Policy per il controllo e la gestione dei Rischi Operativi

Consiglio di Amministrazione del 26 luglio 2023

Indice

1 Premessa

Flowe S.p.A. – Società Benefit o Flowe S.p.A. (di seguito anche Flowe o la Società), interamente controllata da Banca Mediolanum S.p.A., è stata costituita in data 19 luglio 2019 ed è iscritta all'Albo degli Istituti di moneta elettronica – IMEL tenuto dalla Banca d'Italia ai sensi dell'art. 114 quater del D. Lgs. n. 385/1993.

La società, in qualità di Istituto di Moneta Elettronica ha per oggetto: (i) l'attività di emissione e gestione di moneta elettronica; (ii) la prestazione di servizi di pagamento, anche non connessi con tale attività, e (iii) la concessione di finanziamenti nel rispetto di quanto previsto dalle applicabili previsioni di legge e di regolamento con riguardo agli istituti di moneta elettronica e alla loro operatività.

Flowe può altresì esercitare servizi operativi e servizi strettamente connessi, sia all'emissione di moneta elettronica, sia alla prestazione di servizi di pagamento, nel rispetto di quanto previsto dalle applicabili previsioni di legge.

Il contesto del mercato bancario e dei pagamenti in Italia, in cui Flowe si inserisce, è caratterizzato da un crescente livello di maturità digitale, che può essere osservato attraverso lo sviluppo dei pagamenti "cashless" ed il crescente trend di utilizzo del Mobile Banking.

Tale situazione, pone sempre maggiore attenzione ai sistemi di identificazione e gestione dei rischi operativi e, in particolare, a quelli informatici e di sicurezza per i cui presidi specifici si rinvia alle Policy di riferimento.

Modalità e strumenti di controllo di tali rischi, sono in continua evoluzione ed aggiornamento sia in considerazione delle modifiche al contesto normativo che dei continui cambiamenti esogeni ed endogeni del *business* di riferimento del Gruppo Bancario Mediolanum.

Il Consiglio di Amministrazione di Flowe ha nominato un responsabile del Risk Management che si avvale, per lo svolgimento delle attività di controllo dei rischi operativi, della omologa funzione della Capogruppo[1], in base ad un apposito contratto di outsourcing.

Il presente documento è stato elaborato a partire dal framework metodologico in uso presso la Capogruppo Banca Mediolanum S.p.A. e trasmesso alle società del Gruppo Bancario.

La Funzione Risk Management svolge i propri compiti in modo autonomo ed indipendente, svincolata da rapporti gerarchici rispetto ai responsabili dei settori di attività sottoposti a controllo.

Si ricorda che, la Società Flowe S.p.A., non è soggetta a requisito patrimoniale individuale a fronte dei rischi operativi ma concorre al calcolo del requisito patrimoniale consolidato del Gruppo Bancario Mediolanum.

A tal riguardo, in conformità al Regolamento UE 575/2013, che non consente l'utilizzo combinato dei metodi Base e Standardizzato per il calcolo del requisito di fondi propri a fronte del rischio operativo, se non in circostanze eccezionali, si segnala che anche la società Flowe, utilizza la metodologia Standardizzata.

[1] Per semplicità, nel seguito del documento, con Funzione Risk Management o Unità Operational Risk Management si intende quella della Capogruppo che, in base ad apposito contratto di outsourcing, svolge le attività di controllo dei rischi operativi illustrate nel presente documento. Resta inteso che tali attività sono svolte in accordo e sotto la supervisione del responsabile della Funzione Risk Management nominato dal Consiglio di Amministrazione di Flowe.

1.1 AMBITO DEL DOCUMENTO

Il presente documento definisce le regole di governo e le politiche di gestione dei rischi operativi da adottare nell'ambito della società Flowe S.p.A.

Nello specifico, questo documento ha l'obiettivo di:

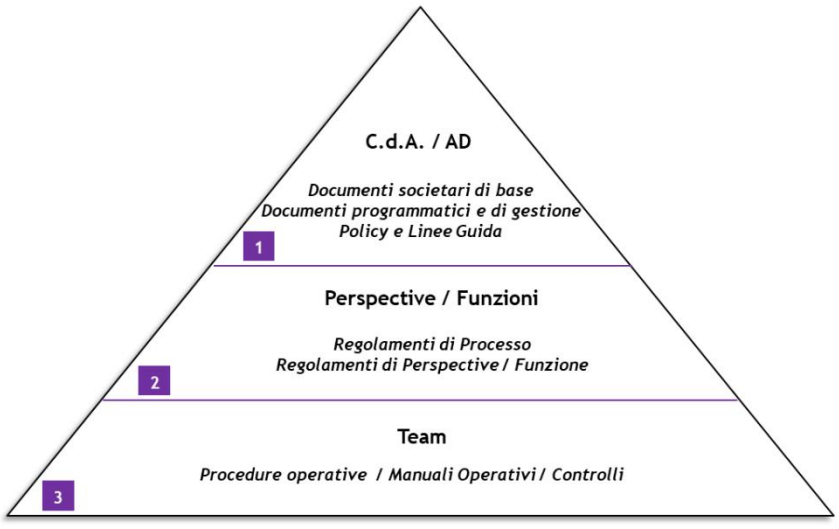
- individuare i principi generali di *governance* dei Rischi Operativi, le finalità, le regole metodologiche e gli strumenti utilizzati per la loro gestione;
- dettagliare i compiti e le responsabilità delle entità organizzative coinvolte ed i processi del *framework* di gestione dei rischi operativi;
- definire i modelli di riferimento per l'individuazione dei rischi operativi e le metodologie per la loro misurazione quantitativa e qualitativa;
- assicurare la conformità con i requisiti espressi dalle Autorità di Vigilanza in materia di rischi operativi;
- fornire una definizione di *Operational Risk* e dotare la società di un glossario di riferimento per le tematiche relative alla gestione dei rischi operativi.

Le unità organizzative della società sono chiamate, a vario titolo, a supportare il processo di controllo e gestione dei rischi operativi ciascuna nei limiti della propria competenza ed in funzione del grado di esposizione ai fattori di rischio e della complessità organizzativa dell'attività svolta.

Il coinvolgimento delle strutture della società in tale processo, definito nel dettaglio nel corso del documento, favorisce la diffusione a tutti i livelli aziendali della "cultura della gestione del rischio".

Con riferimento alla "Policy sulle modalità di redazione, approvazione, diffusione ed aggiornamento della Normativa Interna" di Flowe, il presente documento si colloca al livello di vertice della piramide documentale richiamata nello schema seguente.

Modello della normativa interna di riferimento



1.2 DESTINATARI DEL DOCUMENTO

Il presente documento è approvato dal Consiglio di Amministrazione di Flowe S.p.A. e diffuso all'interno della Società.

1.3 RESPONSABILITÀ DEL DOCUMENTO

L'aggiornamento e la revisione del presente documento sono di responsabilità della Funzione Risk Management di Flowe.

1.4 PERIMETRO DI APPLICAZIONE

I rischi operativi, a differenza dei rischi finanziari e di credito, non si limitano alle attività di investimento e gestione patrimoni o alle attività di erogazione, ma hanno caratteristiche di pervasività sull'intera struttura aziendale.

Alla luce delle caratteristiche dei rischi operativi, il processo di identificazione, misurazione monitoraggio e gestione degli stessi non può prescindere dall'analisi delle attività delle Società del Gruppo Bancario rispetto ai principali processi aziendali.

Le società ambito di applicazione del modello di *governance* dei rischi operativi sono, *in primis*, le società del Gruppo Bancario Mediolanum, a cui Flowe S.p.A. appartiene, e che, con presidi diretti o decentrati, adottano il framework predisposto da Banca Mediolanum in funzione della complessità delle attività svolte, dell'esposizione ai rischi operativi e delle indicazioni normativo – regolamentari specifiche, nel rispetto del principio di proporzionalità.

2 Definizioni e Principi

Nel presente capitolo sono richiamate le principali definizioni relative alle attività di controllo e gestione dei rischi operativi.

2.1 RISCHI OPERATIVI: DEFINIZIONE E MISSIONE

Il Gruppo Mediolanum definisce i rischi operativi come:

"il rischio che comportamenti illegali o inappropriati dei collaboratori, carenze o malfunzionamenti tecnologici, errori o carenze nei processi operativi e fattori esterni possano generare perdite economiche o danni patrimoniali e talvolta impatti di carattere legale - amministrativo".

Possiamo pertanto definire l'*Operational Risk Management* (di seguito ORM) presso il Gruppo Bancario Mediolanum come il processo dedicato all'identificazione, misurazione, monitoraggio e gestione del rischio operativo, nel rispetto delle linee guida in tema di rischi e del loro controllo, espresse dal Consiglio di Amministrazione.

Tale obiettivo generale si declina nei seguenti obiettivi specifici:

- identificare e valutare il profilo di rischio operativo esistente in unità organizzative, prodotti, processi, sistemi informativi;

- supportare le scelte strategiche fornendo una valutazione dei rischi operativi insiti in nuove attività, prodotti, processi, accordi di esternalizzazione e sistemi;
- progettare e realizzare interventi volti a ridurre, trasferire e/o mitigare i rischi operativi, anche con il coinvolgimento delle linee operative;
- diffondere la cultura della gestione del rischio all'interno della società e favorire comportamenti e scelte operative consapevoli e coerenti;
- dotarsi di un sistema di gestione dei rischi operativi integrato, prevedendo un coordinamento con le attività svolte da tutte le unità deputate ad attività specialistiche nonché una stretta interrelazione con i referenti di linea.

2.2 TERMINOLOGIA IN USO PER IL CONTROLLO E LA GESTIONE DEI RISCHI OPERATIVI

Si riportano di seguito le definizioni dei principali termini in uso nel processo di controllo e gestione dei rischi operativi. Tali definizioni si rendono necessarie per permettere a tutti gli attori coinvolti nella gestione dei rischi operativi di utilizzare termini e acronimi che sottintendono processi e modalità coerenti in materia di rischi operativi.

BUSINESS LINE

Le attività del Gruppo Bancario possono essere suddivise in un numero standard di *business line,* per riflettere il differente profilo di rischio all'interno del Gruppo.

Nell'approccio Standardizzato sono previste le seguenti otto linee di *business:*

- Corporate Finance;
- Trading and Sales;
- Retail Banking;
- Commercial Banking;
- Payment and Settlement;
- Agency Services;
- Asset Management;
- Retail Brokerage.

BASIC INDICATOR APPROACH (BA O BIA)

Metodo base di misurazione del capitale regolamentare: prevede il calcolo del requisito patrimoniale come una percentuale della media triennale dell'indicatore rilevante (15%).

STANDARDISED APPROACH (TSA O SA)

Approccio *standardizzato* di misurazione del capitale regolamentare: gli enti calcolano il requisito in materia di fondi propri per il rischio operativo come la media triennale della somma dei requisiti annuali in materia di fondi propri per tutte le *business line.* Il requisito

annuale in materia di fondi propri per ogni linea di attività è pari al prodotto del corrispondente fattore beta (specifico coefficiente definito dall'organo di vigilanza) e della parte dell'indicatore rilevante classificata nella linea di attività interessata.

ADVANCED MEASUREMENT APPROACH (AMA)

Secondo tale approccio, il capitale regolamentare per i rischi operativi è pari alla misura di rischio generata dai modelli interni di quantificazione, subordinatamente ai requisiti qualitativi e quantitativi espressi dal Regolamento UE n. 575/2013.

RISK SELF ASSESSMENT (RSA)

Il *Risk Self Assessment* rappresenta un processo di autovalutazione del profilo di rischio delle UO/società appartenenti al Gruppo tramite l'utilizzo di questionari *ad hoc* da sottoporre ai responsabili delle unità organizzative che possono generare/gestire i rischi operativi.

RISK SELF ASSESSMENT INTEGRATO

Il processo di Risk Self Assessment Integrato ricomprende l'analisi dei rischi operativi, ivi compresi quelli ICT, di sicurezza e reputazionali, giungendo ad una valutazione dei fattori di rischio e dei controlli. Il fulcro del processo integrato è l'*event type* di 2° livello del rischio operativo. La riconduzione al modello degli eventi favorisce lo sviluppo di una visione di insieme della rischiosità afferente a un dato processo o unità organizzativa, giungendo così ad una valutazione della rischiosità complessiva per ogni dimensione organizzativa indagata.

KEY RISK INDICATOR (KRI)

Sono indicatori di rischio raccolti e analizzati al fine di individuare in anticipo situazioni di rischiosità operativa e reputazionale, anche potenziale, da sottoporre ad analisi.

LOSS DATA COLLECTION (LDC)

Processo che consente l'individuazione, il censimento, la validazione ed il monitoraggio delle perdite operative e garantisce il mantenimento di un elevato standard qualitativo in termini di attendibilità, completezza e tempestività delle informazioni raccolte e delle serie storiche dei dati di perdita.

OPERATIONAL RISK MANAGEMENT (ORM)

Processo di identificazione, misurazione, monitoraggio e gestione del rischio operativo, nel rispetto della propensione al rischio espressa dall'azionista attraverso il Consiglio di Amministrazione.

EL *EXPECTED LOSS* (PERDITA ATTESA)

Valore atteso (medio) delle perdite operative, riferite ad una "classe di rischio" o all'intera società, che si manifestano entro un intervallo temporale di un anno.

UL *UNEXPECTED LOSS* (PERDITA INATTESA)

Perdita eccedente la perdita attesa, riferita ad una "classe" o all'intera società, calcolata sulla distribuzione di rischio a un livello di confidenza del 99,9% su un orizzonte temporale di un anno.

2.3 PRINCIPI ORGANIZZATIVI: IL CONTROLLO RISCHI OPERATIVI NEL SISTEMA DEI CONTROLLI INTERNI

Il sistema dei controlli interni è costituito dall'insieme delle regole, delle procedure e delle strutture organizzative che mirano ad assicurare l'efficacia ed efficienza dei processi aziendali, la salvaguardia del valore del patrimonio aziendale e la buona gestione di quello detenuto per conto della clientela, l'affidabilità e integrità delle informazioni contabili e gestionali, nonché la conformità delle operazioni con la legge, la normativa di vigilanza, le norme di autoregolamentazione e le disposizioni interne dell'impresa.

I soggetti che svolgono funzioni di amministrazione e direzione rivestono un ruolo fondamentale per la definizione di un adeguato sistema organizzativo e per la realizzazione di un efficiente sistema dei controlli interni.

L'attività di controllo non può essere demandata esclusivamente ad alcuni specifici uffici o agli organi collegiali di sorveglianza e controllo. Tutte le funzioni devono avere un proprio ruolo nel verificare le operazioni poste in essere, secondo differenti livelli di responsabilità.

In generale, è compito degli Organi di vertice promuovere la diffusione di una cultura dei controlli che renda, a tutti i livelli, il personale consapevole del proprio ruolo, anche con riferimento alle attività di controllo, e favorisca il coinvolgimento di tutte le strutture aziendali nel perseguimento degli obiettivi della Società.

Il Sistema dei Controlli Interni della Società è articolato secondo più livelli che prevedono:

- **controlli di linea (c.d. "controlli di primo livello"):** diretti ad assicurare il corretto svolgimento delle operazioni. Tali controlli sono effettuati dalle stesse strutture operative (ad es., controlli di tipo gerarchico, sistematici ed a campione), anche attraverso unità dedicate esclusivamente a compiti di controllo che riportano ai responsabili delle strutture operative (ovvero eseguiti nell'ambito del back office) e, quando possibile, sono incorporati nelle procedure informatiche. Secondo tale configurazione, le strutture operative sono le prime responsabili del processo di gestione dei rischi. Nel corso dell'operatività giornaliera tali strutture sono chiamate, infatti, ad identificare, misurare o valutare, monitorare, attenuare e riportare i rischi derivanti dall'ordinaria attività aziendale in conformità con il processo di gestione dei rischi. Inoltre, tali strutture devono rispettare i limiti operativi loro assegnati coerentemente con gli obiettivi di rischio e con le procedure in cui si articola il processo di gestione dei rischi;

- **controlli sulla gestione dei rischi e di conformità alle norme (c.d. controlli di secondo livello):** hanno l'obiettivo di assicurare: (i) il rispetto dei limiti assegnati alle varie funzioni operative; e (ii) la coerenza dell'operatività delle singole aree produttive con gli obiettivi di rischio-rendimento assegnati, nonché la conformità dell'operatività aziendale alle norme, incluse quelle di autoregolamentazione. Essi sono affidati a strutture diverse da quelle produttive; le funzioni di controllo concorrono alla definizione delle politiche di governo e del processo di gestione dei rischi aziendali. Nello specifico, tali funzioni sono:

    - Funzione di controllo dei rischi (Risk Management);

- Funzione di conformità alle norme (Compliance);
- Funzione di antiriciclaggio;

- **revisione interna (internal audit, c.d. controlli di terzo livello):** in tale ambito rientra la valutazione periodica della completezza, della funzionalità e dell'adeguatezza del sistema dei controlli interni, inclusi quelli sul sistema informativo (ICT audit), con cadenza prefissata in relazione alla natura e all'intensità dei rischi. L'attività è condotta da funzioni diverse e indipendenti da quelle produttive, anche attraverso verifiche in loco.

Per svolgere efficacemente la propria attività di controllo dei rischi, gli addetti della funzione Risk Management hanno accesso a tutte le informazioni aziendali relative sia ai comportamenti sia alle procedure e ai processi interni; ai fini dell'esercizio del controllo, gli addetti possono avvalersi dei dati e delle informazioni rivenienti dai controlli di linea, dal sistema informativo aziendale, dalle verifiche e dagli *assessmen*t effettuati sul posto interagendo direttamente con il personale interessato.

Le modalità di impiego degli strumenti di controllo sono strettamente funzionali alla natura, alle finalità, all'estensione dell'azione di controllo di competenza.

2.4 PRINCIPI GENERALI DELLA GOVERNANCE DEI RISCHI OPERATIVI

Al fine del conseguimento degli obiettivi sopra delineati, il processo di controllo e gestione dei rischi operativi si basa su una serie di principi generali volti alla definizione di un *framework* di controllo dei rischi organico, sistematico e funzionale.

Il suddetto processo rispetta i dettami ed i vincoli di carattere normativo espressi dagli organi competenti e garantisce il perseguimento degli obiettivi fondamentali che una gestione integrata dei rischi operativi richiede.

La definizione di un sistema di *governance* dei rischi non può prescindere dai seguenti principi di carattere generale:

- **completezza** nelle tipologie e nella localizzazione dei rischi operativi da governare;
- **indipendenza** delle funzioni di controllo dei rischi operativi dalle Unità Organizzative (di seguito anche "UO");
- **condivisione e coerenza** fra tutte le unità organizzative e/o società appartenenti al medesimo Gruppo relativamente all'utilizzo di modelli e metodologie uniformi per la raccolta dei dati e delle informazioni e per l'analisi e la misurazione dei rischi;
- **tempestività e continuità** nelle fasi di analisi e misurazione dei rischi e conseguente produzione della reportistica a supporto dei processi decisionali e di controllo;
- **trasparenza e diffusione dei modelli**, delle metodologie e dei criteri di analisi e misurazione utilizzati al fine di facilitare il processo di diffusione culturale e la comprensione delle logiche sottostanti le scelte adottate;
- **responsabilizzazione e delega** da parte del Consiglio di Amministrazione verso le UO nella gestione dei rischi operativi.

