Regolamento
Funzione Risk Management

Regolamento emesso il 09/01/2024
Owner del regolamento: Funzione Risk Management

Indice

1 Premessa

Il presente documento definisce il ruolo e le responsabilità della Funzione Risk Management in coerenza con le disposizioni normative esterne vigenti, con la Relazione sulla Struttura Organizzativa di Flowe S.p.A. (di seguito "Flowe" o "la Società") e con tutta la normativa interna di riferimento relativa al controllo, alla gestione e alla mitigazione dei rischi adottata a livello di Gruppo Bancario. Scopo del presente documento è, pertanto, quello di definire i compiti e le attività predisposte dalla funzione di controllo dei rischi di Flowe nell'ambito del sistema dei controlli interni della Società.

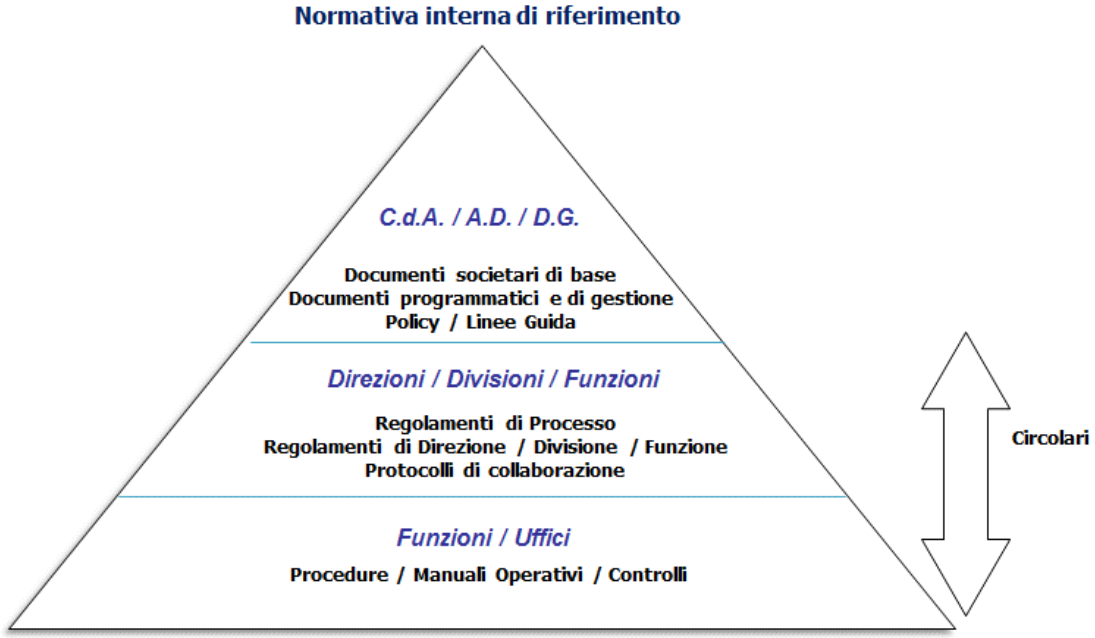
La Funzione Risk Management ha la finalità di collaborare, attraverso un adeguato processo di controllo e gestione dei rischi, alla definizione e all'attuazione delle politiche di governo dei rischi e di garantire il supporto necessario agli Organi Aziendali nel promuovere e diffondere un'adeguata e solida cultura del rischio all'interno della Società.

1.1 Obiettivi del Documento

Il presente documento ha l'obiettivo, all'interno del quadro di riferimento delineato in precedenza, di:

- definire l'ambito di responsabilità della Funzione Risk Management;
- dettagliare quanto già delineato nella Relazione sulla Struttura Organizzativa di Flowe, in relazione all'assetto organizzativo, compiti e responsabilità;
- descrivere gli obiettivi gestionali interni e i processi impattanti la Funzione;
- descrivere le Interrelazioni con altre Unità Organizzative.

Come disposto dal documento Relazione sulla Struttura Organizzativa (RSO), il presente documento si colloca al 2° livello della piramide documentale richiamata nello schema seguente.



