Operational Risk Management

METODOLOGIA DI IDENTIFICAZIONE

- ✓ ***tipo documento***: manuale
- ✓ ***author***: Settore Rischi Operativi e Reputazionali
- ✓ ***reviewer***: Settore Rischi Operativi e Reputazionali
- ✓ ***authorising agent and owner***: Servizio Rischi Operativi e Reputazionali
- ✓ ***dates of development and approval***: 30.06.2018
- ✓ ***version number***: 4
- ✓ ***history of changes to the document*** : 1. Dicembre 2007
  2. September 2015
  3. June 2017
  4. June 2018

Sommario

1. INTRODUZIONE 4

2. MODIFICHE RISPETTO ALLA VERSIONE PRECEDENTE 4

3. I RISCHI OPERATIVI 5

4. LE COMPONENTI DI IDENTIFICAZIONE 7

4.1 Premessa 7
4.2 Overview sul processo di identificazione 8

5. LA LOSS DATA COLLECTION 10

5.1 Premessa 10
5.2 Attività svolte in sede di LDC 11
5.2.1 Processo e aspetti organizzativi 11
5.2.2 Ricerca degli eventi operativi 11
5.2.3 Censimento degli eventi operativi 12
5.2.4 Le perdite operative di confine 21
5.2.5 Le perdite di natura commerciale 25
5.2.6 Gestione degli eventi multi-impatto: definizione di macro-evento 27
5.2.7 Adesione a consorzi esterni (DIPO) 30
5.2.8 Reporting 31

6. INDICATORI 31

6.1 Premessa 31
6.2 Indicatori e loro utilizzo 32

7. ASSESSMENT DEI FATTORI DI CONTESTO E DI CONTROLLO 34

7.1 Processo e aspetti organizzativi 34
7.2 Predisposizione dei questionari 35
7.3 Esecuzione dei questionari 36
7.4 Analisi dei risultati e reporting 39

8. ANALISI DI SCENARIO 39

8.1 Processo e aspetti organizzativi 39
8.2 Analisi dati (Loss Data Collection, Assessment e altre fonti) 41
8.3 Predisposizione dei questionari 44
8.4 Controlli di consistenza sulle domande dello Scenario 45
8.5 Esecuzione dei questionari 47
8.6 Analisi dei risultati e reporting 48

9. TIMING DELLA FASE DI IDENTIFICAZIONE 48

9.1 Sintesi 48
9.2 Loss Data Collection 48
9.3 Assessment 49
9.4 Scenario 50

10. ANNEX 50

10.1 Business Line 50
10.2 Event Type 52

1. INTRODUZIONE

Il presente documento illustra la metodologia di "identificazione" dei rischi operativi, esponendo le scelte metodologiche effettuate per l'individuazione, la raccolta e il censimento di tutte le informazioni rilevanti e utili alla valutazione del profilo di rischio operativo di Gruppo.

I capitoli a seguire forniscono una visione complessiva dell'approccio definito sia per il trattamento delle informazioni quantitative che di quelle qualitative, in un processo strutturato della gestione del rischio operativo declinato nel Framework di Operational Risk.

2. MODIFICHE RISPETTO ALLA VERSIONE PRECEDENTE

Le variazioni rispetto alla versione precedente sono evidenziate.

Nello specifico, si tratta di un ampliamento descrittivo non sostanziale intervenuto nel paragrafo "8.4 Controlli di consistenza sulle domande dello scenario".

3. I RISCHI OPERATIVI

Il Regolamento UE 575 del 26 giugno 2013, relativo ai requisiti prudenziali per gli enti creditizi e le imprese di investimento, recependo le Direttive Comunitarie 2006/48/CE, 2006/49/CE e 2012/648 UE, definisce il Rischio Operativo come **"*il rischio di perdite derivanti dall'inadeguatezza o dalla disfunzione di processi, risorse umane e sistemi interni, oppure da eventi esogeni, ivi compreso il rischio giuridico.*".**

Al fine di comprendere meglio il perimetro di rilevazione definito, il rischio operativo può essere scisso in due entità logiche:

- **Evento**: costituito da un accadimento dovuto a cause di natura operativa (gestione delle risorse umane, dei processi, della tecnologia ed eventi esterni) che comporta la manifestazione di effetti economici negativi (perdite operative);

- **Perdita**: costituita dagli effetti economici negativi derivanti da eventi di natura operativa, aventi impatti (solitamente negativi) sul conto economico.

Le perdite per loro natura possono essere:

- **Effettive**: nel caso in cui rappresentano manifestazioni economiche negative che misurano il danno subito dall'azienda per cause ascrivibili ai rischi operativi (ovvero che producono una corrispondente "scrittura" in conto economico);

- **Non Effettive**: nel caso in cui rappresentano mancati guadagni costituiti dagli introiti futuri che sarebbero stati conseguibili se non si fosse manifestato un inefficace/inefficiente gestione dei fattori interni e/o l'accadimento di eventi esterni (ovvero che non producono una corrispondente "scrittura" in conto economico).

Il perimetro del Gruppo MPS include soltanto le manifestazioni economiche negative, ovvero le perdite effettive:

- ✓ ***Certe in contabilità***: quando riferite in modo specifico a componenti negative del conto economico;

- ✓ ***Stimate in contabilità***: nel caso di accantonamenti a Fondi Rischi ed Oneri dovuti a atti/fatti aziendali già accaduti, il cui *quantum* è ancora incerto (cause legali, sanzioni future, ecc.).

Non sono inclusi nel perimetro:

- ✓ **Costi opportunità**: rappresentano i costi sostenibili e i proventi ottenibili dagli investimenti alternativi cui si è rinunciato impiegando risorse di cui si dispone in quantità limitata;

- ✓ **Programmi d'investimento**: spese annuali/pluriennali stanziate al fine di attuare una risoluzione strutturale alle perdite sostenute, innovando i processi, le tecnologie e le risorse umane in termini di efficacia ed efficienza;

- ✓ **Costi sostenuti per ragioni di ordine commerciale**: rappresentano rimborsi o riliquidazioni effettuati ai clienti, non legati ad effettive inadempienze, ma sostenuti in ogni caso per mantenere il rapporto con la clientela.

4. LE COMPONENTI DI IDENTIFICAZIONE

4.1 Premessa

La "Direttiva di Gruppo in materia di gestione e governo dei rischi operativi" schematizza il framework relativo al modello AMA (Advanced Measurement Approach) in 6 macro-passi:

1. **identificazione**, per la ricerca e il censimento delle perdite operative, di natura oggettiva o soggettiva, attraverso l'analisi di opportune fonti;

2. **misurazione**, per la determinazione del requisito patrimoniale a livello di Gruppo e per le singole società;

3. **monitoraggio**, per una costante verifica degli assorbimenti patrimoniali e delle indicazioni strategiche sulla propensione al rischio sia in termini gestionali che patrimoniali;

4. **gestione/controllo**, per l'individuazione delle azioni di mitigazione, trasferimento e ritenzione del rischio;

5. **manutenzione**, per assicurare nel continuo un progressivo aggiornamento del modello adottato nella gestione dei rischi operativi, della normativa, dei processi, degli applicativi;

6. **validazione interna e revisione**, per garantire le opportune attività di controllo di *compliance* regolamentare, interna ed esterna, del modello[1].

Come già definito, il presente documento ha ad oggetto il macroprocesso ***identificazione***, il quale rappresenta il punto di partenza di un sistema di gestione dei rischi operativi: la qualità delle informazioni raccolte determina la qualità complessiva di tutti gli output di sistema, quantitativi e qualitativi.

Il macroprocesso "identificazione" è principalmente composto di 4 fasi, che ora andremo ad esporre:

- ✓ **Loss Data Collection** (di seguito LDC), per la ricerca, raccolta e analisi descrittiva dei dati quantitativi interni ed esterni riferiti alle perdite operative;

[1] Fino al 2013 l'attività è stata svolta in regime di self-validation, successivamente è stata istituita un'apposita funzione di Validazione dedicata a tale compito; da "Regolamento 1" l'attività è attualmente in carico al *Servizio Validazione Sistemi di Rischio*, definito presso l'Area Validazione, Monitoraggio e Informativa Istituzionale.

- ✓ **Indicatori**: ai fini della identificazione del rischio operativo rileva la produzione di indici basati su driver aziendali, trasversali alla banca e di natura eterogenea (es. la numerosità dei reclami ricevuti, il turn over del personale). Le evidenze risultanti dagli indicatori vengono utilizzate come dati di input per il processo di Monitoraggio Gestionale e possono essere impiegate per quello di Analisi di Scenario;

- ✓ **Assessment** dei fattori di rischio e di controllo, rivolto al Middle Management per l'autovalutazione della qualità dei presidi (in altri termini, qualità della gestione dei fattori di rischio) posti in essere per la gestione ed il controllo dei singoli eventi di rischio connessi ai processi aziendali;

- ✓ **Analisi di Scenario**, per l'identificazione da parte del Top Management delle principali aree di criticità aziendale con l'obiettivo sia di quantificare il capitale a rischio sulla base delle stime soggettive (cd. Expert Opinion), sia di individuare le opportune azioni di mitigazione/trasferimento/ritenzione dei rischi.

4.2 Overview sul processo di identificazione

L'identificazione dei rischi richiede un'attività di indagine e d'analisi estesa a tutte le principali attività di business e infrastrutturali.

L'informazione più rilevante ai fini della determinazione del valore a rischio, nel sistema adottato dal Gruppo MPS, è costituita dai dati storici di perdita interni ed esterni.

La raccolta dei dati storici interni ed esterni, ovverosia la componente quantitativa, si realizza attraverso il processo di **Loss Data Collection**.

Con riferimento alla raccolta dei dati esterni, il gruppo MPS ha scelto di aderire al consorzio italiano per raccolta delle perdite operative (DIPO).

La scelta di introdurre due fonti di raccolta si basa sulla necessità di raccogliere informazioni relative sia alla gestione interna sia all'andamento generale del sistema esterno di riferimento.

La serie storica dei dati di perdita interni ed esterni, tuttavia, può essere insufficiente a descrivere completamente il profilo di rischio come ad esempio nei seguenti casi:

- *Nuove aree di business/prodotti*: in questo caso non si hanno a disposizione dati di perdita per valutare la relativa rischiosità operativa.
- *Evoluzioni del contesto operativo e del sistema dei controlli*: l'attualità dei dati storici non è scontata a fronte di evoluzioni della realtà operativa aziendale (le perdite storiche sono definite *backward-looking*).

Esistono quindi dei limiti insiti nelle informazioni storiche, che richiedono l'introduzione di informazioni di natura qualitativa per una migliore definizione del profilo di rischio.

L'analisi qualitativa ha l'obiettivo di raccogliere valutazioni soggettive sull'evoluzione dei rischi aziendali (*forward-looking*), richiede giudizi espressi da risorse esperte (*qualificati responsabili di unità di business*) ed è composta da due momenti di analisi, il cui livello di dettaglio è relativo all'interlocutore al quale si rivolgono:

- **Assessment dei Fattori di Contesto e di Controllo**: rappresenta il primo momento dell'analisi ed è rivolto al Middle Management, al quale ci si rivolge per la raccolta di informazioni *qualitative* sul livello di presidio posto nelle attività in relazione ai rischi. Rappresenta il momento di analisi di maggior dettaglio.
- **Analisi di Scenario**: è il secondo momento dell'analisi ed è rivolto al Top Management, presso il quale si effettua la raccolta di *stime soggettive* sugli impatti economici derivanti dal manifestarsi degli eventi di rischio operativo, nonché le relative indicazioni gestionali e di mitigazione. Questo passo rappresenta il momento di analisi di più alto livello.

Al fine di individuare i destinatari di Assessment e Scenario in ciascuna azienda del Gruppo per l'esecuzione delle relative analisi vengono valutati i seguenti aspetti:

- **complessità organizzativa** (numero di Unità Organizzative esistenti, loro interconnessione e numero di linee gerarchiche, numero di dipendenti, ecc.):
  - ✓ ad una maggiore complessità dell'entità organizzativa si associa una maggiore diffusione delle informazioni rilevanti e quindi la necessità di coinvolgere un numero maggiore di interlocutori;
  - ✓ ad una minore complessità organizzativa consegue una maggiore concentrazione delle informazioni rilevanti e quindi la possibilità di coinvolgere un numero minore di interlocutori.

- **coinvolgimento di tutto il management di riferimento** (al livello più adeguato)
  - ✓ per la definizione di un'ottimale metodologia di Scenario ad ogni ciclo di analisi, nella considerazione che il questionario varia in relazione alle criticità e ai rischi identificati e devono essere coinvolti i Top Manager di pertinenza e in grado di fornire un view completa
  - ✓ per responsabilizzare le linee operative nella gestione dei rischi operativi e creare una cultura del rischio tesa a creare valore per l'azienda.

.

In tale contesto sono stati individuati i *tipici* destinatari di Assessment e Scenario delle aziende del Gruppo in particolare:

- ✓ *Assessment*: Responsabili di Uffici/Servizi della Capogruppo o unità organizzative poste sotto la Direzione Generale per le controllate;
- ✓ *Scenario*: Responsabili di Direzione (o delle Aree che riportano direttamente al DG) per la Capogruppo e Direttori Generali delle controllate.

