di frequenza relativa a ciascuna unità considerata all'interno della banca;
- **2° Metodo:** nel secondo metodo andiamo a considerare di base che gli importi delle perdite nelle varie unità di misura sono correlati, sia attraverso un diretto modello di dipendenza o mediante l'introduzione di uno shock comune di perdita che interessa differenti unità di misure simultaneamente;
- **3° Metodo:** qui le dipendenze vengono introdotte solamente a livello di perdite aggregate per ogni unità di misura.

Il primo e il terzo metodo sono di solito quelli più utilizzati sia per la loro semplicità nell'implementazione, sia perché risulta complesso poter formulare un modello coerente che riesca a definire le dipendenze a livello del loro ammontare per ciascuna unità.

Le misurazioni della correlazione sulla frequenza sono per questa ragione utilizzate per la derivazione di modelli di correlazione a livello di perdita aggregata, assumendo alla base l'indipendenza degli importi.

Si sono susseguiti diversi autori che hanno avanzato proposte di modelli in cui la correlazione è introdotta esclusivamente a livello aggregato, altri si sono a lungo dibattuti per comprendere se fosse corretto o meno considerare o no gli effetti della mitigazione assicurativa, la quale potrebbe aggiungere altri livelli di dipendenza che risulterebbe complicato da modellare con l'applicazione diretta di una copula⁵¹ o di un modello di correlazione.

Quando parliamo di correlazione possiamo trattarla in diverse maniere, prima tra queste è discutere della correlazione in serie.

La correlazione in serie fa riferimento alla correlazione che c'è all'interno di una stessa unità di misura andandola a considerare per più periodi di tempo successivi, dunque non considerando le perdite di natura differente.

Varie considerazioni similari sostengono che effettivamente le dipendenze che ci sono all'interno di una stessa classe di rischio dovrebbero essere teoricamente superiori rispetto alle dipendenze tra classi diverse.

Le perdite nella stessa combinazione di Business Line e di Event Type hanno le medesime influenze provenienti dagli stessi processi interni e dalla stessa struttura di gestione, oltre a realizzarsi all'interno dello stesso ambiente lavorativo.

Nomi di studiosi come Eric Cope e Gianluca Antonini hanno riconosciuto che per modellare adeguatamente le dipendenze in serie tra le distribuzioni di frequenza potesse essere utile ricorrere all'utilizzo della distribuzione Binomiale Negativa, o anche una distribuzione di Poisson non omogenea.

Abbiamo citato il termine "dipendenza", e per questa citazione è necessaria una trattazione a sé.

La dipendenza è un concetto ancora più ampio della correlazione in quanto coglie dipendenze differenti rispetto a quella lineare solamente; ad esempio, due rischi possono essere dipendenti sebbene non siano correlati. Nel caso si decida di ricorrere al LDA, si disporrà per ogni tipo di rischio operativo e di Business Line l'intera distribuzione di perdita annuale, e per tale distribuzione sarà possibile prendere in considerazione delle dipendenze diverse oltre che delle correlazioni tra i rischi operativi.

Lo strumento che ci permette di considerare tutti i legami tra i rischi che appartengono a ciascuna unità di misura che consideriamo, è la funzione copula citata precedentemente.

La funzione copula esprime le relazioni che esistono tra distribuzioni univariate di ogni unità e la distribuzione multivariata connessa. Nei vari

⁵¹ Una copula è una funzione matematica utilizzata nella gestione del rischio per poter descrivere la dipendenza tra variabili casuali. In ambito finanziario, le copule sono particolarmente utili per modellare e analizzare la correlazione tra diverse fonti di rischio. Le copule permettono di separare la struttura di dipendenza tra variabili dalle distribuzioni marginali di queste variabili. Questo sta a significare che si può modellare la relazione tra variabili senza dover necessariamente fare assunzioni specifiche sulle distribuzioni di ciascuna variabile.

studi, una varietà di funzioni copule è stata ideata e progettata per catturare gli aspetti specifici della distribuzione congiunta, come le relazioni di dipendenza sulle code.

La Copula è una funzione che lega le distribuzioni marginali univariate di variabili casuali alla sua relativa distribuzione multivariata.

Se ad esempio u_1, u_2, \dots, u_d sono i valori di N funzioni di ripartizione univariate, dunque una Copula è una funzione $C(u_1, u_2, \dots, u_d) \rightarrow [0,1]$: questo ci consente di esprimere tutti i legami possibili tra due o più variabili come la correlazione, cograduazione, concordanza e così via dicendo, e descrivere la struttura di dipendenza quanto più precisamente.

Il termine cograduazione si riferisce alla proprietà di due o più variabili casuali di avere le stesse graduazioni marginali, cioè le loro distribuzioni cumulative sono uguali. Tale proprietà implica che le variabili abbiano la stessa distribuzione marginale, il che è un aspetto molto rilevante nel momento in cui si utilizzano copule per modellare le dipendenze tra variabili.

Le copule sfruttano il concetto di cograduazione per rappresentare le dipendenze tra variabili casuali, ciononostante vi sono dei vantaggi e delle limitazioni. I vantaggi di cui vanta la cograduazione sono due:

- **Modellazione flessibile:** separando le distribuzioni marginali dalla struttura di dipendenza, le copule permettono una modellazione più flessibile delle dipendenze tra variabili;
- **Analisi delle dipendenze estreme:** sono molto efficaci nel catturare le dipendenze nelle code delle distribuzioni, andando a migliorare la gestione del rischio di eventi estremi.

Naturalmente presenta anche delle limitazioni, che, come i vantaggi, sono due:

- **Calibrazione Complessa:** la calibrazione delle copule richiede dei dati adeguati e può essere molto complessa, richiedendo strumenti statistici avanzati;
- **Comprensione e Implementazione:** ambedue le funzioni richiedono delle competenze avanzate che possono spesso rappresentare una barriera per alcuni praticanti.

Lo studio che viene fatto della dipendenza tra le varie tipologie di rischio, e dunque tra le variabili casuali X_{ij} che rappresentano le perdite annuali della Business Line "i" e dell'event type "j", risulta completamente indipendente rispetto alla forma delle singole distribuzioni prese individualmente. Così facendo si possono superare le ipotesi che ne semplificano i modelli classici ed è possibile, inoltre, mediante le funzioni copula sottolineare caratteristiche rilevanti delle variabili che vengono studiate, aspetti come l'asimmetria e la leptocurtosi⁵².

⁵² La leptocurtosi è un termine statistico utilizzato per descrivere una caratteristica specifica della distribuzione di probabilità di una variabile casuale. Specificamente si riferisce ad una distribuzione che presenta delle code più spesse e un picco più alto rispetto alla distribuzione normale. La leptocurtosi si caratterizza per delle Code Spesse, che stanno a significare che gli eventi estremi sono più probabili in una distribuzione leptocurtica; per dei Picchi Elevati, in quanto

Dovendo applicare, dunque, il meccanismo di aggregazione delle perdite individuali tenendo conto della struttura di dipendenza tra le diverse perdite, è indispensabile individuare esattamente la struttura di dipendenza che lega le variabili che bisogna aggregare e solo in un momento successivo andare a scegliere la giusta funzione copula che ne possa cogliere la struttura di dipendenza che intercorre tra le due perdite operative.

Una soluzione ottimale per questo processo fu proposta da Alexander nel 2003, quando propose di esaminare il comportamento dei rischi al variare di fattori comuni tra loro. L'obiettivo era quello di poter esaminare le variazioni di alcuni "Key Risk Indicator" al mutare di alcuni "Key Risk Driver"⁵³: se alcune categorie di rischio operativo sembrano essere influenzate dai KRD in questione e si registra una variazione simile di segno, allora la struttura di dipendenza di tali rischi può considerarsi positiva, se invece la variazione ha segno positivo per una parte di rischi e l'altra parte registra il segno negativo, la struttura di dipendenza sarà negativa.

Lo studioso Cosma a tal proposito ha proposto un esempio in cui si considera un cambiamento nelle politiche di gestione previste all'interno di un'istituzione bancaria per l'anno successivo (dunque parliamo di una variazione che si induce nei Key Risk Driver) e si procede alla valutazione dell'effetto probabile che si può avere sui KRI delle differenti tipologie di rischio operative.

Supponiamo che una banca preveda per l'anno seguente di: attuare un ridimensionamento del personale di back office, di sviluppare dei prodotti più articolati inserendo un team di esperti ed esternalizzare, oltre che migliorare, i sistemi informatici.

Si propongono di seguito i risultati dell'analisi sottolineando che una variazione sfavorevole del rischio (cioè un aumento) si manifesta con il segno "+" mentre una variazione favorevole (cioè con una diminuzione) con il segno "-".

indica che c'è una maggiore frequenza di valori vicini alla media rispetto alla distribuzione normale. La leptocurtosi è misurata dal coefficiente di kurtosi. Una distribuzione normale ha un coefficiente di kurtosi pari a 3; se una distribuzione ha un coefficiente di kurtosi maggiore di 3, allora è considerata leptocurtica. Il coefficiente di kurtosi si calcola come: $Kurtosi = \frac{E[(X-\mu)^4]}{\sigma^4}$.

⁵³ I Key Risk Drivers sono i fattori sottostanti ai KRI che influenzano i rischi aziendali. Identificare tali fattori aiuta a comprendere meglio da dove derivano i rischi e quali sono le cause principali che li alimentano. Ad esempio, per una società di trasporto, i Key Risk Drivers potrebbero includere la sicurezza delle infrastrutture, i costi del carburante e le normative governative.

| Event Type | Ridimensionamento del personale | Sviluppo di prodotti complessi | Esternalizzazione e miglioramento di sistemi IT | Variazione complessiva |
|---|---------------------------------|--------------------------------|---|------------------------|
| 1) Frode interna | + | + | - | + |
| 2) Frode esterna | + | 0 | - | 0 |
| 3) Rapporto di impegno e sicurezza sul lavoro | + | 0 | + | + |

| | | | | |
|--|---|---|---|----------|
| 4) Clientela, prodotti e prassi operative | 0 | + | 0 | + |
| 5) Danni alle strutture fisiche | 0 | 0 | 0 | 0 |
| 6) Interruzioni dell'operatività e disfunzioni dei sistemi informatici | 0 | + | - | 0 |
| 7) Esecuzione, consegna e gestione dei processi | + | + | + | + |

Fonte: Cosma (2008)

Ciò che è possibile notare è l'effetto complessivo per ogni rischio e andare a concepire come dipendenti quei rischi che subiscono una variazione complessiva uguale o allo stesso modo contraria. Ovviamente viene fornita ogni valutazione effettuata per ciascuna variazione teorica riportata, tutto dovuto alle tre decisioni gestionali.

È stato sostenuto che, ad esempio, lo sviluppo di prodotti complessi e l'inserimento di un nuovo team di esperti quantitativi potesse incrementare il numero e anche la gravità delle frodi interne. Il ricorso ad un uso di sistemi nuovi e anche molto più complessi può aumentare il rischio di eventuali disfunzioni ed errori attinenti al sistema informativo.