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

L'approvazione di questo documento è a cura dell'Amministratore Delegato. Questo Regolamento viene aggiornato a fronte di significative variazioni negli elementi precedentemente citati.

1.2 STRUTTURA DEL DOCUMENTO

Il Regolamento si compone complessivamente di cinque capitoli, oltre al presente.

Di seguito sono descritte sinteticamente le principali tematiche trattate in ogni capitolo:

- Capitolo 2: Posizionamento organizzativo

Obiettivo del capitolo è descrivere il posizionamento della Funzione Risk Management nell'ordinamento organizzativo di Flowe.

- Capitolo 3: Responsabilità

Obiettivo del capitolo è descrivere i ruoli e le responsabilità della Funzione Risk Management nell'ambito:

  - delle politiche di governo dei rischi
  - del processo di gestione e controllo dei rischi rilevanti

- Capitolo 4: Processi

Obiettivo del capitolo è descrivere le attività della Funzione Risk Management in relazione alla gestione e al controllo dei rischi rilevanti e alla predisposizione del reporting. Management.

Sono, inoltre, richiamati i principali strumenti informatici utilizzati a supporto dei processi e dei compiti attribuiti alla Funzione Risk Management.

- Capitolo 5: Interrelazioni con le altre Unità Organizzative

Obiettivo del Capitolo è elencare le principali Unità Organizzative che interagiscono con la Funzione Risk Management relativamente alle attività da quest'ultimo effettuate.

- Capitolo 6: Il quadro normativo di riferimento

Obiettivo del Capitolo è descrivere il quadro normativo di riferimento nell'ambito delle attività svolte dalla Funzione Risk Management, considerando sia le disposizioni normative "esterne" (normativa di primo e secondo livello) che le disposizioni normative "interne" (policy, regolamenti di processo, procedure operative etc.).

2 Posizionamento organizzativo

Il Consiglio di Amministrazione di Flowe S.p.A. ha nominato un responsabile del Risk Management che si avvale, per le attività di controllo dei rischi, della omologa funzione della Capogruppo[1] Banca Mediolanum, in base ad un apposito contratto di outsourcing.

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

La Funzione Risk Management trova autonoma collocazione nella struttura organizzativa della Società in staff al Consiglio di Amministrazione, a cui riporta direttamente. Tale posizionamento è funzionale allo svolgimento, in maniera efficace, dell'attività di interrelazione diretta con l'Organo amministrativo nonché con quello di Controllo attraverso l'attivazione di appropriati flussi informativi.

Il presente documento è stato elaborato a partire dal framework metodologico in uso presso Banca Mediolanum S.p.A. e trasmesso alle società del Gruppo Bancario. In coerenza con le disposizioni di Vigilanza, la Funzione è distinta e indipendente dalle funzioni aziendali incaricate della "gestione operativa" dei rischi, che incidono sull'assunzione dei rischi da parte dei responsabili di processo, modificando il profilo di rischio di Flowe.

Di seguito si riportano le responsabilità ed i ruoli assegnati alla Funzione Risk Management nell'ambito del processo di gestione e controllo dei rischi.

3 Responsabilità

Come descritto all'interno del documento Relazione sulla Struttura Organizzativa (RSO), la Funzione Risk Management costituisce la struttura organizzativa di cui Flowe si è dotata per identificare, misurare/valutare, monitorare e gestire i rischi a cui la stessa è o potrebbe essere esposta.

L'attività identificazione dei rischi rilevanti per Flowe viene svolta dalla Capogruppo Banca Mediolanum nell'ambito dello svolgimento del processo ICAAP/ILAAP del Gruppo Bancario. La Funzione Risk Management di Flowe, per il corretto svolgimento delle responsabilità assegnate dal Consiglio di Amministrazione, ha il compito di individuare e curare gli strumenti e le metodologie idonee ad assicurare una piena comprensione, un efficace monitoraggio e un'efficiente gestione dei rischi rilevanti, fornendone un'adeguata rappresentazione attraverso strumenti di misurazione coerenti con le metodologie adottate e la produzione di reportistica periodica indirizzata al Consiglio di Amministrazione, all'Organo di Controllo e alle funzioni operative.