I due processi, all'interno del più ampio *Operational Risk Framework*, sono finalizzati da un lato alla stima del capitale a rischio (basato anche su stime soggettive) e dall'altro alla raccolta delle informazioni gestionali, che sono di supporto alla definizione di un adeguato "Piano di Mitigazione Rischi Operativi".

Come verrà evidenziato nel seguito del documento, l'approccio adottato prevede che gli input informativi siano raggruppati sulla base di "modelli di classificazione", per utilizzare in maniera omogenea tutte le principali fonti informative, sia interne (qualitative e quantitative) che esterne (dati di provenienza esterna).

5. LA LOSS DATA COLLECTION

5.1 Premessa

Il modello di raccolta dei dati storici si basa su due principali fonti informative: una fonte interna, che consente di raccogliere informazioni sulla gestione pregressa delle attività del Gruppo, ed una fonte esterna (DIPO), che consente di raccogliere le informazioni di sistema.

A seguire vengono descritti brevemente gli aspetti di processo, presentando:

- ✓ le fonti informative che alimentano il modello;

- ✓ le modalità di censimento ed il set di dati a corredo delle perdite;
- ✓ le modalità di trattamento dei fattori di rischio.

5.2 Attività svolte in sede di LDC

5.2.1 Processo e aspetti organizzativi

Il processo di LDC è articolato nei seguenti sottoprocessi:

- **Ricerca:** consiste nelle attività di ricerca delle perdite operative e di individuazione delle fonti informative dalle quali attingere i dati di perdita, oltre che di definizione e formalizzazione delle modalità di censimento;
- **Censimento:** per l'acquisizione dei dati di perdita individuati, effettuandone la registrazione nel *database* dedicato alle attività di LDC secondo le modalità di censimento definite;
- **Partecipazioni a consorzi esterni:** attività di ricezione/trasferimento dei dati da/a consorzi esterni per iniziative di data pooling e benchmarking;
- **Reporting:** sintesi dei principali accadimenti e dei trend di perdite/accadimenti.

A seguire verrà fornita una descrizione di dettaglio.

5.2.2 Ricerca degli eventi operativi

Le perdite operative hanno un "ciclo di vita" che inizia con la **manifestazione dell'evento** e termina con la **contabilizzazione degli effetti** di perdita. In questo contesto la ricerca degli eventi di rischio con l'individuazione delle perdite ad essi collegate si concentra in via generale su due elementi:

- individuazione delle "fonti informative", ovvero delle strutture all'interno dell'organizzazione presso le quali è possibile rintracciare le informazioni relative al **manifestarsi** di eventi operativi e dei loro effetti di perdita; tali strutture gestiscono o hanno conoscenza degli eventi operativi e del loro ciclo di vita e possono essere dotate di archivi "stand-alone" (che vanno dal cartaceo agli applicativi office o sviluppati ad hoc) oppure di sistemi "legacy" (ovvero applicativi di supporto alle principali attività della Società, collegati generalmente ad altri sistemi/punti della

Banca per condividere le informazioni, potendo avere o meno anche un collegamento diretto con la contabilità), nei quali registrano gli eventi in esame, per gestirli secondo le specifiche della struttura;

- verifica presso contabilità generale delle **contabilizzazioni** degli effetti di perdita, ad esempio con l'esame delle componenti negative di bilancio dove si possono trovare le scritture di perdita a fronte di rischi operativi (voci di Conto Economico e Fondo Rischi), in raccordo con le informazioni disponibili presso la fonte informativa (che potrebbe già disporre di un collegamento con la contabilità se ad es. utilizza sistemi "legacy") oppure con la necessità di dover associare l'evento fornito dalla fonte ai suoi effetti a bilancio, se la fonte informativa non alimenta direttamente la contabilità.

Una struttura è ritenuta "adeguata" ad essere una fonte informativa in una logica di "buona gestione" (e quindi allo scopo di fornire all'operational risk "adeguate" informazioni relative agli eventi di rischio e agli effetti di perdita), se rispetta alcuni requisiti minimi:

- *tempestività*: vicinanza temporale della fonte all'evento di perdita;
- *completezza*: quantità/qualità dell'informazione contenuta;
- *accessibilità*: possibilità di attingere, a basso costo, ai dati che è in grado di fornire, al fine di reperire efficientemente tutte le informazioni di interesse minimizzando l'impatto in termini di reingegnerizzazione e di cambiamenti di organizzazione/prassi operative.

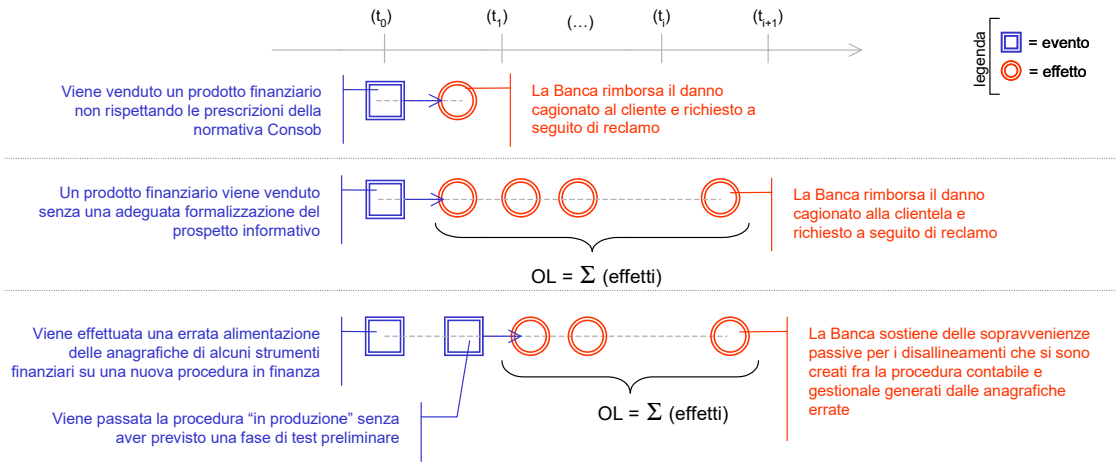
Per ogni fonte individuata, il gestore Operational Risk presente a livello di ciascuna entità giuridica formalizza le modalità di estrazione e invio delle informazioni e la relativa periodicità, fornendo istruzioni operative ai proprietari delle fonti stesse. La raccolta di tutte le Fonti Informative e delle modalità ad oggi individuate di LDC per la singola Fonte sono presenti nel "**Manuale delle Fonti Informative**", cui si rinvia per i dettagli.

5.2.3 Censimento degli eventi operativi

Eventi e loro rappresentazione

Un **evento** di rischio operativo è costituito da uno o più accadimenti (**effetti**) che danno luogo, ciascuno, ad una o più perdite (operational loss).

Le relazioni che intercorrono tra l'accadimento pregiudizievole e le manifestazioni economiche negative ad esso connesse, sono descritte da una "catena evento-effetto" che può essere di tipo **semplice** (con un solo accadimento pregiudizievole) o **complessa** (con più accadimenti pregiudizievoli connessi tra loro), come esposto nella figura seguente:



Nei primi due esempi l'accadimento è semplice (un solo evento di rischio operativo), nel terzo caso l'accadimento pregiudizievole è complesso (due eventi di rischio operativo, concatenati tra loro, che concorrono alla manifestazione delle perdite), con una "catena evento-effetto" che presenta differenti "profondità" in relazione alla dimensione/durata temporale di manifestazione.

La **perdita operativa**, per definizione, rappresenta l'effetto economico negativo derivate da un evento operativo e che viene rilevato nella contabilità aziendale, con impatto sul conto economico. Si possono distinguere alcune situazioni per le quali le **perdite** si possono catalogare in differenti tipologie:

- **perdita istantanea**: gli effetti si esauriscono nel periodo di osservazione (ad esempio, la giornata operativa o come nel caso di una rapina);

- **perdita sequenziale (multiple-time loss)**: si tratta di perdite riferite ad uno stesso evento ma che si verificano/manifestano in momenti successivi, come ad esempio nel caso delle cause legali (con effetti perdita dati da: spese legali, spese per perizie, accantonamenti e loro variazioni, esborsi, ecc.) che generano impatti in un periodo di tempo spesso lungo.

- **perdite multi-effetto (multiple-effect losses)**: si tratta di un insieme di perdite riferibili allo stesso evento che colpiscono però differenti segmenti di operatività; si pensi al caso di una catastrofe naturale oppure ad un guasto IT che causa l'interruzione di diverse attività.

- **perdite operative di confine**: con i rischi di credito (**credit risk boundary losses**) e con i rischi di mercato (**market risk boundary losses**), definite rispettivamente come perdite su crediti e perdite di mercato derivanti da eventi di rischio operativo (si vedano anche i dettagli nel paragrafo dedicato)

- **rapidly recovered loss events**: sono le "perdite prontamente recuperate", che vengono completamente o parzialmente recuperate entro 5 giorni dalla data di accadimento dell'evento

- **near miss**: ovvero le "quasi perdite", eventi di rischio operativo che non determinano una perdita

In merito al censimento delle tipologie di perdita elencate, la metodologia di Loss Data Collection implementata dal Gruppo MPS (in conformità a quanto previsto dalla normativa di Vigilanza Prudenziale) prevede quanto segue:

- l'importo della perdita viene censito al lordo dei recuperi da polizze assicurative o da altri meccanismi di trasferimento del rischio; il caso include perdite istantanee, sequenziali e multi effetto

- le perdite operative di confine con i rischi di mercato (market risk boundary losses) sono incluse nel DB Operational Risk;

- le perdite operative al confine con i rischi di credito (credit risk boundary losses) riferite ad eventi di frode sono incluse nel DB Operational Risk;

- le "perdite prontamente recuperate" (rapidly recovered loss events) e le "quasi perdite" non entrano nel DB dei rischi operativi.

Il set di informazioni associato ad ogni evento è costituito dagli elementi che consentono di identificarne i **tempi** e i **modi** della **manifestazione** con i relativi **impatti**. Tali elementi sono tipicamente i seguenti:

A. date di riferimento (accadimento, rilevazione, contabilizzazione)

B. collocazione dell'evento rispetto all'attività della banca (identificazione della *Business Line*)

C. identificazione della tipologia di accadimento (identificazione dell'*Event Type)*

D. importi di perdita e recupero (quest'ultimo ove presente)

E. descrizione dell'accaduto ed aspetti contabili (date e conti di contabilizzazione)

A. Date di Riferimento

Ogni evento di perdita operativa può essere caratterizzato da una serie di date di riferimento che ne contraddistinguono l'evoluzione, dall'istante in cui si manifesta fino alla definitiva contabilizzazione della perdita connessa. Si possono individuare degli attributi temporali legati all'evento o alla perdita operativa.

Nell'ambito dell'Evento distinguiamo tra:

- ✓ *Data di inizio accadimento:* è definita come data in cui si verifica l'evento pregiudizievole
- ✓ *Data di fine accadimento*: viene utilizzata per gli eventi che si verificano in un determinato arco temporale, non "puntualmente" (diversamente la data di inizio e fine accadimento coincidono)
- ✓ *Data di rilevazione:* data in cui si è venuti a conoscenza dell'evento pregiudizievole

Per alcune categorie di evento le tre date tendono a coincidere; si pensi al caso di eventi criminosi quali rapine, scassi bancomat o danni ai beni per i quali necessariamente la banca viene a conoscenza dell'evento nella stessa data in cui accade. Nella maggioranza dei casi trascorre un certo tempo dal momento in cui un evento accade a quello in cui viene rilevato ed inizia a manifestare i suoi effetti contabili.

Si riportano alcuni esempi a titolo esemplificativo per ciascuna classe di rischio:

1 - Frodi Interne

"Un dipendente si è appropriato di somme di pertinenza della clientela depositate su conti correnti"

- La **data di inizio accadimento** corrisponde alla prima data in cui sono state effettuate le operazioni irregolari;
- La **data di fine accadimento** corrisponde alla data in cui è stata effettuato l'ultimo prelievo dai conti della clientela;

- La **data di rilevazione** è la data in cui si è venuti a conoscenza dell'evento e, nello specifico caso, può corrispondere alla data di inizio del servizio ispettivo che lo ha portato alla luce, oppure alla data di notifica di una citazione o di arrivo di un reclamo da parte della clientela danneggiata dalla frode.

2 - Frodi Esterne

"Dal 2003 al 2005 sono stati deliberati numerosi mutui a fronte della presentazione di documentazione artefatta relativa alle garanzie, alle condizioni reddituali e alle perizie."

- La **data di inizio accadimento** corrisponde alla data di erogazione del primo mutuo (anno 2003);

- La **data di fine accadimento** corrisponde alla data in cui è stata concesso l'ultimo mutuo (2005);

- La **data di rilevazione** è la data in cui si è venuti a conoscenza dell'evento e, nello specifico caso, può corrispondere alla data di inizio del servizio ispettivo che lo ha portato alla luce, oppure alla data di notifica di una citazione o di arrivo di un reclamo da parte della clientela danneggiata dalla frode.

"Il 16.10.08 è stata commessa una rapina nella filiale xxx".