In via generica possiamo constatare che una variazione complessiva analoga⁵⁴ delle varie tipologie di rischio che subiscono un'influenza dagli shock sui medesimi Key Risk Driver, fa comprendere l'esistenza di una struttura positiva di dipendenza tra questi, differentemente una variazione complessiva inversa suggerisce una struttura negativa di dipendenza.

Nel caso in cui dovesse esserci incertezza o assenza di variazioni complessive dei KRI, si suggerisce una relazione di indipendenza tra questi.

Questa metodologia ci permette di comprendere i fattori e l'effetto di differenti politiche di gestione sulle diverse tipologie di rischio.

V. Strategie di Gestione e Mitigazione del Rischio Operativo

Gestione Proattiva

Introdurre il concetto di "gestione proattiva" all'interno del contesto delle strategie di gestione e mitigazione del rischio operativo implica anticipare e affrontare le sfide potenziali prima che si trasformino in problemi reali. In un mondo aziendale sempre più complesso e dinamico, adottare un approccio proattivo diventa cruciale per garantire la continuità operativa e ridurre al minimo gli impatti negativi derivanti da eventi imprevisti. La gestione proattiva non si limita alla semplice risposta agli incidenti, ma piuttosto si concentra sull'identificazione precoce dei rischi, sull'implementazione di misure preventive e sulla creazione di una cultura organizzativa orientata alla prevenzione e alla prontezza. Questo approccio non solo permette alle aziende di anticipare e gestire meglio le situazioni di crisi, ma contribuisce anche a promuovere la resilienza aziendale e a mantenere un vantaggio competitivo nel mercato.

Tra le varie strategie relative alla gestione proattiva possiamo iniziare la nostra discussione con un approccio già citato nel capitolo precedente: **i sistemi di Self-Assessment.**

Tal sistemi sono caratterizzati da diversi componenti chiave:

1. **Identificazione dei Rischi:** le unità operative hanno l'incarico di identificare i rischi che sono associati ai loro processi. Questo può comportare l'inclusione dei rischi legati a errori umani, frodi, guasti tecnologici e problemi di conformità;

⁵⁴ S'intendono variazioni analoghe in termini di segno.

2. **Valutazione dei Rischi:** una volta espletata la prima funzione, dunque l'identificazione, i rischi vengono sottoposti a valutazioni in termini di probabilità di accadimento e impatto potenziale. Questa è una fase nella quale si assegnano dei punteggi ai rischi per dare loro determinate priorità rispetto ad altri;
3. **Controlli e Mitigazioni:** le unità operative sottopongono a valutazione anche i controlli esistenti e determinano se tali controlli sono adatti per i processi di mitigazione dei rischi individuati. Se viene ritenuto necessario, vengono proposti nuovi approcci di controllo o miglioramenti;
4. **Monitoraggio e Reporting:** i risultati che vengono forniti dal self-assessment sono monitorati e vengono riportati regolarmente e periodicamente al management e ai comitati di rischio. Questo è un processo che garantisce l'efficacia delle misure di mitigazione avendo sotto controllo tutti i risultati che si ottengono;
5. **Documentazione e Audit:** tutti i processi che stiamo elencando sono documentati in maniera del tutto accurata. Questa documentazione è vitale per gli audit⁵⁵ interni ed esterni, che hanno il compito di verificarne l'efficacia dei sistemi di gestione del rischio.

Tali sistemi di gestione proattiva vantano numerosi vantaggi come il *coinvolgimento e la consapevolezza* in quanto i sistemi di self-assessment aumentano la consapevolezza dei rischi tra i dipendenti e li coinvolgono attivamente nella gestione del rischio; come la *proattività* dato l'incoraggiamento proattivo alla gestione del rischio, dando la possibilità alle unità operative di affrontare i rischi prima che diventino problematici; come l'*adattabilità* alle specifiche esigenze delle variegate unità operative rendendo la gestione sempre più efficace.

Vi sono naturalmente una serie di aspetti di rilevanza il cui rispetto ne assicura la corretta adozione ed efficacia. È essenziale formare i dipendenti sui concetti chiave del rischio operativo e sulle tecniche di self-assessment, specie perché una comprensione accurata può cercare di far avere una visione corretta e non distorta dei rischi ai dipendenti, così da fornire delle valutazioni oggettive.

Tutto questo richiede a monte un grande supporto del Management che deve supportare attivamente l'implementazione dei sistemi di self-assessment e utilizzare i risultati per migliorare la gestione del rischio. I

⁵⁵ Gli audit interni ed esterni sono ambedue dei processi di valutazione che sono utilizzati dalle organizzazioni per esaminare e valutare la conformità, l'efficacia e l'efficienza dei propri processi, procedure e sistemi. **L'Audit Interno** è condotto da personale interno all'organizzazione o comunque da una funzione di audit interna dedicata. L'audit interno ha lo scopo di valutare e migliorare l'efficacia dei controlli interni, la gestione del rischio e il processo decisionale all'interno dell'azienda. Questo è un tipo di audit che aiuta ad identificare le aree di potenziale miglioramento e anche di inefficienze, oltre a garantire il rispetto del quadro normativo. **L'Audit Esterno** è, invece, condotto da un'entità esterna all'organizzazione, come una società di revisione o un consulente indipendente. Ha lo scopo di valutare la correttezza e l'accuratezza dei conti aziendali e delle pratiche finanziarie, oltre alla conformità con le normative e gli standard contabili applicabili. La sua principale funzione è quella di fornire un'opinione indipendente basata sulla veridicità e affidabilità dei report finanziari dell'azienda.

risultati del processo devono essere integrati nel sistema complessivo di gestione del rischio dell'organizzazione in quanto è indispensabile avere una visione olistica dei rischi.

Come sottolineato da Warren Buffett *“Il rischio viene dal non sapere cosa stai facendo”* ed è per questa ragione che l'utilizzo dei sistemi di self-assessment sono di grande aiuto alle organizzazioni, specie per una migliore comprensione dei propri rischi così da trasformare l'incertezza in opportunità di miglioramento continuo.

Tali sistemi si basano su interviste alle diverse business unit, e spesso prevedono un vero e proprio rating del rischio operativo, che misura la probabilità e la severity delle diverse tipologie di eventi. Di seguito riporteremo una tabella con un esempio di questionario destinato all'unità di negoziazione titoli e volto alla misura della PE di un vettore di eventi riconducibili ai consueti quattro fattori di rischio.

| Fattore di rischio | Eventi | Giudizio Qualitativo | Rating (1=basso, 10=alto) | Probabilità |
|--------------------|--|----------------------|---------------------------|-------------|
| Risorse Umane | Frode; Negligenza, Violazione di regole interne | Medio-basso | 3 | 0,3%-0,5% |
| | | Medio | 5 | 1,0%-2,0% |
| | | Alto | 9 | 7,0%-10,0% |
| Tecnologia | Blocco dei sistemi, Errori Software, Telecomunicazioni | Medio | 4 | 0,5%-1,0% |
| | | Medio-alto | 8 | 5,0%-7,0% |
| | | Basso | 2 | 0,1%-0,3% |
| Processi | Model Risk, Rischio di transazione, Rischio di documentazione | Alto | 10 | >10,0% |
| | | Medio | 6 | 2,0%-3,0% |
| | | Medio-basso | 3 | 0,3%-0,5% |
| Eventi Esterni | Rischio politico, Rischio regolamentare/fiscale, Eventi naturali | Basso | 1 | 0,0%-0,1% |
| | | Medio-alto | 8 | 5,0%-7,0% |
| | | Basso | 2 | 0,1%-0,3% |

I giudizi sintetici che sono rappresentati all'interno della tabella dovrebbero riflettere tanto il rischio intrinseco di una certa unità organizzativa quanto il livello e la qualità dei sistemi di controllo disponibili. In effetti, l'introduzione di un sistema di controlli interni più efficace dovrebbe, a parità di altre condizioni, condurre a dei rating migliori e dunque ad un minor ammontare di rischi.

La principale controindicazione di tali meccanismi di autodiagnosi è che essi si basano principalmente sulle valutazioni del management, cioè degli stessi soggetti che, mediante le loro scelte gestionali, determinano il livello di rischio operativo fronteggiato dalla banca. C'è dunque il pericolo di una coincidenza tra controllato e controllore, che è possibile arginare in due modi:

- Gli exposure indicator e i livelli di rischio che sono rilevati per ogni business unit dovrebbero essere riscontrati utilizzando ulteriori fonti normative, anche esterne e risultare in linea con le valutazioni medie disponibili a livello di settore bancario; in altri termini, se è vero che una banca può avere un livello di rischio diverso rispetto alla media di settore, i dati esterni dovrebbero sempre essere utilizzati come termine di paragone per verificare la credibilità del processo di self-assessment;
- La valutazione del profilo di rischio di ogni business unit, sebbene sia alimentata con dati e giudizi provenienti dalla stessa business unit, dovrebbe fare capo a un'unità indipendente, in seno al risk management o all'internal audit, la cui azione sia guidata da criteri rigorosi, obiettivi, ben definiti e coerenti, con le prassi migliori di settore. Questi criteri devono essere resi espliciti, aggiornati periodicamente e applicati in modo del tutto omogeneo a tutte le unità organizzative e le attività oggetto di indagine.

I sistemi di autodiagnosi presentano ulteriori vantaggi rispetto a quelli elencati precedentemente. In primis costituiscono un approccio relativamente flessibile e facilmente adattabile alla complessità organizzativa delle diverse banche. In termini differenti, si prestano ad essere implementati a diversi livelli di sofisticazione, considerando il livello di rischio della banca e della qualità dei controlli in essere, oltre che del budget che la stessa banca ha allocato alla stima del rischio operativo.

In secundis, un sistema basato su interviste con il middle management rappresenta non solo uno strumento di rilevazione e misura del rischio, ma anche un veicolo per diffondere e accrescere, in banca, la consapevolezza circa l'importanza delle perdite operative e la necessità di intervenire adeguatamente sulle loro determinanti.

Un altro strumento indispensabile per la gestione del rischio sono i KRI, Key Risk Indicator o indici di rischio.

I KRI sono degli indicatori di rischio che hanno il compito di aiutare le aziende nell'identificazione e conoscenza dei pericoli e delle debolezze, oltre ad essere indispensabili per un'ampia gestione e controllo dei rischi. Ogni contesto aziendale con qualsivoglia dimensione necessita di un sistema adeguato a proteggerla da rischi operativi, reputazionali e finanziari.

Tali indicatori sono considerati degli indici *predittori* in quanto sono in grado di poter generare previsioni di eventi negativi. La funzione che ricoprono è anche di monitoraggio e avviso che deve essere fatto ai responsabili aziendali quando si rileva un'esposizione al rischio.

Col seguente modus operandi si può intervenire in modo tempestivo dinanzi ad una eventuale crisi.

I KRI di natura finanziaria sono di aiuto nella quantificazione del rischio di mercato, delle modifiche normative o il rischio competitivo, nel monitoraggio e controllo dei rischi mediante delle attività e processi gestionali relativi al rischio stesso.