Con riferimento all'attività di emissione di moneta elettronica e prestazione di servizi di pagamento, per Flowe assume particolare rilevanza il presidio dei rischi operativi, inclusi quelli relativi al rischio ICT e di sicurezza e di natura legale, e dei rischi reputazionali.

Brevemente possiamo riepilogare le seguenti definizioni dei principali rischi, rilevanti per Flowe, di cui la Funzione svolge attività di gestione e mitigazione:

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

Conduct Risk: Quale sottocategoria di rischio operativo, può essere definito in linea generale come il rischio attuale o prospettico di perdite conseguenti a casistiche di offerta inappropriata di servizi finanziari, incluse fattispecie di condotta inadeguata (dolo / negligenza) da parte della Banca e della rete di vendita.

Rischio ICT e di sicurezza: il rischio di incorrere in perdite dovuto alla violazione della riservatezza, carente integrità dei sistemi e dei dati, inadeguatezza o indisponibilità dei sistemi e dei dati o incapacità di sostituire la tecnologia dell'informazione (IT) entro ragionevoli limiti di tempo e costi in caso di modifica dei requisiti del contesto esterno o dell'attività (agility), nonché i rischi di sicurezza derivanti da processi interni inadeguati o

errati o da eventi esterni, inclusi gli attacchi informatici o un livello di sicurezza fisica inadeguata.

Il **rischio di reputazione** viene definito sinteticamente come rischio attuale o prospettico di flessione degli utili o del capitale derivante da una percezione negativa dell'immagine della banca da parte dei clienti, controparti, azionisti della banca, investitori o autorità di vigilanza.

Completano l'elenco delle definizioni i seguenti rischi:

Rischio strategico: definito come Il rischio attuale o prospettico di flessione degli utili o del capitale derivante da cambiamenti del contesto competitivo o da decisioni aziendali errate, attuazione inadeguata delle decisioni, scarsa reattività a variazioni di contesto competitivo.

Climate Risk: i cambiamenti climatici e il degrado ambientale danno origine a mutamenti strutturali che influiscono sull'attività economica e, di conseguenza, sul sistema finanziario. Nell'ambito dei rischi climatici e ambientali rientrano comunemente i due fattori di rischio principali: il rischio fisico e il rischio di transizione.

Rischio di Esternalizzazione: rischio connesso a «Un accordo di qualsiasi forma tra un ente, un istituto di pagamento o un istituto di moneta elettronica e un fornitore di servizi in base al quale quest'ultimo svolge un processo, un servizio o un'attività che sarebbe altrimenti svolto/a dall'ente, dall'istituto di pagamento o dall'istituto di moneta elettronica stesso.» [EBA/GL/2019/02].

In particolare, la Funzione Risk Management, conformemente a quanto disposto nella normativa di riferimento, persegue i seguenti scopi, tramite i processi dettagliati nel corso del documento:

- riceve ed esamina gli aggiornamenti di Policy e linee guida predisposti dalla Funzione Risk Management della Capogruppo valutandone, di volta in volta, l'applicabilità e l'eventuale necessità di integrare la normativa interna della società oppure di recepire quella consolidata;
- definisce, sviluppa e manutiene nel tempo il framework metodologico di controllo ed i sistemi di misurazione di tutti i rischi rilevanti per Flowe nel rispetto delle disposizioni normative vigenti e delle linee guida emanate dalla Capogruppo;
- predispone l'informativa periodica di rischio della Società per il Consiglio di Amministrazione;
- analizza i rischi dei nuovi prodotti e servizi e di quelli derivanti dall'ingresso in nuovi segmenti operativi e di mercato o dall'esternalizzazione di processi e servizi;
- recepisce le linee guida per controllo e la gestione dei rischi climatici e ambientali contenute nella Policy di Gestione dei Rischi Climatici e Ambientali della Capogruppo, che risultano attualmente applicabili nell'ambito dei processi di presidio dei rischi operativi e reputazionali;
- gestisce e supervisiona i rischi connessi agli accordi di esternalizzazione nell'ambito del sistema dei controlli interni;
- verifica, raccoglie e riconcilia, in collaborazione con le preposte unità organizzative della Società, delle perdite rivenienti da rischi operativi;
- analizza le perdite originate dai rischi operativi, definendo piani di azione e verificando il completamento degli stessi;
- definisce il piano di assessment integrato sui rischi operativi e reputazionali;