Al fine di garantire il rispetto dei principi appena definiti, Flowe adotta la presente Policy che definisce il quadro di riferimento generale per la gestione ed il controllo dei rischi operativi, nell'ambito del modello di rischio di Gruppo.

3 La *governance* di controllo e gestione dei rischi operativi

3.1 GLI OBIETTIVI DELLA GOVERNANCE

I principali obiettivi da perseguire nel governo dei rischi operativi per rispondere pienamente ai fattori di cambiamento che stanno caratterizzando il contesto competitivo e normativo di riferimento e nel rispetto della *mission* dell'ORM, sono i seguenti:

- contribuire a preservare il capitale economico aziendale e massimizzare il valore economico per l'azionista, evitando esposizioni incoerenti rispetto alle linee guida in tema di rischi e di loro monitoraggio definite dal Consiglio di Amministrazione;
- assicurare che i rischi potenzialmente presenti nelle differenti aree operative siano correttamente identificati, misurati, controllati e gestiti secondo metodologie e procedure formalizzate, condivise e continuativamente sottoposte ad attività di manutenzione;
- mantenere la qualità dei sistemi e dei processi di gestione del rischio allineati agli *standard* delle *best practice* di mercato;
- garantire la produzione di informativa e reportistica accurate e tempestive per i diversi livelli organizzativi responsabili delle attività di gestione e di controllo;
- assicurare il rispetto dei requisiti organizzativi previsti in materia dagli organismi di Vigilanza nazionali ed internazionali;
- promuovere la diffusione sistematica di una cultura coerente ed omogenea di gestione dei rischi operativi.

3.2 ARCHITETTURA ORGANIZZATIVA DI RIFERIMENTO

L'architettura organizzativa di supporto al processo di gestione dei rischi operativi è costituita da una serie di entità organizzative e dalle loro interrelazioni.

Il disegno del modello organizzativo per la gestione dei rischi operativi all'interno del Gruppo Bancario Mediolanum deve essere tale da garantire:

- la coerenza con il modello organizzativo ed il rispetto dei vincoli e delle relazioni interne esistenti;
- il coinvolgimento di molteplici unità organizzative nell'ambito del processo ORM;
- l'ottimizzazione e la valorizzazione dei presidi organizzativi, delle interrelazioni e dei flussi informativi intercorrenti fra le unità organizzative esistenti.

Gli attori coinvolti nel processo di ORM sono molteplici e sono diffusi in tutte le realtà organizzative del Gruppo.

In particolare, le attività previste a livello regolamentare e gestionale di identificazione, misurazione, mitigazione e reportistica dei rischi operativi sono svolte in outosourcing dall'Unità Operational Risk Management di Banca Mediolanum.

Per Flowe, tale unità:

- definisce il modello di controllo e gestione del rischio operativo, del rischio ICT e di sicurezza e dei rischi derivanti dagli accordi di esternalizzazione, aggiornando le rispettive Policy di riferimento, in linea con i modelli definiti dalla Capogruppo;
- pianifica e svolge gli assessment dei rischi operativi e reputazionali, aggiornando i punti di controllo associati alle unità organizzative analizzate (risk factor control assessment) e le valutazioni dei rischi relative alle attività esternalizzate;
- identifica (con il risk owner) le azioni di mitigazione dei rischi operativi e ne monitora il completamento;
- svolge le campagne periodiche di analisi di rischio ICT e di sicurezza per le applicazioni in esercizio, nell'ambito dell'assessment integrato;
- raccoglie e analizza gli "indicatori di rischio" denominati Key Risk Indicator;
- verifica, raccoglie e riconcilia, con il supporto delle altre unità organizzative, le perdite rivenienti da rischi operativi;
- analizza le perdite originate dai rischi operativi, definisce i piani di azione registrandoli nell'apposito registro e ne verifica il completamento;
- riferisce sulla posizione di rischio assunta dalla Società, assicurando la disponibilità di informazioni appropriate sui rischi operativi agli Organi Aziendali;
- valuta ex ante la rischiosità operativa dei progetti innovativi, in particolare, la commercializzazione di nuovi prodotti, l'offerta di nuovi servizi (generic assessment) o, in generale, nuove iniziative/cambiamenti rilevanti con significativo impatto IT;
- partecipa, per gli aspetti di sua competenza, alla formulazione dei pareri preventivi, in capo alla Funzione Risk Management, ad esempio in occasione dell'esternalizzazione di funzioni aziendali.

3.3 IL RUOLO DEGLI ORGANI AZIENDALI NELLA GESTIONE E CONTROLLO DEI RISCHI OPERATIVI

Di seguito sono illustrati i principali compiti e responsabilità degli organi aziendali, rilevanti nell'ambito del complessivo *framework* di gestione e controllo dei rischi operativi.

Per la descrizione dettagliata del ruolo di tali organi aziendali, si rinvia al documento "Relazione sulla Struttura Organizzativa" di Flowe S.p.A.

3.3.1 CONSIGLIO DI AMMINISTRAZIONE

Il Consiglio di Amministrazione è l'organo investito di tutti i più ampi poteri per l'amministrazione ordinaria e straordinaria della Società senza esclusione di sorta, con facoltà di compiere tutti gli atti ritenuti opportuni per il raggiungimento e l'attuazione degli scopi sociali. È l'Organo responsabile della gestione aziendale. In tale ambito, in particolare:

- definisce e approva gli obiettivi, le strategie, il profilo e i livelli di rischio della Società, definendo le politiche aziendali e quelle del sistema dei controlli interni; ne verifica periodicamente la corretta attuazione e coerenza con l'evoluzione dell'attività aziendale;
- approva le politiche di gestione dei rischi della Società, nonché le relative procedure e modalità di rilevazione e controllo;
- approva e verifica periodicamente, con cadenza almeno annuale, la politica per il governo e la gestione dei rischi di sicurezza;
- verifica che l'assetto delle funzioni aziendali di controllo della Società sia definito in coerenza con il principio di proporzionalità e con gli indirizzi strategici e che le

funzioni medesime siano dotate di risorse qualitativamente e quantitativamente adeguate;
- stabilisce i principi e gli obiettivi della gestione della continuità operativa;
- adotta, tempestivamente, idonee misure in presenza di carenze o anomalie nel funzionamento dell'organizzazione aziendale;
- esamina annualmente il piano di attività dell'Internal Audit e delle funzioni di controllo di secondo livello (Risk Management, Compliance e Antiriciclaggio).

3.3.2 PRESIDENTE DEL CONSIGLIO DI AMMINISTRAZIONE

Il Consiglio di Amministrazione ha conferito al Presidente, i seguenti poteri:

- promuovere l'effettivo funzionamento del sistema di governo societario di Flowe S.p.A.;
- sovrintendere, insieme all'Amministratore Delegato, ai rapporti con gli organismi istituzionali pubblici e privati, con gli azionisti, nonché alle relazioni esterne della Società;
- assumere, su proposta dell'Amministratore Delegato, qualsiasi provvedimento che abbia carattere d'urgenza nell'interesse della Società e per il quale non si renda possibile convocare nei tempi necessari il Consiglio di Amministrazione, al quale comunque si dovrà riferire alla prima riunione utile.

3.3.3 AMMINISTRATORE DELEGATO

Con il Presidente del Consiglio di Amministrazione svolge un ruolo di rappresentanza della Società nei rapporti con l'esterno ed ha il compito di guidare e coordinare le varie funzioni aziendali al fine di conseguire gli obiettivi fissati dal Consiglio di Amministrazione.

Tra i poteri conferiti all'Amministratore Delegato dal Consiglio di Amministrazione, si richiama, in particolare:

- verificare nel continuo l'adeguatezza del sistema di gestione del rischio della Società, attuare le politiche aziendali, inclusa la politica di gestione del rischio, definite dal Consiglio di Amministrazione e verificarne l'adeguatezza e l'efficace implementazione.

3.3.4 COLLEGIO SINDACALE

L'Organo con funzione di controllo vigila sull'osservanza della legge e dello statuto, sul rispetto dei principi di corretta amministrazione e, in particolare, sull'adeguatezza dell'assetto organizzativo, amministrativo e contabile adottato dalla Società e sul suo concreto funzionamento.

3.3.5 FUNZIONI AZIENDALI DI CONTROLLO

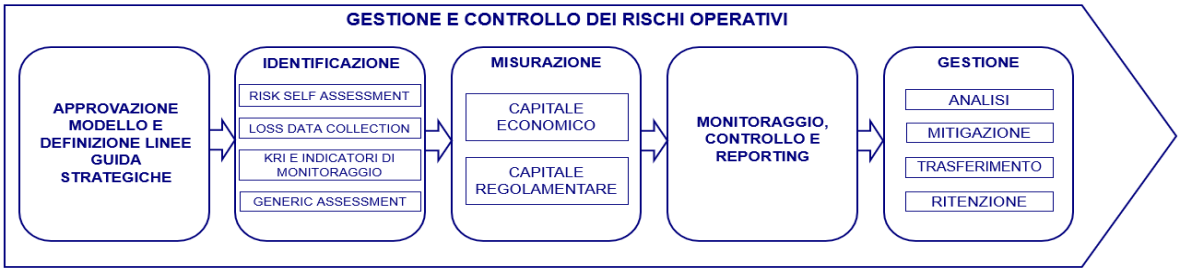
Come già indicato nei paragrafi precedenti, le Funzioni aziendali di Controllo sono le unità organizzative Compliance, Risk Management, Antiriciclaggio e Internal Audit, rispettivamente dedicate, in ottemperanza a quanto previsto dalla normativa vigente, all'espletamento dei controlli nell'ambito del complessivo sistema dei controlli interni.

4 Il *framework* di riferimento per l'Operational Risk Management (ORM)

4.1 DESCRIZIONE DEL *FRAMEWORK* PER LA GESTIONE DEI RISCHI OPERATIVI

La descrizione del complesso processo di controllo e gestione dei rischi operativi che segue illustra il *framework* di riferimento per la gestione integrata del rischio di specie, in termini di metodologie e strumenti necessari per il perseguimento degli obiettivi precedentemente enunciati.

Il processo di gestione e controllo dei rischi operativi adottato dal Gruppo Bancario Mediolanum e da Flowe nello specifico si articola in fasi sequenziali; tali fasi sono rappresentabili come segue:



Ciascuno dei suddetti elementi è caratterizzato da specifici obiettivi, modelli, metodologie, attori e strumenti.

4.2 IDENTIFICAZIONE

L'Identificazione è l'attività di individuazione e raccolta delle informazioni relative ai rischi operativi attraverso il trattamento coerente e coordinato di tutte le fonti di informazione rilevanti. L'obiettivo perseguito è la costituzione di una base informativa completa.

L'identificazione avviene attraverso la definizione e la classificazione delle informazioni necessarie per la gestione integrata dei rischi operativi.

Le informazioni necessarie ai fini ORM sono:

- dati interni di perdita corredati con tutte le informazioni rilevanti ai fini della misurazione e della gestione (inclusi recuperi di natura assicurativa e diretti), raccolti attraverso il processo di ***Loss Data Collection***;
- stime soggettive derivanti dal processo di auto-valutazione del rischio (***Risk Self Assessment*** – RSA o ***Scenario Analysis*** SA);
- stime qualitative di valutazione di nuovi processi o iniziative di *business*, ambito principalmente del cosiddetto ***Generic Assessment*** **(GA)**;
- indicatori andamentali rappresentativi dell'operatività e dei rischi, chiamati internamente ***"Key Risk Indicators"***, base delle analisi gestionali e parte del modello di controllo; tali indicatori possono includere "indicatori di monitoraggio", volti a monitorare eventuali

fenomeni ritenuti rilevanti in termini di tipologia di rischio, frequenza di accadimento e/o di impatto economico.

Si segnala che, nell'ambito dell'identificazione, possono essere ricomprese anche le valutazioni di rischiosità operativa finalizzate al rilascio di pareri preventivi su Operazioni di Maggior Rilievo, in occasione dell'esternalizzazione di funzioni aziendali o in quanto previste dalla Policy di Product Governance.

4.2.1 *LOSS DATA COLLECTION* (LDC)

4.2.1.1 *Framework* metodologico

4.2.1.1.1 OBIETTIVI DELLA LDC

Il processo di LDC è finalizzato all'individuazione, al censimento, alla validazione e al *reporting* delle perdite operative.

Obiettivo della LDC è la raccolta dell'ammontare dell'effetto economico generato da un evento operativo, causato da uno o più fattori di rischio. Le informazioni raccolte sono parte di una relazione tra entità diverse (evento, fattore di rischio ed effetto), descritte compiutamente nei seguenti paragrafi. L'analisi di questa relazione è la chiave per una corretta raccolta delle perdite generate dai rischi operativi e per la misurazione degli stessi.

4.2.1.1.2 CRITERI ALLA BASE DEL PROCESSO DI LDC

Il processo di raccolta dei dati di perdita rappresenta un importante passaggio nel processo di gestione dei rischi operativi che, ad esempio, se confrontato con gli esiti del *Risk Self Assessment*, permette di sempre meglio delineare la misura dell'esposizione ai rischi operativi del Gruppo.

La scelta delle fonti informative da utilizzare nel processo di raccolta deve soddisfare i seguenti criteri:

- **Tempestività**: il tempo intercorrente fra la data di accadimento o di rilevazione di un evento e la data in cui avvengono la segnalazione ed il censimento deve essere il minimo possibile. In tale ottica è preferibile la fonte "più vicina" all'evento e che quindi ne consenta una rilevazione più rapida. La velocità non deve però andare a scapito della qualità dell'informazione, che deve essere comunque privilegiata rispetto alla prima. La tempestività di rilevazione sarà tanto più importante quanto più rilevante è il danno economico generato/generabile dall'evento. Per alcuni eventi di elevata frequenza e basso impatto sono previste delle periodicità di raccolta "convenzionali" (prevalentemente mensili), al fine di non frammentare eccessivamente il processo di raccolta di tali eventi, dal momento che la gestione degli stessi è tempestivamente in carico ad alcune specifiche unità organizzative (es. Happiness & Services, Augmented Intelligence).
- **Completezza ed affidabilità**: le informazioni raccolte devono essere, il più possibile, complete e certe. In tale ottica tanto più la fonte informativa prescelta è in grado di fornire informazioni aggiuntive rispetto al set minimale richiesto, tanto più sarà preferibile rispetto ad altre. Qualora non sia possibile individuare un'unica fonte capace di descrivere compiutamente un evento, sarà necessario coordinare l'impiego di più

fonti per ottenere comunque una descrizione completa ed affidabile di quanto successo.

- **Tracciabilità:** il processo deve essere opportunamente documentato e ricostruibile, sia da parte di Auditor interni, sia da parte di Auditor esterni ed Organismi di Vigilanza.
- **Accessibilità:** il processo deve permettere di avere accesso ai dati nel modo meno oneroso possibile, valutando il trade off tra il costo della raccolta dell'informazione e la rilevanza dell'informazione che si sta ricercando.

L'utilizzo ottimale degli strumenti necessari per la gestione dei rischi operativi è subordinato alla disponibilità di dati che siano:

- **omogenei**: classificati secondo criteri condivisi da tutto il Gruppo;
- **completi**: che tengano conto di tutti gli eventi "materiali" (significativi) di natura operativa verificatisi all'interno del Gruppo;
- **affidabili**: rilevati secondo regole e processi che ne assicurino la correttezza formale e qualitativa.

4.2.1.2 Definizioni e criteri di classificazione

Per una corretta definizione del processo di raccolta dei dati di perdita è necessario identificare le dimensioni rilevanti (entità) e le relazioni che sussistono tra di esse.

Le dimensioni rilevanti per le perdite operative sono:

- **Evento**: singolo accadimento pregiudizievole che può generare direttamente una o più manifestazioni dannose (perdita economica) per la società (più avanti "effetti") e allo stesso tempo determinare ulteriori ricorrenze elementari della medesima entità (eventi), con le quali risulta correlato gerarchicamente a più livelli di aggregazione.
- **Fattore di Rischio**: elementi di criticità / carenze interne che hanno concorso al manifestarsi dell'evento dannoso.
- **Effetto**: singola manifestazione dannosa (perdita economica) derivante direttamente dal verificarsi di un evento pregiudizievole. L'effetto identifica ogni singola conseguenza in un unico contesto spazio-temporale di un evento pregiudizievole; la quantificazione dell'effetto è la misura della perdita operativa subita.

Dopo aver definito le principali entità del *framework* di riferimento per il processo di raccolta, occorre fornire le caratteristiche dell'informazione alla base di ciascuna entità, che ci si prefigge di rilevare mediante la LDC.

4.2.1.2.1 EVENTO

L'elemento portante del processo di LDC è costituito dal **singolo evento pregiudizievole apportatore di perdite operative effettive**.

Per evento pregiudizievole si intende il singolo accadimento che genera una o più perdite. Di ogni evento è possibile identificare due fattori caratteristici quali la **quantità** e il **tempo**.

Rispetto alla **quantità delle manifestazioni** un evento pregiudizievole è:

- singolo;

- multiplo, quando più manifestazioni di perdita sono riconducibili allo stesso evento pregiudizievole e quindi sono generate da una medesima causa.

Rispetto **al tempo** un evento può assumere le caratteristiche intermedie con riferimento alle seguenti situazioni estreme:

- istantaneo, qualora il suo verificarsi provochi un'unica perdita immediata e definitivamente quantificabile (ad esempio, una rapina);
- continuato, qualora un unico evento provochi perdite su un arco temporale non immediatamente definibile (ad esempio, frode continuata operata da un medesimo soggetto su soggetti diversi[2]).

Per ogni evento, occorre valorizzare una serie di informazioni. Le informazioni più importanti, proposte dalla normativa di riferimento come le chiavi di lettura della LDC, sono:

- La **linea di business** (Business Line – di seguito BL) con lo scopo di identificare la tipologia di attività in cui l'evento si è verificato.

Codice Livello	Descrizione Livello
BL01	Corporate Finance
BL02	Trading and Sales
BL03	Retail Banking
BL04	Commercial Banking
BL05	Payment and Settlement
BL06	Agency Services
BL07	Asset Management
BL08	Retail Brokerage

- Il **tipo di evento** verificatosi (Event Type – di seguito ET), il cui scopo è il raggruppamento in classi omogenee della tipologia di accadimento.

Codice Livello 1	Descrizione Livello 1
ET01	Frode Interna
ET02	Frode Esterna
ET03	Rapporto di Impiego e Sicurezza sul Lavoro
ET04	Clientela, prodotti e prassi professionali
ET05	Danni a beni materiali
ET06	Interruzioni dell'operatività e disfunzioni dei sistemi
ET07	Esecuzione, consegna e gestione dei processi

Il Gruppo Bancario Mediolanum si è dotato di un secondo livello di classificazione degli Event Type.

[2] In questi casi si procede al censimento di "Macro Eventi".

Allo scopo di agevolare l'attività di classificazione, è stato predisposto un documento da intendersi come guida, che consente, una volta individuato un evento, di identificarne la tipologia (Manuale Operativo "Processi di identificazione dei Rischi Operativi - Istruzioni di classificazione"). Tale documento costituisce un supporto al fine di garantire omogeneità di approccio nella raccolta dei dati di perdita.