L'importanza dei KRI è giustificata da diversi fattori: senza questi indicatori qualsiasi organizzazione aumenterebbe la probabilità di esposizione ad eventi che la danneggerebbero impattando direttamente sulle proprie attività. La sfida principale per le istituzioni bancarie e assicurative è sia quella di identificare quali indicatori di rischio sono fondamentali, ma anche nel garantire un'adeguata comprensione di questi ultimi.

Le organizzazioni per trasmettere una conoscenza completa ai membri e dipendenti possono, ad esempio, fornire un benchmarking del rischio cosicché abbiano una prospettiva migliore anche per la creazione del processo gestionale del rischio.

I KRI possono essere molto utili nel fornire delle informazioni attuali sullo status del rischio, future circa eventi che potrebbero generarsi in ottica prospettiva o passate su eventi già registrati. È possibile classificare tali indicatori nel seguente modo:

- **Indicatori principali o emergenti:** sono legati al realizzarsi di un rischio futuro;
- **Indicatori attuali:** sono legati alla presenza attuale del rischio;
- **Indicatori passati:** relativi agli eventi già registrati ma che possono ripresentarsi.

È possibile, inoltre, distinguere i KRI da altri due indicatori che sono sempre molto rilevanti nella gestione del rischio: KCI e KPI.

I KCI, Key Control Indicators, si riferiscono ad una metrica che monitora costantemente l'efficacia che devono avere i controlli. Si ricorre a tali indicatori per definire i controlli a livello aziendale e continuare il monitoraggio degli obiettivi prefissati e il loro conseguimenti. Naturalmente, sono i responsabili di questo comparto a definire i livelli di tolleranza per i controlli.

Distintamente abbiamo i KPI, Key Performance Indicators. Questi indicatori sono definiti indicatori chiave di prestazione e sono delle metriche che qualsiasi organizzazione ha a disposizione per poter tener traccia, misurare e condurre analisi della salute finanziaria dell'azienda.

Da un punto di vista specifico, i KPI finanziari fanno parte di una serie di categorie, tra cui indici di redditività, liquidità, solvibilità, ma anche di efficienza e valutazione.

Questi KPI a breve termine forniscono delle informazioni chiave che bisogna monitorare quotidianamente per poter cogliere delle opportunità, o per poter comprendere quando attivare il ridimensionamento alla vista di difficoltà in arrivo. Portiamo di seguito una lista di alcuni KPI economico-finanziari da monitorare quotidianamente:

- i. **Posizione Finanziaria Netta (PFN):** è un indicatore finanziario che misura la differenza tra le attività liquide e le passività finanziarie. Nel

- pratico, rappresenta la situazione debitoria finanziaria di un'azienda. Una PFN positiva esplica una situazione dell'azienda in cui ha più liquidità rispetto ai debiti, mentre una PFN negativa segnala una maggiore esposizione debitoria rispetto alla liquidità disponibile.
- ii. **Margine Operativo Lordo (MOL):** è noto anche come EBITDA ed è un indicatore finanziario che misura la redditività operativa di un'azienda prima della deduzione di interessi, tasse, deprezzamento e ammortamento. Il MOL rappresenta il flusso di cassa generato dalle operazioni principali dell'azienda escludendo gli effetti delle decisioni finanziarie e delle politiche fiscali. Questo indicatore è utilizzato per poter valutare la capacità dell'azienda di generare dei profitti operativi e per confrontare la performance tra diverse aziende o settori.
 - iii. **Capacità di restituzione del debito (PFN/MOL):** è un indicatore che misura la capacità di un'azienda di ripagare i propri debiti utilizzando i suoi guadagni operativi. Un valore più basso del rapporto PFN/MOL indica una migliore capacità di gestione del debito, dato il fatto che l'azienda sarà in grado di generare sufficienti profitti operativi per far fronte ai propri obblighi finanziari. Un rapporto più alto, invece, può segnalare potenziali difficoltà nell'onorare i debiti.
 - iv. **Fabbisogno di capitale circolante:** rappresenta l'importo di risorse finanziarie necessarie per coprire il ciclo operativo di un'azienda, ovvero la gestione quotidiana delle attività correnti come crediti, debiti e scorte. Esso indica quanto capitale è richiesto per finanziare le operazioni aziendali fino al momento in cui i ricavi delle vendite vengono incassati. Una gestione efficace del FCC è cruciale per garantire la liquidità aziendale e il regolare svolgimento delle attività operative, prevenendo potenziali crisi di liquidità
 - v. **Rapporto di indebitamento:** è un indicatore finanziario che misura il grado di leva finanziaria di un'azienda, confrontando il totale dei debiti con il totale del patrimonio netto. Esso fornisce un'idea di quanto l'azienda dipende dal finanziamento esterno (debiti) rispetto alle risorse proprie (patrimonio netto). Un alto rapporto di indebitamento può indicare un elevato rischio finanziario, poiché l'azienda ha una maggiore quantità di debiti rispetto al proprio capitale, mentre un basso rapporto indica una minore dipendenza dai debiti e quindi un rischio finanziario inferiore.
 - vi. **Cash flow (Flusso di cassa):** è un indicatore finanziario che rappresenta l'ammontare di denaro che entra ed esce da un'azienda durante un determinato periodo di tempo. Esso riflette la capacità dell'azienda di generare liquidità attraverso le sue attività operative, di investimento e di finanziamento. Il cash flow positivo indica che l'azienda sta generando più liquidità di quanta ne stia spendendo, mentre un cash flow negativo può indicare problemi di liquidità. Il cash flow è cruciale per valutare la salute finanziaria e la capacità di un'azienda di sostenere le proprie operazioni e investimenti futuri.

Dopo aver avanzato anche degli esempi dei KPI è possibile dedurre come differiscono dai KRI in quanto i KRI forniscono delle metriche che sono relative ai rischi e al potenziale impatto sulla realtà aziendale, possiamo considerarli come degli alert per il monitoraggio, la gestione e la mitigazione dei rischi. Distintamente, i KPI ci dimostrano quanto l'organizzazione stia procedendo verso la direzione giusta attenendo ai suoi scopi e obiettivi.

Un'altra strategia ideale per la gestione del rischio richiama il ruolo delle polizze assicurative.

L'acquisto di coperture assicurative per far fronte alle perdite che derivano dalla manifestazione del rischio operativo è una strategia che si è andata diffondendo ultimamente ed è stata resa possibile da recenti innovazioni di prodotto che sono state rese note da grandi gruppi assicurativi e di riassicurazione.

Parliamo di una vera e propria forma di "outsourcing" in cui l'istituzione bancaria, con il pagamento di un premio, passa all'assicuratore tutte le conseguenze finanziarie ed economiche che si possono registrare dalla manifestazione del rischio operativo. L'impegno dell'assicuratore sarà quello di rivalere l'assicurato del danno sofferto sempre nei limiti che sono stati previsti dalla polizza; la copertura di alcuni rischi operativi viene affidata a delle società specializzate. È chiaro che l'assunzione dei rischi da parte della figura dell'assicuratore è vincolata ad una serie di principi, conosciuti come *principi di assicurabilità*:

- a. Il rischio deve avere legami con un numero molto elevato di unità omogenee tra loro, ed è un presupposto per poter attivare il processo assicurativo che si basa sulla legge dei grandi numeri⁵⁶.
- b. È necessario definire il danno potenziale per evitare situazioni in cui l'assicuratore possa riferirsi a rischi che possono causare danni simulabili.
- c. Esclusivamente gli eventi aleatori devono causare il danno in questione.
- d. L'entità del danno potenziale deve essere considerevole, perché se così non fosse, i soggetti sarebbero in posizione di non essere tenuti necessariamente alla copertura assicurativa.
- e. Bisogna rendere accessibile il costo delle assicurazioni così da avere un numero ingente di assicurati.
- f. Deve essere possibile determinare a priori la frequency di accadimento del rischio: cioè si deve avere la possibilità di disporre di un'osservazione quantitativa dei rischi assicurabili così da poter avere informazioni sulla frequenza di accadimento, aspetto indispensabile per una corretta politica di pricing.

⁵⁶ La legge dei grandi numeri è un principio statistico fondamentale nelle assicurazioni che afferma che, all'aumentare del numero di polizze sottoscritte, i risultati reali tendono a coincidere con quelli previsti. Questo principio consente agli assicuratori di prevedere con maggiore precisione le perdite e di determinare premi assicurativi più accurati. In pratica, più ampio è il portafoglio di polizze di un'assicurazione, più stabili e prevedibili saranno i risultati finanziari, riducendo l'incertezza e il rischio complessivo.

I contratti assicurativi sono spesso definiti come “capitale assicurativo” dato che come il capitale proprio, fanno fronte ad eventuali perdite evitando che possano essere compromesse le ragioni dei terzi creditori. Distintamente dal capitale proprio è la capacità di assorbimento delle perdite del capitale assicurativo che non è universale ma selettiva, cioè limitata alle perdite originate dagli eventi specifici che sono stati indicati nella polizza.

Questa strategia di gestione si utilizza spesso per *Low Frequency and High Impact Events*, dovuti generalmente a fattori esterni di tipo naturale, politico o regolamentare, e quindi eventi di rischio non controllabili direttamente dalla banca.

La scelta di voler esternalizzare questa tipologia di rischio è comprovata da due vantaggi che sono legati all'accensione di un contratto assicurativo:

- **Risk Polling:** s'intende la diversificazione dei rischi grazie alla quale gli oneri che un assicuratore assume sono inferiori rispetto a quelli che sono stati fronteggiati in precedenza dai singoli assicurati, questo a causa dell'imperfetta correlazione tra i rischi dei vari clienti.
- **Cash Flow Smoothing:** s'intende la stabilizzazione dei profitti che migliora l'*earnings quality* e riduce il costo del capitale tradizionale con un accrescimento del valore di mercato della banca, cioè delle azioni che sono possedute dagli azionisti.

La scelta di trasferimento dei rischi è una scelta finanziaria: siamo consapevoli del fatto che la copertura assicurativa viene vista come un aspetto che consente di beneficiare in via diretta della riduzione dell'impatto finanziario di un evento che è legato ai rischi operativi e in via indiretta di una serie di servizi che sono offerti dall'assicuratore in termini di monitoraggio esterno e investigazione.

I benefici che derivano dai due aspetti citati prima, *Risk Polling* e *Cash Flow Smoothing*, sono ridotti dai limiti che caratterizzano il contratto assicurativo: il capitale assicurativo è solamente un capitale che si impegna a pagare l'assicuratore, quando si materializzerà l'evento citato nella polizza. E' per questa ragione che l'adempimento di questo obbligo dipende dal merito creditizio o comunque dalla solvibilità della compagnia di assicurazione.

Questo comporta che i rischi operativi non saranno eliminati in toto, bensì verranno trasformati in rischi di credito.