- identifica, con le unità organizzative interessate, le azioni di intervento per la mitigazione dei rischi rilevati e ne monitora la relativa realizzazione;
- è responsabile della gestione complessiva e supervisione dei rischi ICT e di sicurezza, in recepimento di quanto previsto dalla normativa di riferimento;
- svolge la campagna periodica di analisi del rischio ICT e di sicurezza delle applicazioni in esercizio, al fine di identificarne, analizzarne e valutarne periodicamente il rischio residuo e, nei casi in cui esso superi la propensione al rischio, supportare nella definizione delle azioni necessarie al trattamento del rischio;
- contribuisce alla definizione dei principi e delle regole ad alto livello in ambito Sicurezza Informatica e partecipa al processo di classificazione, analisi e segnalazione dei gravi incidenti di Sicurezza Informatica;
- presidia la normativa specialistica di competenza e attua gli interventi di adeguamento, in collaborazione con le altre funzioni aziendali;
- promuove la diffusione di una cultura aziendale maggiormente orientata alla gestione dei rischi.

4 Processi

Di seguito vengono dettagliate le attività della Funzione Risk Management in relazione alla gestione e al controllo dei rischi rilevanti e alla predisposizione del reporting e flussi informativi verso gli Organi aziendali.

4.1 PROCESSO DI AGGIORNAMENTO DELLA NORMATIVA INTERNA

La Funzione di Risk Management definisce, sviluppa e manutiene nel tempo il framework metodologico di controllo ed i sistemi di misurazione di tutti i rischi rilevanti per Flowe, nel rispetto delle disposizioni normative vigenti e delle linee guida emanate dalla Capogruppo. In tale ambito, in particolare, predispone e aggiorna la “Policy per il controllo e la gestione dei Rischi Operativi”, la “Policy di Gestione del Rischio Informatico”, la “Policy in materia di esternalizzazioni” e la “Policy per il controllo del rischio di reputazione”.
Accanto alle Policy, che descrivono in dettaglio i processi di seguito sintetizzati, possono essere previsti anche specifici manuali operativi, quali strumenti di supporto per un corretto svolgimento delle attività in carico all’Unità.

4.2 PIANIFICAZIONE DELLE ATTIVITÀ

La Funzione Risk Management predispone annualmente il programma delle attività che intende svolgere, definendo un piano dettagliato delle proposte e degli ambiti in cui è chiamata ad operare, e lo sottopone all’approvazione del Consiglio di Amministrazione.

La programmazione delle attività, necessaria per individuare e valutare con sistematicità, efficienza ed efficacia le aree e gli ambiti maggiormente a rischio, i relativi interventi di gestione e le connesse priorità di intervento, si basa su un’attività di analisi e approfondimento che tiene conto anche delle eventuali carenze emerse nei controlli effettuati nell’anno precedente. Nel piano di attività sono quindi individuate:

- attività di controllo che il Risk Management pone in essere nell’ambito delle sue attività tipiche;

- focus specifici e follow-up connessi ad eventuali carenze emerse nei controlli periodici;
- monitoraggio di eventuali nuovi rischi identificati e pertanto non ancora compresi nel processo di gestione integrata dei rischi;
- monitoraggio dell'efficacia di eventuali interventi di prevenzione e mitigazione del rischio promossi dal Consiglio di Amministrazione;
- le tempistiche di svolgimento e/o la periodicità.