Il modello di Gruppo prevede l'arricchimento della classificazione dell'evento, rispetto all'identificazione della Business Line e dell'Event Type di appartenenza, con ulteriori elementi necessari a identificare la dimensione temporale di accadimento e di gestione dell'evento, il contesto organizzativo in cui l'evento si origina e si manifesta e le cause/vulnerabilità che lo determinano. La registrazione degli eventi deve essere quindi corredata dai seguenti elementi:

- Date di riferimento;
- Dimensione Organizzativa;
- Fattori di Rischio.

Le date di riferimento

Ogni evento da cui la perdita è scaturita è caratterizzato da una serie di date di riferimento che ne contraddistinguono l'evoluzione, dall'istante in cui si manifesta l'evento pregiudizievole, alla definitiva contabilizzazione della perdita stessa.

Si possono individuare:

- **Data di accadimento**: data in cui si verifica l'evento pregiudizievole.
- **Data di rilevazione**: data in cui si viene a conoscenza dell'evento dannoso. La si distingue dalla successiva e si è interessati a rilevarla per valutare quanto tempo intercorre tra il momento in cui si rileva un evento rispetto a quando si è manifestato (data di accadimento) e/o a quando si procede alla sua registrazione sul DB di raccolta (data di registrazione).
- **Data di registrazione**: data in cui si inserisce nel *Loss Data Base* l'evento pregiudizievole.
- **Data di prima contabilizzazione**: data corrispondente a quella della prima perdita effettiva associata all'evento.
- **Data di chiusura evento**: data in cui l'evento ha cessato di produrre i suoi effetti e si ha certezza degli impatti economico-patrimoniali eventualmente generati.

La dimensione organizzativa

In considerazione del fatto che uno degli obiettivi del processo di LDC, nello specifico, e della gestione dei rischi operativi, più in generale, è rappresentato dall'analisi delle perdite operative nei diversi comparti della struttura organizzativa, un'informazione rilevante da considerare è il "dove" è accaduto l'evento ovvero "dove" si è verificata la perdita.

Le informazioni sulla dimensione organizzativa che è necessario associare ad un evento di perdita operativa sono le seguenti:

- Società e Unità organizzativa dove si è verificato l'evento. Può essere diversa da quella/quelle dove si è originato l'evento e dove sono stati subiti gli effetti;
- *Business Line* di Basilea associata alla Unità organizzativa interna dove si è verificato l'evento. La classificazione di riferimento è quella proposta dal Comitato di Basilea. Un evento, accaduto in una determinata linea di business, potrebbe avere effetto su più di una linea di business.

Fattore di Rischio

Il processo di raccolta dati annovera tra i suoi obiettivi quello di fornire indicazioni di natura gestionale, ossia un adeguato supporto informativo al processo di *decision making*, con particolare riferimento all'analisi degli aspetti critici di natura operativa e alle possibili azioni di carattere mitigativo da intraprendere.

A tale scopo, in fase di definizione dei modelli d'Identificazione, è stato esplicitato quale sua componente, il Modello dei Fattori di Rischio (Cfr. Allegato 3).

Il suddetto modello, si sostanzia in uno schema classificatorio dove vengono elencate una serie di voci raggruppate in base a quattro elementi di vulnerabilità che possono concorrere al manifestarsi di eventi dannosi che generano perdite operative.

I quattro fattori che compongono il primo livello del modello sono i seguenti:

- Risorse Umane;
- Sistemi IT, Sicurezza Dati, Infrastrutture telematiche;
- Processi e procedure, rapporti con controparti commerciali e Autorità di Vigilanza;
- Fattori Esterni & Infrastrutture Fisiche.

Il Modello dei Fattori di Rischio risponde alla domanda "perché succede l'evento?"

Un'informazione rilevante da considerare è "chi gestisce il fattore di rischio". L'informazione sulla dimensione organizzativa che è necessario associare al fattore di rischio è l'unità organizzativa interna in cui si origina l'evento e quella che gestisce il fattore di rischio. Possono essere diverse da quella dove si è verificato l'Evento e da quella dove si sono subiti gli Effetti.

4.2.1.2.2 EFFETTO E PERDITA OPERATIVA

Si definisce perdita operativa l'insieme degli effetti economici negativi derivanti dall'accadimento di un evento operativo. Questo può avvenire sotto forma di:

- **perdite effettive:** flusso economico negativo sostenuto per effetto di un evento pregiudizievole;
- **costi opportunità:** effetto economico generato dagli investimenti alternativi cui si è rinunciato impiegando una risorsa di cui si dispone in quantità limitata, in questo caso alla base del provento non conseguito c'è una decisione aziendale;
- **mancati guadagni:** costituiti dagli introiti che sarebbero stati conseguiti se non si fosse manifestata un'inefficace/inefficiente gestione dei processi interni e/o l'accadimento di eventi esterni;

- ***near misses*:** (quasi perdite) sono eventi di rischio operativo che non hanno determinato una perdita economica;
- **perdita "per aggiustamento"**: regolamento contabile di un evento "operativo" la cui sistemazione non causa, se non apparentemente, una perdita, in quanto si tratta di sistemazione di un "dovuto".

Si segnala, inoltre, che alcuni eventi potrebbero anche avere come effetto dei **guadagni**.

Le perdite effettive sono **oggettive e misurabili** in quanto appositamente censite nel sistema contabile o gestionale della Società o tali per cui sia possibile rintracciarne l'impatto economico, a prescindere dalle modalità di contabilizzazione. Il valore da registrare è il costo necessario per la risoluzione dell'evento, esclusi i costi sostenuti per il "miglioramento dei controlli", in azioni preventive ed in investimenti in nuovi sistemi, al lordo delle somme eventualmente recuperate (assicurative, garanzie o altro).

Le perdite possono essere classificate in base alla certezza del flusso economico distinguendo tra:

- **perdite certe**: l'ammontare della perdita è quantificabile, definitivo e sicuro;
- **perdite transitorie**: l'ammontare della perdita non è sicuro, l'importo stimato viene accantonato in un fondo. La perdita diventa certa appena l'importo viene confermato;
- **perdite stimate**: l'ammontare della perdita è un'approssimazione della perdita, dedotta tramite stime/calcoli standardizzati effettuati internamente. Tale tipo di perdita non potrà mai rientrare nella categoria delle perdite certe.

Ai fini regolamentari, tra i criteri indicati per poter adottare il metodo standardizzato, è prevista la raccolta dei dati rilevanti sul rischio operativo, incluse le perdite significative.

Il Gruppo Bancario Mediolanum, classifica tali perdite tra le **perdite effettive**, rintracciabili nelle voci di contabilità e/o in archivi gestionali, caratterizzate da **certezza della quantificazione** dell'ammontare in quanto **passate a conto economico** (con l'inclusione di accantonamenti specifici e l'esclusione di quelli generici).

A fini gestionali interni, la raccolta delle perdite è stata estesa anche alle seguenti tipologie:

- costi opportunità:
- mancati guadagni;
- *near misses;*
- perdite per aggiustamento;
- eventi profittevoli.

Distinguendo tra:

- perdite certe;
- perdite stimate, ovvero quelle perdite non rintracciabili sul conto economico, ma stimabili attraverso sistemi di rilevazione aziendali definiti con criteri rigorosi ed uniformi all'interno del Gruppo (ad esempio attraverso l'utilizzo di costi *standard* forniti periodicamente dal settore Pianificazione Operativa e Controllo di Gestione di Banca Mediolanum che svolge in outsourcing il servizio).

La classificazione delle perdite operative è arricchita dalla raccolta di altre informazioni, alcune rilevanti soprattutto a fini gestionali.

In particolare, le informazioni di maggior rilievo sono:

- l'importo;
- le date di riferimento;
- la dimensione organizzativa;
- la tipologia di effetto;
- la tipologia di recupero.

L'importo

Un'informazione rilevante con riferimento agli "effetti" è quella relativa all'importo della perdita complessiva derivante dall'accadimento di un evento pregiudizievole.

A tal proposito, le componenti di maggior interesse (per fini gestionali e regolamentari) rappresentative dell'importo di perdita associato all'evento rilevato, sono quelle che consentono di valutare oltre all'impatto lordo dell'evento anche eventuali recuperi economici derivanti da rimborsi assicurativi o non.

In particolare, si identificano tre componenti:

- ammontare lordo, con riferimento a tutte le perdite operative ad esso riconducibili;
- eventuali recuperi non assicurativi (es. garanzie);
- eventuali rimborsi assicurativi.

Con riferimento agli importi di "perdita operativa", sono state identificate delle soglie minime per la rilevazione di eventi di perdita operativa. In sintesi, le soglie attualmente previste a livello di Gruppo Mediolanum sono riepilogate nella tabella seguente:

Classe di rischio		Stima della soglia migliore (€)
ET1	Frode interna	1.000
ET2	Frode esterna	50
ET3	Rapporto di Impiego e Sicurezza sul Lavoro	Nessuna soglia
ET4	Clientela, prodotti e prassi professionali	100
ET5	Danni a beni materiali	100
ET6	Interruzione dell'operatività e disfunzioni dei sistemi	100
ET7	Esecuzione, consegna e gestione dei processi	100

Si ritiene che, la mancata raccolta degli eventi la cui perdita totale non supera le soglie sopra sintetizzate, non influenzi dal punto di vista statistico la qualità della base dati o esigenze gestionali di controllo dei rischi.

Le date di riferimento

Ogni perdita operativa può essere caratterizzata da tre diverse date:

- la data in cui la perdita si è manifestata (**Data perdita**) oppure la data in cui è stata inserita in contabilità (**Data di contabilizzazione**). Tali date permettono di assegnare la competenza economica della perdita in questione;
- la data in cui si inserisce nel *Loss Data Base* l'effetto generato dall'evento pregiudizievole (**Data di registrazione)**. Nella maggioranza dei casi tale data coincide con la data di registrazione dell'evento.

Con riferimento al tempo che intercorre tra la data di accadimento dell'evento e quella di manifestazione degli effetti si possono anche avere tipi di perdite "sequenziali". Si intende un insieme di perdite che si verificano in momenti successivi ma che sono riferibili allo stesso evento.

La dimensione organizzativa

Le informazioni sulla dimensione organizzativa che è utile associare alle perdite operative sono:

- l'Unità Organizzativa Interna che ha subito la perdita;
- la *Business Line* di Basilea associata alla UO Interna che ha subito la perdita; la classificazione di riferimento, come per gli eventi, è quella proposta dal Comitato di Basilea.

Con riferimento alla dimensione organizzativa del Gruppo, le perdite operative possono anche essere "multi effetto". Si intende un insieme di perdite che colpiscono differenti entità (ad esempio, unità organizzative, società, ecc.) ma sono riferibili allo stesso evento. Ad esempio, perdite che hanno origine da eventi che si verificano presso funzioni centrali di supporto a più linee di *business* (es. funzione IT) ovvero, quelle connesse ad eventi esterni che coinvolgono più entità giuridiche/unità organizzative (es. disastri naturali, attentati terroristici, ecc.).

La tipologia di effetto

Ciascuna perdita diretta, stimata o contabilizzata, o il costo-opportunità, è caratterizzata dell'entità "Effetto". È prevista una classificazione *standard* per ***Loss Effect Type*** (Cfr. Allegato 4) degli effetti a cui ricondurre il dato di perdita.

La tipologia di recupero

I recuperi si possono suddividere in:

- **recuperi diretti**, qualora non vi sia stato il pagamento anticipato di una somma per ottenerli. Si pensi alla sostituzione di un pezzo in garanzia;
- **recuperi indiretti**, qualora per ottenerli si sia pagata in anticipo una determinata somma di denaro. Principalmente appartengono a questa categoria i recuperi di tipo assicurativo che, ad evento avvenuto, si ottengono dalla compagnia assicuratrice solo se è stato correttamente

pagato il premio e se l'evento occorso rientra tra quelli assicurati dalla polizza.

La classificazione dei recuperi, che possono essere compresenti su ogni singolo evento, adottata dal Gruppo Mediolanum, prevede la loro suddivisione in:

- recuperi assicurativi;
- recuperi infragruppo (ovvero provenienti da altre società interne al Gruppo Mediolanum);
- garanzie;
- altri recuperi (Non Assicurativo).

Ulteriori informazioni da raccogliere per ogni singolo recupero sono:

- data richiesta;
- data di ottenimento;
- importo richiesto;
- importo ottenuto;
- polizza di riferimento (per i recuperi assicurativi).

4.2.1.3 Fonti informative

4.2.1.3.1 DEFINIZIONE

Nell'ambito della definizione del processo di *Loss Data Collection*, un aspetto fondamentale è l'individuazione delle Fonti Informative presso cui rilevare i dati di perdita operativa.

I principi alla base del processo di rilevazione sono sintetizzabili come segue:

- l'evento è certo ed è classificabile come "rischio operativo";
- l'evento potrà essere censito, anche se non si conoscono nel dettaglio gli effetti economici dell'evento stesso. Talvolta l'attività di "arricchimento" delle informazioni relative all'evento per completare il *set* informativo minimale alla base del processo di LDC avviene coinvolgendo molteplici unità organizzative;
- l'unità che trasmette l'evento può essere differente dall'unità nella quale si è generato. Questo accade tipicamente per gli eventi gestiti in modo accentrato da unità specializzate nella raccolta e gestione di segnalazioni di problemi/errori classificabili come "rischi operativi".

Pur mantenendo la centralità dell'"evento" quale chiave primaria di lettura della base informativa dei dati di perdita operativa, il principio che guida nell'individuazione delle fonti è quello di spostarsi dalle unità "che rilevano" l'evento laddove si manifesta a quelle "che processano" gli effetti che da esso sono scaturiti fino alla richiesta di contabilizzazione (eventuale) delle relative perdite.

4.2.1.3.2 APPROCCIO PER LA RACCOLTA

Affinché i dati raccolti siano omogenei, completi e affidabili il processo di raccolta dei dati di perdita deve essere preceduto da un accurato lavoro propedeutico volto ad individuare le fonti informative per la raccolta.

Le fonti informative possono essere contabili o gestionali. Con riferimento al diverso grado di utilizzo dei due tipi di fonti nell'ambito del processo di raccolta, il processo di LDC può essere:

- "*event driven*": i punti di partenza sono l'evento di perdita e l'unità operativa in cui si manifestano gli effetti. I dati sono raccolti "a monte", ossia dai sistemi extra contabili presenti nelle UO dove si verifica l'evento. La fonte che porta alla registrazione dell'evento è tipicamente in prossimità del punto dove si manifesta lo stesso.
- "*accounting driven*": i dati sono raccolti "a valle", ossia dal sistema di Contabilità Generale. È necessario quindi individuare e disciplinare la contabilizzazione dei Loss Data in tale sistema. Resta comunque necessaria un'attività di arricchimento manuale dei dati raccolti.

Il modello quindi prevede:

- utilizzo diretto delle fonti gestionali. Il processo di raccolta è imperniato sull'attività svolta dai *Focal Point* ORM, responsabili della raccolta delle informazioni relative a perdite di natura operativa subite dalla UO di appartenenza o da altre UO per conto delle quali effettuano la funzione di "*focal point*" nel processo di raccolta dati e arricchimento delle informazioni. Talvolta, le unità coinvolte in tale processo possono essere più di una, al fine di disporre del completo *set* informativo necessario a raccogliere correttamente l'evento;
- utilizzo delle fonti contabili per il riscontro e la quadratura delle rilevazioni effettuate attraverso le fonti di tipo gestionale. Dall'attività di riconciliazione è possibile raccogliere le evidenze dei:
    - dati di perdita registrati contabilmente ma non ancora rilevati gestionalmente;
    - dati rilevati gestionalmente per i quali non è ancora avvenuta la relativa contabilizzazione.

L'attività d'individuazione delle fonti informative non è statica ed esclusivamente propedeutica all'implementazione del processo di raccolta dei dati di perdita, si tratta bensì di un'attività continua, necessaria al fine di garantire l'attualità delle fonti e delle perdite rispetto all'evoluzione della realtà aziendale ed al perimetro osservato.

4.2.1.3.3 MAPPATURA DELLE FONTI INFORMATIVE

Tale attività viene effettuata nel dettaglio in fase di impianto e di avvio del processo e viene aggiornata periodicamente, per tenere conto di modifiche organizzative, di prodotto, di processo oppure a seguito di variazioni dei piani dei conti di contabilità.

La mappatura puntuale delle fonti informative è disponibile nel "Manuale Operativo" di *Loss Data Collection* in uso presso l'Unità Operational Risk Management di Banca Mediolanum.

4.2.1.3.4 CRITERI DI VALUTAZIONE

Un'ultima considerazione riguarda l'introduzione di criteri che permettano di valutare il grado di efficienza di ogni singola fonte individuata in relazione alle sue caratteristiche d'impiego nell'ambito del processo di *Loss Data Collection*.

Sono tre i parametri di ausilio in questo senso:

- ***tempestività:*** si intende la rapidità con cui la fonte fornisce l'intero set informativo richiesto. Essa si può misurare in termini di tempo intercorrente fra la data di rilevazione di un evento e la data in cui avviene la registrazione della perdita che da esso è scaturita;
- ***completezza:*** si fa riferimento alla quantità d'informazione che contiene il dato fornito dalla fonte. Quanto più essa è in grado di fornire informazioni aggiuntive rispetto al set informativo di base, tanto più sarà apprezzabile in questo senso. In generale, è possibile che le fonti, singolarmente prese, non soddisfino tutti i requisiti di informazione ricercata. In tal caso sarà chiaramente più impegnativo coordinare l'impiego di più fonti per ottenere comunque la raccolta del set informativo necessario ai fini di LDC;
- ***accessibilità***: si intende la possibilità di attingere, nel modo meno oneroso possibile ai dati che essa è in grado di fornire.

I tre parametri permettono di valutare la "bontà" di ogni singola fonte e intervengono direttamente nel processo decisionale finalizzato a valutare gli interventi per riorganizzare i flussi informativi del processo sottostante, in modo da automatizzare quanto più possibile la raccolta dati.

A tal proposito, per condurre una corretta analisi costi/benefici, ci sono ulteriori variabili da considerare:

- il ***numero di perdite*** di cui si trova informazione presso una data fonte: quanto più cresce tale numero, tanto più sarà verosimile un intervento per "recuperare" in pieno tale fonte (automatizzandola, o comunque migliorandone le caratteristiche correnti, laddove possibile);
- l'***importo complessivo*** delle perdite di cui si trova traccia presso una data fonte rapportato all'ammontare complessivo rilevato, ad esempio, nell'arco di un esercizio.

Tale analisi consentirà dunque di determinare dove convenga intervenire su una fonte, o per automatizzarne lo sfruttamento, o per migliorare tempestività e completezza dell'informazione fornita.

4.2.1.4 Il processo di LDC

4.2.1.4.1 CARATTERISTICHE GENERALI

Il processo di LDC consente l'individuazione, il censimento, la validazione e la produzione di un *reporting* delle perdite operative, garantendo:

- **accuratezza dell'informazione**: le informazioni censite, oltre a rientrare fra quelle individuate come rilevanti per la raccolta, devono prioritariamente rispondere a requisiti di completezza ed affidabilità;
- **tempestività della raccolta**: gli eventi operativi dovrebbero essere censiti in un istante il più ravvicinato possibile al momento in cui è possibile quantificarne l'impatto ossia al momento in cui gli effetti da essi scaturiti si concretizzano in una manifestazione economica negativa. La celerità della rilevazione, tuttavia, non deve essere all'origine di una scarsa qualità dell'informazione;
- **completezza** delle serie storiche di perdita rispetto alla rappresentazione del profilo di rischio operativo del Gruppo.