- La **data di inizio accadimento** corrisponde alla data della rapina;

- La **data di fine accadimento** è uguale alla data di inizio accadimento trattandosi in questo caso di un evento puntuale;

- La **data di rilevazione** corrisponde alla data della rapina.

Rientrano in questa classe ad es. gli scassi bancomat o alle cassette di sicurezza, per le quali le 3 date tendono a coincidere.

3 - Rapporti di Impiego

"Il dipendente chiede un risarcimento per presunto ingiusto licenziamento irrogatogli in data 27.05.2004"

- La **data di inizio accadimento** corrisponde alla data di licenziamento;
- La **data di fine accadimento** è uguale alla data di inizio accadimento trattandosi in questo caso di un evento puntuale;
- La **data di rilevazione** corrisponde alla data della citazione alla banca per ingiusto licenziamento.

"Il dipendente lamenta di essere stato vittima di mobbing a far data dal 01.01.2003 fino al 01.01.2009 data in cui si è dimesso e richiede il risarcimento danni"

- La **data di inizio accadimento** corrisponde alla data di inizio del fenomeno di discriminazione (01.01.2003);
- La **data di fine accadimento** è pari al 01.01.2009, fine del fenomeno di discriminazione;
- La **data di rilevazione** è pari alla data di notifica della citazione alla banca.

4 - Clienti Prodotti e prassi operativa

"Il cliente espone reclamo alla banca lamentando la non adeguata informativa nell'ambito del collocamento di un piano finanziario"

- La **data di inizio accadimento** corrisponde alla data di vendita del piano finanziario;
- La **data di fine accadimento** è uguale alla data di inizio accadimento trattandosi in questo caso di un evento puntuale;
- La **data di rilevazione** corrisponde alla data in cui la banca ha ricevuto il reclamo venendo così a conoscenza dell'evento.

"Il cliente cita la banca per l'applicazione sul conto corrente di interessi anatocistici a far data dal 01.01.2005 al 31.12.2007"

- La **data di inizio accadimento** corrisponde alla data di inizio applicazione degli interessi (01.01.2005);
- La **data di fine accadimento** è pari al 31.12.2007;
- La **data di rilevazione** corrisponde alla data in cui la banca ha ricevuto la citazione venendo così a conoscenza dell'evento.

5 - Danni a Beni Immobili

Questa classe di rischio contiene per lo più eventi di tipo puntuale; si pensi al caso di disastri naturali, atti vandalici, terremoti. Come nel caso delle rapine, le tre date (inizio e fine accadimento, rilevazione) tendono a coincidere con la stessa giornata.

6 - Disfunzioni ai Sistemi

"Dal 1 gennaio 2007 per circa 6 mesi il sistema di calcolo delle commissioni da applicare ai conti correnti della clientela ha causato addebiti non dovuti. La banca è venuta a conoscenza del fatto successivamente ad un reclamo di un cliente"

- La **data di inizio accadimento** corrisponde alla data di inizio applicazione delle commissioni (01.01.2007);
- La **data di fine accadimento** è pari al 01.07.2007;
- La **data di rilevazione** corrisponde alla data in cui la banca ha ricevuto il primo reclamo.

7 - Esecuzione consegna e gestione del processo

"*Il dipendente di una filiale ha eseguito in data 15/02/2010 un bonifico per conto di un cliente duplicando l'importo per errore. La banca non riesce a recuperare l'importo ed è costretta ad incamerare la perdita"*

- La **data di inizio accadimento** corrisponde alla data di esecuzione del bonifico;
- La **data di fine accadimento** è uguale alla data di inizio trattandosi di un evento puntuale;
- La **data di rilevazione** corrisponde alla data in cui la banca si è accorta dell'evento o eventualmente la data dell'eventuale reclamo del cliente.

B - collocazione dell'evento - Business Line

Nell'attività di censimento, l'associazione dell'evento di perdita alla BL deve riflettere oggettivamente il contesto interno (business e/o organizzazione) ed esterno (variabili ambientali). A tal fine, tutte le attività devono essere classificate nelle "linee di business" in modo esclusivo ed esaustivo. Nella raccolta delle perdite si può riscontrare il caso di un accadimento imputabile a due o più BL. In questi casi si utilizza per passi il criterio della "prevalenza": le perdite non sono suddivise pro quota fra le diverse BL, ma sono attribuite ad una sola di esse per l'intero valore. Le BL utilizzate per la Loss Data Collection sono le 9 Business Line definite a livello regolamentare (si rinvia al paragrafo dedicato alle BL per i dettagli):

1. Corporate Finance
2. Trading and Sales
3. Retail Banking
4. Commercial Banking
5. Payment and Settlement
6. Agency Services
7. Asset Management
8. Retail Brokerage
9. Corporate Items (*solo banche AMA*)

C - identificazione della tipologia di accadimento – Event Type

Gli eventi sono invece classificati nelle 7 seguenti classi di rischio regolamentari:

1. Frode Interna
2. Frode Esterna
3. Rapporto di Impiego e Sicurezza sul lavoro
4. Clientela, Prodotti e Prassi operativa
5. Danni a beni materiali
6. Interruzioni dell'operatività e disfunzioni dei sistemi informatici
7. Esecuzione, consegna e gestione del processo

Sulla base della tassonomia di riferimento regolamentare, è stato introdotto il modello interno di classificazione detto "Modello Integrato dei Rischi" (MIR). Il MIR definisce il modello degli eventi di rischio operativo adottato dal Gruppo MPS: tale modello è definito ai primi due livelli di classificazione sulla base delle indicazioni regolamentari. I livelli di ulteriore dettaglio sono invece costituiti da un insieme di casistiche interne e ricorrenti per supportare il personale operativo nella classificazione delle informazioni quali-quantitative. Si rinvia al paragrafo dedicato all'ET per i dettagli.

Per gli effetti economici dell'evento (perdita, accantonamento e recupero) individuiamo come attributo temporale la ***Data di contabilizzazione***, che rappresenta la data in cui gli effetti di perdita sono contabilizzati.

A. importi di perdita e recupero (quest'ultimo ove presente)
B. descrizione dell'accaduto ed aspetti contabili (date e conti di contabilizzazione)

D - Importi di perdita e recupero

In relazione all'**importo,** si possono distinguere 3 elementi:

- ✓ ammontare di importo al lordo degli effetti di perdita;
- ✓ ammontare dei recuperi assicurativi;
- ✓ ammontare di altro generi di recuperi (es. recuperi infragruppo).

L'evento deve essere corredato sempre dall'importo di perdita e deve contemplare gli eventuali recuperi, suddivisi per tipologia (assicurativo, non assicurativo)

E - descrizione dell'accaduto ed aspetti contabili

Sinteticamente per tali entità si può indicare quanto segue:

- ✓ **descrizione**: comprendere la natura del danno subito è fondamentale per classificare la perdita; una buona descrizione (accurata e dettagliata) è indice di un elevato livello di comprensione dell'evento.
- ✓ **aspetti contabili - voce contabile**: l'indicazione della destinazione contabile (voce contabile, numero di conto, ecc) consente di indirizzare l'attività di quadratura funzionale all'esigenza di accertare il completo censimento degli eventi.

5.2.4 Le perdite operative di confine

La circolare Banca d'Italia n°263 del 27 dicembre 2006 individuava le "perdite operative di confine con i rischi di credito" (credit risk boundary losses) e le "perdite operative di confine con i rischi di mercato" (market risk boundary losses) "*rispettivamente nelle perdite su crediti e di mercato derivanti da eventi di rischio operativo. Ad esempio, per il primo tipo, le perdite derivanti da errori o frodi nel processo di concessione e gestione del credito, per il secondo, le perdite conseguenti a errori di inserimento dei prezzi o delle quantità nelle procedure di negoziazione dei titoli o a violazioni dei limiti operativi*".

Il Regolamento UE 575 del 26 giugno 2013 prevede in particolare che:

- le perdite operative di confine con i rischi di mercato siano incluse nella raccolta dei dati di perdita concorrendo quindi alla determinazione del requisito patrimoniale a fronte dei rischi operativi;

- le perdite operative di confine con i rischi di credito siano registrate nella banca dati sul rischio operativo e rilevino separatamente. Tali perdite non sono soggette al calcolo del requisito a fronte dei rischi operativi a condizione che siano trattate ai fini del calcolo dei requisiti in materia di rischio di credito.

Perdite di Confine con i Rischi di Mercato nel Gruppo MPS

I rischi di mercato rappresentano una tipologia di rischio direttamente collegata all'operatività sui mercati finanziari. A tale categoria di rischio, infatti, si riconducono le variazioni del valore di mercato delle posizioni, che derivano da mutamenti avversi ed inattesi dei tassi di interesse, dei cambi e dei prezzi dei corsi azionari, delle merci, dei parametri complessi relativi a questi fattori di rischio (volatilità implicita, correlazione, ecc.), così come a fattori di rischio specifici riconducibili alla situazione dell'emittente. In questo contesto le perdite operative di confine con i rischi di mercato (***market risk boundary loss***) sono definite come le "*perdite di mercato derivanti da eventi di rischio operativo*", quali ad esempio quelle conseguenti ad errori nell'inserimento dei prezzi, delle quantità, alla violazione dei limiti operativi, etc.

Nella maggior parte dei casi gli eventi operativi sono legati alle operazioni di regolamento, con errori commessi dagli operatori nell'inserimento dei prezzi o delle quantità. Tale casistica rientra nell'ambito dell' Event Type 7 "Esecuzione, consegna e gestione dei processi", con impatti generalmente di piccolo rilievo, seppure possano evidenziarsi anche perdite significative per rari o specifici errori. Un'altra tipologia di eventi operativi che impattano sui rischi di mercato è quella relativa alle "Frodi interne" da parte dei trader della banca. Gli eventi in questo caso vengono catalogati nell'Event Type 1, sono a frequenza molto bassa ma potenzialmente collegati anche a perdite significative.

Quando un trader (o un'altra unità organizzativa cui competono i controlli) individua un errore nell'esecuzione di un ordine, tipicamente ciò che avviene è che lo stesso trader provvede a correggere l'operazione errata, bilanciandola nei limiti concessi alla sua autonomia. A causa delle variazioni registrate sui mercati nel lasso di tempo, seppur breve, intercorso tra le due operazioni, può accadere tuttavia che l'errore operativo possa in ogni caso determinare un eventuale utile/perdita pari alla differenza tra le due operazioni.

In situazioni di questo genere, si prevede che:

- ✓ gli eventuali guadagni determinati da eventi di rischio operativo profittevoli (qual è il caso della correzione di un ordine che determina un saldo positivo) non siano inclusi nel data set per il calcolo del requisito patrimoniale;
- ✓ in caso di perdite "prontamente recuperate" (ovvero con "perdita recuperata entro cinque giorni dalla data di accadimento") con recupero parziale, sia incluso nel data set di calcolo l'importo della perdita al netto del recupero; nel caso in esame, quindi, l'importo da rilevare e da censire è l'eventuale saldo negativo tra l'ordine errato e l'operazione correttiva.

Ciò che si richiede quindi ad un sistema avanzato di gestione dei rischi operativi è la capacità di identificare gli eventuali saldi negativi risultanti dalla correzione di errori nell'esecuzione degli ordini. In tale contesto, il Gruppo MPS ha definito un processo strutturato all'interno della Loss Data Collection per individuare e censire le perdite di confine sul mercato, operando una distinzione che caratterizza l'operatività di trading sui mercati finanziari collegata a errori nell'operatività in conto proprio (che genera market boundary loss), ad errori nell'operatività in conto terzi (che genera operational loss pure) oppure a frodi interne.

Si rinvia al Manuale delle Fonti per un eventuale dettaglio dedicato alle perdite di confine (paragrafo *market risk boundary loss*).

Perdite di Confine con i Rischi di Credito nel Gruppo MPS

Le perdite operative di confine con i rischi di credito sono definite come le perdite su crediti derivanti da eventi di rischio operativo. Le perdite di confine sono pertanto strettamente connesse ai processi di recupero del credito ed in generale sono determinate da fattori di rischio operativo come, per esempio, l'incompletezza dalla documentazione, i finanziamenti ottenuti in maniera fraudolenta, il mancato seguimento delle garanzie, ecc.

Relativamente alla modalità di trattamento di queste perdite il Regolamento UE 575 cita: "Tali perdite (perdite da rischio operativo collegate al rischio di credito, N.d.R.) non sono soggette all'applicazione del requisito previsto per il rischio operativo a condizione che l'ente sia tenuto a continuare a trattarle come rischio di credito ai fini del calcolo dei requisiti in materia di fondi propri.".

Il Gruppo MPS ha definito in modo strutturato un processo interno di gestione delle perdite **credit boundary** che valuta, nelle situazioni in cui si è in presenza di una riduzione della capacità di recupero

del credito originata da eventi operativi, la rilevanza della componente di "rischio operativo" su quella di "credito", per definire la catalogazione dell'evento in ambito operational risk.