4.3 PROCESSO DI CONTROLLO E GESTIONE DEI RISCHI OPERATIVI

Il processo di gestione e controllo dei rischi operativi si articola nelle seguenti fasi sequenziali:

4.3.1 IDENTIFICAZIONE

L'"Identificazione" rappresenta l'attività di individuazione e raccolta delle informazioni relative ai rischi operativi attraverso il trattamento coerente e coordinato di tutte le fonti di informazione rilevanti. Si compone delle seguenti attività di:

Risk Self Assessment (RSA): tale processo si svolge con frequenza annuale, oltre che per i rischi operativi anche per quelli reputazionali, giungendo ad una valutazione ex-ante dei rischi cui un'unità organizzativa è esposta, sulla base di stime soggettive da parte dei responsabili della gestione del rischio e attraverso una valutazione dei controlli in essere. Le valutazioni sono integrate con le informazioni raccolte nel processo di gestione del rischio ICT e di sicurezza e includono scenari di rischio derivanti dall'esternalizzazione di attività o processi.

È prevista una fase di analisi preliminare basate sulla raccolta ed elaborazione di informazioni provenienti da diverse fonti interne ed esterne, tra le quali, in particolare, le evidenze del processo di Loss Data Collection.

Loss Data Collection (LDC): il processo è finalizzato all'individuazione, al censimento, alla validazione e al reporting delle perdite operative. L'attività di LDC consiste nella raccolta dell'ammontare dell'effetto economico generato da un evento operativo, corredato con tutte le informazioni rilevanti ai fini della misurazione e della gestione (inclusi i recuperi). Particolare attenzione viene posta nell'analisi degli eventi di maggiore gravità e scarsa frequenza, condividendo con le unità organizzative coinvolte apposite azioni di mitigazione.

Key Risk Indicators (KRI): raccolta e analisi di indicatori, al fine di individuare situazioni di possibile rischiosità operativa e reputazionale, anche potenziale, da sottoporre ad approfondimenti.

Specifiche analisi dell'esposizione ai rischi (c.d. **Generic Assessment)**, eseguite al fine di effettuare valutazioni ex ante, con particolare riferimento alla nascita di nuovi prodotti/servizi, all'avvio di nuovi processi operativi, all'ingresso in nuovi business o alla sottoscrizione/revisione di accordi di esternalizzazione.

4.3.2 MISURAZIONE

La Misurazione è l'attività di analisi e valorizzazione della rischiosità. E' un'attività finalizzata alla conoscenza completa del profilo di rischio complessivo aziendale e alla quantificazione di un:

- **Capitale Regolamentare;**
- **Capitale Economico.**

La misurazione del **Capitale Regolamentare** è effettuata, in collaborazione con l'Ufficio Bilancio Individuale e Consolidato di Banca Mediolanum, sulla base delle disposizioni normative e prevede l'applicazione di una metodologia di calcolo basata sulla classificazione delle attività delle società del Gruppo Bancario nelle otto linee di business regolamentari. A fronte di tale classificazione, viene calcolato il requisito di fondi propri individuale e di Gruppo Bancario applicando le apposite formule.

Flowe, che non è soggetta a requisito patrimoniale individuale a fronte dei rischi operativi, concorre al calcolo del requisito patrimoniale consolidato del Gruppo Bancario Mediolanum.

La misurazione del **capitale economico** di Gruppo Bancario si riferisce alla misurazione dei rischi ai fini interni, svolta utilizzando un approccio integrato che riflette sia le perdite effettive da rischi operativi che quelle potenziali, valutate al netto dell'efficacia dei controlli posti in essere per la loro mitigazione. Tale attività di misurazione si basa pertanto sulle risultanze del processo di identificazione dei rischi, applicando un modello statistico attuariale, e costituisce uno strumento di verifica dell'adeguatezza del capitale regolamentare a fronte dei rischi operativi.