Al fine di conseguire questi obiettivi è necessaria la creazione di:

- una **cultura aziendale e di Gruppo** ottenuta attraverso il coinvolgimento diffuso delle strutture organizzative nelle attività di LDC, la definizione e diffusione di una metodologia unica e condivisa;
- un **processo formalizzato** in cui le attività di LDC (ricerca, censimento, validazione e *reporting*) costituiscono i principali sottoprocessi;
- un **processo dinamico** in grado di aggiornare le fonti informative presso cui rilevare le perdite operative e rappresentare fedelmente la rischiosità operativa aziendale seguendo le evoluzioni e i mutamenti della struttura organizzativa, dei processi e dei prodotti.

4.2.1.4.2 IL RIFLESSO ORGANIZZATIVO

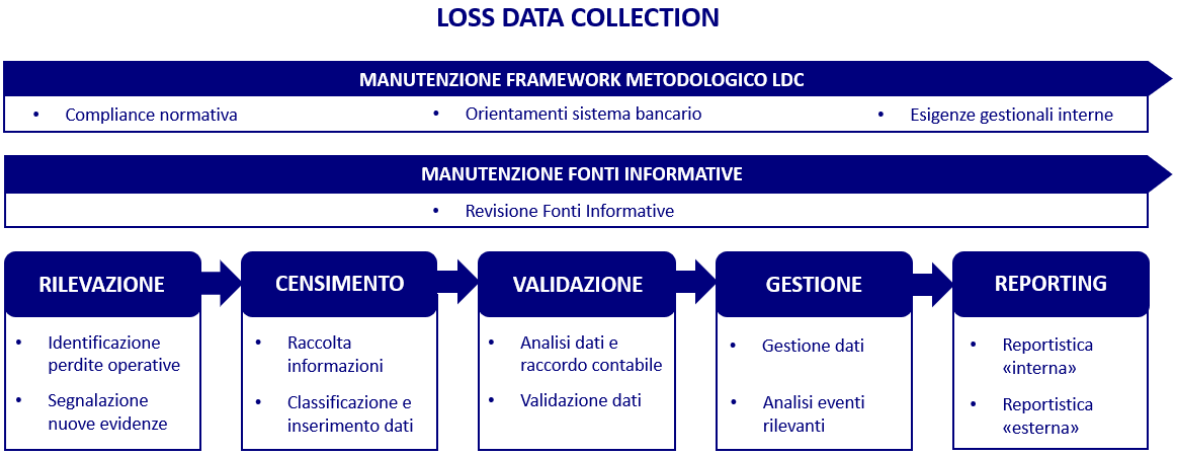
Le figure professionali coinvolte nel processo di LDC sono:

- **Unità Operational Risk Management di Banca Mediolanum:** è il responsabile finale della LDC a livello di Gruppo, segue la gestione di tempi e scadenze, coordina i *focal point* di ORM e ne segue le attività. È, inoltre, responsabile delle proposte di aggiornamento delle convenzioni interne ed esterne, aggiorna i *Focal Point* ORM su evoluzioni del contesto organizzativo e metodologico del processo. Inoltre, l'Unità Operational Risk Management della Banca fornisce in outsourcing a Flowe le attività di gestione dei rischi operativi della Società.
- ***Focal Point* ORM:** sono responsabili degli adempimenti operativi relativi alle attività di individuazione e segnalazione delle perdite operative. Si avvalgono del supporto dell'Unità Operational Risk Management per ogni problematica di carattere tecnico e metodologico. Le informazioni fornite dai *Focal Point* di ORM sono arricchite con il contributo di altre strutture aziendali, tra cui *in primis* la divisione Amministrazione, Contabilità e Bilancio di Banca Mediolanum.

4.2.1.4.3 IL PROCESSO

Dopo aver definito il *framework* metodologico entro cui sviluppare il processo di *Loss Data Collection*, è necessario descrivere in modo dettagliato fasi ed attività in cui il processo stesso si articola, avendo cura di specificare gli attori coinvolti.

La figura seguente rappresenta in modo schematico l'articolazione del processo di LDC in fasi e attività.



Rilevazione

Identificazione Perdite Operative

I *Focal Point* ORM, nell'ambito della normale operatività espletata, identificano quali tra i dati gestiti rispondono alla definizione di perdita operativa.

L'unità Operational Risk Management fornisce, ove richiesto, supporto ai *Focal Point* ORM nell'attività di identificazione delle perdite operative analizzando i casi dubbi e verificandone l'effettiva rispondenza ai requisiti definiti dal *framework* metodologico.

Segnalazione nuove evidenze

I *Focal Point* ORM segnalano all'Unità Operational Risk Management eventuali casi di perdita operativa non codificati tra le tipologie identificate nell'ambito del *framework* metodologico definito.

L'Ufficio effettua le dovute analisi dei casi segnalati avviando, laddove si renda necessario, la fase di "Manutenzione delle Fonti Informative" e/o di "Manutenzione del *Framework* Metodologico".

Censimento

Raccolta informazioni

I *Focal Point* ORM raccolgono le informazioni di cui dispongono per la caratterizzazione delle perdite operative e le comunicano all'Unità Operational Risk Management.

L'Unità Operational Risk Management raccoglie le altre informazioni necessarie per un'ulteriore caratterizzazione delle perdite operative, anche richiedendo la collaborazione di altri *Focal Point* ORM e/o delle Unità Organizzative presso cui si è verificato l'evento operativo. (Ad es. informazioni sulle cause alla base dell'evento verificatosi per la definizione dei Fattori di Rischio, informazioni necessarie a identificare correttamente l'evento da cui la perdita operativa è scaturita e/o a ricollegare più perdite allo stesso evento, informazioni relative alla quantificazione della perdita).

Classificazione e inserimento dati

L'Unità Operational Risk Management, sulla base dei criteri di classificazione univocamente definiti a livello di Gruppo, individua gli attributi che caratterizzano il singolo evento di perdita,

ricodificando le informazioni raccolte ad esso relative secondo gli schemi classificatori disponibili.

Documenta la presenza di eventuali "scarti", ove rilevanti, e ne fornisce evidenza ai *Focal Point* ORM.

L'Unità Operational Risk Management monitora costantemente l'attività di classificazione dei dati e di codifica delle informazioni al fine di garantire la correttezza e l'omogeneità a livello aziendale.

Validazione

Analisi dati e raccordo contabile

L'Unità Operational Risk Management effettua costantemente un'analisi puntuale dei dati ricevuti e/o inseriti sottoponendo al responsabile della Funzione Risk Management di Flowe i casi ritenuti critici. Verifica la qualità dei dati in termini di rispondenza alle definizioni metodologiche e di univocità dei criteri di classificazione. Condivide, con i *Focal Point* ORM, eventuali modifiche da apportare.

Ove possibile, si accerta della rispondenza contabile ed extra-contabile dei dati inseriti di concerto con il *Focal Point* ORM e avvalendosi del supporto della divisione Amministrazione, Contabilità e Bilancio e del settore Pianificazione Operativa e Controllo di Gestione di Banca Mediolanum, che svolgono il servizio in outsourcing.

Validazione dati

L'Unità Operational Risk Management valida gli eventi inseriti nel momento in cui ha la certezza che tutti i suoi effetti si sono manifestati e sono stati registrati.

Gestione

Gestione dati

L'ORM di Gruppo effettua un'analisi d'insieme degli eventi operativi registrati verificando la riconduzione dei dati di perdita agli eventi operativi secondo la logica "*Event-Guide*". Attraverso un impiego coordinato delle diverse Fonti Informative, identifica le catene causali (eventi collegati), laddove presenti.

Analisi eventi rilevanti

L'Unità Operational Risk Management individua, anche su diretta segnalazione dei *Focal Point ORM*, eventi operativi di particolare rilevanza (per entità dell'impatto, frequenza di accadimento, natura, etc…). Raccoglie, ove necessario, ulteriori informazioni per una migliore comprensione dell'Evento. Comunica quanto rilevato alle unità preposte alla gestione dei rischi con le quali condivide le azioni da intraprendere al fine di una corretta gestione e mitigazione degli stessi.

In particolar modo sono considerati rilevanti gli eventi con un impatto economico (certo o stimato) superiore a 10.000 €. Per tali eventi possono essere condotte analisi di dettaglio, chiedendo ai responsabili la compilazione di una scheda evento riepilogativa nella quale viene richiesta anche l'identificazione di azioni volte alla mitigazione del rischio e del ripetersi dell'evento.

Inoltre, con riferimento al processo di rilevazione e comunicazione dei **gravi incidenti di sicurezza informatica o operativi**, è previsto il coinvolgimento dell'Unità Operational Risk Management nella raccolta dei dati relativi all'impatto economico.

Reporting

Nell'ambito del processo di LDC sono previste specifiche attività di reportistica interna.

L'Unità Operational Risk Management supporta il responsabile della Funzione Risk Management nella predisposizione dei *report* per la comunicazione con le altre funzioni aziendali (Unità Organizzative, Alta Direzione, Consiglio di Amministrazione) a cui vengono inviati con le frequenze e contenuti variabili in funzione dell'organo a cui sono destinate e in considerazione della rilevanza dei rischi ambito di monitoraggio.

Unitamente agli eventi di perdita rilevanti, sono ambito di monitoraggio i "piani di azione" avviati al fine di mitigare il rischio del ripetersi degli stessi. Dei piani d'azione vengono registrate e monitorate anche le seguenti informazioni aggiuntive: orizzonte temporale, responsabile della gestione e stato di avanzamento.

Manutenzione framework metodologico LDC

Il *framework* metodologico della *Loss Data Collection* può essere modificato: a seguito di aggiornamenti normativo- regolamentari, dagli orientamenti interpretativi delle associazioni di categoria, e, infine, per esigenze gestionali interne, comunque non in conflitto con le normative vigenti.

Compliance normativa

L'Unità Operational Risk Management cura l'adeguamento del *framework* metodologico rispetto alle evoluzioni della normativa, verificando la *compliance* delle definizioni assunte, delle ipotesi logico-funzionali formulate, delle scelte di carattere metodologico-organizzativo. Condivide eventuali modifiche/integrazioni che si rendano necessarie con il responsabile della Funzione Risk Management, con la Funzione Compliance e con l'Alta Direzione.

Ogni integrazione e aggiornamento alla metodologia verrà portato a conoscenza delle strutture coinvolte nel processo.

Orientamenti Sistema bancario

L'Unità Operational Risk Management di Banca Mediolanum provvede ad una periodica revisione del *framework* metodologico di LDC di Gruppo Bancario, definito analizzando in modo critico mutamenti significativi dell'orientamento del sistema bancario in materia, con particolare riguardo ai modelli di riferimento adottati e quindi ai criteri di classificazione stabiliti. Sottopone al Responsabile della Funzione Risk Management eventuali modifiche da apportare.

Ogni integrazione e aggiornamento viene portato a conoscenza degli attori coinvolti nel processo.

Manutenzione Fonti Informative

Revisione Fonti Informative

L'Unità Operational Risk Management, anche attraverso il diretto coinvolgimento dei *Focal Point* ORM, provvede ad una periodica revisione delle Fonti Informative individuate.

In particolare, richiedendo ove necessario la collaborazione di altri settori / uffici, l'Unità Operational Risk Management:

- verifica puntualmente la significatività delle fonti in relazione alle evoluzioni del contesto organizzativo;
- verifica il livello complessivo di copertura del perimetro d'indagine garantito dalla Fonti individuate, in relazione ai mutamenti dello scenario di riferimento;
- procede, se necessario, ad una attività di "ri-mappatura" delle tipologie di perdita oggetto di rilevazione sulle fonti disponibili;
- procede all'individuazione di nuove fonti in presenza di nuove tipologie di perdita da inserire nel perimetro d'indagine non coperte dalle Fonti attuali.

Infine, l'Unità Organization & Business Continuity provvede a segnalare tempestivamente, alla funzione Risk Management, eventuali mutamenti dello scenario organizzativo di Flowe.

4.2.2 RISK SELF ASSESSMENT

4.2.2.1 Caratteristiche generali

Il processo di *Risk Self Assessment* dei rischi operativi è parte dei processi di identificazione e valutazione *ex-ante* dei rischi operativi di un'unità organizzativa e/o di un processo effettuata sulla base di stime soggettive e modelli di auto-valutazione da parte del responsabile della gestione del rischio.

Rappresenta un utile strumento di gestione, soprattutto in termini di corretta percezione della rischiosità dei processi da parte dei responsabili delle unità organizzative.

Inoltre, oltre ad essere uno strumento di rilevazione dei rischi (*ex-ante*) rappresenta un indispensabile supporto della diffusione della cultura del controllo, soprattutto se confrontato con i risultati del processo di *Loss Data Collection*, volto alla rilevazione *ex-post* dei rischi operativi.

Gli esiti di tale valutazione costituiscono parte integrante del controllo del profilo di rischio operativo della Società e sono utilizzati a fini gestionali per la prevenzione e l'attenuazione dei rischi operativi. In tale ottica, gli esiti di questa attività possono anche costituire la base su cui impostare analisi di scenario o di stress da parte della Funzione Risk Management.

La metodologia adottata persegue i seguenti obiettivi:

- identificare e misurare i rischi operativi;
- assicurare il coinvolgimento dei responsabili delle Unità Organizzative nel processo di "autodiagnosi";
- integrare più fonti di informazione (soggettiva ed eventualmente quantitativa), utilizzando, quando ritenuto opportuno, anche un supporto quantitativo per esprimere l'esito del giudizio di assessment;
- esprimere in termini di rischio le informazioni raccolte per poter confrontare la rischiosità di diverse entità organizzative (UO, Società);
- valorizzare l'ottica prospettica intrinseca nei giudizi soggettivi espressi, facendo riferimento a valutazioni ex-ante dei rischi potenziali di un'Unità Organizzativa;
- ottenere risultati aggregati per diverse tipologie di Unità Organizzative;

- supportare il processo gestionale per la prevenzione e l'attenuazione dei rischi operativi, mediante l'identificazione di apposite azioni di mitigazione;
- contribuire alla crescente diffusione della cultura del controllo e della sensibilità agli eventi, possibile fonte di rischi operativi.

4.2.2.2 Linee guida delle attività *Risk Self Assessment*

Il processo di *Risk Self Assessment* si ispira, in generale, alle seguenti linee guida:

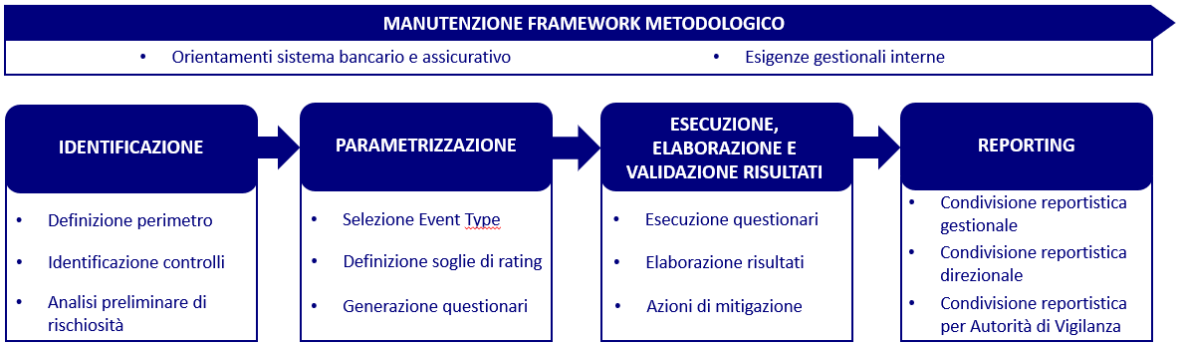
- l'attività di RSA prevede l'analisi preliminare dei processi delle Unità Organizzative in un'ottica di esposizione al rischio, identificando *ex ante* i fattori di rischio insiti nei processi stessi, indipendentemente dalla rilevazione di perdite storiche;
- i questionari di RSA possono essere eseguiti su tutte le Unità Organizzative, graduandone la profondità, la frequenza di esecuzione e le priorità in funzione del rischio potenziale delle aree oggetto di analisi;
- l'attività di RSA può adottare dei questionari solo "qualitativi" nel caso di rischi non ritenuti particolarmente significativi, mentre per talune tipologie di evento può prevedere anche una quantificazione soggettiva dei rischi operativi delle Unità Organizzative rispetto a 3 elementi:
    - la frequenza media (numero medio di volte che si stima l'evento possa accadere, tenendo già in considerazione la valutazione di adeguatezza dei controlli);
    - l'impatto economico tipico o medio (moda o perdita media stimata di ogni potenziale evento, tenendo già in considerazione l'adeguatezza dei controlli);
    - l'ipotesi di perdita nel caso peggiore (*Worst Case*);

- l'analisi preliminare di RSA si basa altresì sulla rilevazione delle perdite operative, evidenziate dal processo di Loss Data Collection, o su altre informazioni disponibili (es. reclami, rilievi audit, valutazioni del rischio IT, processi esternalizzati, etc.);
- l'*output* del processo di RSA quantitativo produce valori di perdita attesa, inattesa e VaR delle attività oggetto di analisi. Tale risultato, integrato con valutazioni di carattere qualitativo, consente di addivenire ad una valutazione complessiva della rischiosità *ex ante* gravante su una determinata Unità Organizzativa.
- ai fini di una migliore rappresentazione dei risultati, la valutazione quantitativa dei rischi operativi di un'area può essere espressa, in sede di *reporting,* anche attraverso l'attribuzione di un *rating* di rischiosità, determinato sulla base di "soglie di accettabilità economica del rischio potenziale" dell'area stessa, definite preliminarmente all'avvio dell'attività di *risk self assessment.*

4.2.2.3 Il processo

Il processo di *Risk Self Assessment*, si sviluppa in più fasi ed attività, così come di seguito rappresentato.

RISK SELF ASSESSMENT



4.2.2.3.1 IDENTIFICAZIONE

L'obiettivo principale della fase di identificazione è l'individuazione delle Unità Organizzative (di seguito UO) su cui effettuare il processo di RSA integrato secondo un approccio *Risk Based.*

A tale fine occorre:

- definire il perimetro di analisi;
- identificare i controlli associati;
- svolgere un'analisi preliminare della rischiosità.

Definizione del perimetro

Preliminarmente all'avvio dell'attività di *Risk Self Assessment*, l'Unità Operational Risk Management procede all'identificazione delle Unità Organizzative e dei relativi *event type* da sottoporre alle analisi quali/quantitative, in funzione della valutazione economica del capitale a rischio (potenziali perdite operative), delle perdite registrate negli anni passati, della collocazione organizzativa delle medesime (unità di coordinamento vs unità di linea) e di altre considerazioni di carattere qualitativo (ad es. revisioni assetto organizzativo, esternalizzazione di processi, nuovi *business*, etc.), definendo eventualmente specifiche priorità di intervento, per consentire la tempestiva attivazione di azioni di gestione e mitigazione dei rischi a cui le attività sono esposte. Il dettaglio delle Unità oggetto di assessment e, se previste, delle relative soglie di rischiosità operativa è preventivamente condiviso con l'Amministratore Delegato.