Vi sono, in aggiunta, dei problemi di asimmetria informativa che si concretizzano in due modalità e due istanti differenti:

1. **Adverse Selection:** s'intende la selezione avversa che si manifesta a priori dalla stipula del contratto. Nell'operatività, la richiesta di coperture assicurative arriva dalle aziende più rischiose di solito, le quali dovrebbero pagare un premio superiore rispetto a quello medio per ottenere la copertura necessaria, però questo non accade dato che traggono vantaggio nelle difficoltà delle compagnie di assicurazione nel quantificare accuratamente la rischiosità dei vari clienti, portandole ad

un punto in cui sono tenute a praticare un premio uniforme a tutte le controparti con caratteristiche simili. Questo scoraggia ovviamente i clienti migliori che non sono più disposti a pagare un premio superiore rispetto a quello che avrebbero pagato in caso di assenza di asimmetria informativa.

2. **Moral Hazard:** si richiama qui l'azzardo morale. Una volta che la polizza assicurativa viene stipulata, il cliente non manterrà più sotto controllo il rischio, dal momento in cui le perdite sono a carico dell'assicuratore. È per questa ragione che nelle polizze si prevedono delle franchigie o scoperti, cosicché una parte della perdita rimane in capo al cliente.

Tra le varie metodologie di trasferimento dei rischi operativi abbiamo compreso come quello assicurativo rappresenta quello principale.

In Italia le polizze che sono stipulate dal settore creditizio sono riclassificabili come segue:

- a) **Polizza Bankers Blanket Bond (B.B.B.):** è una forma di assicurazione progettata per proteggere le istituzioni finanziarie, come banche o istituti di credito, contro le perdite causate da frodi, appropriazioni indebite, furti interni, frodi informatiche e altre attività fraudolente di origine dolosa da parte di dipendenti o terze parti, indipendentemente dal fatto che si parli di eventi interni o esterni.
- b) **Polizza informatica:** è un tipo di assicurazione progettata per proteggere le aziende contro le perdite finanziarie e i danni causati da eventi legati alla tecnologia e alla sicurezza informatica. Questi eventi possono includere violazioni dei dati, attacchi informatici, interruzioni del servizio, perdita di dati, responsabilità derivante da violazioni della privacy e altre situazioni legate alla gestione dei dati e dei sistemi informatici.
- c) **Polizza RCT/O:** l'oggetto di tale polizza è la responsabilità civile per dei danni corporali e materiali che sono stati provocati in maniera involontaria a terzi, come una conseguenza di un accadimento accidentale riconducibile all'esercizio dell'attività bancaria. Tra le garanzie è compresa la responsabilità civile per infortuni sul lavoro sofferti dai dipendenti o lavoratori che sono addetti alle attività per cui è stata fissata la copertura.
- d) **Polizza RC professionale:** l'obiettivo è indennizzare la banca da quanto è tenuta a pagare come responsabile civilmente ai sensi della legge a titolo di risarcimento di perdite patrimoniali involontarie e cagionate a terzi, a causa di errori commessi dai dipendenti durante l'attività bancaria.
- e) **Polizza D&O-RC amministratori e sindaci:** vuole indennizzare gli organi societari da quanto sono tenuti a pagare danni a titolo di risarcimento. Questi organi sono responsabili civilmente ai sensi di legge per delle perdite patrimoniali causate involontariamente a terzi, a causa

di azioni illecite commesse durante la carica indicata e per la quale era sottoscritta l'assicurazione.

- f) **Polizza infortuni e sanitaria dei dipendenti:** ha l'obiettivo di liquidare un capitale in caso di invalidità o morte di uno dei dipendenti a causa di un infortunio o malattia.
- g) **Polizza per opere d'arte:** è una tipologia di polizza che ha l'obiettivo di tutelare il patrimonio artistico delle banche alle quale offre una garanzia per i rischi a cui sono esposte all'interno e all'esterno dei propri locali.
- h) **Polizza incendio:** ha l'obiettivo di coprire i fabbricati che sono destinati all'attività e il relativo contenuto dal rischio di incendio, eventi naturali, sociopolitici e catastrofali.

Oltre queste polizze conosciute, vi sono anche altre due che mancano nell'offerta assicurativa in Italia:

- **Unauthorised Trading:** è una tipologia di polizza assicurativa che ha l'obiettivo di tutelare la banca nel caso di perdite che si possono registrare provenienti da attività non autorizzate, il che sta a significare che il trading è svolto oltre i limiti consentiti. Altri esempi di attività non autorizzate sono le operazioni occultate o falsamente contabilizzate e la creazione di documenti relativi a false transazioni o non esistenti.
- **FIORI-Financial Institutions Operational Risk Insurance:** è una tipologia di polizza assicurativa introdotta negli anni 90 acquistabile e adatta principalmente a grandissimi gruppi bancari attivi sulla scena finanziaria globale. Garantisce una copertura relativa alle perdite che derivano da disfunzioni tecniche, frodi interne ed esterne, rischi legali.

Controlli Interni nella Gestione del Rischio e il Ruolo della Compliance

Per assicurarsi un'adeguata gestione del rischio operativo è necessario che la complessiva macchina funzioni con tutti i suoi ingranaggi, accertandosi infine che la funzione di compliance sia sempre resa effettiva. La funzione di compliance gioca un ruolo cruciale nella gestione del rischio operativo all'interno di un'organizzazione.

La compliance, o conformità normativa, si riferisce all'adesione a leggi, regolamenti, linee guida e standard interni ed esterni che regolano le attività di un'azienda. La gestione efficace del rischio operativo attraverso la compliance tocca diversi aspetti chiave.

In primo luogo, la funzione di compliance aiuta a identificare i rischi associati alla non conformità con leggi e regolamenti; questo aspetto include il monitoraggio delle normative vigenti e l'anticipazione dei cambiamenti normativi che potrebbero poi influire sulle operazioni aziendali.

La compliance sviluppa e implementa controlli interni per potersi accertare che l'azienda rispetti tutte le normative applicabili, per cui l'implementazione dei controlli interni aiutano a prevenire delle violazioni e a ridurre il rischio di sanzioni, multe e danni reputazionali.

La funzione di compliance organizza anche dei programmi di formazione per i dipendenti andando a lavorare e agire sulla consapevolezza dei requisiti normativi e sui rischi associati. È necessaria tale formazione affinché possa garantire che i dipendenti comprendano le loro responsabilità e le procedure da seguire per il mantenimento della conformità. In aggiunta, la compliance monitora in maniera del tutto costante le operazioni aziendali per assicurarsi che i controlli siano realmente efficaci e che le pratiche operative siano allineate con le normative: questo comporta audit regolari e revisioni delle procedure aziendali.

Nel caso in cui si dovessero registrare delle violazioni normative, la funzione di compliance agisce anche nella gestione del processo di indagine, valutazione e risoluzione. Questo può includere la segnalazione alle autorità competenti e anche l'implementazione di azioni correttive per poter prevenire future violazioni.

Un'altra funzione che svolge la compliance è quella di supporto alla governance aziendale assicurando che il consiglio di amministrazione e il management siano adeguatamente informati sui rischi normativi e sulle misure di mitigazione: questo naturalmente include la redazione di rapporti e la partecipazione a comitati di rischio.

Proprio in virtù di tali aspetti che emergono dalla funzione di compliance è doveroso discutere sulle pratiche per la gestione del rischio operativo e come siano strettamente connesse con i controlli interni per la gestione del rischio.

Nel 2003 il Comitato di Basilea pubblicò un documento intitolato "*Sound Practices for the Management and Supervision of Operational Risk*", documento in cui erano indicati i principi guida che le banche e le autorità di vigilanza dovevano seguire per assicurare una gestione e supervisione efficace del rischio operativo. Nel 2011 si ritenne indispensabile aggiornare il documento del 2003 incorporando in uno nuovo l'evoluzione delle migliori pratiche e enunciando 11 principi da dover seguire scrupolosamente.

Questo documento ha portato a riflettere sulle strutture di cui bisognava disporre per una corretta supervisione del sistema gestionale del rischio operativo, sul ruolo da dover affidare ai vari organi dell'organigramma aziendale e alle varie funzioni che coinvolgevano i diversi livelli decisionali come il top management e il CDA.

Prima di enunciare gli 11 principi del documento, una piccola parentesi è doveroso riservarla alle funzioni che sono espletate dalle autorità di vigilanza:

- ⇒ Le autorità di vigilanza svolgono in via diretta o indiretta una valutazione indipendente delle politiche bancarie, dei sistemi di cui dispongono e dei processi relativi al comparto gestionale del rischio operativo. Esempi di tali aspetti possono essere: sistemi di controllo interni, metodologie di monitoraggio e reporting, indicatori di rischio;
- ⇒ Le autorità di vigilanza esigono che tutte le banche possano sviluppare un sistema di gestione del rischio operativo che rispetti tutte le indicazioni sottolineate dal Comitato di Basilea;
- ⇒ Si assicurano che le istituzioni che fanno parte di un gruppo adottino un sistema di gestione adeguato;
- ⇒ Nel caso in cui vengono rilevate delle carenze, è possibile affrontarle mediante delle azioni che tengono conto delle circostanze particolari nelle quali la banca si trova;
- ⇒ Incoraggia gli sviluppi dei processi di risk management mediante un meccanismo con cui le autorità monitorano e confrontano le situazioni che sono presenti nelle differenti istituzioni, garantendo così un ritorno di informazioni utili alle banche controllate.

Possiamo passare ora all'enunciazione degli 11 principi fondamentali per la gestione del rischio.

Nel primo principio si enuncia che il ruolo del consiglio di amministrazione sia quello di prendere iniziativa nell'istituzione di una cultura forte di gestione del rischio all'interno della banca, costituendo a livello aziendale un sistema interno per la gestione. Il CdA e l'alta direzione devono istituire norme e incentivi che sono appropriati per un comportamento responsabile e professionale, ed è inoltre compito del CdA assicurarsi che la cultura della gestione del rischio operativo sia presente con continuità nell'intera organizzazione.

La giustificazione di tale principio si basa sul motivo secondo il quale le banche con una forte cultura nella gestione del rischio hanno una minore probabilità di ritrovarsi in eventi dannosi e sono in una posizione preferibile per affrontare a testa alta tali eventi nel caso sopraggiungessero.

Nel secondo principio si sostiene che le banche debbano sviluppare e mantenere una struttura completamente integrata con tutti i processi di risk management che sono presenti nel contesto bancario; la conseguenza è che la struttura che viene scelta per la gestione del rischio deve considerare una serie di fattori che caratterizzano la banca come la sua dimensione, complessità e il suo profilo di rischio.

Per poter avere un quadro generale quanto più preciso, è necessario che tutto sia documentato e riportato nel momento in cui il CdA sia intenzionato ad approvarlo tale quadro.

Nei successivi principi si va a disciplinare il ruolo della Governance, dunque CdA e Alta direzione.

Si fa riferimento, dunque, ai principi 3 e 4 i quali affermano che il consiglio di amministrazione ha il dovere di stabilire, approvare e procedere con delle riesamine periodiche circa il sistema di gestione del rischio, oltre ad avere una funzione di controllo e supervisione sull'alta direzione per accertarsi che politiche, processi e sistemi siano adeguatamente implementati. In aggiunta, il CdA deve approvare e revisionare quella che è la propensione al rischio operativo della banca.