Il modello di riferimento per la quantificazione del capitale economico può essere, pertanto, suddiviso in due macro-componenti:

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

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

4.3.3 MONITORAGGIO, CONTROLLO E REPORTING

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

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

Il principale strumento utilizzato nello svolgimento di tale processo è la produzione di reportistica per le funzioni aziendali interessate, le cui caratteristiche, in termini di contenuto e frequenza, sono sintetizzate nella tabella seguente:

Destinatario	Contenuto	Frequenza
Consiglio di Amministrazione / Amministratore Delegato	Resoconto attività annuali e pianificazione anno successivo	Annuale
Consiglio di Amministrazione / Amministratore Delegato	Informativa periodica sull'andamento dei controlli e sulle perdite operative	Semestrale
Amministratore Delegato	Condivisione ex-ante del piano di assessment ed ex-post dei risultati dello stesso	Annuale
Responsabili delle Unità Organizzative	Esiti assessment e azioni di mitigazione, eventuali perdite rilevanti e piani di azione	In sede di assessment e/o ad evento
Comitato Rischi della Capogruppo	Andamento periodico perdite operative di Gruppo Bancario (incluse eventuali perdite della Società)	Almeno trimestrale

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

Nell'ambito del Monitoraggio, Controllo e Reporting dei rischi operativi la Funzione contribuisce, inoltre, al processo di Risk Appetite Framework (RAF) di Gruppo.

4.3.4 GESTIONE

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

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

In base alle evidenze emerse in fase di analisi è possibile definire le politiche di gestione dei rischi operativi, la valutazione dell'opportunità di avviare eventuali progetti e piani di azione volti a mitigare i rischi operativi e la definizione delle priorità, anche rispetto ad altri progetti in corso, sono valutati, in primis, dai Responsabili delle Unità Organizzative (risk owner).

L'Unità Operational Risk Management svolge attività di rilevazione, monitoraggio e presidio dei piani di azione / azioni di mitigazione rispetto alle scadenze concordate, supporto

operativo, ove richiesto, e fornisce la necessaria informativa agli organi di controllo interno, attraverso la produzione di apposita reportistica.

La gestione attiva dei rischi operativi può essere completata anche attraverso l'insieme di attività che permettono di trasferire l'effetto finanziario su terzi e quindi attraverso soluzioni di natura assicurativa.

4.4 PROCESSO DI VALUTAZIONE DEI RISCHI CONNESSI ALLE ESTERNALIZZAZIONI

Al fine di presidiare i rischi derivanti dalle scelte effettuate in materia di esternalizzazione, Banca Mediolanum si è dotata di una politica di esternalizzazione predisposta in ottemperanza alla circolare n. 285 di Banca d'Italia "Disposizioni di vigilanza per le banche" e l'ha trasmessa anche alle altre società del Gruppo.

In particolare, il modello di controllo adottato prevede in capo all'Unità Operational Risk Management le attività di:

- valutazioni di impatto potenziale degli accordi di esternalizzazione in termini di rischi operativi (inclusi quelli ICT e legali) e reputazionali. La metodologia di valutazione applicata è conforme a quelle previste dai framework di controllo e gestione dei rischi operativi e reputazionali. In particolare, è prevista l'identificazione di scenari di eventi di rischio e dei relativi impatti potenziali, l'analisi dei fattori di rischio associati e delle misure previste per la loro mitigazione e, infine, una valutazione complessiva di rischio potenziale residuo. La valutazione tiene, inoltre, conto sia dei rischi associati ad eventuali sub-esternalizzazione che di quelli di concentrazione e derivanti dall'esternalizzazione di diverse funzioni a livello dell'ente;
- processi di monitoraggio nel continuo delle funzioni esternalizzate. La Funzione Risk Management raccoglie gli esiti delle attività di monitoraggio dei fornitori messe in atto dalle funzioni preposte e provvede ad integrare la reportistica periodica prodotta.

Inoltre, l'Unità provvede anche alla manutenzione e supervisione del registro delle esternalizzazioni che viene alimentato dalla stessa, per le informazioni di propria pertinenza, e dalle altre Funzioni coinvolte nel processo di gestione e monitoraggio delle esternalizzazioni.