Identificazione dei controlli

L'identificazione dei punti di controllo, adottati nei processi oggetto di *assessment*, persegue il fine di ottenere delle valutazioni di rischio "residuale", che considerino il disegno ed il funzionamento dei controlli in essere, ovvero riflettano, in caso di controlli inesistenti o inefficaci, la maggiore esposizione potenziale al fattore di rischio. In tale ambito si suggerisce talvolta l'opportunità di introdurre un'azione volta a tenere sotto controllo il rischio (c.d. "azione di mitigazione").

Analisi preliminare di rischiosità

Prima dell'avvio del processo di *assessment* vengono raccolte ed elaborate le informazioni provenienti da diverse fonti interne ed esterne (es: Internal Audit, Organismo di Vigilanza, Compliance, Autorità di Vigilanza, ecc.) utili ad individuare, per ogni singola Unità Organizzativa oggetto di assessment, la rischiosità e, di conseguenza, gli event type qualitativi e quantitativi e, per questi ultimi, il capitale da allocare per la determinazione del rating.

4.2.2.3.2 PARAMETRIZZAZIONE

Una volta individuate le unità organizzative della struttura aziendale che devono essere coinvolte nel processo di RSA, si procede con la parametrizzazione ovvero con la selezione degli *event type*, la definizione di soglie di rating, laddove previste, e la costruzione dei questionari.

Selezione degli event type

La selezione degli *event type*, tiene conto non solo delle perdite operative registrate, ma si basa anche sull'analisi di ulteriori dati, quali i controlli mappati, l'esito degli assessment ed i cataloghi dei rischi[3] condivisi nell'anno precedente, le azioni di mitigazione, la mappatura delle applicazioni IT, esternalizzazione di processi, specifici driver dimensionali, consentendo in tal modo di definire la modalità di assessment a seconda che si tratti di un *event type* con valenza solo qualitativa o anche quantitativa. La definizione di tali *event type* si basa pertanto sulla combinazione di elementi oggettivi, quali ad esempio la presenza di perdite operative, e di elementi soggettivi, quali la conoscenza della rischiosità dell'Unità Organizzativa e dei possibili scenari di perdita.

A titolo di esempio, la presenza di una perdita operativa associata ad un *event type* non necessariamente determina la sua scelta, in quanto potrebbe essere una perdita associata ad un processo non più in essere e pertanto non ripetibile.

Definizione delle soglie

La definizione delle soglie, ove prevista, ha l'obiettivo di rappresentare la valutazione quantitativa degli *event type* oggetto di analisi in classi di rating e parte dal capitale regolamentare e/o economico della Società.

Il rating così definito può essere assimilabile ad un vero e proprio "risk appetite" ovvero al livello di rischio che un'Unità Organizzativa/Società intende assumere per il perseguimento dei propri obiettivi (strategici), sulla cui base è possibile valutare l'opportunità o meno di eventuali azioni di mitigazione della rischiosità rilevata e delle relative priorità.

Le classi di rating rappresentano i seguenti rischi:

A. rischio fisiologico: situazione tollerata, rischio di perdite operative nei limiti di accettabilità;
B. rischio medio: rischio di perdite non trascurabile, primo segnale di allerta;
C. rischio significativo: situazione problematica, è consigliabile prevedere un'analisi più approfondita per valutare l'opportunità di un intervento di mitigazione;

[3] Si tratta di un documento (formato excel) che classifica le tipologie di evento di rischio operativo articolandole sulla base di tre livelli di specificità (vedi Allegato 2), aggiungendo, pertanto, un ulteriore livello di dettaglio rispetto al catalogo delle domande. Viene trasmesso preventivamente e condiviso nel corso degli assessment con gli intervistati supportandoli, in tal modo, nel processo di identificazione e analisi dei rischi cui sono esposte le Unità organizzative oggetto di analisi.

D. rischio elevato: la gravità della situazione indica la necessità di un tempestivo intervento di mitigazione.

Generazione dei questionari

La fase di parametrizzazione termina con la generazione del questionario per Unità Organizzativa oggetto di *assessment*. Si definiscono così i diversi *event type* che saranno oggetto di valutazione qualitativa sui fattori di rischio e sui controlli e, laddove previsto, anche quantitativa, per determinare delle stime soggettive di rischiosità.

I criteri di scelta degli *event type* di un questionario sono legati agli obiettivi di:

- ottenere, oltre alle stime soggettive, indicazioni di carattere gestionale sullo stato dei fattori di rischio per indirizzare le attività di mitigazione;
- permettere l'identificazione delle priorità degli interventi di miglioramento organizzativo e tecnologico, attraverso un'analisi di scenario dettagliata;
- indagare in modo completo il secondo livello di *event type* di Basilea.

4.2.2.3.3 ESECUZIONE, ELABORAZIONE E VALIDAZIONE DEI RISULTATI

Esecuzione del questionario

Nella fase di esecuzione dei questionari di RSA al responsabile dell'Unità Organizzativa, per ogni tipologia di evento (cd. *event type*), verrà richiesto di:

- valutare i quattro fattori di rischio (People, Process, System, External factors) per stimare la vulnerabilità di ciascun fattore in relazione ad ogni *event type* considerato;
- fornire le seguenti stime per gli *event type* quantitativi selezionati:
    - *frequenza* media, numero medio di eventi attesi nell'arco temporale di riferimento;
    - *impatto tipico*, valore più frequente di perdita attesa;
    - *impatto peggiore*, massima perdita che si può verificare relativamente all' *event type* considerato;
    - *orizzonte temporale* associato al caso peggiore, intervallo di tempo in cui ci si attende si possa manifestare l'impatto peggiore;
- validare ed eventualmente aggiornare le valutazioni sui relativi controlli a presidio di eventuali fenomeni di rischiosità e già fornite in fase di Identificazione.

Con riferimento agli scenari oggetto di analisi anche nell'ambito del Rischio ICT e di sicurezza, la stima delle grandezze utilizzate per la valutazione quantitativa degli *event type* ad esso associati, è elaborata a partire dalle rilevazioni effettuate nell'ambito del processo di valutazione del rischio IT.

Preventivamente all'intervista, vengono trasmessi al responsabile dell'unità organizzativa: i risultati dell'assessment dell'anno precedente (qualora disponibili), gli eventi di perdita registrati, le azioni di mitigazione e i piani di azione in corso, il catalogo dei rischi (proposto o condiviso nel corso dell'*assessment* precedente) e i punti di controllo censiti.

Elaborazione dei risultati

Una volta concluso il questionario, viene effettuata l'analisi di coerenza dei risultati ottenuti e di seguito consolidati, assegnando un rating qualitativo per i fattori di rischio e quantitativo, laddove prevista una valutazione quantitativa degli *event type*.

In base ai rating quali/quantitativi assegnati e/o in considerazione del VaR stimato, si richiede di porre in essere adeguate azioni di mitigazione.

Il report, con evidenza dei dati definitivi, viene salvato nelle carte di lavoro, previa condivisione con l'Unità Organizzativa oggetto di assessment.

Infine, viene effettuata un'analisi di back testing prima della chiusura definitiva delle sessioni annuali di assessment. Le evidenze di tale attività possono portare, nei casi di particolare rilevanza, alla condivisione di nuove stime con il responsabile dell'unità organizzativa, oppure, nei restanti casi, essere utilizzate a supporto del ciclo di assessment successivo.

Azioni di mitigazione

Le azioni di mitigazione hanno l'obiettivo di ridurre l'esposizione ai rischi operativi e reputazionali.

Tale esposizione è rilevata tramite l'attività di assessment oggetto dei presenti paragrafi, ma anche a seguito di specifici assessment (generic assessment) o del verificarsi di eventi che evidenzino dei gap nei processi interessati.

4.2.2.3.4 REPORTING

A conclusione dell'attività di RSA viene prodotto, a beneficio del Responsabile dell'Unità Organizzativa esaminata, un apposito resoconto contenente:

- il *report* con la sintesi dei risultati quantitativi (in termini di *expected loss*, *unexpected loss* e VaR) e/o qualitativi dell'*assessment* e il catalogo dei rischi condiviso, evidenziando le informazioni più importanti in modo graduato in funzione della rilevanza delle stesse;
- l'elenco dei controlli mappati e/o aggiornati (RFCA);
- le eventuali azioni di mitigazione condivise con il Responsabile in sede di assessment, con le relative priorità e scadenze;
- copia del questionario utilizzato per l'assessment con evidenza delle risposte fornite, mantenuto a disposizione del Responsabile dell'Unità Organizzativa interessata.

In seguito all'avvio dell'azione di mitigazione condiviso, l'Unità Operational Risk Management, verifica con periodici follow up che il piano venga effettivamente realizzato e che le scadenze siano effettivamente rispettate. Nel caso in cui le scadenze non siano rispettate, si procederà alla verifica delle motivazioni e in base alla gravità del rischio da gestire si provvederà a valutare la nuova scadenza del piano, di concerto con l'Unità Responsabile dell'azione. Le azioni di mitigazione sono, inoltre, incluse nel report periodico di sintesi dei rilievi di tutte le Funzioni Aziendali di Controllo, previsto dal Regolamento del processo di gestione dei rilievi emessi dalle funzioni aziendali di controllo.

Infine, a conclusione degli assessment viene predisposta una reportistica di sintesi, portata all'attenzione dell'Amministratore Delegato, col fine di illustrare le principali evidenze emerse.

4.2.2.3.5 *RISK FACTOR CONTROL ASSESSMENT* (RFCA)

Nel processo di identificazione e valutazione *ex-ante* dei rischi operativi, si inserisce la mappatura dei controlli associati ai processi, grazie alla quale, unitamente al *Risk Self Assessment*, è possibile effettuare un'analisi completa dell'esposizione al rischio di una Unità Organizzativa. Infatti, se i controlli si ritengono efficaci o adeguati, l'esposizione ad un determinato rischio diminuisce, viceversa, in caso di controlli inesistenti o inefficaci, il fattore di rischio potrebbe aumentare. In questo caso è necessario valutare la possibilità di introdurre un'eventuale azione di mitigazione, volta a tenere sotto controllo il rischio.

Il processo di "mappatura dei controlli" viene attivato in 3 momenti:

Processo di Risk Self Assessment

In occasione dell'*assessment* annuale, si procede alla mappatura e all'aggiornamento[4] di tutti punti di controllo associati ai processi aziendali, valutando l'efficacia dei medesimi in termini di «disegno» e «funzionamento»[5]. Qualora non vi siano controlli o siano rilevate delle carenze si attiva, ove possibile, una specifica azione di mitigazione con l'obiettivo di ridurre o tenere monitorato il rischio rilevato.

Studio di Manuali, Regolamenti di Settore, Procedure, etc.

In momenti diversi dal *Risk Self Assessment* è possibile trarre spunto per la mappatura dei controlli da documenti ufficiali, emanati o aggiornati in corso d'anno.

Loss Data Collection

Nel momento in cui si registra un evento rilevante, l'Unità Operational Risk Management provvede ad approfondire le ragioni che l'hanno generato e condividere eventuali controlli da porre in essere per evitare che tale evento si verifichi nuovamente.

4.2.3 *GENERIC ASSESSMENT* E ALTRE VALUTAZIONI DI RISCHIOSITÀ OPERATIVA POTENZIALE

Unitamente all'approccio descritto con riferimento al processo di *Risk Self Assessment,* possono essere svolti specifici *assessment* – "Generic Assessment" - per effettuare valutazioni *ex ante*, con particolare riferimento a:

- nascita di nuovi prodotti/servizi, ingresso in nuovi mercati o avvio di nuovi processi operativi;
- *re-engineering* di processi, scelte di esternalizzazione di attività o processi, interventi sulla struttura organizzativa, adozione di nuovi applicativi;

Il *Generic Assessment* assume la forma di un questionario standardizzato per la valutazione "qualitativa" degli eventi ambito di analisi e può costituire la base per avviare approfondimenti in sede di assessment per le Unità Organizzative coinvolte.

Obiettivo del *Generic Assessment* è anche quello di contribuire, in una visione integrata dei rischi, al monitoraggio, se del caso, del rischio reputazionale, oltre chedi favorire l'aggiornamento dei modelli di controllo e delle procedure alla base degli stessi.

[4] In tale fase si procede ad aggiornare tutti i controlli, anche quelli non soggetti a modifica, specificando che vengono confermati, non solo quelli relativi all'unità oggetto di *assessment,* ma eventualmente anche delle unità cd. "figlie".

[5] Sulla base della valutazione del disegno e del funzionamento dei controlli è possibile attribuire un giudizio di efficacia basato su quattro livelli: "efficace", "parzialmente efficace", "parzialmente inefficace", "inefficace".

Gli esiti dei *Generic Assessment* vengono inclusi nella reportistica ad uso gestionale e istituzionale predisposta per le funzioni e gli organi aziendali interessati.

L'unità Operational Risk Management è, inoltre, coinvolta in specifiche valutazioni previste dalle Policy adottate in materia di Product Governance, Operazioni di Maggior Rilievo ed Esternalizzazione di funzioni aziendali.

Anche in questi casi, le metodologie di analisi e valutazioni applicate contengono i seguenti elementi comuni con il Generic Assessment:

- analisi degli scenari potenziali di rischio operativo e, ove applicabili, reputazionali;
- valutazione qualitativa di rischio residuo, che tiene conto dei presidi di mitigazione identificati;
- formulazione di eventuali suggerimenti / raccomandazioni ad ulteriore mitigazione dei rischi identificati.

4.2.4 KEY RISK INDICATORS E INDICATORI DI MONITORAGGIO

L'analisi degli "indicatori di rischio" (*Key Risk Indicators*) è un utile elemento per identificare e approfondire eventuali anomalie, errori o malfunzionamenti, che, se non tempestivamente presidiati, potrebbero comportare eventi di rischio operativo con impatti economico-finanziari e/o reputazionali anche rilevanti.

Il livello di riferimento di tali indicatori è tarato sulla base di opportuni livelli di soglia/andamentali, impostati sulla base di orizzonti predefiniti di rilevazione e tenendo conto della sensibilità e dell'esperienza della funzione Risk Management o delle altre Unità Organizzative coinvolte nella raccolta dei dati.

Ove definiti, tali valori rappresentano il limite oltre il quale la situazione osservata richiede analisi ed approfondimenti, da cui possono scaturire azioni correttive, interventi di mitigazione o modifiche ai livelli di soglia, qualora divenuti non significativi.

Tali evidenze, possono, inoltre, rappresentare *input* per indirizzare eventuali RSA o contribuire ad alimentare indicatori di Risk Appetite Framework definiti dall'Unità Operational Risk Management di Banca Mediolanum a livello di Gruppo Bancario.

Inoltre, nell'ambito dei Key Risk Indicators, al fine di monitorare eventuali fenomeni considerati rilevanti, per tipologia di rischio, in termini di frequenza di accadimento e/o di impatto economico, vengono definiti anche gli **indicatori di monitoraggio**, volti a rappresentarne l'andamento nel tempo e analizzarne tempestivamente eventuali incrementi significativi. Tali indicatori sono attualmente monitorati dall'Unità Operational Risk Management di Banca Mediolanum a livello consolidato di Gruppo Bancario e sono oggetto di rappresentazione al Consiglio di Amministrazione della Capogruppo con frequenza trimestrale.

Infine, si specifica che nel perimetro di monitoraggio è stato introdotto un indicatore complessivo di Gruppo Bancario, denominato "*Significant Operational Losses*", nel cui calcolo confluiscono anche le perdite operative rilevate dalla società Flowe. Per tale indicatore è stata, inoltre, definita una soglia che rappresenta il limite oltre il quale è necessario attivare un processo di escalation volto ad individuare le eventuali azioni correttive da intraprendere.

Tale indicatore è stato definito nell'ambito dell'esercizio annuale di Recovery Plan, condotto dalla Capogruppo.

L'attività di raccolta e monitoraggio dei *Key Risk Indicators* è stata attivata per la Società nell'ambito del monitoraggio dei rischi ICT e di sicurezza.

4.3 MISURAZIONE

La Misurazione è l'attività di analisi e valorizzazione della rischiosità. È un'attività finalizzata alla conoscenza completa del profilo di rischio complessivo dell'impresa, ed alla quantificazione del capitale a rischio per ciascuna unità.

La misurazione porta alla quantificazione di un:

- capitale regolamentare;
- capitale economico.

4.3.1 MISURAZIONE DEL CAPITALE REGOLAMENTARE

La misurazione ai fini regolamentari, effettuata sulla base delle disposizioni normative, prevede 4 modalità di calcolo dei requisiti patrimoniali a fronte dei rischi operativi:

1. *Basic Indicator Approach* (BIA): prevede il calcolo del requisito patrimoniale come una percentuale della media triennale dell'indicatore rilevante (15%);
2. *The Standardized Approach* (TSA): gli enti calcolano il requisito in materia di fondi propri per il rischio operativo come la media triennale della somma dei requisiti annuali in materia di fondi propri per tutte le *business line*. Il requisito annuale in materia di fondi propri per ogni linea di attività è pari al prodotto del corrispondente fattore beta (specifico coefficiente definito dall'organo di vigilanza) e della parte dell'indicatore rilevante classificata nella linea di attività interessata;
3. *Alternative Standardised Approach* (ASA): per le *business line* "servizi bancari al dettaglio" e "servizi bancari a carattere commerciale" l'indicatore rilevante è pari all'ammontare nominale dei crediti e degli anticipi moltiplicato per un fattore (0,035);
4. *Advanced Measurement Approach* (AMA): secondo tale approccio, il capitale regolamentare per i rischi operativi è pari alla misura di rischio generata dai modelli interni di quantificazione, subordinatamente ai requisiti qualitativi e quantitativi espressi dal Regolamento (UE) N. 575/2013.

A partire dall'entrata in vigore, il 01 gennaio 2014, del Regolamento UE 575/2013, l'utilizzo combinato del metodo Base e del metodo Standardizzato per il calcolo del requisito di fondi propri a fronte del rischio operativo non è consentito, se non in circostanze eccezionali.

Flowe, che non è soggetta a requisito patrimoniale individuale a fronte dei rischi operativi, concorrerà, al calcolo del requisito patrimoniale consolidato del Gruppo Bancario Mediolanum adottando un approccio di misurazione di tipo Standardizzato.

Tra i requisiti per l'adozione del metodo Standardizzato, è prevista l'applicazione di una metodologia di calcolo basata sulla classificazione delle attività delle società nelle otto linee di *business* indicate dall'articolo 317 del suddetto Regolamento (si veda la tabella riportata sotto).

A fronte di tale classificazione, viene calcolato il requisito di fondi propri di Gruppo Bancario per linea di *business* come prodotto tra la parte dell'indicatore rilevante, grandezza contabile definita dalle voci e dai principi elencati nell'articolo 316 del suddetto Regolamento, classificata nella Linea di Business e il fattore beta associato a ciascuna linea.

Linea di Business	Parametro di riferimento (β)
Corporate Finance	18%
Trading & Sales	18%
Retail Brokerage	12%
Commercial Banking	15%
Retail Banking	12%
Payment & Settlement	18%
Agency Services	15%
Asset Management	12%

Il requisito di fondi propri complessivo è poi ottenuto come media delle tre ultime osservazioni su base annuale della somma dei requisiti in materia di fondi propri per tutte le linee di *business.*

L'indicatore rilevante si calcola come somma degli elementi positivi e negativi elencati di seguito:

1. Interessi e proventi assimilati
2. Interessi e oneri assimilati
3. Proventi su azioni, quote ed altri titoli a reddito variabile/ fisso
4. Proventi per commissioni/provvigioni
5. Oneri per commissioni/provvigioni
6. Profitto (perdita) da operazioni finanziarie
7. Altri proventi di gestione.[6]

Tale processo di misurazione viene svolto dall'Ufficio Bilancio Individuale e Consolidato di Banca Mediolanum in collaborazione con l'Unità Operational Risk Management.