I principi 5, 6 e 7 sono invece relativi all'Alta direzione. In questi principi si indicano i compiti di quest'ultima, che sono quelli di sviluppare una struttura di governance chiara e robusta per avere l'approvazione del CdA, struttura che deve contenere linee trasparenti e dotata di piena responsabilità. L'Alta direzione ha anche la responsabilità sulla definizione di tutta l'organizzazione delle politiche, dei processi e dei sistemi per la gestione del rischio, in quando devono essere coerenti con il livello di propensione al rischio.

Nei principi 8 e 9 si concretizzano le raccomandazioni che il Comitato fa, raccomandazioni tramite le quali desidera indurre le banche allo sviluppo di tecniche di gestione e strutture funzionali ad hoc per i rischi operativi.

Il comitato negli ultimi principi, infine, sottolinea l'importanza per le banche di disporre di un business in grado di operare nel tempo cercando di mantenere sempre testa ai vari mutamenti esterni in cui si può trovare, cercando sempre di essere trasparente verso il mercato.

Il principio 10, per l'appunto, afferma che le banche dovrebbero strutturare dei piani di business elastici così da poter garantire un operato continuativo e limitando le perdite in caso di disfunzioni connesse al complessivo business bancario.

Le banche dovrebbero attuare il processo di revisione dei piani di business periodicamente per assicurare eventuali strategie a cui ricorrere in casi di emergenza.

In ultimo il principio 11 relativo al ruolo dell'informativa al pubblico. Secondo questo principio le banche devono produrre documenti contenenti informazioni esaustive che possano consentire a tutti i portatori d'interessi aziendali di valutare l'approccio che utilizzano nella gestione del rischio.

Le istituzioni finanziarie oggi giorno garantiscono a se stesse una maggiore probabilità di successo se nei processi di gestione coinvolge tutti gli stakeholder e i portatori d'interesse. Se poniamo un esempio, il chief operating officer⁵⁷ di una investment bank riveste un ruolo principale nella trasmissione

⁵⁷ Il Chief Operating Officer (COO) è un alto dirigente all'interno di un'azienda che è responsabile della gestione delle operazioni quotidiane e dell'implementazione delle strategie aziendali. Il ruolo varia a seconda delle dimensioni, del settore e della struttura organizzativa, ma le sue responsabilità principali includono la supervisione delle attività operative giornaliere dell'azienda, lavorare a stretto contatto con il CEO e altri dirigenti per tradurre la strategia aziendale in piani operativi concreti, assicura che le strategie a lungo termine vengano implementate in maniera

della comprensione delle pratiche di gestione del rischio operativo a tutti i livelli aziendali, così da riunire i più importanti portatori di interessi e facendo anche da arbitro nelle situazioni in cui le opinioni vanno in contrasto.

Il Fallimento della Barings Bank: Un caso esemplare di Rischio Operativo

Il caso della Barings Bank del 1995 è uno degli esempi più noti di fallimento bancario causato da una gestione inadeguata del rischio operativo. Complessivamente la Barings Bank, una delle banche più antiche e rispettate del Regno Unito, fu costretta a dichiarare bancarotta a seguito delle azioni di un singolo dipendente, Nick Leeson, che riuscì a nascondere enormi perdite speculative di 1 miliardo di dollari sui mercati finanziari.

Procedendo con una panoramica del caso iniziamo parlando della Barings Bank che aveva una lunga storia di successo (di circa 223 anni prima di questo fallimento) ed era molto rispettata come banca d'affari. Ma nel febbraio del 1995 con un capitale di 900 milioni di dollari subì un improvviso arresto. Nel 1993, Nick Leeson è stato nominato direttore generale della filiale Barings Futures della banca a Singapore ed era responsabile delle operazioni di trading e anche del controllo delle stesse, il che creava un chiaro conflitto di interessi. Grazie alla sua capacità di gestire sia le funzioni di trading che quelle di back office, è riuscito a nascondere le sue attività commerciali non autorizzate per oltre un anno.

I dirigenti senior della Barings provenivano principalmente da un background di banca d'affari e dunque sapevano molto poco di trading, specie di fronte agli ampi profitti, che avrebbero dovuto far capire al management che si stavano assumendo rischi sostanziali, continuavano a credere che Leeson

efficace quotidianamente, spesso sovrintende alla funzione delle risorse umane garantendo che il reparto HR possa far raggiungere all'azienda i suoi obiettivi operativi, è responsabile del monitoraggio delle performance operative mediante gli indicatori KPI, ha la responsabilità del controllo del budget operativo, può rappresentare l'azienda in relazioni con partner esterni e in ultimo funge da ponte tra i vari dipartimenti interni al conteso aziendale facilitando la comunicazione e collaborazione.

deteneva posizioni equivalenti sulla Borsa monetaria internazionale di Singapore (Simex) e sulla Borsa di Osaka; dunque, si stava realizzando un profitto a basso rischio.

In effetti, Leeson negoziava contratti derivati sulle due borse che erano, in alcuni casi, di tipo diverso e, in altri casi, per importi non corrispondenti. Ad esempio, Leeson ha eseguito una strategia di trading nota come "straddle", con l'obiettivo di realizzare un profitto vendendo opzioni put e call sullo stesso strumento finanziario sottostante, in questo caso l'indice Nikkei 225.

Uno straddle generalmente produce dei guadagni positivi quando i mercati sono stabili, ma può comportare ingenti perdite se i mercati sono volatili.

Leeson creò un conto di errore numerato "88888" come area di deposito per eventuali premi o perdite da lui realizzati; quest'ultimo sostiene di aver inizialmente aperto il conto per nascondere una singola perdita di 20.000 sterline derivante da un errore di conteggio, fino a quando non è riuscito a compensare la differenza attraverso il trading. Tuttavia, ha continuato poi a contabilizzare varie perdite sul conto e ha anche continuato ad aumentare il volume degli scambi e il livello di assunzione del rischio.

Leeson ha aumentato la dimensione delle sue posizioni aperte anche se le sue perdite aumentavano a causa della volatilità dei mercati; ciononostante, quando un terremoto in Giappone causò un forte calo dell'indice azionario Nikkei 225, le posizioni di trading non autorizzate di Leeson subirono enormi perdite e la sua operazione fallì. Il 3 marzo 1995 la banca olandese ING acquistò la Barings per 1 sterlina.

Si può sostenere che questo incidente sia causato da un solo individuo, ma in realtà è da attribuire alla struttura sottostante dell'azienda, e in particolare alla mancanza di equilibri interni.

Riassumiamo ora gli eventi in ordine cronologico prima di discuterli in ottica di Operational Risk.

- **1993:** Nick Leeson diventa direttore generale di Barings Futures (Singapore), gestendo le attività Simex (Singapore International Monetary Exchange) della banca.
- **Gennaio 1994:** entro questa data Leeson iniziò a vendere opzioni put e call sull'indice azionario Nikkei 225, collocando i premi guadagnati sul conto errore numero 88888. Questa strategia, nota come straddle, è essenzialmente una scommessa sulla stabilità dei prezzi di mercato.
- **24 febbraio 1994:** un memorandum del comitato patrimoniale e passivo della Barings valuta il portafoglio di opzioni a 2,8 miliardi di yen.
- **Luglio 1994-agosto 1994:** James Baker, un revisore interno, trascorre due settimane a Singapore indagando sugli immensi profitti che vengono realizzati lì. Baker identifica la debolezza dei controlli interni e raccomanda che il direttore generale non sia più responsabile del back office. In risposta, ad Hong Kong, viene affidata la responsabilità part-time di vigilare sul back office ad un manager finanziario separato.

- **Agosto 1994:** nel tentativo di valutare meglio il proprio rischio complessivo, Barings istituisce una funzione integrata di Tesoriera e Rischio del Gruppo, che fa capo ad un nuovo comitato di attività e passività (Alco).
- **Dicembre 1994:** una successiva indagine della Barings rileva che, per ragioni sconosciute, Leeson aveva accumulato una perdita pari a 7,7 miliardi di yen sul conto entro la fine del 1994.
- **23 gennaio 1995:** il Nikkei 225 crolla di 1.000 punti dopo che un terremoto colpisce il cuore industriale del Giappone. Leeson iniziò ad acquistare contratti futures di marzo e giugno 1995 sul Nikkei 225.
- **26 gennaio 1995:** il team dei futures di Londra dà a Barings Alco Committee una presentazione sull'operazione Baring Futures (Singapore), in cui si afferma che Leeson sta gestendo un book perfettamente abbinato: long ad Osaka, ma short dello stesso importo su Simex.
- **8 febbraio 1995:** Coopers & Lybrand decide di non firmare i conti di Barings finchè non sarà possibile chiarire alcuni punti con Leeson.
- **23 febbraio 1995:** alla chiusura delle negoziazioni, il conto errori contiene 55.399 contratti Nikkei con scadenza a marzo e 5.640 con scadenza a giugno. Al 25 febbraio la perdita della Simex ammontava a 59 miliardi di yen.
- **24 febbraio 1995:** il Barings Board si riunisce per discutere un'analisi frettolosamente preparata circa le transazioni nel conto 88888.
- **3 marzo 1995:** la banca olandese ING accetta di acquistare la Barings per 1 sterlina e di assumersi tutte le sue passività.

Il crollo della Barings ha confermato che i controlli interni alla Barings erano chiaramente insufficienti per poter rilevare cosa stesse accadendo con le operazioni di derivati di Leeson. Ha perso così tanto denaro speculando sullo yen che ha portato al crollo dell'intera banca prima ancora che il top management sapesse cosa stava accadendo. Sebbene i resoconti iniziali parlassero della attività fraudolenta di Leeson e le prove suggeriscono che Leeson era effettivamente coinvolto in transazioni altamente speculative e cercava deliberatamente di ingannare i suoi superiori, le sue azioni non furono l'unica ragione del fallimento della banca.

Comunicazioni interne, controlli e canali di responsabilità inadeguati, supervisione normativa insufficiente, ed è stata rivelata una mancanza di comunicazione tra le autorità di regolamentazione del Regno Unito, del Giappone e di Singapore.

L'aspetto più chiaro della mancanza di comunicazione interna è che sui mercati dei futures era risaputo che la Barings stesse costruendo una posizione sempre più rischiosa. L'incapacità del management della Barings di prevenire il collasso di quest'ultima è anche il risultato degli errori nei controlli interni e nei canali di responsabilità della Barings.

Tuttavia, gli alti dirigenti erano già stati messi a conoscenza delle azioni di Leeson già nel 1992: a quel tempo il capo delle operazioni della Barings Securities a Singapore allertò la direzione della società a Londra dei potenziali pericoli derivanti dalla gestione da parte di Leeson sia del trading che delle operazioni finanziarie.

Dalle prove alla data ultima sembra che le preoccupazioni non siano state effettivamente comunicate ai revisori esterni della Barings, che quasi certamente le avrebbero incluse nella relazione annuale sui sistemi di gestione e di controllo, basata sulle normative bancarie del Regno Unito.