4.5 PROCESSO DI CONTROLLO E GESTIONE DEL RISCHIO REPUTAZIONALE

Il processo di identificazione, valutazione e mitigazione dell'esposizione al rischio reputazionale è svolto nell'ambito delle attività di Risk Self Assessment condotte annualmente sulle diverse unità organizzative con riferimento ai rischi operativi. In tale sede, la Funzione Risk Management richiede ai responsabili delle unità organizzative, che svolgono attività con impatto sui valori critici percepiti dagli stakeholder, una valutazione qualitativa in merito all'esposizione al rischio reputazionale e analizza, inoltre, dati o documenti che possano portare a una migliore valutazione sull'adeguatezza dei presidi in essere. Tra questi elementi assumono particolare rilievo, tra gli altri, fattori quali i reclami ricevuti dalla clientela, gli esposti e le richieste ricevute dalla autorità di Vigilanza.

Qualora in sede di risk assessment emergano situazioni di criticità in termini di esposizione a possibili rischi reputazionali, la Funzione Risk Management condivide le azioni da porre in essere con il responsabile dell'unità organizzativa interessata e ne monitora la realizzazione.

A fronte di un evento ad alto impatto reputazionale, spetta al Responsabile della Funzione Risk Management, di concerto con i responsabili delle unità organizzative interessate, attivare un apposito contingency plan che individui e ponga in essere una specifica proposta di intervento a mitigazione del rischio reputazionale, con l'obiettivo di ridurre a un livello

ritenuto accettabile i possibili danni conseguenti a un incidente reputazionale, indentificando altresì le cause dell'evento per prevenirne un'eventuale ripetizione.

Gli esiti delle valutazioni effettuate sono tenuti in debito conto ai fini della pianificazione delle proprie attività e nella predisposizione delle relazioni periodiche agli Organi Aziendali.

In particolare, si richiama la Relazione annuale sul processo di controllo e presidio dei rischi operativi e reputazionali, presentata dal Responsabile della Funzione Risk Management di Flowe al Consiglio di Amministrazione, che riassume gli esiti delle attività svolte e riporta il piano delle attività per l'anno successivo per entrambe le fattispecie di rischio.

4.6 PROCESSO DI GESTIONE DEL RISCHIO ICT E DI SICUREZZA

La gestione del rischio ICT e di sicurezza è un processo articolato che si sviluppa nelle seguenti macro-fasi:

4.6.1 GOVERNANCE DEL RISCHIO ICT E DI SICUREZZA

Il processo di Governance del Rischio ICT e di Sicurezza ha come obiettivo definire e mantenere aggiornati il modello, la metodologia, il processo e le procedure di gestione del rischio ICT e di sicurezza, in relazione ai cambiamenti del contesto, dell'organizzazione e delle strategie ICT della Società, ai cambiamenti normativi ed all'evoluzione del panorama delle minacce IT. In tale ambito, il Risk Management si occupa della definizione e aggiornamento degli Scenari di Rischio ICT, dei cataloghi dei presidi di controllo, degli indicatori di rischio ICT (KRIs) e dei flussi informativi con le strutture di riferimento per le tematiche afferenti alla valutazione, gestione e monitoraggio del rischio ICT e di sicurezza.

L'Unità Operational Risk Management contribuisce, inoltre, alla definizione dei principi e delle regole ad alto livello in ambito Sicurezza Informatica e partecipa alla redazione della "Policy di sicurezza informatica".

4.6.2 VALUTAZIONE DEL RISCHIO ICT E DI SICUREZZA

Il Processo di Valutazione del Rischio ICT e di Sicurezza ha lo scopo di valutare il rischio ICT e di sicurezza a cui sono esposti gli asset ICT e si applica, inoltre, alle nuove iniziative/cambiamenti rilevanti, incluso il ricorso fornitori terzi nell'ambito dei servizi e sistemi ICT. La fase di valutazione del rischio ICT e di sicurezza è ripetuta, con frequenza almeno annuale, su tutte le applicazioni afferenti al Sistema Informativo della Società nell'ambito delle campagne annuali di assesment.