4.3.2 MISURAZIONE DEL CAPITALE ECONOMICO

La valutazione dell'adeguatezza del capitale regolamentare, calcolato applicando i metodi di misurazione previsti dalla normativa di vigilanza e richiamati nel precedente capitolo, trova riscontro nel confronto tra quest'ultimo e un requisito di capitale economico o interno di Gruppo Bancario, calcolato utilizzando un approccio integrato che riflette sia le perdite effettive da rischi operativi che quelle potenziali, valutate al netto dell'efficacia dei controlli posti in essere per la loro mitigazione.

Il modello di riferimento per il calcolo del capitale economico può essere, pertanto, suddiviso in due macro componenti:

- un "capitale storico": calcolato utilizzando dati interni di perdita raccolti nel processo di Loss Data Collection (LDC);
- un "capitale prospettico": calcolato utilizzando stime prospettiche fornite dal management delle società del Gruppo Bancario Mediolanum nell'ambito del processo di Risk Self Assessment (RSA).

[6] Per le correzioni e gli ulteriori requisiti da applicare ai fini del calcolo dell'indicatore si rimanda all' art. 316 del Regolamento UE 575/2013.

Il capitale economico è ottenuto dall'integrazione della stima del capitale storico e del capitale prospettico ed è calcolato usando un sistema di indicatori che ponderano il contributo delle due stime di capitale.

Il processo di misurazione del capitale economico descritto include nella base dati di *Loss Data Collection,* utilizzata per il calcolo del "capitale storico", anche i dati di perdita della società Flowe. Analogamente, contribuiscono alla determinazione del capitale prospettico anche i risultati dei questionari di Risk Self Assessment elaborati per la società.

4.4 MONITORAGGIO, CONTROLLO E REPORTING

La Capital Requirements Regulation evidenzia, come requisito essenziale per gli enti che utilizzano modelli di tipo standardizzato, l'esistenza di un processo strutturato di reporting verso gli organi aziendali coinvolti a vario titolo nei processi di controllo e gestione dei rischi operativi.

In particolare, l'articolo 320, "Criteri per il metodo standardizzato", prevede che *"l'ente dispone di un sistema di comunicazione verso l'alta dirigenza che fornisce segnalazioni sull'esposizione al rischio operativo ai responsabili delle funzioni rilevanti all'interno dell'ente".*

La valutazione dei rischi a cui sono esposti i processi aziendali ne prevede, pertanto, la sintesi in appositi *report*, la cui fruizione è a supporto sia delle linee operative, direttamente interessate dai processi di gestione e mitigazione dei rischi, che dell'Alta Direzione e del Consiglio di Amministrazione.

Anche le Disposizioni di vigilanza per gli istituti di pagamento e gli istituti di moneta elettronica prevedono che *"Le funzioni aziendali di controllo presentano agli organi aziendali, almeno una volta all'anno, relazioni sull'attività svolta e forniscono agli stessi organi consulenza per i profili che attengono ai compiti di controllo svolti."*

Le attività di monitoraggio, controllo e *reporting* sono diretta conseguenza delle preliminari fasi di identificazione e misurazione che consentono di analizzare l'esposizione complessiva ai rischi operativi delle varie unità di *business* e di segnalare tempestivamente eventuali criticità riscontrate.

Il principale strumento utilizzato nello svolgimento di tale processo è la produzione di reportistica per le funzioni aziendali interessate.

La seguente tabella sintetizza le caratteristiche, in termini di contenuto e frequenza, della reportistica prodotta con riferimento ai rischi operativi di Flowe S.p.A., in quanto facente parte del Gruppo Bancario Mediolanum:

Destinatario	Contenuto	Frequenza
Consiglio di Amministrazione / Amministratore Delegato	Resoconto attività annuali e pianificazione anno successivo	Annuale
Consiglio di Amministrazione / Amministratore Delegato	Informativa periodica sull'andamento dei controlli e sulle perdite operative	Semestrale

Amministratore Delegato	Condivisione *ex-ante* del piano di *assessment* ed *ex-post* dei risultati dello stesso	Annuale
Comitato Rischi della Capogruppo	Andamento periodico perdite operative di Gruppo Bancario (incluse eventuali perdite della Società)	Almeno trimestrale
Responsabili Unità organizzative	Esiti *assessment* e azioni di mitigazione, eventuali perdite rilevanti e piani di azione	In sede di *assessment* e/o ad evento

In particolare, la **relazione sul processo di controllo e presidio dei rischi operativi**, ha i seguenti principali obiettivi:

- valutare la qualità del sistema di gestione dei rischi operativi, nonché la sua rispondenza nel tempo alle prescrizioni normative esterne ed interne, alle esigenze operative aziendali e all'evoluzione del mercato di riferimento;
- documentare le principali evidenze riscontrate nei processi di identificazione e presidio dei rischi operativi nell'esercizio di riferimento, anche attraverso l'analisi dei piani di azione in corso e da avviare per un'efficace gestione dei rischi operativi nel loro complesso.

La relazione intende quindi fornire un'adeguata informativa sulle attività di controllo e gestione dei rischi operativi in uso presso la Società e, previo esame ed approvazione da parte del Consiglio di Amministrazione, viene trasmessa al Risk Management di Banca Mediolanum affinché possa procedere alla predisposizione della relazione consolidata di Gruppo.

Con riferimento alla normativa di Vigilanza disciplinata dalla Circolare di Banca d'Italia n. 286, relativa alle istruzioni per la compilazione delle **segnalazioni prudenziali** per i soggetti vigilati, si cita anche la reportistica semestrale inoltrata all'ufficio Segnalazioni di Vigilanza di Banca Mediolanum, contenente la ripartizione delle perdite operative, di Gruppo Bancario per linee di business e per eventi di perdita, incluse informazioni di dettaglio con riferimento agli eventi con le perdite più rilevanti rilevate nel periodo di riferimento.

Inoltre, la funzione Risk Management elabora annualmente, in collaborazione con le unità Augmented Intelligence e IT Security di Banca Mediolanum la "Relazione sulle risultanze dell'analisi dei rischi operativi e di sicurezza relativi ai servizi di pagamento", in attuazione a quanto richiesto dalle Direttiva PSD2 e Circolare n. 285 di Banca d'Italia.

Periodicamente, vengono inoltre valutati gli aggiornamenti e le revisioni della presente policy, coerentemente con le linee guida di Gruppo Bancario.

Inoltre, nell'ambito del "**Risk Appetite Framework**" il Capitale Economico di Gruppo Bancario è stato individuato quale indicatore strategico e viene sottoposto a monitoraggio periodico dalla Capogruppo Banca Mediolanum, al fine di verificare il rispetto dei livelli di Risk Appetite, Risk Tolerance e Risk Capacity, con riferimento al rischio operativo complessivo di Gruppo Bancario.

Oltre al Capitale Economico, sono stati definiti i seguenti ulteriori indicatori strategici basati sulle perdite operative di Gruppo Bancario, che hanno l'obiettivo di rafforzarne il monitoraggio offrendo un quadro di maggiore dettaglio su specifiche sottocategorie: Indicatore rischio di condotta, Indicatore altri rischi legali e Indicatore anomalie operative. Gli eventi di perdita della Società Flowe contribuiscono al calcolo di tali indicatori.

4.5 GESTIONE

La fase di Gestione del Rischio Operativo si pone come obiettivo la valutazione periodica delle "strategie per il controllo e la riduzione del rischio", decidendo, in base alla natura e all'entità dello stesso, se assumerlo, se attuare politiche di mitigazione o trasferirlo a terzi, in relazione alla propensione al rischio espressa dal Vertice aziendale.

Il processo decisionale di scelta delle modalità più opportune e convenienti per la gestione del rischio si basa su un'analisi costi/benefici razionale, consapevole, mirata e oggettiva.

In estrema sintesi, le priorità di intervento nei processi di gestione e mitigazione dei rischi operativi sono definite sulla base:

- del rating attribuito in sede di Risk Self Assessment;
- delle evidenze emerse in sede di *Risk Self Assessment* o in occasione di specifici *assessment (Generic Assessment*);
- della rilevazione di controlli inesistenti o inefficaci nell'ambito del processo di *Risk Factor Control Assessment*;
- dell'eventuale registrazione di perdite rilevanti manifestatesi nello svolgimento di un determinato processo.

Le attività di gestione, nel rispetto dei vincoli normativi e delle richieste degli Organi di Vigilanza e tenuto conto del livello complessivo di *risk appetite*, si ispirano a principi di **"pragmatismo"** ed "**efficacia**", per trovare il giusto equilibrio tra:

- costi degli interventi di prevenzione e controllo dei rischi;
- potenziali perdite patrimoniali indotte dal verificarsi di fattori di rischio.

Nei paragrafi seguenti si illustra sinteticamente il processo alla base della definizione dei piani di azione/azioni di mitigazione dei rischi operativi.

Si segnala che, la valutazione dell'opportunità di avviare eventuali progetti e piani di azione volti a mitigare i rischi operativi e la definizione delle priorità, anche rispetto ad altri progetti in corso, sono valutati, *in primis*, dai Responsabili delle Unità Organizzative (risk owner).

4.5.1 ANALISI

Preliminarmente all'attivazione di processi di gestione dei rischi operativi è necessario svolgere un'analisi del contesto normativo e organizzativo di riferimento, oltre che delle evidenze raccolte nei precedenti processi di identificazione, misurazione e gestione di rischi operativi.

In particolare, la fase di analisi prevede generalmente le seguenti principali attività:

- identificazione del perimetro organizzativo di riferimento: unità organizzative coinvolte nel processo, procedure e processi operativi, localizzazione organizzativa, strumenti in uso;
- identificazione del contesto normativo: analisi del perimetro normativo di riferimento rispetto ai processi operativi analizzati al punto precedente;
- analisi progetti già in corso di implementazione, per aumentare snellezza operativa, efficienza organizzativa o migliore aderenza normativa;
- analisi risultati precedenti attività di "identificazione" dei rischi operativi: in particolare, esame dell'attività svolta nel corso dei processi di *Risk Self Assessment* e *Loss Data Collection* relativamente all'unità organizzativa e ai processi ambito di analisi;
- approfondimenti organizzativi sulle possibili azioni di mitigazione/gestione dei rischi operativi, ove necessario, avvalendosi della collaborazione della Funzione Compliance, dell'Unità Augmented Intelligence, dell'Unità Happiness & Services, o dell'Unità Organization & Business Continuity.

4.5.2 GESTIONE OPERATIVA E PIANI DI AZIONE/AZIONI DI MITIGAZIONE

In base alle evidenze emerse in fase di analisi è possibile definire le politiche di gestione dei rischi operativi, che potrebbero consistere in azioni di:

- controllo: interventi preventivi;
- riduzione: tipicamente caratterizzata da interventi di reingegnerizzazione dei processi;
- contenimento o trasferimento, mediante scelte di natura assicurativa o finanziaria.

Ambito del presente paragrafo sono soprattutto le logiche alla base degli interventi di controllo e "riduzione" dei rischi operativi e la definizione di piani di azione/azioni di mitigazione.

Le attività di costruzione di scenari alternativi sono effettuate avvalendosi della collaborazione del responsabile dell'Unità Organizzativa direttamente coinvolta nella gestione dei processi ambito di approfondimento, oltre che dell'Unità Augmented Intelligence (ove siano previste delle implicazioni informatiche) e dalla Settore Pianificazione Operativa e Controllo di Gestione di Banca Mediolanum, per supportare le analisi economiche (costi/investimenti e benefici) relative ai piani di azione.

In taluni casi, qualora gli impatti economici di rischio e di progetto fossero particolarmente rilevanti, vengono coinvolte strutture decisionali di tipo "collegiale", coerentemente ai processi di approvazione di budget e investimenti in uso presso il Gruppo Mediolanum.

La Funzione Risk Management svolge attività di rilevazione, monitoraggio e presidio dei piani di azione / azioni di mitigazione rispetto alle scadenze concordate, supporto operativo, ove richiesto, e fornisce la necessaria informativa agli organi di controllo interno, attraverso la produzione di apposita reportistica.

A completamento del piano di lavoro concordato si definiranno chiuse le attività. Il risultato del progetto viene valutato rispetto ai risultati effettivamente conseguiti, nell'ambito dei processi di identificazione dei rischi operativi precedentemente descritti.

4.5.3 POLITICHE DI CONTENIMENTO/TRASFERIMENTO

La gestione attiva dei rischi operativi può essere completata anche attraverso l'insieme di attività che permettono di trasferire l'effetto finanziario su terzi. Queste soluzioni possono essere di natura assicurativa o possono basarsi su schemi di natura finanziaria.

Con riferimento specifico alle politiche di trasferimento dei rischi si richiamano le polizze assicurative sottoscritte dalle società del Gruppo per fronteggiare eventi particolarmente rischiosi che potrebbero derivare:

- dal comportamento scorretto di collaboratori;
- dal verificarsi di eventi esterni non prevedibili e, talvolta, di impatto rilevante (es. incendio);
- dai nuovi rischi di tipo informatico (es. copertura assicurativa Cyber Risk);
- da previsioni normative specifiche (es. assicurazione per la responsabilità civile professionale a norma dell'articolo 5, paragrafo 4, della direttiva (UE) 2015/2366).

La politica di trasferimento dei rischi viene valutata in primis dal responsabile dell'unità organizzativa che presidia il fattore di rischio, chiedendo ove ritenuto opportuno, il coinvolgimento della Funzione Risk Management.

5 Strumenti informatici

Nel presente capitolo sono indicati i principali strumenti informatici utilizzati a supporto delle attività del processo di controllo e gestione dei rischi operativi. Per un dettaglio sulle loro caratteristiche si rimanda ai rispettivi manuali operativi.

In particolare, per le attività di controllo sui rischi operativi, si utilizzano i seguenti supporti informatici:

- *OpRisk Evolution*, della società List, applicativo a supporto delle attività di analisi dei rischi rispetto ai principali processi aziendali;
- *Sap* e *Tagetik* applicativi di contabilità generale e di consolidamento dei dati contabili a livello di Gruppo utilizzati per il calcolo del requisito patrimoniale e per l'espletamento delle attività propedeutiche alle segnalazioni di Vigilanza;
- strumenti di *Office automation*, soprattutto a supporto del processo di *reporting*.

OpRisk Evolution, rappresenta il database principale per l'identificazione dei Rischi Operativi. In tale "*repository*" sono archiviate e storicizzate le attività svolte con riferimento ai processi di *Risk Self Assessment* e *Loss Data Collection*.

Inoltre, si precisa che, su tale strumento, è stata effettuata una mappatura ai fini gestionali interni dei processi e delle unità organizzative delle società del Gruppo.

6 Il Rischio ICT e di sicurezza

La Circolare di Banca d'Italia n° 285 del 17 dicembre 2013 al titolo IV capitolo 4 (Sistema Informativo) definisce il **rischio ICT e di sicurezza** come:

"il rischio di incorrere in perdite dovuto alla violazione della riservatezza, carente integrità dei sistemi e dei dati, inadeguatezza o indisponibilità dei sistemi e dei dati o incapacità di sostituire la tecnologia dell'informazione (IT) entro ragionevoli limiti di tempo e costi in caso di modifica dei requisiti del contesto esterno o dell'attività (agility), nonché i rischi di sicurezza derivanti da processi interni inadeguati o errati o da eventi esterni, inclusi gli attacchi informatici o un livello di sicurezza fisica inadeguata. Nella rappresentazione integrata dei rischi aziendali a fini prudenziali (ICAAP), tale tipologia di rischio è considerata, secondo gli specifici aspetti, tra i rischi operativi, reputazionali e strategici".

Le "Disposizioni di vigilanza per gli istituti di pagamento e gli istituti di moneta elettronica", indicano tra i rischi che assumono particolare rilievo per tali società anche il rischio relativo alla sicurezza, definito come:

"il rischio derivante dall'inadeguatezza o dalla mancanza di processi interni oppure da eventi esogeni che hanno, o potrebbero avere, un effetto negativo sulla disponibilità, integrità e riservatezza dei sistemi che impiegano le tecnologie dell'informazione e della comunicazione (ICT) e/o delle informazioni utilizzate per la prestazione dei servizi di pagamento."

La gestione del rischio ICT e di sicurezza, nel Gruppo Bancario Mediolanum si svolge attraverso un articolato processo che mira a identificare le vulnerabilità del sistema informatico, le possibili minacce, i controlli e le misure di sicurezza implementate, nonché a stimare i potenziali danni provocati sugli asset IT dal manifestarsi di insiemi omogenei di minacce, definiti "scenari" di Rischio ICT, e la relativa probabilità di accadimento.

In particolare, la gestione del rischio ICT è un processo articolato che si sviluppa in macro-fasi, per la cui illustrazione dettagliata si rinvia alla "Policy di Gestione del rischio Informatico" di Flowe, che prevedono, il coinvolgimento della Funzione Risk Management, degli utenti di riferimento dei diversi servizi/applicazioni, degli outsourcer e dell'unità organizzativa IT Operation Security & Governance, che si avvale del supporto del settore IT Security di Banca Mediolanum.

La definizione di rischio operativo adottata dal Gruppo comprende anche i rischi derivanti da *"carenze o malfunzionamenti tecnologici"* che sono, pertanto, oggetto di identificazione e controllo attraverso il *framework* descritto nei capitoli precedenti. Nel modello degli eventi di rischio operativo sono inclusi, inoltre, la "*Sicurezza dei Sistemi*" e l'"*Interruzioni dell'operatività e disfunzioni dei sistemi*".

Le analisi svolte nell'ambito del framework di controllo del rischio operativo sono integrate e a loro volta messe a fattor comune, con quelle previste dalla Policy di Gestione del Rischio Informatico e con informazioni periodicamente condivise con IT Operation Security & Governance (es. *incident report*, *key risk indicators, …*).
Nello specifico, con riferimento alla fase di identificazione:

- nel processo di *Risk Self Assessment*, è stata sviluppata una metodologia di integrazione delle evidenze emerse nello svolgimento degli assessment di tipo quantitativo, illustrato nel capitolo 4.2.2, con le informazioni raccolte nell'ambito del processo di valutazione del Rischio ICT e di sicurezza;

- nel processo di *Loss Data Collection*, sono previsti flussi informativi per integrare i dati di perdita raccolti con le rilevazioni effettuate nell'ambito della gestione degli incidenti informatici;
- nel processo di raccolta e analisi dei *Key Risk Indicators*, è stato identificato un set di indicatori nell'ambito del rischio ICT e di sicurezza per monitorare il fenomeno di indisponibilità degli asset IT aziendali e il rischio cyber, in termini di esposizione a infezioni degli asset IT e/o frodi informatiche.

Inoltre, ulteriori attività di monitoraggio e valutazione di tipo qualitativo della rischiosità operativa associata a nuove iniziative con significativo impatto ICT possono essere svolte attraverso l'esecuzione di Generic Assessment o altre valutazioni specifiche.