E' importante però comprendere cosa è andato storto, cosa è stato fatto in modo errato e quali controlli non sono stati eseguiti a dovere. Sulla scia di tanti vari scandali di commercianti o dipendenti disonesti, ci sono state poi delle analisi post portem, rapporti di soggetti indipendenti e accertamenti di comitati speciali. In particolare, nel caso storico della condotta fraudolenta di Rusnak⁵⁸, le banche alleate irlandesi hanno incaricato Eugene Ludwig, un ex controllore della valuta statunitense, di fornire un rapporto indipendente ("Rapporto Ludwig") su ciò che era andato storto.

Più recentemente, le perdite sui mercati finanziari derivanti dal crollo del mercato dei mutui subprime hanno innescato una serie di rapporti e raccomandazioni sulla gestione e supervisione del rischio, in particolare il Gruppo di lavoro del Presidente sui mercati finanziari ("PWG") e il Gruppo dei supervisor senior (che è un gruppo internazionale di regolatori finanziari, tra cui la SEC, la FED e l'Ufficio del controllore della valuta).

L'alta direzione e il CdA devono incoraggiare una cultura della conformità e dell'assunzione responsabile dei rischi, nel dettaglio il senior management e i consigli di amministrazione dovrebbero enfatizzare l'integrità e i problemi di conformità devono essere segnalati alle funzioni indipendenti all'interno dell'azienda e indagati e risolti, indipendentemente da chi è coinvolto e da quanto redditizia sembra essere l'unità aziendale.

Nel caso della Barings Bank, il senior management ha ignorato i segnali di potenziali illeciti e non è riuscito a stabilire controlli duraturi o un ambiente di onestà e responsabilità.

In aggiunta, i gestori del rischio e le altre persone incaricate di verificare le posizioni dei trader dovrebbero essere incoraggiati a mettere in discussione tali valutazioni quando appaiono peculiari, indipendentemente dal fatto che il trader abbia o meno successo. Alcuni commentatori hanno notato di recente che una cultura industriale di deferenza da parte dei gestori del rischio nei confronti degli operatori di successo può contribuire a determinare i fallimenti dei prezzi e a valutazioni eccessivamente ottimistiche sui libri contabili delle aziende⁵⁹.

⁵⁸ John Rusnak è un ex trader della Allfirst Financial, una filiale della Allied Irish Banks (AIB), che nel 2002 fu coinvolto in uno scandalo finanziario simile a quello della Barings Bank. Rusnak riuscì a nascondere enormi perdite speculative sul mercato dei cambi attraverso una serie di frodi e manipolazioni contabili. Quando le sue frodi furono scoperte nel 2002, le perdite totali ammontavano a circa 691 milioni di dollaro.

⁵⁹ WilmerHale 2008.

Una chiave, invece, per una struttura di reporting di successo è la completa separazione dei controlli tra front office e back office. Una struttura organizzativa per la supervisione delle attività di negoziazione dovrebbe coinvolgere tre gruppi distinti: front office, back office e compliance.

Nel caso di Barings, Leeson gestiva il back office, quindi c'era l'opportunità di poter manipolare accordi e altri rapporti. La mancanza di segregazione all'interno della sua divisione gli ha permesso di nascondere le sue perdite ai suoi superiori.

Inoltre, una struttura e una pratica di gestione del rischio imperfette possono trasformare rapidamente le esposizioni al rischio di mercato in perdite economiche significative per un'azienda. Poiché il rischio e l'assunzione di rischi sono intrinseci al trading proprietario ed è facile perdere grandi quantità di denaro, è stato sottolineato che è fondamentale per le operazioni di trading utilizzare la migliore tecnologia informatica e i migliori sistemi disponibili. Dovrebbero essere condotte delle revisioni periodiche di tali sistemi e tutte le carenze e le relazioni su come sono state affrontate dovrebbero essere presentate all'audit o ad altri comitati appropriati. Più recentemente, infatti, il Senior Supervisors Group ha osservato, nella sua analisi della gestione del rischio durante le recenti turbolenze dei mercati, che le aziende che tendevano ad affrontare con maggiore successo le turbolenze fino alla fine del 2007 hanno adottato una visione globale delle loro esposizioni.

In particolare, le aziende che hanno subito perdite significative tendevano a mostrare i seguenti punti deboli nella gestione del rischio:

- i. *I controlli deboli sulla crescita potenziale del bilancio, compresi limiti inefficaci alla crescita delle linee di business e scarso monitoraggio delle esposizioni fuori bilancio;*
- ii. *Comunicazioni inadeguate tra l'alta dirigenza, le linee di business e le funzioni di gestione del rischio;*
- iii. *Dipendenza da una gamma ristretta di misure di rischio basate su ipotesi rivelatesi errate e su processi di misurazione difficili da modificare una volta diventato evidente che le ipotesi sottostanti erano errate;*
- iv. *Un'attenzione insufficiente alle questioni relative alla valutazione, compreso l'eccessivo affidamento ai rating creditizi e lo sviluppo inadeguato di modelli per la valutazione di titoli complessi o potenzialmente illiquidi.*

In conclusione, il caso Barings rimane un esempio classico di come il fallimento nel gestire il rischio operativo possa portare a conseguenze catastrofiche per un'istituzione finanziaria.

Citiamo di seguito anche altri episodi di scandali bancari/incidenti di grandi dimensioni legati al rischio operativo.

Société Générale

Sono state notate carenze significative nei controlli interni, attività commerciali non autorizzate, pirateria informatica e violazione della fiducia che implicava uno sforzo consapevole da parte del trader disonesto di ingannare i suoi manager.

Jérôme Kerviel è accusato di aver causato enormi perdite da parte di un singolo trader non autorizzato. Nel corso del 2007 ha effettuato scambi non autorizzati per un valore di 30 miliardi di euro. sui futures delle Borse europee, aggiudicandosi entro la fine dell'anno 1,4 miliardi di euro. Dopo aver mascherato l'importanza della sua esposizione e dei suoi guadagni con operazioni fittizie, nel gennaio 2008 ha continuato a effettuare operazioni ancora più grandi. La banca ha dichiarato di aver deliberatamente deciso di perdere denaro nel 2008 per ridurre l'entità sospetta dei suoi guadagni del 2007.

È stato lo scandalo che ha scosso il mondo bancario. La banca francese Société Générale ha recentemente rivelato i dettagli di un disastro creato da un membro disonesto che è costato all'istituto 7,2 miliardi di dollari in operazioni fraudolente. Fu il più grande scandalo del genere nella storia a quella data.

Terremoto del 17 agosto 1999 e perdite bancarie

Il 17 agosto 1999 un terremoto di magnitudo MW 7,4 colpì le province di Kocaeli e Sakarya nella Turchia nordoccidentale, una regione densamente popolata nel cuore industriale della Turchia. Il terremoto del 17 agosto è considerato il più grande evento che abbia devastato un'area moderna e industrializzata dal terremoto di Tokyo del 1923. La tragedia ha creato gravi perdite e danni alle filiali bancarie. Le operazioni bancarie scoppiarono e il recupero di queste perdite richiese molto tempo e per i recuperi furono spese ingenti somme di denaro.

Daiwa Bank

Uno dei suoi dipendenti, Toshihide Iguchi, commerciava illegalmente negli Stati Uniti Buoni del Tesoro per oltre undici anni senza essere scoperti, causando alla banca una perdita accumulata di 1,1 miliardi di dollari. Toshihide Iguchi iniziò a commettere frodi nel 1984 per coprire le sue perdite iniziali nel trading di obbligazioni. Nel corso degli anni, continuò a nascondere perdite crescenti attraverso ulteriori operazioni illecite e falsificazioni contabili. Iguchi riuscì a nascondere le perdite falsificando registri contabili e distruggendo documenti relativi alle transazioni. La mancanza di controlli interni rigorosi e una supervisione adeguata facilitò le sue attività fraudolente. Nel 1995, Iguchi scrisse una lettera ai dirigenti della Daiwa Bank confessando le sue attività fraudolente e le perdite accumulate. La banca inizialmente tentò di gestire la situazione internamente, ma la notizia trapelò rapidamente, causando un grave danno reputazionale e finanziario.

Le autorità statunitensi, tra cui la Federal Reserve e il Dipartimento di Giustizia, intervennero rapidamente. La Daiwa Bank fu accusata di aver fallito

nel rilevare e prevenire la frode, e le fu imposto di chiudere tutte le sue operazioni negli Stati Uniti entro un periodo stabilito.

La banca fu multata per 340 milioni di dollari dalle autorità statunitensi, e diversi alti dirigenti furono costretti a dimettersi. Toshihide Iguchi fu arrestato e condannato a quattro anni di carcere per frode bancaria e altri reati.

Lo scandalo, però, causò un danno significativo alla reputazione della Daiwa Bank, portando a una ristrutturazione interna e alla fusione con altre banche giapponesi. Nel 2000, Daiwa Bank si fuse con Kinki Osaka Bank per formare Resona Bank, come parte di un più ampio consolidamento del settore bancario giapponese.

VI. Quadro Normativo

Sfondo Normativo e regolamentare di riferimento per la gestione dei rischi operativi in banche e assicurazioni.

Un grande apporto, se non quello principale, è stato fondamentale dato dal Comitato di Basilea per la vigilanza bancaria (CBVB). Tale Comitato è l'organizzazione principale preposta per la definizione degli standard internazionali per la regolamentazione prudenziale relativa al settore bancario. E' stato istituito nel 1974 dai governatori delle banche centrali dei Paesi del G10 in seguito ad alcuni gravi episodi di crisi del mercato finanziario internazionale, tra cui il fallimento della banca tedesca Herstatt.

I membri del Comitato provengono da 13 Paesi diversi: Belgio, Canada, Francia, Germania, Giappone, Gran Bretagna, Italia, Lussemburgo, Paesi Bassi, Spagna (che è membro da febbraio 2001), Stati Uniti, Svezia e Svizzera. Ogni Paese è rappresentato da esponenti della banca centrale e di eventuali altri organi di vigilanza sul sistema bancario.

Il Comitato rappresenta un foro per la discussione e la cooperazione in materia di vigilanza sull'attività bancaria internazionale. Inizialmente, il suo lavoro si è focalizzato su filiali e sussidiarie di banche estere e su come ripartire le relative responsabilità (funzione di vigilanza e funzione di prestatore di ultima istanza) fra autorità del Paese ospitante (host country) e quelle del Paese d'origine della casa-madre (home country).

Le proposte e le raccomandazioni del Comitato riguardavano solo l'attività bancaria internazionale svolta mediante filiazioni estere ed erano guidati da due principi: fare in modo che nessun insediamento bancario sfuggisse alla vigilanza di un'autorità e garantire che tale vigilanza fosse adeguata. Queste proposte e raccomandazioni sono sfociate poi in un documento "Il Concordato" del 1975, rivisto nel 1983.

Dalla seconda metà degli anni Ottanta, i compiti del Comitato si sono progressivamente estesi a tutti gli strumenti per rendere più efficace la vigilanza sulle banche. Il Comitato persegue questo obiettivo in tre modi: mediante lo scambio di informazioni sulle politiche di vigilanza dei singoli Paesi, migliorando le tecniche di vigilanza sull'attività bancaria internazionale e fissando standard di vigilanza minimi. In particolare, il Comitato ha dedicato grande attenzione ai requisiti minimi patrimoniali a cui spetta il compito di garantire la solvibilità delle singole istituzioni, e dunque la stabilità dell'intero sistema bancario internazionale, ma anche condizioni competitive uniformi alle banche dei diversi Paesi operanti su scala internazionale.