In sintesi le 2 situazioni che possono presentarsi sono le seguenti:

a. frodi interne ed esterne sul credito

1. finanziamenti ottenuti in maniera fraudolenta per i quali le irregolarità si manifestano nella fase della prima erogazione (garanzie falsificate, documentazione reddituale artefatta, frode da sedicente, ecc);
2. operazioni di credito costituite in maniera regolare, ma che divengono critiche successivamente alla prima erogazione per un'intervenuta attività fraudolenta; si pensi al caso di un'azienda in procinto di fallire che presenta documentazione falsa alla banca per continuare ad avere credito;
3. erogazione di credito con comportamenti interni posti in essere in palese violazione della normativa interna o con evidente dolo da parte del dipendente, anche (ma non solo) finalizzati all'ottenimento di un vantaggio economico o personale.

Tali perdite vengono individuate utilizzando le segnalazioni della funzione Audit e l'ammontare di perdita classificato a contenzioso nei database di rischio di credito viene utilizzato come importo di perdita per l'evento di rischio operativo.

A partire dal 30 giugno 2017, questi eventi vengono censiti e catalogati all'interno del DB dei rischi operativi ai soli fini gestionali per effettuare analisi su fenomeni e trend.

Infatti, queste perdite di confine con il credito, essendo già trattate ai fini del calcolo del requisito a fronte del rischio di Credito, non vengono utilizzate per finalità di calcolo regolamentare per i rischi operativi, ma vengono collezionate solo a scopo gestionale ed analitico.

b. errori che riducono la capacità di recupero sul credito (credit boundary)

In questo caso si è in presenza di una riduzione della capacità di recupero del credito (o di una totale impossibilità di recuperarlo) originata da eventi operativi di errore o negligenza nella gestione dei processi e delle operazioni, come ad esempio a causa di carenze documentali (inesistenza, incompletezza, non corretta formalizzazione della documentazione, ecc.), nella gestione dei processi (ritardi nel trattamento delle pratiche a contenzioso, delle garanzie, ecc.).

Tali eventi vengono censiti e catalogati all'interno del DB dei rischi operativi, in una partizione dedicata. Anche in questo caso tali eventi che non vengono utilizzati per il calcolo del requisito patrimoniale, nel caso in cui siano trattati ai fini del rischio di credito.

Il Gruppo MPS analizza tali perdite nell'ambito delle analisi di Scenario e al fine di individuare eventuali azioni di mitigazione, prevenzione e attenuazione del profilo di rischio operativo.

Si rinvia al Manuale delle Fonti per un eventuale dettaglio dedicato alle perdite di confine (paragrafo *credit risk boundary loss*).

5.2.5 Le perdite di natura commerciale

Le perdite sostenute per ragioni di ordine commerciale sono rappresentate da rimborsi o riliquidazioni effettuate ai clienti non legati ad effettive inadempienze, ma sostenuti in ogni caso per mantenere/rafforzare la relazione con la clientela.

Si pensi ad esempio al caso in cui il cliente, per uno specifico prodotto, lamenti l'applicazione di commissioni maggiori rispetto a quelle offerte dai competitor della banca. In questo caso si può decidere di modificare le condizioni applicate al cliente rimborsando la differenza tra quanto inizialmente pattuito e quanto applicato sulla base delle nuove condizioni. Il rimborso effettuato al cliente non rappresenta perciò una perdita operativa, poiché il rimborso non è motivato da un'inadempienza della banca, ma semplicemente dall'esigenza di rafforzare il rapporto commerciale con il cliente.

La metodologia del Gruppo MPS non prevede la raccolta di questi eventi, che in genere si configurano come **storni di ricavi** o **rettifiche di minori costi contabilizzati nell'esercizio in corso o in quelli precedenti**, definiti anche tecnicamente **sconti o abbuoni** (per i ricavi) o **ricalcoli di competenze** (ad esempio per conguagli di interessi passivi riferiti a liquidazioni di esercizi precedenti, ecc.).

Si riportano di seguito alcuni esempi di eventi di natura commerciale:

- ✓ *"Il cliente X propone alla Banca di trasferire alcuni importanti mutui, accesi presso altro istituto, a condizione di veder migliorare le condizioni applicate dal competitor ai rapporti attualmente in essere. L'accoglimento della richiesta rappresenta un'ottima occasione commerciale, seppure rappresenti una deroga che comporterà un minore guadagno per la Banca"*

- ✓ *"Il cliente Z concorda con la sua filiale la modifica delle condizioni applicate ma non provvede a presentarsi in filiale per firmare la relativa modulistica, non facendo completare l'iter. Il cliente, in seguito, lamenta la mancata applicazione di quanto richiesto e la banca decide di rimborsarlo nonostante non ci sia stata nessuna omissione (è il cliente a non aver provveduto ad apporre la firma nella relativa documentazione, completando il percorso amministrativo)".*

Le casistiche ora descritte possono inoltre, in alcuni casi, comportare una contestazione informale o un reclamo, anche se di fatto non sono stati commessi errori da parte della banca. In generale, a fronte di un reclamo, si possono distinguere due situazioni:

- la banca accetta di rimborsare quanto richiesto dal cliente, riconoscendo in questo caso l'errore o l'inadempienza;

- la banca decide di rimborsare solo allo scopo di mantenere la relazione con il cliente, pur non essendoci un'effettiva inadempienza (rimborsi di natura commerciale).

Tutte le casistiche di reclamo formale sono censite all'interno della serie storica, nella volontà di considerare e tracciare nella LDC, anche a titolo prudenziale, ogni aspetto di contestazione cui sia stato dato seguito con un esborso.

Infine, le perdite sostenute per motivi di ordine commerciale si devono distinguere da quelle di natura "reputazionale". Si possono infatti verificare alcune situazioni in cui la banca decida di accettare l'assunzione di alcuni costi per porre un limite o fermare i possibili effetti negativi (in senso reputazionale) di specifici eventi, seppure tali accadimenti non siano legati a responsabilità da parte della banca (spesso si tratta di eventi di natura "sistemica"). I costi aggiuntivi vengono sostenuti quindi per evitare i possibili danni reputazionali derivanti e conseguenti all'evento, nel caso in cui questo perdurasse nel tempo, creando un'alea di incertezza e possibile danno alla reputazione aziendale.

Questi casi non vengono inclusi dal perimetro di raccolta nel caso in cui gli organi direttivi della banca forniscano documentazione (normativa interna, circolari, comunicazioni alla clientela) idonea a

identificarli e a chiarire le motivazioni delle scelte adottate, diversamente prudenzialmente vengono inclusi nelle perdite.

5.2.6 Gestione degli eventi multi-impatto: definizione di macro-evento

introduzione

Nella raccolta dei dati di perdita operativa si evidenziano, a volte, gruppi di eventi di rischio operativo che possono essere considerati "effetti" generati da una sola "causa comune", con caratteristiche molto simili alla natura di evento multi – effetto o sequenziale. Si pensi, ad esempio, ad una frode interna su conti dei clienti: avremo potenzialmente tante perdite associate ai rimborsi dovuti ai clienti danneggiati dalla frode ("causa comune") per ciascun reclamo, causa legale, transazione ("effetti") che la banca dovrà fronteggiare.
Saper cogliere il "comune denominatore" di più accadimenti pregiudizievoli dall'osservazione, a volte estemporanea, di singoli effetti registrati anche a grande distanza di tempo uno dall'altro, non è sempre semplice, e prevede un'indagine accurata e dedicata.

Nella volontà di dettagliare tale contesto ed illustrare come identificare, distinguere e registrare queste tipologie di eventi di rischio operativo (caratterizzati dall'essere tutti "collegabili" ad un unico evento "causa") procediamo definendoli in prima battuta come eventi "multi-impatto", per delinearne la natura.

analisi

Gli "eventi multi-impatto" si possono riscontrare in svariati ambiti dell'operatività bancaria e a titolo di maggiore esemplificazione, riportiamo a seguire alcuni esempi:

- ***Esempio 1:*** *Frode interna su alcuni conti dei clienti operata dal medesimo soggetto in momenti diversi.*
  - ✓ L'evento unico censito sarà composto da tanti effetti associati a tutte le perdite connesse a rimborsi alla clientela in seguito a reclami/citazioni/transazioni avvenute in relazione all'evento di frode.
- ***Esempio 2:*** *Errore nella procedura di calcolo degli interessi di alcuni clienti.*
  - ✓ Anche in questo caso la banca potrebbe ricevere reclami o citazioni da parte dei clienti che hanno subito un danno e pertanto gli impatti saranno costituiti dai rimborsi effettuati.

- ***Esempio 3:*** *Rapina/scasso bancomat.*
  - ✓ Gli effetti sono l'ammanco di contante per rapine oltre alle spese per la riparazione dell'immobile (danno al muro, ecc) o per la riparazione del bancomat.

Gli "eventi multi-impatto" così posti si possono allora suddividere in due "macro" categorie:

1. Eventi "singoli": eventi di rischio operativo che hanno caratteristiche multi - impatto perché sono eventi multi-effetto e/o sequenziali (es. singole cause legali, singole rapine, ecc) e i cui "effetti" sono costituiti dalle sole perdite collegate all'evento che è unico: si pensi ad esempio ad una causa legale (evento unico) le cui perdite (effetti) sono costitute dagli accantonamenti, dall'esborso per sentenza e dalle parcelle dei legali, oppure ad una rapina (evento unico) con perdite (effetti) costituite da contante rapinato e danni eventuali; tali eventi "racchiudono" in loro stessi tutto il corredo informativo del multi - impatto (sono di tipo multi - effetto e/o sequenziali) ma hanno effetti che non sono tra loro separabili concorrendo, necessariamente insieme, a formare la perdita (in una causa legale non possiamo separare ad es. le spese dall'accantonamento);
2. Eventi "composti": ad esempio un gruppo di cause e/o reclami associati allo stesso accadimento pregiudizievole iniziale al quale sono tutti collegati: gli "effetti" dell'accadimento pregiudizievole sono tutti eventi di rischio operativo e sono separabili perché presi singolarmente rappresentano un accadimento completo, e non sono singole perdite come nel caso precedente.

Mentre gli eventi "singoli" hanno la necessità di essere correttamente registrati (come multi effetto o sequenziali) al fine di non perdere parte degli effetti di perdita ad essi associati, gli eventi di tipo "composto" sono di interesse rilevante anche perché la loro corretta identificazione consente di delimitare fenomeni specifici, che hanno peraltro un impatto diffuso su più "centri" di perdita.

Su tale seconda tipologia di eventi, dobbiamo però operare un'ulteriore distinzione.

Si consideri ad esempio il default Lehman: tale accadimento ha comportato reclami e cause legali ma non rappresenta (il default) un evento di rischio operativo. Alcune di queste cause e reclami sono vinti dal cliente nel caso specifico in cui si evidenzi una situazione che comporta un evento di rischio operativo, come ad es. la mancata firma della documentazione di vendita, lo smarrimento della documentazione a corredo, l'errata profilatura del cliente, ma si parla sempre di eventi di soccombenza associati ad accadimenti di rischio operativo legati al singolo cliente/alla singola vendita: non tutte le vendite di obbligazioni Lehman infatti sono perdita operativa ma solo ed esclusivamente quelle in cui la

specifica vendita non è stata fatta in modo "corretto", comportando rischio operativo, e ciò è indipendente dalla fattispecie "default Lehman".

Possono quindi esistere accadimenti che non sono eventi di rischio operativo, cui seguono però eventi di rischio operativo, indicando come:

- *il rischio operativo sia insito nell'effetto e non nella causa;*
- *la "causa comune" rappresenti un "denominatore comune" non afferente al rischio operativo;*
- *gli effetti di tale accadimento sono perciò separati tra loro;*
- *in tali casi, se i processi della banca e i sistemi di controllo hanno funzionato correttamente, a fronte della causa "scatenante" non si registrano eventi di rischio operativo.*

In generale quindi un accadimento, se non è di rischio operativo, potrà portare a iniziative nei confronti della Banca, ma in questo caso facendo venir meno il concetto di multi-impatto.

conclusioni

Abbiamo allora individuato una migliore definizione di "multi-impatto", sulla quale concentriamo alcune specifiche riflessioni, considerando quanto segue:

1. **Eventi multi-impatto "singoli"**: eventi di rischio operativo, come ad esempio una rapina o una causa legale, che hanno caratteristiche multi-impatto poiché di tipo multi-effetto e/o sequenziali, ma i cui "effetti" sono le perdite collegate all'evento, non separabili tra loro e appartenenti allo stesso unico evento di rischio operativo.

   → *Tali eventi hanno la necessità di essere correttamente registrati in LDC al fine di non perdere gli effetti di perdita ad essi associati, ma sono parte della normale tipologia di eventi raccolti in LDC e non verranno ulteriormente approfonditi nel seguito; da ora ci riferiremo a tale tipologia di evento con il termine "multi-effetto" o "sequenziale" a seconda della loro natura.*

2. **Eventi multi - impatto "composti"**: ad esempio un gruppo di cause e/o reclami associati allo stesso accadimento pregiudizievole iniziale e al quale sono tutte collegate: gli "effetti" dell'accadimento pregiudizievole sono tutti eventi di rischio operativo e non semplici effetti (perdite) come nel caso precedente.