Le analisi condotte dalle Funzione Risk Management, con riferimento al Rischio ICT e di sicurezza, sono incluse nella reportistica periodica prodotta e illustrata nel paragrafo 4.4.
Infine, la funzione Risk Management, con frequenza annuale, predispone il Rapporto Sintetico sul Rischio ICT e di sicurezza.

7 Il Rischio di Condotta

Ulteriore sotto-categoria del Rischio Operativo, particolarmente rilevante per Il Gruppo Bancario Mediolanum, è:

"Il corrente o potenziale rischio di incorrere in perdite economiche generato dalla fornitura inadeguata di servizi finanziari, compresi i casi di dolo o negligenza".

Il Rischio di Condotta è, in linea con le "Guidelines on common procedures and methodologies for the SREP" del 19 dicembre 2014, identificato "*come parte del rischio legale nell'ambito di applicazione del rischio operativo"* [7].ma, in considerazione della sua pervasività su comparti e processi aziendali, gli attori coinvolti nel suo presidio sono molteplici e diffusi all'interno della struttura organizzativa.

Si richiamano di seguito, le Unità Organizzative principalmente coinvolte nelle analisi relative alla condotta nella fornitura di prodotti e servizi:

- Funzione Risk Management, nello svolgimento del framework di controllo e gestione dei rischi operativi, monitora l'esposizione agli eventi riconducibili alle tipologie "Frode Interna" e "Clientela, prodotti e prassi professionali", nonché a ogni altro accadimento, non riconducibile nelle categorie predette, ma comunque connesso al rischio di condotta.

[7] Le linee-giuda riportano, inoltre, le seguenti principali fattispecie:

"a. vendita fraudolenta di prodotti, nei mercati al dettaglio e all'ingrosso;

b. vendite incrociate forzate (pushed cross-selling) di prodotti a clienti privati, come ad esempio conti bancari packaged o prodotti aggiuntivi di cui i clienti non hanno bisogno;

c. conflitti di interesse nella conduzione delle operazioni;

d. manipolazione dei tassi di interesse di riferimento, dei tassi di cambio o di altri strumenti finanziari o indici per migliorare i profitti degli enti;

e. barriere poste alla possibilità di cambiare prodotti finanziari durante il loro ciclo di vita e/o di passare ad altri fornitori di servizi finanziari;

f. canali di distribuzione mal progettati che possono dare origine a conflitti di interesse con falsi incentivi;

h. rinnovi automatici di prodotti o penalizzazioni in caso di dismissione e/o trattamento ingiusto dei reclami dei clienti."

- Funzione Compliance, ha la responsabilità di presidiare il rischio di non conformità alle norme, sia esterne che interne. In particolare, i rischi operativi sono quindi valutati principalmente nella prospettiva dei rischi di condotta ed in tale prospettiva la Funzione è responsabile della valutazione dei processi, in relazione alle differenti aree di business, che hanno impatto su tale tipologia di rischio sia a livello ex-ante, mediante la validazione dei processi e della e della normativa interna, sia a livello ex-post, attraverso verifiche specifiche sui processi in termini di adeguatezza e di efficacia.
- Funzione Antiriciclaggio, cui compete la verifica nel continuo che le procedure aziendali siano coerenti con l'obiettivo di contrastare la violazione di norme in materia di riciclaggio e finanziamento al terrorismo.

Come per il rischio ICT e di sicurezza, anche il rischio di condotta è integrato nel *framework* di gestione dei rischi operativi descritto nei capitoli precedenti e dunque oggetto di identificazione e controllo.

Sia i processi di controllo, che l'esito delle verifiche svolte, sono illustrati in policy / regolamenti e relazioni / report periodicamente predisposti principalmente dalla Capogruppo Banca Mediolanum per cui *in primis* tale rischio è rilevante.

8 La normativa esterna di riferimento

Di seguito viene evidenziato il quadro normativo di riferimento per il processo di controllo e presidio dei rischi operativi, costituito principalmente dai seguenti riferimenti:

- Disposizioni di vigilanza per gli istituti di pagamento e gli istituti di moneta elettronica emesse da Banca d'Italia il 23 luglio 2019;
- Direttiva 2013/36/UE (direttiva Capital Requirements Directive – CRD IV), 26 giugno 2013;
- Circolare di Banca d'Italia n. 285 (Disposizioni di vigilanza per le banche), 17 dicembre 2013;
- Provvedimento della Banca d'Italia del 23 luglio 2019 (Disposizioni di Vigilanza per gli istituti di pagamento e gli istituti di moneta elettronica, che modifica le disposizioni del 17 maggio 2016);
- Regolamento UE 575/2013 (Capital Requirements Regulation – CRR), 26 giugno 2013;
- Circolare di Banca d'Italia n. 286 (Istruzioni per la compilazione delle segnalazioni per i soggetti vigilati), 17 dicembre 2013;
- "Review of the Principles for the Sound Management of Operational Risk", emessa dal Comitato di Basilea il 6 ottobre 2014.

9 Normativa interna di riferimento

Risultano essere parte integrante della presente policy i seguenti documenti di Gruppo emessi dalla Capogruppo Banca Mediolanum S.p.A. nonché documenti emessi da Flowe stessa:

- Linee Guida e principi base di Coordinamento di Gruppo tra Organi e Funzioni di Controllo di Banca Mediolanum;
- Relazione sulla Struttura Organizzativa di Flowe S.p.A.;
- regolamento della Funzione Risk Management di Banca Mediolanum;
- il documento Risk Appetite Framework di Banca Mediolanum;
- Regolamento del processo di valutazione dell'adeguatezza patrimoniale (ICAAP) e della liquidità (ILAAP) di Banca Mediolanum;
- la Policy di Gestione del Rischio Informatico di Flowe S.p.A;
- la Policy per la gestione del rischio di reputazione di Flowe S.p.A.;
- la Policy in materia di esternalizzazioni di Flowe S.p.A.

Allegato 1) Linee di Business regolamentari

Linea di Business	Elenco Attività	Parametro di riferimento (β)
Corporate Finance	*Fusioni, Acquisizioni, Attività di collocamento (OPA, OPV, collocamenti privati – c.d. blocchi, emissioni obbligazionarie). Investment Banking in equity e capitale di debito (IPO, privatizzazioni, syndications, piazzamenti privati secondari, sottoscrizioni, etc.). Valutazioni d'azienda. Cartolarizzazioni per conto terzi. Gestione straordinaria di finanza d'impresa. Aumenti di capitale (solo come lead manager). Servizi di consulenza e ricerca (struttura di capitale, strategia industriale, undertakings, ristrutturazione, etc.). Consulenza d'investimento come business specifico.*	18%
Trading and Sales	*Negoziazione in conto proprio del portafoglio di trading. Gestione della tesoreria e funding in conto proprio (Asset & Liability Management, etc.). Cartolarizzazioni in conto proprio.* *Ricezione/trasmissione ed esecuzione di ordini verso clienti corporate e clienti professionali* [2]*.* *Attività di consulenza, assunzione a fermo, collocamento di strumenti finanziari/prodotti assicurativi (bancassurance, fondi, GPM, GPF, equity, bond, derivati, etc) verso clienti corporate e clienti professionali.*	18%
Retail Banking	*Prestiti/Depositi (anche a clienti "private" e SME). Garanzie e impegni finanziari (anche a clienti "private" e SME). Credito al consumo per clienti retail. Leasing/Factoring. Altri tipi di transazioni con controparti retail non allocati in altre "linee di business". Servizi ancillari ad attività retail come servizi di incasso e pagamento (carte di debito e di credito, trasferimento fondi ed altri pagamenti per conto di clienti, cambio valuta, etc.) e custodia ed amministrazione titoli.*	12%
Commercial Banking	*Prestiti/Depositi. Garanzie e impegni finanziari. Leasing/Factoring. Finanziamenti all'esportazione e al commercio. Altri tipi di transazioni con controparti corporate non allocati in altre "linee di business". Servizi ancillari ad attività corporate come servizi di incasso e pagamento (trasferimento fondi ed altri pagamenti per conto di clienti, cambio valuta, etc.) e custodia ed amministrazione titoli. Reddito netto (ad esempio cedole e dividendi) su portafogli non di trading.*	15%
Payment and Settlement	*Sistemi di pagamento (EBA, BIREL, TARGET, CLS, SWIFT, etc.). Sistema di compensazione e regolamento carte di credito (MASTERCARD, VISA, AMEX, etc.). Trasferimento fondi (come business specifico). Banca Corrispondente. Servizi di compensazione e regolamento.*	18%
Agency Services	*Banca depositaria. Custodia e servizi correlati (gestione contante e garanzie reali, depositi presso terzi, etc.) come business specifico. Servizi di esattoria. Servizi di tesoreria Enti. Banca Fiduciaria.*	15%
Asset Management	*Gestione Portafogli ed altre forme di gestione del risparmio (fondi comuni di investimento, fondi di pensione, GPM, GPF, hedge fund, etc.). Si intende solo la produzione e non la distribuzione di prodotti di risparmio gestito; fa eccezione l'attività di collocamento a clienti professionali effettuata da società dedicate.*	12%

Linea di Business	Elenco Attività	Parametro di riferimento (β)
Retail Brokerage	*Ricezione/trasmissione ed esecuzione di ordini verso clienti retail, "private" e SME. Attività di consulenza, assunzione a fermo, collocamento di strumenti finanziari/prodotti assicurativi (bancassurance, fondi, GPM, GPF, equity, bond, derivati, etc.) verso clienti retail, private e SME.*	12%

Allegato 2) Identificazione: Modello degli eventi di perdita – Catalogo Rischi

LIVELLO 1	DEFINIZIONE	LIVELLO 2	LIVELLO 3
01 - FRODE INTERNA	Perdite dovute a frode, appropriazione indebita o violazioni di leggi, regolamenti o direttive aziendali - ad esclusione degli episodi di discriminazione o mancata applicazione di condizioni paritarie - che coinvolgono almeno una parte interna	01_01 - Attività non autorizzata	*Transazioni non segnalate (intenzionalmente)*
			Transazioni non autorizzate
			Errata valutazione della posizione della clientela (intenzionale)
			Autorizzazione di esposizioni oltre le facoltà
			Deroghe, variazioni pricing non autorizzate
		01_02 - Furto e frode da personale interno	*Frodi interne nel credito*
			Attività fraudolenta nell'intermediazione mobiliare
			Sottrazione di informazioni da parte del personale
			Distruzione malevola e fraudolenta di asset aziendali da parte di dipendenti
			Riciclaggio di denaro
			Furti e appropriazioni indebite/rapina
			Distruzione dolosa di documenti o altri valori
			Contraffazione/falsificazioni
			Traenza di assegni senza copertura
			Utilizzo di conti altrui/sostituzione di persona/etc
			Market abuse
02- FRODE ESTERNA	Perdite dovute a frode, appropriazione indebita o violazione di leggi da parte di un terzo senza	02_01 - Furto e frode da esterni	*Furto ed appropriazioni indebite*
			Falsificazioni
			Manipolazione assegni da parte di terzi/traenza di assegni senza copertura

LIVELLO 1	DEFINIZIONE	LIVELLO 2	LIVELLO 3
	collaborazione di una parte interna		*Utilizzo di conti altrui /sostituzione di persona / ecc.*
			Truffe con carte bancomat o di credito (duplicazioni, furti, prelievi indebiti)
			Rapine ed estorsioni
			Frodi esterne nel credito
		02_02 - Sicurezza dei sistemi	*Attacchi deliberati ai sistemi applicativi (via malware, phishing, insider mirati)*
			Intrusioni fisiche nei data center
			Sottrazioni di informazioni (hackeraggio con perdita pecuniaria)
03 - RAPPORTO DI IMPIEGO E SICUREZZA SUL LAVORO	Perdite derivanti da atti non conformi alle leggi o agli accordi in materia di impiego, salute e sicurezza sul lavoro, dal pagamento di risarcimenti a titolo di lesioni personali o da episodi di discriminazione o mancata applicazione di condizioni paritarie verso i dipendenti	03_01 - Rapporto di impiego	*Licenziamento illegittimo*
			Demansionamento/rivendicazioni di qualifica superiore/retribuzione
			Cause di lavoro, problemi nella gestione delle relazioni con dipendenti
			Attività sindacali
		03_02 - Sicurezza sul lavoro	*Danni a persone e cose con responsabilità banca*
			Eventi relativi alla salute e alla sicurezza dei dipendenti
			Malattie professionali e rischio di contagio/pandemia
		03_03 - Discriminazioni/ condizioni non paritarie	*Ogni tipo di discriminazione (motivati da identità di genere, religione) / Mobbing*
04 - CLIENTELA, PRODOTTI EPRASSI PROFESSIONALI	Perdite derivanti da inadempienze, involontarie, per negligenza, o intenzionali (qualora vi sia vantaggio per la Banca), relative a obblighi professionali verso i clienti (inclusi i requisiti di fiducia e	04_01 - Adeguatezza, informativa e rapporti fiduciari	*Violazione di linee guida impartite dalla clientela/violazione della fiducia*
			Adeguatezza del servizio di investimento/prodotto finanziario alle caratteristiche del cliente (mancato rispetto del profilo di rischio)
			Obblighi di informazione verso la clientela
			Inadempienza contrattuale e adeguatezza obblighi di informativa e trasparenza dell'offerta

LIVELLO 1	DEFINIZIONE	LIVELLO 2	LIVELLO 3
	di idoneità) ed il mercato in generale; ovvero relative alla configurazione/predisposizione di prodotti e/o servizi alla clientela		*Violazione della privacy ed uso illecito di informazioni*
			Strategie di vendita aggressive
			Operazioni disposte al solo fine di generare commissioni ("churning")
		04_02 - Prassi di business o di mercato improprie	*Anatocismo*
			Manipolazione e pubblicità ingannevole
			Antitrust e pratiche di mercato e commerciali improprie
			Insider trading (per conto dell'azienda)
			Attività non autorizzate dalla Vigilanza
			Riciclaggio di denaro proveniente da attività illecite
			Evasione ed elusione delle tasse
			Finanziamento terroristico
			Negligenza professionale
			Mancato rispetto policy/regolamenti
			Mancato rispetto degli obblighi contrattuali da/verso controparti di business e agenti
			Atti di discriminazione nel mercato o verso l'esterno (per esempio verso categorie di clientela o di fornitori)
			Violazione di norme di settore
		04_03 - Difetti nella produzione	*Vizi di prodotto (contrattualistica non adeguata, mancata autorizzazione, ecc.)*
			Iter di approvazione prodotto incompleto/inadeguato (attività dei Comitati, consulenza, funzioni di controllo, ecc.)
			Errori nei modelli (difetti/vizi del modello di calcolo/simulazione/modelli di pricing errati)
			Indagini sulla clientela insufficienti od inadeguate

LIVELLO 1	DEFINIZIONE	LIVELLO 2	LIVELLO 3
		04_04 - Selezioni, sponsorizzazioni e limiti di esposizione	*Superamento dei limiti di esposizione concordati con il cliente*
			Cause o transazioni per Revocatoria Fallimentare / Cause o transazioni ex art. 44 Legge Fallimentare
		04_05 - Attività di consulenza	*Controversie riguardo alla performance effettiva*
			Reclami sull'attività di consulenza informativa
05 - DANNI DA EVENTI ESTERNI	Perdite dovute a smarrimento o danni ad attività materiali rivenienti da catastrofi naturali o altri eventi	05_01 - Catastrofi e altri eventi	*Disastri naturali*
			Incidenti d'auto coinvolgenti dipendenti nello svolgimento di attività lavorative
			Eventi socio-politici e terroristici
			Incidenti a clienti o terzi nei locali della Banca
			Incendi ed esplosioni, cortocircuiti
			Mancato rispetto di norme di pubblica sicurezza
			Atti di vandalismo con danni fisici ai beni di proprietà
			Guasti meccanici e rotture/infiltrazioni d'acqua
			Danni ai beni della banca per negligenza professionale
06 - INTERRUZIONI DELL'OPERATIVITA' E DISFUNZIONI DEI SISTEMI	Perdite dovute a interruzioni dell'operatività o a disfunzioni dei sistemi informatici	06_01 - Sistemi	*Guasti nell'hardware aziendale*
			Malfunzionamento applicazioni software
			Dati degli archivi non corretti o inutilizzabili (Data Integrity)
			Telecomunicazioni (impossibilità di utilizzare i mezzi di comunicazione)
07 - ESECUZIONE, CONSEGNA E GESTIONE DEI PROCESSI	Perdite dovute a carenze nel trattamento delle operazioni o nella gestione dei processi, nonché nelle relazioni con	07_01 - Avvio, esecuzione e completamento delle transazioni	*Comunicazioni fuorvianti*
			Errori di inserimento, tenuta o caricamento dei dati
			Capital management
			Errori/ritardi di esecuzione delle operazioni verso il cliente

LIVELLO 1	DEFINIZIONE	LIVELLO 2	LIVELLO 3
	controparti commerciali, venditori e fornitori		*Errori/ritardi nelle operazioni verso soggetti diversi da clienti*
			Mancata/errata/ritardata informativa verso il cliente
			Negligenze nella gestione delle garanzie
			Mancato rispetto manuali operativi, procedure
			Errori o ritardi in materia fiscale
			Negligenza nella tenuta delle basi di dati
		07_02 - Monitoraggio e reporting	*Inadempienze negli obblighi di segnalazione*
			Mancato/errato/ritardato Reporting Interno
			Inaccurate segnalazioni all'esterno (perdite effettive)
		07_03 - Acquisizione della clientela e relativa tenuta della documentazione	*Assenza di autorizzazioni o di manleve del cliente o di documentazione legale*
			Documentazione mancante, incompleta o errata
			Mancanza firma cliente su documento contrattuale o obbligatorio (es. Privacy)
			Perdite legate ad anagrafica non corretta
		07_04 - Gestione dei conti della clientela	*Accesso non autorizzato ai conti*
			Errata gestione operatività delegato
			Perdite o danni ai beni del cliente dovuti a negligenza
		07_05 - Controparti commerciali	*Errori/ritardi nel regolamento delle operazioni (titoli, estero, derivati, ecc)*
			Non rispetto delle performance minime
			Inadempienze verso controparti diverse dalla clientela
			Controversie con controparti diverse della clientela
		07_06 - Venditori e fornitori	*Controversie con venditori e fornitori*
			Controversie con Outsourcer
			Non rispetto dei Livelli di Servizio

Allegato 3) Identificazione: Modello dei fattori di rischio

LIVELLO 1	LIVELLO 2	ESEMPI
FR_1 - RISORSE UMANE	FR_1_1 - Carenze/Inadeguatezze nella gestione della posizione contrattuale/fiscale/previdenziale del dipendente	*Carenza/inadeguatezza del processo di gestione della posizione fiscale dei dipendenti*
		Carenza/inadeguatezza del processo di gestione della posizione previdenziale dei dipendenti
		Inadeguata applicazione livelli contrattuali
	FR_1_2 - Inadeguata applicazione delle norme sulla sicurezza sul posto di lavoro	*Inadeguata applicazione delle norme sulla sicurezza sul posto di lavoro*
	FR_1_3 - Inadeguata gestione del "clima aziendale"	*Inadeguato sistema comunicazione*
		Inadeguato sistema premiante
		Inadeguato sistema retribuzione
	FR_1_4 - Inadeguate politiche di gestione della privacy del personale dipendente	*Inadeguate politiche di gestione della privacy del personale dipendente*
	FR_1_5 - Negligenza, Incompetenza o Impreparazione professionale	*Inadeguata assegnazione responsabilità (in relazione alle professionalità)*
		Inadeguata gestione della conoscenza
		Inadeguato sistema formazione
		Inadeguato sistema selezione (assunzione)
	FR_1_6 - Inefficiente/inefficace/inadeguata organizzazione del lavoro	*Inadeguata allocazione risorse*
		Inadeguata distribuzione carichi di lavoro
		Mancanza di una chiara assegnazione dei ruoli alle risorse
FR_2 - SISTEMI IT, SICUREZZA DATI,	FR_2_1 - Assenza/Inadeguatezza delle policy di sicurezza con riferimento	*L'accesso alla sala dove risiedono application e data server non viene realizzato per mezzo di strumenti che consentono di*