Il Comitato non dispone di alcun potere legislativo o autorità sopranazionale; le sue proposte non hanno alcun valore legale. Il suo compito è quello di definire linee-guida e raccomandazioni che possano poi essere recepite dalle singole autorità politiche e di vigilanza nazionali.

Il Comitato di Basilea riporta al Comitato dei Governatori delle banche centrali dei Paesi del G10, che si riunisce periodicamente presso la Banca dei Regolamenti Internazionali.

A partire dalla metà degli anni Novanta, il Comitato di Basilea ha sovente collaborato con l'International Organization of Securities Commissions (IOSCO), l'organo che riunisce le autorità di governo dei mercati regolamentati e di vigilanza sugli intermediari mobiliari.

Dal 1995, il Comitato e lo IOSCO hanno emesso numerosi rapporti congiunti sull'attività di negoziazione in strumenti derivati svolta dalle banche e dalle imprese d'investimento. Con riferimento alla vigilanza sui conglomerati finanziari, il Comitato di Basilea ha recentemente collaborato con le autorità di vigilanza del settore assicurativo e mobiliare, istituendo nel 1996 il Joint Forum of Financial Conglomerates, un organo incaricato di favorire la cooperazione e lo scambio di informazioni tra autorità di vigilanza.

Con il secondo accordo internazionale preposto per la misurazione del capitale e dei coefficienti patrimoniali, noto come Basilea II, è stata richiesta la creazione di 4 sottocomitati:

- **L'Accord Implementation Group (AIG):** questo comitato favorisce quello che è lo scambio di informazioni utili per adozione dell'accordo e delle strategie. All'interno di tale comitato si presenta anche un sottogruppo che gestisce le problematiche del rischio operativo.
- **La Capital Task Force (CTF):** questo comitato gestisce tutte le modifiche e le interpretazioni dell'accordo sul capitale.

- **Il Risk Management Group (RMG):** lo scopo di questo comitato è lo sviluppo di nuovi standard per la gestione del rischio operative e tecniche per i modelli di allocazione del capitale di vigilanza previsto sempre dagli accordi.
- **Il Transparency Group:** questo comitato ha il ruolo di esaminare i principi attinenti agli obblighi di informazioni che devono rispettare le banche.

La storia del Comitato di Basilea si inizia a concretizzare nel 1988, anno in cui fu proposto un sistema di misurazione dell'adeguatezza patrimoniale. Si giunge così a Basilea I. Il risultato che si voleva ottenere era quello di poter fissare e definire i requisiti di capitale di cui bisognava dotarsi per potersi proteggere dal rischio di credito.

Negli anni che vanno dal 1993 al 1996 si discusse a lungo circa l'inclusione nel primo accordo di alcuni parametri necessari e studiati solamente successivamente e vari approcci distinti per mitigare il rischio di mercato.

Ci furono poi numerosi sviluppi del settore che hanno condotto ad una vera e propria rivisitazione di Basilea I, anche successivamente a diverse criticità a cui furono esposte le banche.

Nel 1998 assistiamo alla nascita del nuovo accordo sul capitale: Basilea II.

Sebbene questa data segni la nascita dell'accordo, solamente ben 9 anni dopo entrerà completamente in vigore. Questo fu giustificato da una serie di studi aggiuntivi che furono fatti successivamente per poter riflettere al meglio sull'esposizione al rischio operativo di ogni singola banca e quantificare i requisiti di capitale necessari per proteggersi da tale rischio.

L'accordo si fonda su una tripartizione in tre pilastri⁶⁰:

- **Primo Pilastro:** all'interno di questo primo pilastro si espongono le modalità di calcolo dei requisiti patrimoniali complessivi che possano far fronte ai rischi di credito, di mercato e operativo. I requisiti di capitale, però, vengono stimati ad hoc da ogni banca, e per la determinazione ritroviamo tre elementi che costituiscono il capitale di vigilanza⁶¹: Patrimonio di base (Tier 1), Patrimonio supplementare (Tier 2) e Tier 3. Il patrimonio di base è costituito dal capitale azionario e le riserve palesi che sono gli unici elementi del capitale comuni ai diversi sistemi bancari

⁶⁰ Basel Committee on Banking Supervision, *International Convergence of Capital Measurement and Capital Standards: a Revised Framework, Comprehensive Version*, Bank for International Settlements, Basel, June 2006.

⁶¹ Il "capitale di vigilanza" si riferisce al capitale che una banca o un'istituzione finanziaria deve mantenere per soddisfare i requisiti regolamentari imposti dalle autorità di vigilanza finanziaria. Questo capitale è fondamentale per garantire la stabilità e la solvibilità dell'istituzione, proteggendo i depositanti e il sistema finanziario nel suo complesso. Lo scopo del Capitale di Vigilanza è quello di assicurare che le banche dispongano di risorse sufficienti per coprire perdite inattese, proteggendo così i depositanti, ridurre il rischio sistemico garantendo che le banche possano resistere a shock finanziari senza fallire, rafforzare la fiducia degli investitori e dei clienti nella solidità delle istituzioni finanziarie. Le autorità di regolamentazione monitorano costantemente il livello di capitale delle banche attraverso dei report periodici e ispezioni. In caso di non conformità, le banche possono essere soggette a sanzioni, restrizioni operative o altre misure correttive.

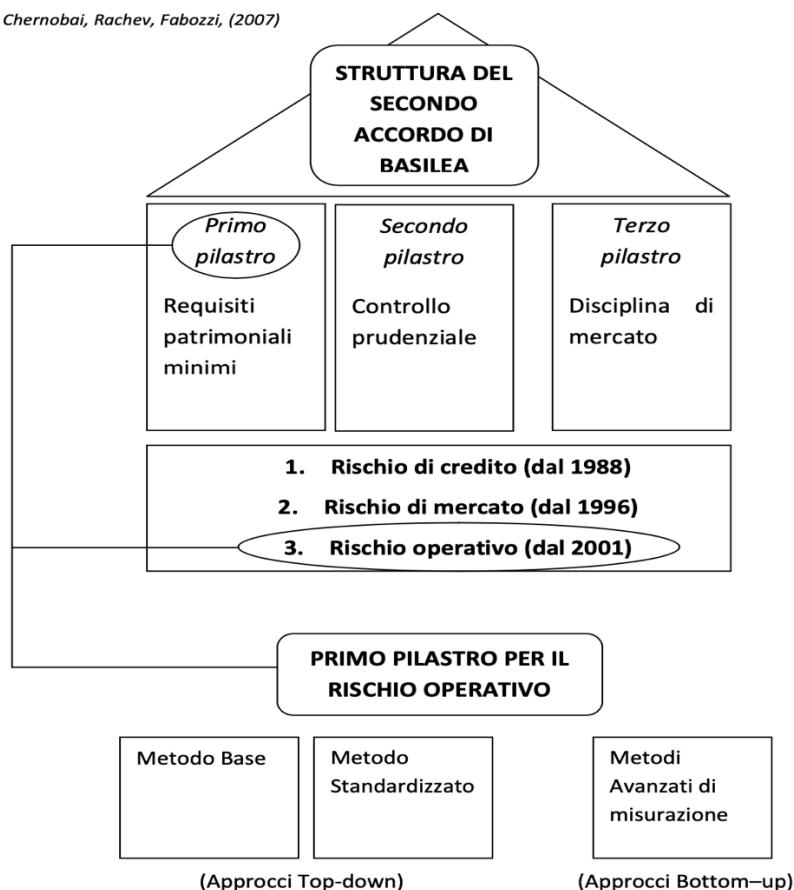
dei paesi. Il patrimonio supplementare è costituito da riserve occulte, dunque quelle non iscritte in bilancio, riserve di valutazione, accantonamenti generali/riserve generali per perdite su crediti e strumenti ibridi di capitale-debito. Il Tier 3, invece, è caratterizzato da debiti subordinati a breve termine e viene utilizzato principalmente per la copertura del rischio di mercato.

- **Secondo Pilastro:** in questo pilastro si presentano i principi essenziali per il controllo prudenziale, le linee guida per la gestione del rischio, e dunque azioni di trasparenza e responsabilità. Inoltre, si discute del trattamento del rischio di tasso di interesse nel banking book⁶², rischio di credito, cartolarizzazione. Il Comitato ha elencato, inoltre, dei principi fondamentali mediante i quali si svolge l'attività di supervisione del capitale di vigilanza. Bisogna disporre di un procedimento atto al controllo dell'adeguatezza patrimoniale delle banche in rapporto al loro profilo di rischio e strategia di mantenimento, è possibile adottarlo anche con delle supervisioni da parte del CdA e dell'alta direzione; le autorità di vigilanza richiedono che le istituzioni bancarie praticino le loro funzioni operative avendo una dotazione patrimoniale che non sia mai al di sotto dei coefficienti minimi obbligatori, ma sempre al di sopra, così da creare un cuscinetto.
- **Terzo Pilastro:** qui è ricompresa tutta la parte dedicata alla Disciplina di Mercato. Lo scopo è quello di individuare un insieme di requisiti di trasparenza informativa che faranno in modo di consentire a chi opera nel mercato di disporre di informazioni indispensabili sull'esposizione ai rischi, sui processi di valutazione dei rischi e sull'adeguatezza patrimoniale degli intermediari. Alle banche è richiesto di fornire delle descrizioni dettagliate sulla loro struttura di capitale, sulle strategie di gestione del rischio che vogliono adottare, delle politiche di trasferimento del rischio operativo e anche del processo di valutazione che adottano nello stabilire l'onere da rischio operativo che deve gravare sul capitale.

È stato riportato uno schema riassuntivo del Secondo Accordo di Basilea che ha un collegamento con i capitoli precedenti nei quali abbiamo ampiamente discusso dei diversi metodi presenti nel primo pilastro relativo al rischio operativo.

⁶² Il "banking book" (portafoglio bancario) si riferisce alla parte del bilancio di una banca che comprende tutte le attività finanziarie che sono destinate a essere mantenute fino alla scadenza o per un lungo periodo, piuttosto che essere negoziate a breve termine. Le attività nel banking book sono principalmente investimenti e prestiti che la banca intende tenere per generare reddito tramite interessi e non per la loro rivendita.

Fonte: Chernobai, Rachev, Fabozzi, (2007)



La questione del rischio operativo è stata ampiamente trattata anche in Basilea III.

Basilea III è un insieme di riforme normative sviluppate sempre dal Comitato di Basilea per la vigilanza bancaria, progettato per rafforzare la regolamentazione, la supervisione e la gestione del rischio all'interno del settore bancario. Queste riforme sono state introdotte in risposta alla crisi finanziaria del 2007-2008 che ha evidenziato gravi lacune nei requisiti patrimoniali e di liquidità delle banche.

L'obiettivo principale di Basilea III è aumentare la resilienza delle banche agli shock economici e finanziari, migliorando la loro capacità di assorbimento delle perdite senza ricorrere all'intervento dei contribuenti.