   → ***Se tali eventi hanno come causa comune <u>un evento di rischio operativo</u>**, allora vengono considerati "veri" eventi multi-impatto e sono oggetto di un'ulteriore analisi al fine di valutarne sia l'impatto*

*attuale/futuro che le misure di mitigazione da adottare; la registrazione di tali accadimenti vedrà i singoli eventi cumulati in un unico "**macroevento**":*

→ ***Se tali eventi hanno come causa comune <u>un evento non di rischio operativo</u>** sappiamo che la "causa comune" non rappresenta in realtà un elemento unificante e che gli effetti di tale accadimento sono perciò eventi separati tra loro. E' interesse della Banca dare una corretta registrazione in LDC degli "effetti" in esame ricordando che non rispondono alla tipologia di evento multi-impatto/macroevento, riconducendosi alla normale tipologia di eventi singoli raccolti.*

censimento del macroevento

A fronte dell'analisi esposta il Gruppo MPS ha definito dal 2010 di utilizzare il "**macroevento**" per la rappresentazione di specifici fenomeni che rientrano nella definizione data, ponendo a supporto della loro registrazione nel DB dei rischi operativi, una specifica funzionalità da utilizzare in sede di Loss Data Collection (funzionalità "macro-evento" in "OpRiskEv"). La loro presenza nel DB sarà quindi caratterizzata da tante registrazioni singole per ogni evento ("effetto") che verranno poi funzionalmente aggregate dallo strumento sotto un solo codice "macroevento" (che è la "causa comune"); questa funzionalità consente di non perdere la visione del singolo evento con le sue caratteristiche (perdite, accantonamenti, ecc) consentendo nel contempo l'aggregazione di tutti gli accadimenti collegati in un solo accadimento (il "macroevento") con caratteristiche mutuate dai suoi "effetti".

5.2.7 Adesione a consorzi esterni (DIPO)

Il Gruppo MPS aderisce al consorzio Data Base Italiano Perdite Operative (DIPO) per raccogliere informazioni sugli eventi di rischio di sistema, sia per esigenze di benchmarking che per il calcolo del Capitale a Rischio (per i dettagli metodologici su tale aspetto si rimanda al documento di misurazione).

Il Gruppo MPS partecipa al consorzio con la qualifica di aderente a livello di gruppo, ricevendo ed inviando dati al Consorzio secondo un processo strutturato che prevede strumenti, tempistiche e responsabilità definite dal DIPO. Il flusso Dipo viene inserito nel database utilizzato per il calcolo del requisito a giugno e a dicembre di ciascun anno. In particolare a maggio viene inserito il flusso DIPO relativo all'aggiornamento di dicembre dell'anno precedente, mentre a novembre viene utilizzato il flusso DIPO relativo all'aggiornamento di giugno dell'anno in corso. Per i dettagli sul processo si rinvia ai manuali DIPO.

Ai fini di analizzare le perdite interne sostenute dal gruppo in ottica di benchmarking, viene effettuata semestralmente una analisi di confronto tra i dati di perdita interni e quelli del sistema bancario italiano (DIPO). I dati sono gli stessi utilizzati ai fini del calcolo del requisito. Ogni aderente, compreso Montepaschi, invia al DIPO semestralmente i dati di perdita, ricevendone in ritorno i flussi di dati di tutto il consorzio in forma anonima. Gli aderenti sono divisi in gruppi, definiti Peer groups, sulla base dei costi operativi e del margine di intermediazione. Il Gruppo Montepaschi appartiene al Peer 1 insieme ad altre 8 principali banche italiane. Il confronto viene effettuato comparando l'andamento delle perdite operative di Montepaschi, rapportate al Total Asset del Gruppo, all'andamento delle perdite operative delle altre banche italiane appartenenti allo stesso Peer, anch'esse rapportate al Total Asset complessivo. Il confronto viene fatto per anno di rilevazione, sia a livello complessivo che per event type. I dati interni non contengono le perdite relative alle revocatorie fallimentari, poiché incluse nel calcolo del requisito del rischio di credito, pertanto i dati relativi ai peers vengono depurati di questa componente in modo da renderli confrontabili.

5.2.8 Reporting

E' definita una relazione periodica con la quale si riassumono tutti i principali aspetti emersi dal processo di Loss Data Collection: nuovi accadimenti rilevati, aggiornamento su eventi passati che spesano ancora nel periodo, evidenza sui fenomeni e sull'andamento delle perdite nel tempo, impatti a Conto Economico e Fondo Rischi derivanti dagli eventi, focus sugli accadimenti rilevanti e significativi.

Il reporting è mantenuto a disposizione del top management e delle strutture di controllo e di vigilanza.

6. INDICATORI

6.1 Premessa

I Key Risk Indicators (KRIs) vengono costruiti al fine di monitorare i principali cambiamenti del contesto operativo. Essi sono utili per identificare le attuali e potenziali fonti di rischio. Vengono costruiti a partire da indicatori gestionalmente utilizzati e monitorati, relativi alle diverse aree di business del Gruppo (comparti) e sono scelti come "alert" qualitativi di rischio operativo dopo una opportuna selezione a partire da un insieme più ampio. Tale selezione sarà oggetto di rivalutazioni periodiche.

I KRI presentano le caratteristiche di essere:

- facilmente misurabili: si tratta di informazioni già utilizzate dalle varie strutture aziendali;

- rilevanti: sono indicatori che presentano una data sensibilità alle fonti di rischio interne ed esterne;
- predittivi: sono relativi a cambiamenti in atto o che si sono già verificati, che possono potenzialmente esporre la banca a futuri rischi operativi.

6.2 Indicatori e loro utilizzo

Le aree di business (comparti) del Gruppo a cui appartengono gli indicatori sono:

- ✓ Compliance,
- ✓ Wealth Management,
- ✓ Liquidità,
- ✓ Mercato,
- ✓ Pianificazione,
- ✓ Risorse Umane,
- ✓ Credito,
- ✓ Legale.

A questi comparti, i cui indicatori sono calcolati su dati interni, è stato aggiunto un indicatore macroeconomico (Pil consuntivo, fonte Bloomberg), al fine di includere anche informazioni relative al contesto di riferimento.

All'interno di ogni comparto (ad esempio Compliance) sono stati individuati, con l'ausilio delle funzioni interessate, diversi indicatori (ad esempio numero di reclami evasi, tempi medi di evasione reclami, ecc.).

Compliance	Pianificazione	Risorse Umane
Numero clienti privati attivi non profilati completi Mifid su totale clienti privati attivi	Raccolta a vista conti corr pass	N.assunzioni/organico
Portafogli di clienti in consulenza avanzata con scostamento rispetto al modello su totale portafogli in consulenza avanzata	Raccolta a vista dep a risp	N.adesione fondo di solidarietà/organico
	Raccolta a breve termine-certif dep<18m	N.esodo incentivato/organico
	Raccolta a breve termine-gof raccolta	N.dimissioni/organico
Numero reclami evasi su numero reclami pervenuti	Raccolta a breve termine-pct	N.licenziam/organico
	Raccolta a breve estero	N.pensionamento/organico
Giorni medi di evasione reclami	Raccolta a m. lungo termine-certif dep>18m	Ore formazione/organico
	Raccolta a m. lungo termine-obbligaz senior	Tasso di assenza (gg assenza/gg lavorati nell'anno)
Numero operazioni in derivati OTC a clientela Retail su totale numero operazioni in derivati OTC	Raccolta a m. lungo termine-prestito subordinato	Nuove cause contenz passivo/organico
	Impieghi a vista	Spese del personale ind.per infl/organico
Numero di ndc con consenso privacy firmato su totale ndc con rapporti in essere	Impieghi a scadenza Italia	
	Impieghi a scadenza estero	**Credito**
Wealth Management	Impieghi a m. lungo termine -cred spec	Nuove sofferenze/ non sofferenze anno prec.(importi)
Volumi GP Azionarie	Impieghi a m. lungo termine -mutui	Nuove sofferenze/ non sofferenze anno prec.(teste)
Volumi GP Bilanciate	Impieghi a m. lungo termine -altri impieghi	Incagli/tot.crediti(teste)
Volumi GP Obbligazionarie	**Legale**	Incagli/tot. crediti (importi)
Volumi GP Total Return	Nuove cause per anatocismo/numero clienti	Sofferenze /tot crediti(importi)
Volumi GP Liquidità	Nuove cause per piani finanziari/numero clienti	Sofferenze/tot. crediti(teste)
	Nuove cause per credito/numero clienti	Nuovi flussi/tot.crediti anno precedente(importi)
Liquidità	Nuove cause per titoli in default/numero clienti	Nuovi flussi/tot.crediti anno precedente(teste)
Saldo liquidità operativa 1 mese	Nuove cause per altro/numero clienti	**Mercato**
Limite liquidità operativa 1 mese	**Macroeconomico**	VaR PNV
Ratio 1 liquidità strutturale	PIL	Volumi hedge fund

Per tutti gli indicatori all'interno di ogni comparto vengono costruiti tre indici:

1) *Indicatore di continuità*: misura se la variazione dell'indicatore nell'ultimo periodo temporale (indipendentemente dal segno) risulta significativa rispetto all'andamento storico delle variazioni (considerando la deviazione standard). Si assegna valore 1 all'indice se la variazione è significativa.
2) *Confronto con la media della serie storica*: se il valore assunto dall'indicatore gestionale dell'ultimo periodo considerato è maggiore/minore della media della serie storica a disposizione, l'indice assume valore 0/1 a seconda dell'impatto che l'indicatore ha sul profilo di rischio che si sta indagando. Se all'aumentare del valore dell'indicatore aumenta la rischiosità, quando tale valore risulta superiore alla media viene assegnato valore 1 e 0 in caso contrario. Nel caso invece che la rischiosità diminuisca all'aumentare del valore dell'indicatore viene assegnato valore 1 quando il valore è inferiore alla media e 0 nel caso opposto.
3) *Confronto con il periodo precedente*: attribuisce un "alert" sempre con la logica 0/1 a seconda del segno che l'indicatore gestionale assume rispetto al periodo temporale precedente. Anche in questo caso, se all'aumentare del valore dell'indicatore aumenta la rischiosità, quando tale valore risulta superiore a quello del periodo precedente verrà assegnato valore 1 e 0 in caso contrario. Nel caso invece la rischiosità diminuisca all'aumentare del valore dell'indicatore verrà assegnato valore 1 quando il valore è inferiore rispetto al periodo precedente e 0 nel caso opposto.

Per ogni indicatore viene quindi calcolata la media dei 3 indici, che rappresenta il singolo KRI.

Dalla media dei singoli KRI all'interno di ogni comparto si ottiene un unico valore (KRI di comparto) che può assumere valori compresi tra 0 ed 1 e che offre un giudizio di sintesi sull'esposizione del comparto al Rischio Operativo.

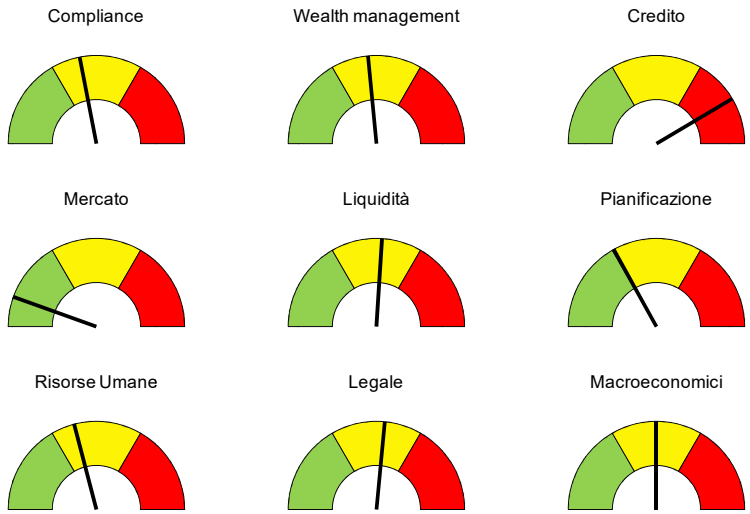


Figura 1. Cruscotto KRI Dicembre 2014

Tali indicatori sono utilizzati dalla Funzione Rischi Operativi anche per l'integrazione quali – quantitativa.

7. ASSESSMENT DEI FATTORI DI CONTESTO E DI CONTROLLO

7.1 Processo e aspetti organizzativi

L'Assessment dei fattori di contesto e di controllo (di seguito Assessment) è rivolto al *Middle Management* (responsabili di processo) ed è finalizzato all'autovalutazione sulla qualità dei presidi posti in essere per la gestione e il controllo dei singoli eventi di rischio tipici.

Il processo è articolato nei seguenti sotto-processi:

- ✓ **Predisposizione dei questionari,** in cui ogni azienda compone la catena "unità organizzative/processi/rischi" associando gli eventi di rischio operativo alle unità organizzative definite come responsabili di processo dal punto di vista dell'Operational Risk;

- ✓ **Esecuzione dei questionari**, che consiste nella compilazione del questionario e nello svolgimento del *data quality*;

- ✓ **Analisi Risultati e Reporting**, al fine di individuare ed evidenziare i risultati delle valutazioni raccolte sugli eventi di rischio associati alle unità organizzative, da trasmettere alle funzioni Locali e di Gruppo.

Di seguito vengono descritte le metodologie di "Predisposizione dei questionari", "Esecuzione dei questionari", "Analisi risultati e reporting".

7.2 Predisposizione dei questionari

Il questionario di Assessment (anche indicato come RSA – Risk Self Assessment) è costituito in sintesi dalla lista dei processi in carico ad una struttura, definiti a livello di regolamento interno, per i quali si richiede una valutazione di adeguatezza del presidio rispetto ai rischi tipici identificati per quel processo.