LIVELLO 1	LIVELLO 2	ESEMPI
INFRASTRUTTURE TELEMATICHE	all'aspetto del controllo degli accessi (fisici) alla sala macchine (tipicamente dove risiedono application e data server)	*identificare il personale autorizzato (es. lettori di badge, porte apribili dall'interno, etc...)*
		Non esiste una procedura che regola gli accessi dei consulenti e dei tecnici esterni alla Sala Server
		Non risultano definite le azioni da intraprendere in caso di violazioni di accesso
		Non sono previste o risultano inadeguate misure di sicurezza della sala dove risiedono application e data server (es. telecamere a circuito chiuso, installazione di barriere anti-intrusione dall'esterno: grate, vetri anti-sfondamento)
	FR_2_2 - Assenza/Inadeguatezza delle policy di sicurezza con riferimento all'aspetto del controllo degli accessi (logici)	*Non è prevista o risulta inadeguata la procedura per la creazione/modifica/cancellazione di una utenza di accesso*
		Non è previsto un accesso differenziato ai Sistemi Applicativi sulla base della regola "need to know, need to do" (profili di accesso)
		Utilizzo di utenze di accesso di gruppo e non di utenze di accesso individuale
	FR_2_3 - Assenza/Inadeguatezza delle politiche di Network Security	*Inadeguata configurazione dei firewall (non garantisce ad es. che vi siano connessioni solo strettamente necessarie alla normale operatività aziendale)*
		Inadeguata segmentazione logica della rete (i segmenti di rete che ospitano i server con i dati più critici non risultano protetti da firewall)
		Inadeguatezza del processo di gestione dei software antivirus (non risultano installati su tutti i sistemi presenti nella rete, ritardi nell'aggiornamento dei motori e delle liste di virus del prodotto)
		Inadeguatezza del processo di gestione del servizio di accesso da remoto (ad es. non sono utilizzati meccanismi diffusi tipo Strong Authentication basato su Token o One Time Password)

LIVELLO 1	LIVELLO 2	ESEMPI
		L'accesso fisico alle apparecchiature di commutazione di rete (router, switch) non è regolamentato e consentito al solo al personale autorizzato;
		Le password utilizzate per l'autenticazione degli utenti non rispettano i requisiti minimi di network security (lungh. > 6 caratteri, composizione alfanumerica, periodo di validità non > di 15 giorni)
		Non è prevista un sistema di cifratura delle informazioni scambiate sulla rete (ed in particolare modo quelle strategiche per il business aziendale) e di autenticazione dei soggetti (infrastrutture di chiavi pubblica e chiave privata per l'autenticazione,
		Non è previsto un tool di Intrusion Detection che permetta di individuare in tempo reale eventuali tentativi di intrusione nella rete
	FR_2_4 - Il Software dedicato alla gestione degli accessi risulta inadeguato o erroneamente configurato	*Le password associate alle utenze di accesso sono visibili in chiaro quando digitate*
		Mancata disabilitazione di una utenza dopo N tentativi di accesso incorretto con password errata
		Non è prevista la disconnessione di una sessione di collegamento dopo N minuti che il terminale è idle
		Non è stato definito un periodo di validità delle password
	FR_2_5 - Inadeguatezza delle regole di accesso ai dati	*Accesso ai dati di produzione avviene, da parte dell'utente, non solo per mezzo dei sistemi transazionali, ma anche direttamente sui dati stessi*
		Non è chiara la separazione fra chi sviluppa programmi (e dovrebbe avere accesso alle basi dati di prova) e chi ha accesso alle basi dati effettive, cioè utenti finali, sistemisti operatori e data base administrators
		Assenza/inadeguatezza di un piano della sicurezza logica

LIVELLO 1	LIVELLO 2	ESEMPI
	FR_2_6 - Non è stata prevista o risulta inadeguata l'amministrazione della sicurezza logica IT aziendale	*Non è stata definita una figura di Security Administration con compiti esclusivi di amministrazione della sicurezza*
		Non sono stati definiti i compiti del Security Administrator
	FR_2_7 - Non sono previsti strumenti in grado di risalire all'autore di un tentativo di violazione o ad una violazione	*Non risultano definite opportune azioni da intraprendere sulla base delle violazioni/tentativi di violazione riscontrati*
		Non viene effettuata la registrazione delle violazioni e dei tentativi di violazione
	FR_2_8 - Assenza/inadeguatezza di procedure per far fronte all'indisponibilità di dati e/o applicazioni	*Inadeguatezza del Capacity Planning rispetto alle esigenze dell'Unità di Business*
		Inadeguatezza o mancata definizione e/o attuazione delle politiche di back-up (di sistema, dei dati e dei programmi)
		L'infrastruttura tecnologica (capacità elaborativa, struttura trasmissiva) risulta inadeguata alle esigenze dell'Unità di Business
		Non risulta sviluppato, implementato, periodicamente testato e mantenuto un adeguato piano per la gestione del business interruption (Disaster Recovery Plan)
		Non sono previste e/o sono non funzionanti le seguenti apparecchiature di "controllo ambientale": uninterruptable power supply; sistemi di condizionamento; sistemi di rilevamento calore, fumi ed acqua; sistemi antincendio.
	FR_2_9 - Inadeguatezza dei processi atti garantire la rilevanza dell'informazione (in termini di tempestività, ossia di efficienza/efficacia delle applicazioni a fornire le informazioni richieste, e di utilizzabilità,	*Assenza di strumenti di raccolta e sistematizzazione della informazione (operational data warehouse, data mart) e/o di supporto alle decisioni (decision support systems)*
		Assenza/inadeguatezza di un piano strategico di IT per ottimizzare gli investimenti in IT ed assicurare che le iniziative IT supportino i piani di medio e lungo termine dell'Unità di Business

LIVELLO 1	LIVELLO 2	ESEMPI
	ossia di rispondenza delle informazioni elaborate	*Manca un approccio continuo alla valutazione delle esigenze informative dell'Unità di Business*
		Manca un coinvolgimento degli utenti finali nel disegno, sviluppo dei sistemi applicativi
		Manca un coinvolgimento degli utenti finali nell'analisi ed approvazione delle applicazioni sviluppate per assicurare che soddisfino i requisiti richiesti
	FR_2_10 - Inadeguatezza dei processi di sviluppo e manutenzione ai sistemi (applicazioni, DBMS)	*Assenza o parziale implementazione di prodotti di Data Dictionary*
		Assenza o parziale implementazione di prodotti software di Change Management applicativo che consentano di automatizzare l'attività a supporto dello sviluppo e manutenzione software
		Inadeguatezza/Assenza delle procedure di autorizzazione ed approvazione del management per lo sviluppo e l'implementazione dei sistemi applicativi utente
		La direzione e l'utente non sono coinvolti nelle fasi di progettazione, sviluppo, test e conversione di ogni nuovo sistema (o sistema esistente ma sostanzialmente modificato)
		Non risultano definite le responsabilità per lo sviluppo, la gestione operativa, la manutenzione dei sistemi applicativi utente
		Non vengono utilizzate tecniche standard per la programmazione e la documentazione dei nuovi sistemi
	FR_2_11 - Inadeguatezza del processo di acquisizione Hardware, Software, altre risorse IT	*Inadeguatezza del processo di acquisizione Hardware, Software, altre risorse IT*
	FR_2_12 - Inadeguatezza/carenze nel processo di monitoring del Data Processing	*Non è prevista o risulta inadeguata una reportistica per il monitoraggio della processazione automatica dei dati (tipicamente batch) con evidenza di scarti e/o casi anomali*

LIVELLO 1	LIVELLO 2	ESEMPI
		Risultano assenti/inadeguati strumenti per il monitoraggio della processazione automatica dei dati (tipicamente batch) con particolare evidenza a casi anomali e/o scarti
FR_3 - PROCESSI E PROCEDURE, RAPPORTI CON CONTROPARTI COMMERCIALI E AUTORITA' DI VIGILANZA	FR_3_1 - Carenze / inadeguatezze nella gestione del rapporto con gli outsourcer/fornitori	*Assente / Inadeguato processo di archiviazione della documentazione relativa al rapporto con outsourcer/fornitori*
		Assenza / inadeguatezza di formalizzazione del rapporto con gli outsourcer/fornitori (comunicazione, modalità e livello di erogazione dei servizi)
		Carente / Inadeguata definizione sulle modalità e il livello di erogazione del servizio (SLA)
		Carenze / Inadeguatezze nel processo di comunicazione da/verso gli outsourcer
		Inadeguato processo di selezione dei fornitori esterni
	FR_3_2 - Assenza / Inadeguatezza / Inefficienza / Inefficacia del sistema dei controlli di processo (specific, pervasive, monitoring)	*Assenza / Inadeguatezza / Inefficienza / Inefficacia dei controlli di linea di tipo "monitoring" (controlli di alto livello operati sui processi aziendali dal management responsabile; disegnati ed utilizzati per monitorare l'efficacia di un controllo specifico*
		Assenza / Inadeguatezza / Inefficienza / Inefficacia dei controlli di linea di tipo "pervasive" (controlli disegnati per operare lungo l'intero percorso tracciato dai processi aziendali: segregation of duties, procedure di archiviazione, ...)
		Assenza / Inadeguatezza / Inefficienza / Inefficacia dei controlli di linea di tipo "specific" (controlli eseguiti nell'ambito dell'operatività stessa del processo: test a campione, verifica del rispetto dei parametri predefiniti di processo)
	FR_3_3 - Assenza / Inadeguatezza definizione SLA tra unità interne (laddove è presente un rapporto cliente-fornitore fra unità interne)	*Assenza / Inadeguatezza definizione SLA tra unità interne (laddove è presente un rapporto cliente-fornitore fra unità interne)*

LIVELLO 1	LIVELLO 2	ESEMPI
	FR_3_4 - Carenze / inadeguatezze nel processo di formalizzazione del rapporto con le controparti di mercato	*Carenze / inadeguatezze nel processo di formalizzazione del rapporto con altre controparti*
	FR_3_5 - Carenze / inadeguatezze nella gestione operativa del rapporto le controparti di mercato	*Carenze / inadeguatezze nella gestione operativa del rapporto le controparti di mercato*
	FR_3_6 - Inefficienza / Inefficacia dei processi (disegno, attività, attori)	*Inadeguatezza / Ridondanza /Inefficiente collocazione dei livelli di autorizzazione nell'ambito del processo*
		Inadeguatezza del disegno dei processi
		Mancata o inadeguata definizione degli attori di processo e relativo livello di responsabilità
		Non puntuale attribuzione delle attività agli attori di processo ("chi fa che cosa")
		Non puntuale definizione delle attività di processo
	FR_3_7 - Carenze/inadeguatezze nello sviluppo/gestione dei nuovi prodotti (servizi)	*Carenze/inadeguatezze nel processo che regolamenta la commercializzazione di nuovi prodotti (servizi)*
		Carenze/inadeguatezze nella fase di definizione degli aspetti contrattuali relativi al prodotto (servizio)
		Carenze/inadeguatezze nella fase di progettazione del prodotto (servizio)
		Carenze/inadeguatezze nella fase di testing del prodotto (servizio)
	FR_3_8 - Inadeguata definizione degli aspetti (trasparenza, correttezza, completezza, tempestività) relativi alla comunicazione di tipo informativo e commerciale verso i clienti	*Inadeguata definizione degli aspetti (trasparenza, correttezza, completezza, tempestività) relativi alla comunicazione di tipo informativo e commerciale verso i clienti*
		Inadeguato processo di comunicazione interna relativa alle modalità di gestione della privacy del cliente

LIVELLO 1	LIVELLO 2	ESEMPI
	FR_3_9 - Non chiara / Inadeguata definizione degli aspetti relativi alla gestione della privacy dei clienti	*Non chiara / Inadeguata definizione degli aspetti relativi alla gestione della privacy del cliente*
	FR_3_10 - Inadeguata gestione delle relazioni esterne (investor relations)	*Inadeguata gestione delle relazioni esterne (investor relations)*
	FR_3_11 - Inadeguate / inefficienti / inefficaci / incorrette politiche di gestione degli aspetti di regulation	*Inadeguate / inefficienti / inefficaci / incorrette politiche di gestione degli aspetti di regulation*
	FR_3_12 - Inadeguate / inefficienti / inefficaci / incorrette politiche di gestione degli aspetti fiscali	*Inadeguate / inefficienti / inefficaci / incorrette politiche di gestione degli aspetti fiscali*
	FR_3_13 - Assenza / Inadeguatezza di passaggi autorizzativi per l'esecuzione delle attività operative	*Assenza / Inadeguatezza di passaggi autorizzativi per l'esecuzione delle attività operative*
	FR_3_14 - Assenza / inadeguatezza misure di controllo verso attività non autorizzate e frodi da parte di dipendenti	*Assenza / inadeguatezza misure di controllo verso attività non autorizzate e frodi da parte di dipendenti*
	FR_3_15 - Inadeguatezze/carenze di Project Management	*Inadeguatezze/carenze di Project Management*
FR_4 - FATTORI ESTERNI & INFRASTRUTTURE FISICHE	FR_4_1 - Assenza / Inadeguatezza misure a fronte di calamità naturali (business continuity plan)	*Assenza di specifiche misure protettive per asset di natura critica*
		Assenza/inadeguatezza business continuity plan
	FR_4_2 - Assenza / inadeguatezza misure di prevenzione e di sicurezza verso atti di natura criminosa (rapine, terrorismo, vandalismo) - "security"	*Assenza / inadeguatezza di procedure gestione valori*
		Assenza / inadeguatezza misure di prevenzione e di sicurezza (es.: cassaforte a tempo, telecamere, sorveglianza, controllo accessi, ...)
		Assenza / inadeguatezza contingency plan

LIVELLO 1	LIVELLO 2	ESEMPI
	FR_4_3 - Assenza / inadeguatezza misure di prevenzione e sicurezza verso eventi di natura accidentale (per causa umana e/o naturale) - "safety"	*Assenza / inadeguatezza misure di prevenzione e sicurezza (es.: estintori, dispositivi salvavita, porte tagliafuoco, manutenzione impianti, rilevatori fumo e acqua, materiali ignifughi, ...) - "safety"*
	FR_4_4 - Assenza / inadeguatezza misure preventive verso frodi da parte esterni	*Assenza / inadeguatezza misure preventive verso frodi da parte esterni*
	FR_4_5 - Inadeguatezza/obsolescenza delle infrastrutture	*Inadeguatezza/obsolescenza delle infrastrutture*

Allegato 4) Identificazione: Modello degli effetti

Tabella di classificazione degli Effetti su 1 livello

LIVELLO 1	DEFINIZIONE/ DESCRIZIONE	ESEMPI
01 - RESPONSABILITÀ LEGALE	Sentenze, compromessi/risarcimenti e altri costi legali	• *Perdite incorse a seguito di procedimenti giudiziari, transazioni o arbitrati (incluse le parcelle agli avvocati esterni, settlement, giudizi pagati, ecc.)* • *Costi legali esterni direttamente associati all'evento* • *Svalutazioni basate sulle pratiche contabili*
02 - AZIONE DELL'AUTORITÀ DI REGOLAMENTAZIONE	Multe e pagamenti diretti ad altre sanzioni (p.e.: revoche di licenza)	• *Multe pagate per violazioni normative* • *Parcelle dovute agli avvocati per la rappresentanza nelle udienze relative a violazioni normative*
03 - PERDITA O DANNO AGLI ASSET FISICI	Riduzione diretta nel valore degli asset fisici per via di certi tipi di accadimenti (negligenza, incendio, terremoto, ecc.)	• *Costi per trasferimenti di breve periodo, per il ripristino dell'attività* • *Ricorso a terzi per non interrompere l'attività* • *Costi di ristrutturazione in seguito a incendio, alluvione e altri disastri* • *Svalutazioni/perdita definitiva di attività in seguito a incendio, alluvione e altri disastri* • *Perdita/distruzione di proprietà intangibili (p.e. i dati)*
04 - RESTITUZIONI	Pagamenti a terzi a seguito a perdite operative per le quali la banca è legalmente responsabile	• *Reclami di clienti dovuti ad interruzione di attività, per le quali la banca è responsabile* • *Risarcimenti richiesti dai clienti a causa di errori di pricing* • *Costi dovuti a ritardi di esecuzione* • *Risarcimenti verso quei clienti per le perdite sofferte a seguito di informazioni confidenziali andate perdute nell'ambito di un furto* • *Risarcimenti a seguito di frodi interne* • *Pagamenti a clienti in seguito a frodi esterne …*

LIVELLO 1	DEFINIZIONE/ DESCRIZIONE	ESEMPI
05 - PERDITE PER ERRORE NON RECUPERATE	Perdite subite quando una terza parte non rispetta le sue obbligazioni verso la banca, e che sono attribuibili ad un errore operativo della banca stessa (avrebbe potuto essere evitato, sebbene la controparte non volesse o non potesse pagare)	• *Fondi trasferiti per errore o doppi pagamenti impossibili da recuperare* • *Perdite operative legate al credito: errori nella documentazione del prestito, inadeguatezza del monitoraggio periodico, failure to perfect security interest (in discussione)* • *Incapacità di ricorrere al netting agreement per inadeguatezze nella documentazione e verifica della controparte (in discussione)*
06 - WRITE-DOWN	Riduzione diretta nel valore dell'attivo dovuta a furto, frode, attività non autorizzata, o perdite di mercato o di credito a seguito di eventi operativi	• *Perdite per mancato realizzo/acquisto di attività nei tempi più convenienti* • *Perdite derivanti da trading non autorizzato* • *Perdite per superamento dei limiti di esposizione sui mercati* • *Minori ricavi per errori di pricing* • *Frodi interne* • *Frodi esterne/furti risultanti in perdite di asset/ricavi* • *Violazione della sicurezza dall'esterno comporta l'ingaggio di consulenti per determinare la natura del problema e risolverlo*
07 - ALTRO (VOCI CHE NON RICADONO IN UNA CATEGORIA SPECIFICA)		• *Costi relativi a spese di consulenza/ a terzi per investigare/ ripristinare* • *Costi associati ad errori nella scelta dell'outsourcer* • *Carenze nei controlli che inducono a perdite operative, con necessità di consulenza per capire la causa del problema e proporre i rimedi*
08 - RISERVA	Riserve o accantonamenti contabili a fronte di specifici eventi operativi e relative variazioni	• *Importi riservati a seguito di contenziosi con la clientela ed eventuali variazioni, compresi smontamenti, di tali riserve.*