I principali elementi qualificanti del nuovo schema di adeguatezza patrimoniale delle banche sono i seguenti:

- Una maggiore qualità del capitale perseguita con tre strumenti: un innalzamento dei requisiti minimi di "common equity" che salgono dal 2% al 4,5% dell'attivo ponderato; l'applicazione, in sede di calcolo del common equity, di una serie di deduzioni prudenziali rivolte, tra l'altro, ad evitare delle sorprese negative nelle fasi di crisi economica; la graduale esclusione dal patrimonio di vigilanza, degli strumenti innovativi di capitale giudicati non sufficientemente "solidi" dal Comitato;

- L'introduzione di un requisito patrimoniale addizionale pari al 2,5% delle attività ponderate per il rischio (*il capital conservation buffer*) volto ad assicurare che le banche mantengano un cuscinetto di capitale da utilizzare per l'assorbimento delle perdite connesse in fasi di elevata turbolenza economica o finanziaria e la possibile introduzione, a discrezione delle autorità di vigilanza nazionali, di un'ulteriore requisito patrimoniale di natura anticiclica (*counter-cyclical buffer*) anch'esso fino al 2,5% delle attività ponderate per il rischio;
- L'introduzione di un tetto alla leva finanziaria delle banche, richiedendo che il patrimonio di vigilanza sia almeno pari al 3% totale dell'attivo non ponderato;
- L'introduzione di nuovi coefficienti minimi a presidio del rischio di liquidità (*liquidity coverage ratio e net stable funding ratio*);
- L'introduzione di nuovi requisiti a fronte del rischio di mercato e del rischio di controparte.

| Tipo di requisito | Entità, in percentuale dei RWA | Basilea 2 | Basilea 3 |
|---|---|-----------|--------------------|
| Common Equity | a.minimo; b.conservation buffer, c.totale (a+b) | 2% | 4,5% 2,5% 7% |
| Tier 1 Capital Ratio | d.minimo e.Totale (c+b) | 4% | 6% 8,5% |
| Total Capital Ratio | f.minimo g.totale (f+b) | 8% | 8% 10,5% |
| Requisiti addizionali macroprudenziali | h.buffer anticiclico i.requisito addizionale per banche sistemiche | | 0-2,5% 1%-3% |

I Nuovi requisiti sono stati introdotti con gradualità, ma a partire dal 2019 sono stati considerati nel complesso pienamente operativi.

È stata fornita anche una nuova definizione di patrimonio di vigilanza (*regulatory capital*) che è diventata più restrittiva.

La nuova normativa attribuisce un ruolo prevalente al capitale di maggiore qualità (*common equity*) composto unicamente dal capitale azionario versato e dalle riserve utili, e deve rappresentare almeno il 4,5% degli attivi ponderati per il rischio.

Basilea III prevede altri due principali aggregati: il patrimonio di base (Tier 1, pari almeno al 6% degli attivi ponderati) e quello supplementare (Tier 2). Viene eliminato il Tier 3.

Il Tier 1 è detto *going concern capital* in quanto può assorbire le perdite lasciando proseguire la banca nella propria attività senza alcun bisogno di metterla in liquidazione. Si compone di: *common equity* Tier 1 (o CET1) che include strumenti contraddistinti da precise caratteristiche come la durata perpetua e la mancanza di un obbligo di distribuzione di dividendi, e altri strumenti di Tier 1 (o AT1) i quali devono rispettare alcuni criteri come la subordinazione rispetto ai restanti creditori della banca, la mancanza di un obbligo di distribuire dividendi, l'assenza di garanzie da parte della banca o di meccanismi di step up.

Il patrimonio supplementare (Tier 2) è detto *gone concern capital* dato che può assorbire le perdite soltanto se la banca viene preventivamente messa in liquidazione. Comprende un'unica categoria di strumenti, cioè i prestiti subordinati che sono caratterizzati da una scadenza originale di almeno cinque anni, rimborsabili anticipatamente su iniziativa dell'emittente.

Per quanto concerne il rischio operativo, Basilea ha eliminato l'approccio dei modelli avanzati (in base al quale ogni banca era libera di sviluppare un proprio modello richiedendone poi la validazione alle autorità) e unifica gli altri due approcci (l'approccio basic e l'approccio standard) rendendoli più sensibili al rischio.

Il nuovo requisito per il rischio operativo sarà dato dal prodotto di due fattori, il *basic indicator component* (BIC) e il cosiddetto *internal loss multiplier* (ILM).

Il BIC è una misura di quanto una banca sia potenzialmente esposta al rischio operativo ed è dato dalla somma di tre aggregati: i proventi da interessi, dividendi e locazioni finanziarie, i ricavi da servizi e i proventi finanziari. Per ognuno di essi, il dato di bilancio medio degli ultimi anni verrà moltiplicato per un coefficiente che dipende dalle dimensioni: 12% per valori inferiori al miliardo di euro, 18% per valori superiori a 30 miliardi di euro, 15% per valori intermedi.

Il secondo fattore ILM misura quanto la banca, in passato, si sia dimostrata concretamente capace di controllare i rischi operativi e dipende dalla media storica delle relative perdite. In questo modo le banche virtuose con poche perdite vengono "premate" con un minor requisito di capitale. Questo si calcola con il seguente approccio algoritmico che confronta le perdite passate (*loss component, LC*) con il BIC:

$$ILM = \ln \left(e + \frac{LC}{BIC} - 1 \right)$$

La componente LC è data da una media ponderata delle perdite passate, dove le perdite particolarmente consistenti (oltre €10 milioni o oltre €100 milioni) ricevono ponderazioni via via più alte, così da “punire” con un ILM particolarmente elevato le banche che hanno sofferto delle perdite molto elevate.

Conclusioni

La gestione dei rischi operativi rappresenta una componente essenziale per la stabilità e la sostenibilità del settore finanziario. Attraverso questa tesi, abbiamo esplorato in modo dettagliato le diverse dimensioni del rischio operativo, fornendo un quadro completo delle tipologie di rischio, dei metodi di quantificazione, delle criticità intrinseche e delle strategie di gestione e mitigazione. Questo percorso ci ha permesso di comprendere come l'attenzione alla gestione del rischio operativo non sia solo una questione di conformità normativa, ma una necessità strategica per la sopravvivenza e la competitività delle istituzioni finanziarie.

Nel primo capitolo, abbiamo definito e classificato i rischi operativi, identificando le principali categorie che includono il rischio di frode interna ed esterna, il rischio di fallimento dei sistemi e dei processi, e il rischio legale e di conformità. Questa analisi ha evidenziato come ogni categoria presenti sfide uniche che richiedono approcci specifici per essere gestite efficacemente.

Il secondo capitolo ha fornito una panoramica sui principali metodi di quantificazione dei rischi operativi. L'analisi del Basic Indicator Approach, dello Standardised Approach, dell'Advanced Measurement Approach e dello stress testing ha messo in luce le peculiarità di ciascun metodo. Abbiamo evidenziato come i metodi più avanzati, seppur complessi e costosi, offrano una maggiore precisione e affidabilità nelle stime del rischio rispetto ai metodi più semplici.

Tuttavia, nel terzo capitolo, abbiamo discusso i limiti e le criticità associate alla quantificazione dei rischi operativi. La disponibilità e qualità dei dati, le difficoltà nella modellizzazione del rischio e l'incertezza intrinseca dei modelli rappresentano ostacoli significativi. Queste problematiche richiedono un approccio cauto e una continua revisione dei modelli utilizzati, per evitare che le stime del rischio siano fuorvianti o inaccurate.

Nel quarto capitolo, abbiamo esplorato le strategie di gestione e mitigazione del rischio operativo, con un focus particolare sul ruolo della compliance. Attraverso il caso studio della crisi della Barings Bank, abbiamo illustrato come la mancata gestione del rischio operativo possa portare a conseguenze catastrofiche. Questo esempio ha sottolineato l'importanza di una cultura aziendale orientata alla gestione del rischio e di una funzione di compliance forte e ben integrata nei processi decisionali.

Infine, il quinto capitolo ha esaminato il quadro normativo di riferimento per la gestione dei rischi operativi in banche e assicurazioni. L'analisi delle normative internazionali, come Basilea III, e delle regolamentazioni specifiche per il settore assicurativo, ha mostrato come queste direttive siano fondamentali per garantire una gestione efficace e coerente dei rischi operativi. Tuttavia, abbiamo anche evidenziato come la conformità normativa, sebbene necessaria, non sia sufficiente da sola a garantire la resilienza delle istituzioni finanziarie, che devono adottare un approccio proattivo e integrato alla gestione del rischio.

In conclusione, la quantificazione e gestione dei rischi operativi costituiscono una sfida complessa ma imprescindibile per le banche e le assicurazioni. Come ha affermato Peter Drucker, "*Quello che non si può misurare, non si può migliorare.*" Questo principio è particolarmente vero nel contesto del rischio operativo, dove la capacità di misurare accuratamente il rischio è la base su cui costruire strategie efficaci di mitigazione e gestione.

Il nostro viaggio attraverso le varie sfaccettature della quantificazione dei rischi operativi ha evidenziato l'importanza di una comprensione approfondita e di un approccio integrato e multidisciplinare. Solo così le istituzioni finanziarie potranno affrontare le sfide del futuro, mantenendo la loro stabilità e contribuendo alla fiducia nel sistema finanziario globale.

Riferimenti Bibliografici

A. Resti, A. S. (2021). *Rischio e valore nelle banche*. Milano: Egea Editore.

Alexander, C. (2003). *Operational Risk: Regulation, Analysis and Management*. London: Pearson Education.

Bolzoni, S. (2016). *Rischio operativo: metodi di quantificazione e gestione*. Milano: Egea Editore.

Capuano, G. &. (2007). *Il rischio operativo nelle banche*. Bologna: Il Mulino.

- Carretta, A. &. (2011). *Gestione del rischio e valore nelle banche*. Milano: McGraw-Hill Education.
- Cruz, M. (2002). *Modeling, Measuring and Hedging Operational Risk*. Chichester: Wiley.
- Deloitte. (2012). *The Advanced Measurement Approach to Operational Risk*. London: Deloitte.
- d'Italia, B. (2013). *Regolamentazione prudenziale per le banche*. Roma.
- Embrechts, P. F. (2005). *Quantitative Risk Management: Concepts, Techniques, and Tools*. Princeton, NJ: Princeton University Press.
- Fiodelisi, F. &. (2010). *Rischio operativo: metodologie e applicazioni*. Milano: Egea Editore.
- Giudici, P. &. (2009). *Risk management nelle banche*. Bologna: Il Mulino.
- Gualandri, E. &. (2009). *Risk management nelle banche*. . Bologna: Il Mulino.
- Sadgrove, K. (2015). *The Complete Guide to Business Risk Management*. Farnham: Gower.
- Supervision, B. C. (2006). *International Convergence of Capital Measurement and Capital Standards*. Basel: Bank for International Settlements.
- Vento, G. A. (2010). *La gestione del rischio operativo nelle banche*. Bologna: Il Mulino.