L'insieme degli eventi di rischio utilizzati per la costruzione dei questionari d'Assessment è costituito da un estratto del "catalogo unico dei rischi", una lista di rischi operativi tipici che raccoglie varie tipologie di accadimenti pregiudizievoli collegabili ai processi. La lista è condivisa periodicamente, ad ogni ciclo di RSA, con le strutture oggetto di Assessment, per il suo continuo aggiornamento in termini di rispondenza al contesto aziendale e al business. A livello normativo è inoltre prevista l'associazione processo – rischio alla stesura di un documento di processo, per descriverne in sede di normazione i rischi tipici.

All'atto dell'esecuzione del questionario di RSA, la prima attività valutativa dell'intervistato (responsabile di processo) consiste nella condivisione (in sede di prima applicazione) o manutenzione (per i successivi Assessment) dell'elenco dei rischi tipici assegnati alla propria UO: gli eventi di rischio sono aggiornati ad ogni Assessment al fine di garantire l'attualità degli stessi e di aumentarne la completezza.

Le strutture interessate in sede di RSA sono tipicamente le funzioni di gestione del business, per rilevanza sull'esecuzione di attività che sono potenzialmente caratterizzate da rischi operativi, e non quelle di supporto (quali ad es. gli staff, i settori dipartimentali, le strutture di controllo, ecc.) che ricoprono ruoli di indirizzo e di coordinamento. I processi valutati sono quelli indirizzati dalla normativa (Regolamento 1) e tra questi vengono indagati, in particolare, quelli più rilevanti in termini di business svolto dalla struttura. La rilevanza viene individuata dall'operational risk e dal business owner in sede di predisposizione del questionario, condividendo sia i processi che sono risultati più significativi dall'RSA precedente, sia quelli che, nel tempo, hanno variato la valutazione di presidio. I processi a maggior rilevanza sono, tipicamente, quelli del Credito, della Finanza e Canali Distributivi. Analogamente viene fatto per i rischi selezionati sul singolo processo, che sono quelli a maggiore valore aggiunto per la determinazione del livello di presidio su tematiche rilevanti e del perimetro di fattori di rischio da monitorare.

7.3 Esecuzione dei questionari

Con il processo di Risk Self Assessment i responsabili di processo (tipicamente a livello di Middle Management) sono chiamati a valutare l'adeguatezza dei presidi sui rischi operativi connessi alle proprie attività, indicando nel questionario se ritengano le procedure seguite (per chiarezza normativa, completezza dei processi, ecc.), le risorse affidate (per numerosità e profilo/skill, ecc.) ed i sistemi utilizzati (per qualità e affidabilità degli applicativi a supporto del business, ecc.), "adeguati" o meno a contrastare e minimizzare il rischio di subire perdite operative. Nel caso in cui il manager ritenga poi che le condizioni di presidio siano "non adeguate" o solo "parzialmente adeguate", l'attività di compilazione del questionario è finalizzata all'individuazione di opportuni interventi di miglioramento della gestione per contribuire alla riduzione del profilo di rischio operativo della Banca.

Valutazione del presidio

La valutazione della qualità del presidio ha l'obiettivo di ridurre il rischio ad un livello ritenuto accettabile, rispettare gli standard normativi e adeguarsi alle best practice di Gruppo. In questo contesto l'intervistato valuta il presidio al rischio come:

1. **adeguato:** i fattori di rischio sono gestiti in modo tale da conseguire la massimizzazione della protezione degli asset e della creazione del valore. Il controllo è previsto e correttamente realizzato in modo da mitigare o annullare gli effetti del rischio;

2. **parzialmente adeguato:** i fattori di rischio sono gestiti in modo tale da rispettare gli standard normativi interni ed esterni minimi, anche se rimangono disallineati in relazione alla best practice di sistema; tramite opportuni interventi è possibile migliorare la protezione degli asset e la creazione di valore. Il controllo è previsto ma non sempre attuato oppure è applicato in maniera non corretta. Inoltre potrebbe essere possibile migliorarne la capacità di protezione degli asset allineandolo alle best practice di sistema;

3. **non adeguato:** gli asset non sono adeguatamente protetti e le modalità di presidio non rispettano i requisiti minimi normativi interni ed esterni e quindi è necessario intervenire. Il controllo non è previsto, oppure sistematicamente non è eseguito.

La valutazione deve tener conto del contesto complessivo di esecuzione di un processo ed, in particolare, se siano state svolte in precedenza azioni di contrasto ai rischi o di mitigazione, considerando lo stato d'implementazione dell'intervento (ad es. se è terminato con successo oppure se è terminato senza raggiungere un risultato accettabile o se l'intervento è ancora in corso).

Identificazione del fattore di rischio

Alla valutazione di *non adeguatezza* o *parziale adeguatezza* del presidio deve seguire l'indicazione, da parte del responsabile di processo, di quale sia il **fattore di rischio** principale che è "causa" della non completa capacità di presidiare il processo e che deve essere meglio governato, o corretto, per riportare il presidio entro il livello di adeguatezza.

Per considerare l'adeguatezza del presidio dal punto di vista dei fattori di rischio, si devono considerare le seguenti caratteristiche:

- ✓ *PROCESSI: il flow di attività deve essere organizzato in modo ottimale, la comunicazione orizzontale e verticale previste in modo da valorizzare la conoscenza esistente e il tutto deve essere descritto da procedure operative interne in linea con la normativa interna ed esterna;*

- ✓ *RISORSE: le risorse devono essere adeguatamente staffate per numero e per profilo professionale; le attività di formazione devono essere previste per garantirne l'aggiornamento;*

- ✓ *SISTEMI: i sistemi devono supportare lo svolgimento delle attività con caratteristiche funzionali consone alle esigenze degli utenti e con caratteristiche tecnologiche di elevato standard qualitativo.*

Il Responsabile di processo deve individuare un solo fattore di rischio sul quale, a suo giudizio, è prioritario intervenire. Spesso è possibile individuare più di un fattore di rischio per il quale è possibile migliorare la gestione, per cui il Responsabile deve effettuare la valutazione di quello che, a suo giudizio, è il *prevalente*. In questo modo viene effettuato un primo *screening* delle informazioni che si dovranno considerare ai fini del miglioramento della gestione.

Intervento di miglioramento della gestione

Dopo aver individuato il *fattore di rischio* per i casi di presidio *non adeguato* o *parzialmente adeguato*, il Responsabile di processo è chiamato a segnalare un intervento di mitigazione specificandone il contesto e gli obiettivi con un'adeguata descrizione. L'intervento potrà essere indicato come "proposto" o "in corso" nel caso in cui sia un'iniziativa proposta dal Responsabile che compila il questionario (e che propone di svolgere un intervento a contrasto dei rischi) oppure sia un'attività già in corso che potrà influenzare positivamente il presidio del processo senza dover intervenire ulteriormente.

Ad ogni intervento deve essere assegnata poi una *priorità* di esecuzione secondo una scala qualitativa:

1. **Alta:** l'evento di rischio tipico, oggetto di valutazione, è considerato dal Responsabile come rilevante in termini di perdite potenziali; l'intervento proposto consentirebbe di migliorare l'efficacia del presidio del rischio con la conseguente diminuzione della perdita potenziale (a titolo di indicazione, l'azione mitigativa proposta, a giudizio del Responsabile, permetterebbe al presidio di "passare di stato");
2. **Media:** l'evento di rischio tipico, oggetto di valutazione, è considerato dal Responsabile come significativo (ma non rilevante) in termini di perdite potenziali; l'intervento proposto consentirebbe di migliorare ulteriormente l'efficacia del presidio del rischio con la conseguente diminuzione della perdita potenziale (a titolo di indicazione, l'azione mitigativa proposta, a giudizio del Responsabile, permetterebbe al presidio di "passare di stato");
3. **Bassa:** l'evento di rischio tipico, oggetto di valutazione, è considerato dal Responsabile come non significativo in termini di perdite potenziali; l'intervento proposto, a giudizio del Responsabile, non permetterebbe al presidio di "passare di stato" pur consentendo di migliorarne ulteriormente l'efficacia con la conseguente diminuzione della perdita potenziale.

In fase di analisi risulta significativo che il Responsabile di processo segnali i progetti/le attività in corso o pianificate che possono avere un impatto mitigativo. In tale senso può esserci un raccordo con le strutture coinvolte nella pianificazione e gestione delle mitigazioni (tipicamente Organizzazione ma anche IT, ecc.) per una migliore descrizione di tali progetti/attività e delle loro implicazioni.

7.4 Analisi dei risultati e reporting

Conclusa la valutazione dei presidi relativi alle catene "unità organizzativa/processo/rischio" da parte dei Responsabili di processo, i Gestori OR redigono un'informativa rivolta alle strutture "superiori" rispetto agli esecutori dell'RSA sia per un loro opportuno allineamento sui risultati delle interviste poste alle strutture sotto la loro responsabilità, sia per un confronto complessivo sui processi sotto la loro ownership, al fine di dare una maggiore completezza e qualità dell'iniziativa.

Al fine di fornire un quadro complessivo sulle evidenze emerse dall'intera attività, viene predisposta una relazione finale che riassume tutti i principali aspetti del processo di Assessment. La relazione (cd "*Relazione Finale di Risk Self Assessment*") descrive le strutture intervistate, i processi analizzati, la qualità dei presidi emersa dai questionari e le azioni di mitigazione indirizzate/proposte, con l'obiettivo di porre in risalto le criticità (in termini di processi non adeguatamente presidiati) e le azioni di miglioramento/correzione che sono state identificate.

Le indicazioni di criticità sui presidi e di miglioramento della gestione che emergono dall'RSA (contenuti nella relazione) sono elementi di input al processo di **Scenario**, nel quale si consolidano le informazioni recepite dalla fase di identificazione in un'attività di valutazione delle criticità operative ad alto livello (lo scenario è rivolto al Top Management). Attraverso l'Analisi di Scenario, vengono associati alle criticità gli interventi di mitigazione più significativi in termini di contrasto ai rischi, finalizzando in modo ottimale le risorse per la definizione e l'implementazione delle misure di correzione. Si rinvia al capitolo dedicato allo Scenario per ogni dettaglio.

8. ANALISI DI SCENARIO

8.1 Processo e aspetti organizzativi

Il processo è articolato nei seguenti sotto-processi:

- **Analisi dei dati LDC ed Assessment**: si analizzano le informazioni derivanti da LDC e da Assessment per individuare fenomeni rilevanti ai fini della valutazione del profilo di rischio prospettico da valutare in sede di Scenario;

- **Analisi di altre fonti di dati**: si analizzano le informazioni derivanti ***(i)*** *dal sistema*, sia dati DIPO rilevanti che perdite esterne individuate come estreme rispetto al dataset di calcolo; ***(ii)*** *da altre fonti*, con evidenze specifiche dal mondo estero (filiali o controllate estere, per arricchire il questionario con fenomeni evidenziatisi all'estero e non ancora rilevanti in Italia), dal mondo bancario (report esterni dell'Arbitro Bancario) oppure da media/internet (news relative al sistema bancario di interesse ai fini della valutazione del profilo di rischio prospettico, ecc.);

- **Predisposizione dei questionari**: gli eventi di rischio rilevati nelle due fasi precedenti (analisi dati LDC, RSA ed altre fonti) vengono aggregati in aree di criticità che raccolgono al loro interno le domande dei questionari. Prima dell'esecuzione dei questionari, le domande sono condivise con le varie funzioni aziendali nell'ambito del "Tavolo Rischi Operativi", un tavolo di lavoro (convocato per ogni sessione di scenario) al quale partecipano varie strutture (tipicamente Audit, Organizzazione, Legale, Compliance, Controlli 262 e, se necessario, con eventuali contributi da parte di altre strutture) che, per competenza e visibilità trasversali sulla Banca e sul business, possono dare un contributo di ampliamento e miglioramento delle tematiche trattate nel questionario, condividendo le risultanze portate al "Tavolo" dall'Operational Risk, ed arricchendole, dove possibile e necessario, in base alle loro conoscenze di "esperti di settore";

- **Esecuzione dei questionari**: per ciascuna domanda del questionario, il Top Management stima:

  - ✓ *Frequenza attesa (frequency)*: stima della frequenza attesa di accadimento con cui il rischio rilevato potrebbe manifestarsi nel periodo di analisi;
  - ✓ *Impatto tipico (severity)*: l'impatto tipico associato al singolo evento di rischio rilevato;
  - ✓ *Caso peggiore (worst case)*: caso peggiore d'impatto;
  - ✓ *Mitigazione*: opportuni interventi di miglioramento della gestione.

- **Analisi risultati e reporting**: vengono formalizzati i risultati dello Scenario per la presentazione ai Responsabili delle Aree di Business.

Di seguito vengono descritte le metodologie per l'Analisi dati (LDC, Assessment e altre fonti), la Predisposizione dei questionari, l'Esecuzione dei questionari e l'Analisi risultati e reporting.

Infine, il Gestore OR di Capogruppo analizza le evidenze di criticità emerse dall'Analisi di Scenario e predispone il "**Piano di Gestione dei Rischi Operativi**" composto dalle azioni di mitigazione ritenute adeguate alla gestione e controllo dei rischi operativi. L'individuazione degli argomenti oggetto di mitigazione è svolta sulla base della rilevanza del VaR, dell'assenza di altri interventi di mitigazione in corso e dalla relazione tra criticità analoghe emerse su tutte le domande del Gruppo. Le azioni emergono generalmente dal questionario di Analisi di Scenario e spesso sono suggerite dalle singole strutture che hanno risposto al Risk Self Assessment e al questionario di Scenario.

Il "Piano" viene condiviso con le strutture owner dell'implementazione delle varie azioni (tipicamente a livello di direzione/area/servizio), in modo da definire nello specifico l'ambito degli interventi, effettuare una valutazione costi-benefici e verificare eventuali sinergie rispetto ad altri interventi o progettualità in corso o programmate. Successivamente il Piano di Gestione viene sottoposto all'approvazione del Comitato Gestione Rischi. La successiva gestione del Piano viene svolta nell'ambito del processo delineato dalla "Policy in materia di gestione dei Gap segnalati dalle Funzioni con compiti di Controllo" (documenti D01822 e D01959).

8.2 Analisi dati (Loss Data Collection, Assessment e altre fonti)

I questionari per le analisi di Scenario sono generati utilizzando un ampio set di informazioni qualitative e quantitative che contribuiscono ad identificare, per ogni area di business/società, le principali aree di rischiosità operativa. All'interno del set informativo impiegato, le fonti di informazioni principalmente utilizzate sono le seguenti:

- Loss Data Collection: evidenze su eventi rilevanti, trend significativi;
- Assessment: evidenze dei presidi giudicati come "non ottimali" in sede di esecuzione dell'RSA;

- Dati esterni: evidenze su eventi rilevanti e trend significativi rilevati dal DIPO.

A tali evidenze si vanno ad aggiungere le ulteriori informazioni provenienti:

- da area estero e filiali estere (per arricchire il questionario con fenomeni evidenziatisi all'estero e non ancora rilevanti in Italia);

- dal sistema bancario (Relazione sull'attività dell'Arbitro Bancario Finanziario che evidenzia fenomeni e trend di rischiosità emersi dall'attività svolta dai Collegi in relazione all'andamento del sistema stragiudiziale nel suo complesso e fornisce informazioni di carattere statistico sui ricorsi presentati, sugli esiti e sugli intermediari interessati);dai media/internet (per news relative al sistema bancario di interesse ai fini della valutazione del profilo di rischio prospettico);

- da segnalazioni su aspetti di business della Banca (ad es. previsioni di cambiamenti organizzativi, IT, esternalizzazioni, ecc);

- da segnalazioni emerse da altre strutture (evidenze di "gap", segnalazioni da Audit, Compliance, Legale, ecc).

I risultati dei processi di Loss Data Collection e di Assessment rappresentano le fonti principali per la predisposizione dei questionari di Scenario e per la definizione della prima versione ("in bozza") del questionario da sottoporre alla condivisione delle funzioni che fanno parte del "Tavolo Rischi Operativi".

Analisi della Loss Data Collection

A partire dalle evidenze di Loss Data più rilevanti si selezionano le tipologie di rischio e di contesto (facendo riferimento alle casistiche di accadimento) per definire le opportune domande da inserire nel questionario di Scenario.

Al fine di discriminare le informazioni, si considerano le perdite maggiormente significative per importo e/o per frequenza sulla base del giudizio esperto del Gestore OR per ogni periodo di rilevazione, in funzione delle esigenze di analisi di ciascun questionario e al fine di dare evidenza ai fenomeni di rischio

materiali. In tale senso, sia l'analisi dei trend di perdita (numero eventi/perdita) che dei fenomeni (ad es. recrudescenza delle frodi su carta di credito, delle rapine, ecc.) porta alla definizione di opportuni ambiti di interesse ai fini della valutazione del profilo di rischio prospettico.

L'analisi incrociata dei contesti in cui si evidenziano le perdite rilevanti , dei fattori di rischio non presidiati, dei fenomeni emersi/in emersione, della "storia" e dei trend delle perdite, delle evidenze di sistema e delle strutture che rilevano le perdite fornisce le informazioni adeguate alla definizione di opportune domande da porre in sede di Scenario, sia in termini di collocazione nel giusto contesto organizzativo (struttura cui porre la domanda in sede di Scenario) sia di corretta formulazione della domanda (rischio oggetto di indagine e contesto della sua potenziale manifestazione).

A titolo di esempio, se nel periodo un fenomeno risulta in crescita oppure se ci sono state perdite rilevanti, è importante verificare se l'argomento sia già trattato in domande ''pregresse" (precedenti sessioni di Scenario), che possono essere arricchite da informazioni più complete includendo il fenomeno osservato nel periodo, oppure, in caso non vi siano domande al riguardo, valutare se definire una nuova domanda da porre in sede di scenario indirizzandola alla struttura che meglio potrà fornire la corretta declinazione del profilo di rischio della Banca in relazione al fenomeno.

Analisi dei risultati di Assessment

A partire dalle evidenze emerse dall'RSA si selezionano le tipologie di rischio e di contesto con presidio non adeguato per andare a definire le opportune domande da inserire nel questionario di scenario.

L'obiettivo è selezionare gli eventi tipici che, dall'RSA, hanno evidenziato una maggiore esposizione al rischio e, a tale fine, per ogni periodo d'indagine, il Gestore OR deve formulare apposite domande di Scenario connesse alle risposte provenienti dal questionario di RSA i cui presidi hanno indicato efficacia valutata "non adeguata" (escludendo quelli in cui è valutata "adeguata"), considerando l'eventuale importanza dei "parzialmente adeguati".

L'analisi incrociata dei processi a presidio non adeguato, dei rischi tipici connessi, dei fattori di rischio non presidiati, delle strutture oggetto di RSA, fornisce le informazioni adeguate alla definizione di opportune domande da porre in sede di Scenario sia in termini di collocazione della domanda nel giusto contesto organizzativo (struttura cui porre la domanda in sede di Scenario) sia di corretta formulazione della domanda (rischio oggetto di indagine e contesto della sua potenziale manifestazione). Il permanere di una "non adeguatezza" nel giudizio di presidio su un processo tra differenti sezioni di RSA (anno

corrente, anni precedenti) comporta la necessaria verifica di presenza dell'argomento nelle sessioni di Scenario.

8.3 Predisposizione dei questionari

Dall'analisi delle informazioni di Loss Data, Risk Assessment e delle altre fonti, effettuata anche in modo "incrociato" tra le singole evidenze per comprenderne eventuali connessioni o ridondanze, l'Operational Risk giunge alla definizione di una "bozza" di questionario di Scenario.

La prima bozza del questionario viene quindi sottoposta dal Gestore OR di Capogruppo all'attenzione della Funzione Organizzazione e dei Servizi Specialistici, ciascuno per le proprie competenze, al c.d. "Tavolo Rischi Operativi".

La composizione "finale" del questionario di Scenario, infatti, avviene al Tavolo Rischi Operativi, gruppo di lavoro al quale partecipano, oltre all'ORM, le funzioni Audit, Organizzazione e altre strutture/aree di business necessarie per l'interpretazione delle criticità operative (tipicamente Legale e Compliance); obiettivo del "Tavolo" è dare un contributo di ampliamento e miglioramento delle tematiche trattate nel questionario condividendo le risultanze portate al "Tavolo" dall'Operational Risk, ed arricchendole, dove possibile e necessario, in base alla loro conoscenza di "esperti di settore"[2].

Selezionati i rischi rilevanti e i fenomeni da valutare in sede di Scenario, la costruzione del questionario segue i seguenti passi:

- **Questionario per area di business/servizio**: per ogni società (in funzione dell'organizzazione aziendale) sono individuate aree di business/servizio omogenee utili ai fini dello Scenario e alla definizione del profilo di rischio per tipo di business (es. Retail, Corporate, Credito, Operation, ecc.) e per ogni area individuata si definisce un questionario di Scenario;

  Sezioni del questionario per area di criticità: ciascun questionario viene suddiviso in "sezioni/aree di criticità" costituite da "insiemi di situazioni" che condividono problematiche simili, anche facendo riferimento ad ambiti/contesti operativi simili; per ogni sezione si indicano le attività che la caratterizzano A titolo esemplificativo, un'area di criticità/sezione potrebbe essere definita come segue: "*Nell'ambito dell'operatività del Leasing Immobiliare, sono emersi*

[2] Per quanto riguarda le Controllate, lo schema di lavoro si replica, attivando al "tavolo" della singola Società anche le figure dell'OR di Capogruppo, di Audit e Organizzazione di Capogruppo, per opportuno raccordo con la Capogruppo sia in termini di tematiche che di riscontro e allineamento.

aspetti di rilievo relativamente all'istruttoria, all'analisi del rischio e alla delibera in termini di: a) carenze informative nella documentazione tecnica dell'immobile e nella perizia; a) assenza di un elenco di professionisti che possano svolgere il ruolo di Direttori dei Lavori", ed in tale sezione si porranno tutte le domande di pertinenza.

- **Domande associate ad ogni sezione**: ad ogni sezione si associano le domande pertinenti, per argomento, con la sezione. Le domande sono costituite dagli Eventi di Rischio Operativo legati all'area di criticità. Continuando il precedente esempio, una delle domande che si potrebbero definire nella sezione è la seguente: "*Nel caso del Leasing Immobiliare a SAL, qual è il rischio di subire perdite in seguito al mancato/non corretto monitoraggio dei lavori in corso d'opera?*". La domanda è classificata: "Esecuzione, consegna e gestione del processo".

Il questionario così definito e arricchito (modificato e/o ampliato sulla base delle informazioni, degli skill e del know-how dei vari convenuti) viene quindi portato all'attenzione del **T**op Management per la definizione delle risposte con la fase di "esecuzione".

8.4 Controlli di consistenza sulle domande dello Scenario

Una volta costruito il questionario come indicato in precedenza, viene svolto un controllo per garantire l'assenza di aggregazioni/frammentazioni di eventi di rischio simili presenti nelle relative domande del questionario.

Si procede come segue:

1) le domande vengono suddivise per i diversi Event Type di Basilea, a livello 2
2) all'interno di ciascun ET di secondo livello possono essere considerate domande diverse, riferite a specifici processi/attività, che vengono identificati associando alla domanda un "**Ambito**" ed un "**Tema**", così definiti:
    a. ***Ambito***: si tratta dell'ambito di rischio operativo, circonstanziato sul business, che consente di raggruppare insieme domande diverse che riguardano gli stessi specifici processi/attività, come ad esempio nei seguenti casi:
        - ✓ Ambito 1 "Finanza" [che raccoglie le domande del business/processo/attività Finanza]
        - ✓ Ambito 2 "Operatività di Amministrazione, Bilancio e di Vigilanza"

- ✓ Ambito 3 "Fornitori ed opere"
- ✓ ecc.

L'ambito consente un primo raggruppamento ed ogni ambito si dettaglia poi in differenti "temi".

b. ***Tema***: all'interno del singolo "ambito" (che raccoglie processi/attività omogenei sul business) il "tema" consente di descrivere in modo più dettagliato le possibili criticità relative ai processi ed alle attività in esame; a titolo di esempio, riprendendo due dei precedenti "ambiti" si ha:

- ✓ **Ambito 1 "Finanza"**
  - **Tema 1.1** "Monitoraggio dei limiti"
  - **Tema 1.2** "Errori e carenze nell'aggiornamento del pricing"
  - …
- ✓ **Ambito 2 "Operatività di Amministrazione, Bilancio e di Vigilanza"**
  - **Tema 2.1** "Errata rappresentazione in Bilancio del risultato economico di competenza"
  - …

3) ciascuna domanda relativa ad una "tripletta" ("Event Type" - "Ambito" - "Tema") può essere poi indirizzata o meno alle varie Società del Gruppo e - all'interno della singola Società - alle singole Unità Organizzative. In questo contesto, quindi, ogni tripletta "***Event Type***", "***Ambito***", "***Tema***" viene a sua volta mappata su "***Società***" ed "***Unità Organizzativa***".

Il controllo consiste nel verificare che esista una sola domanda per la stessa tripletta "Event Type", "Ambito", "Tema" abbinata alla singola coppia "Società" ed "Unità Organizzativa" garantendo che non ci siano aggregazioni o frammentazioni di eventi di rischio simili nelle diverse domande poste con il questionario. In generale, l'assegnazione della classe di rischio ("Tipo") tiene conto dell'ET della domanda catalogata nel repository e dalla Funzione Compilatrice.
Nel caso di domande riferite allo stesso fenomeno che possono generare effetti di perdita differenti (es. cause e reclami), l'assegnazione della classe di rischio avviene sulla base della Funzione Compilatrice (es se i fenomeni vengono valutati dalla Funzioni Legale o Compliance), oppure sulla base della rilevanza storica del fenomeno e delle ulteriori informazioni fornite dall'Assessor.

Potenzialmente, pertanto, la medesima tripletta "ET-Ambito-Tema" può essere valutata da funzioni differenti purché si riferiscano ad effetti di perdita diversi. Una domanda quindi può essere presente su più strutture ma la valutazione riguarda aspetti diversi di uno stesso fenomeno.

8.5 Esecuzione dei questionari

Nella fase di esecuzione dei questionari, le valutazioni richieste sono espresse dal Top Management in un'ottica "forward-looking". Le valutazioni fornite rappresentano una stima delle potenziali perdite operative e devono, pertanto, essere espresse al lordo dei relativi rimborsi assicurativi che si prevede possano essere ottenuti. Le stime soggettive richieste per ogni domanda sono tre:

- ✓ ***Frequenza attesa*** (frequency): stima della frequenza attesa di accadimento con cui il rischio rilevato potrebbe manifestarsi nel periodo di analisi;
- ✓ ***Impatto tipico*** (severity): l'impatto più frequente associato al singolo evento di rischio rilevato;
- ✓ ***Caso peggiore*** (worst case): caso peggiore d'impatto.

In sede di esecuzione dei questionari, inoltre, vengono individuate le leve gestionali praticabili per un efficace ed efficiente trattamento delle criticità. A tal fine, con il Top Management vengono condivisi:

- ✓ i **fattori di rischio** su cui intervenire;
- ✓ gli **interventi di mitigazione**, trasferimento e ritenzione del rischio.

Per agevolare l'esecutore nel fornire le valutazioni vengono poi inserite nel questionario le valutazioni fornite l'anno precedente unitamente ad un insieme di informazioni relative al fenomeno oggetto di valutazione (dati di perdita storica interni/esterni sottostanti alla domanda, evidenze di RSA per il fenomeno, riflessioni fatte al "Tavolo", fattore di rischio che nella precedente versione aveva indirizzato l'ambito della criticità), in modo da comporre un quadro di dati a corredo della domanda e della sua valutazione da parte dell'esecutore.

Le classi di valori scelte dall'intervistato permettono di ottenere, attraverso un modello sottostante statistico/attuariale, per ogni rischio rilevato, una stima della distribuzione della perdita attesa ed inattesa e del Capitale a Rischio (si rinvia al manuale di misurazione per ogni approfondimento).

Come indicato in precedenza, l'output dello Scenario costituisce l'elemento fondamentale per la predisposizione del "**Piano di Gestione**", iniziativa inclusa nella fase di "Gestione e Controllo" con la quale vengono definiti gli interventi di mitigazione, ritenzione e trasferimento dei rischi.

8.6 Analisi dei risultati e reporting

Conclusa l'analisi di Scenario, viene predisposto il Report Conclusivo di Scenario per ciascuna Struttura intervistata dove sono riportate le evidenze di rischiosità emerse, le aree di criticità ed i relativi interventi di mitigazione. Il reporting viene veicolato alla Funzione Audit, alle varie Direzioni ed alle singole strutture che hanno partecipato all'esecuzione del questionario.

9. TIMING DELLA FASE DI IDENTIFICAZIONE

9.1 Sintesi

Le fasi esposte nei capitoli precedenti si sviluppano in un processo a durata complessiva annuale, che dettagliamo a seguire per quanto riguarda le tempistiche di esecuzione della Loss Data Collection, del Risk Assessment e dell'Analisi di Scenario.

9.2 Loss Data Collection

Il processo si svolge nel continuo nel corso dell'anno, con le attività di raccolta, controllo, lavorazione e censimento dei dati effettuate a periodicità tipicamente mensile (per la quasi totalità della Fonti), o trimestrale (per alcune poche Fonti, in relazione alla specifica tipologia di dati e di lavorazione). A completamento delle attività viene prodotta specifica reportistica periodica (tipicamente trimestrale) con la quale si riassumono tutti i principali aspetti emersi dal processo di Loss Data Collection: nuovi accadimenti rilevati, aggiornamento su eventi passati che spesano ancora nel periodo, evidenza sui

fenomeni e sull'andamento delle perdite nel tempo, impatti a Conto Economico e Fondo Rischi derivanti dagli eventi, focus sugli accadimenti rilevanti e significativi. I principali aspetti emersi dal processo di LDC sono posti all'attenzione del Top Management tramite reportistica periodica rappresentata al Comitato Gestione Rischi ed al Comitato Direttivo.

Nel "Manuale delle Fonti" il dettaglio delle lavorazioni.

9.3 Assessment

Il processo si svolge nel corso del primo semestre e si articola principalmente in 3 momenti:

- predisposizione dei questionari, con raccordo verso le strutture destinatarie dell'Assessment per una condivisione di completezza dei processi analizzati e di review sui rischi da valutare;

- esecuzione dei questionari, con il contatto, il supporto e il seguimento delle strutture coinvolte nello svolgimento dell'Assessment al fine di garantire qualità, completezza e tempestività di esecuzione;

- analisi dei dati, per verificare gli esiti delle interviste (identificazione dei processi più critici, degli ambiti migliorati nel tempo, ecc.).

A seguire lo svolgimento delle 3 fasi vengono prodotte:

- ✓ un'informativa verso le strutture "superiori" rispetto agli esecutori dell'RSA, sia per un loro opportuno allineamento sui risultati delle interviste poste alle strutture sotto la loro responsabilità, sia per un confronto complessivo sui processi sotto la loro ownership, al fine di dare una maggiore completezza e qualità dell'iniziativa;

- ✓ una relazione di sintesi (cd "*Relazione Finale di Risk Self Assessment*") dove si descrivono le strutture intervistate, i processi analizzati, la qualità dei presidi emersa dai questionari e le azioni di mitigazione indirizzate/proposte, con l'obiettivo di porre in risalto le criticità (in termini di processi non adeguatamente presidiati) e le azioni di miglioramento/correzione che sono state identificate. La relazione, che evidenzia le criticità emerse in sede di RSA (processi ritenuti non adeguatamente presidiati) serve come input al processo di Scenario.

9.4 Scenario

Il processo si svolge nel corso del secondo semestre e si articola principalmente in 2 momenti, così riassumibili:

- predisposizione dei questionari, con la raccolta documentale, l'esecuzione del "Tavolo OR" e la definizione dei questionari da sottoporre al Top Management;

- esecuzione dei questionari, con il contatto, il supporto e il seguimento delle strutture coinvolte nello svolgimento dello Scenario, al fine di garantire qualità, completezza e tempestività di esecuzione.

A seguire lo svolgimento delle 2 fasi viene prodotta una relazione di sintesi (cd "*Relazione Finale di Scenario*") dove si descrivono le strutture intervistate, i rischi analizzati, le criticità emerse (in termini di rischi a maggiore rilevanza) e le azioni di miglioramento/correzione che sono state identificate; tali azioni saranno poi input per il processo di "**mitigazione dei rischi operativi**" (*il Gestore OR di Capogruppo analizzando le evidenze di criticità emerse dall'Analisi di Scenario predispone il "Piano di Gestione dei Rischi Operativi", composto dalle azioni di mitigazione ritenute adeguate alla gestione e controllo dei rischi operativi. Il "Piano" viene condiviso con le strutture owner dell'implementazione delle varie azioni e viene approvato dal Comitato Gestione Rischi. La gestione del piano di mitigazione avviene nell'ambito del processo delineato dalla "Policy di gestione dei Gap" segnalati dalle strutture di controllo*).

10. ANNEX

10.1 Business Line

Le Business Line o "linee di business", sono definite come le aree di affari in cui vanno suddivise le attività aziendali. La normativa prevede la seguente classificazione:

1. **Corporate finance** Fusioni, Acquisizioni, Attività di collocamento (OPA, OPV, collocamenti privati – c.d. blocchi, emissioni obbligazionarie). Investment Banking in azioni 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.

2. **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 professionali. Attività di consulenza, assunzione a fermo, collocamento di strumenti finanziari e prodotti assicurativi (bancassurance, fondi, GPM, GPF, azioni, obbligazioni, derivati, etc) verso clienti corporate e professionali.

3. **Retail banking** Prestiti e Depositi. Garanzie e impegni finanziari. Credito al consumo per clienti retail. Leasing e 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 (collocamento di carte di debito e di credito, trasferimento fondi ed altri pagamenti per conto di clienti, cambio valuta, etc.) e custodia ed amministrazione titoli.

4. **Commercial banking** Prestiti e Depositi. Garanzie e impegni finanziari. Leasing e 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 contodi clienti, cambio valuta, etc.) e custodia ed amministrazione titoli. Reddito netto (ad esempio cedole e dividendi) su portafogli non di trading.

5. **Payment and settlement** Servizi e sistemi di pagamento, regolamento e compensazione (EBA, BIREL, TARGET, CLS, SWIFT, MASTERCARD, VISA, AMEX, etc.). Emissione e gestione di strumenti di pagamento e trasferimento fondi come business specifico. Banca corrispondente.

6. **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.

7. **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.

8. **Retail brokerage** Ricezione, trasmissione ed esecuzione di ordini verso clienti retail. Attività di consulenza, assunzione a fermo, collocamento di strumenti finanziari e prodotti assicurativi (bancassurance, fondi, GPM, GPF, azioni, obbligazioni, derivati, etc.) verso clienti retail.

9. **Corporate Items** (*solo banche AMA*) Attività che riguardano la banca nella sua interezza, quali dichiarazione annuale delle tasse, azioni o responsabilità degli esponenti aziendali, ecc.

Nel "**Manuale delle Fonti Informative**" si indicano i dettagli e le regole di catalogazione degli eventi raccolti dalle Fonti Informative.

10.2 Event Type

La classificazione degli eventi in ET si basa sulla comprensione di quanto accaduto e nella relativa catalogazione dell'evento in una delle 7 categorie indicate da Basilea:

Classificazione (ET Basilea)	Dettaglio	Esempi
1 Frode interna	attività non autorizzate, frodi, furti	appropriazione indebita, svolgimento di attività senza autorizzazione
2 Frode esterna	furto, frode	furti, frodi, rapine, scassi ATM, ecc
3 Rapporti di impiego e sicurezza sul lavoro	atti non conformi agli accordi in materia di impiego o violazione degli accordi contrattuali	discriminazioni, mancanze contrattuali, retributive, contributive, ecc
4 Clienti prodotti e prassi operativa	perdite derivanti da inadempienze, involontarie o per negligenza, relative a obblighi professionali verso clienti ovvero dalla natura o dalle caratteristiche del prodotto/servizio prestato	violazioni delle disposizioni legislative che regolano l'adeguatezza e gli obblighi di informativa nei confronti della clientela (trasparenza, privacy, interpretazione delle norme, collocamento di prodotti non correttamente illustrati), violazioni delle clausole contrattuali, pratiche di mercato improprie (antitrust, antiriciclaggio e insider trading), errato sviluppo di prodotti/servizi, errori nella valutazione dei bisogni del cliente e nella gestione dei limiti di esposizione
5 Danni a beni materiali	danni per eventi naturali, accidentali, vandalici	eventi dannosi che colpiscono beni mobili/immobili di proprieta' o di terzi sui quali risponde la Banca
6 Interruzioni dell'operativita' e disfunzioni dei sistemi	guasti a sistemi hardware, software, telecomunicazioni e fornitura servizi	guasti a sistemi hardware, software, telecomunicazioni e fornitura servizi
7 Esecuzione, consegna e gestione dei processi	errori, negligenze, inadempienze nell'avvio, nella esecuzione e nella consegna delle operazioni, sia verso i clienti che verso controparti commerciali, venditori e fornitori	errori nell'esecuzione di operazioni di incasso e pagamento, nelle disposizioni di pagamento, nella gestione di strumenti finanziari, ovvero danni causati alla clientela per il mancato rispetto dei termini contrattuali e/o delle disposizioni di legge, controversie per mancato rispetto degli accordi di fornitura,

Sulla base della tassonomia di riferimento regolamentare così riportata:

Codice Primo Livello	Descrizione Primo Livello	Codice Secondo Livello	Descrizione Secondo Livello
1	Frode interna	1	Attività non autorizzata
		2	Furto e frode
2	Frode esterna	1	Furto e frode
		2	Sicurezza dei sistemi
3	Rapporto di impiego e sicurezza sul lavoro	1	Rapporto di impiego
		2	Sicurezza sul lavoro
		3	Discriminazioni/condizioni non paritarie
4	Clientela, prodotti e prassi di business	1	Adeguatezza informativa e rapporti fiduciari
		2	Pratiche di business o di mercato improprie
		3	Difetti nella produzione
		4	Selezione, sponsorizzazione e limiti di esposizione
		5	Attività di consulenza
5	Danni a beni materiali	1	Disastri ed altri eventi
6	Interruzione dell'operatività e disfunzione dei sistemi	1	Sistemi
7	Esecuzione, consegna e gestione dei processi	1	Avvio, esecuzione e consegna delle operazioni
		2	Monitoraggio e reporting
		3	Acquisizione dei clienti e relativa documentazione
		4	Rapporti continuativi e di corrispondenza con la clientela
		5	Controparti commerciali
		6	Venditori e fornitori

il Gruppo MPS ha introdotto un modello interno di classificazione detto "**Modello Integrato dei Rischi**" (MIR) che amplia i due livelli di classificazione regolamentari con ulteriori dettagli, per una più granulare identificazione degli eventi in adeguati ET.

Nel "**Manuale delle Fonti Informative**" si indicano i dettagli e le regole di catalogazione in ET degli eventi raccolti dalle Fonti Informative, con il dettaglio del MIR.