In tale ambito l'Unità Operational Risk Management:

- pianifica ed esegue la campagna di analisi del rischio ICT e di sicurezza periodica per le applicazioni in esercizio, che permette di identificarne il rischio residuo. In particolare, supporta l'Utente Responsabile nella stima degli impatti potenziali afferenti agli scenari di rischio ICT definiti per ciascuna applicazione in perimetro, mentre per quanto concerne la componente di probabilità di accadimento, collabora con gli IT risk control owner all'identificazione dell'efficacia dei presidi di sicurezza, anche attraverso verifiche specifiche. Infine, calcola il rischio residuo per le applicazioni in perimetro integrando la numerosità degli incident impattanti gli asset ICT;
- contribuisce, tramite verifiche di secondo livello, ad identificare eventuali rischi ICT e di sicurezza rivenienti dalle nuove iniziative/cambiamenti rilevanti, incluso il ricorso fornitori terzi nell'ambito dei servizi e sistemi ICT;

- definisce ed aggiorna i Key Risk Indicators (KRI), con il supporto dell'Unità IT Operation Security & Governance, per la valutazione nel continuo dell'esposizione al rischio ICT e sicurezza degli asset ICT, e più in generale, del Patrimonio Informativo della società;
- supporta l'Utente Responsabile, con il contributo dell'Unità IT Operation Security & Governance, nella definizione di eventuali misure compensative / presidi IT da integrare nei Piani di Trattamento, da definirsi anche in relazione al livello di propensione al rischio ICT e di sicurezza definito, e ne monitora l'implementazione.

4.6.3 MONITORAGGIO E REPORTING

L'Unità Operational Risk Management monitora costantemente il rischio residuo assunto dall'intermediario e la sua coerenza con gli obiettivi e l'appetito di rischio definiti, inoltre, predispone la reportistica inerente l'esito del Processo di Valutazione del Rischio ICT e di Sicurezza condividendo con gli Utenti Responsabili i report di accettazione del rischio residuo e curando annualmente la predisposizione di un Rapporto Sintetico sulla situazione del Rischio ICT e di sicurezza e relazione sulle risultanze dell'analisi dei rischi operativi e di sicurezza relativi ai servizi di pagamento da sottoporre al Consiglio di Amministrazione.

L'esito delle analisi svolte è, inoltre, messo a fattor comune con altre Unità Organizzative coinvolte nel complessivo presidio del rischio ICT e di sicurezza, tra cui *in primis* dell'Unità IT Operation Security & Governance.

Sono previsti, infine, opportuni flussi informativi al fine di integrare le rilevazioni svolte nell'ambito del framework di controllo dei rischi operativi con le evidenze raccolte nell'ambito del Processo di Valutazione del Rischio ICT sopra descritto.

4.7 PRINCIPALI STRUMENTI UTILIZZATI

A supporto dei processi e dei compiti attribuiti alla Funzione Risk Management si richiamano di seguito i principali strumenti informatici utilizzati:

- OpRisk Evolution applicativo a supporto attività di analisi dei rischi rispetto ai principali processi aziendali
- Sap e Easyfinance applicativi di contabilità generale e di consolidamento dei dati contabili a livello di Gruppo utilizzati per il calcolo del requisito patrimoniale e per l'espletamento delle attività propedeutiche alle segnalazioni di Vigilanza
- CMT- Cost Management, applicazione utilizzata per la gestione dei processi di budget, contratti fornitori, pratiche di spesa e autorizzazione fatture. Costituisce, inoltre, il principale repository delle informazioni presenti nel registro degli accordi di esternalizzazione conclusi dalle società italiane del Gruppo Bancario
- Strumenti di Office automation, soprattutto a supporto del processo di gestione del rischio ICT e di Sicurezza e, in generale, di reporting

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

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

5 Interrelazioni con le altre Unità Organizzative

Di seguito vengono elencate le principali Unità Organizzative che interagiscono con la Funzione Risk Management relativamente alle attività da quest'ultimo effettuate.

Per maggiori dettagli sui rapporti tra la Funzione e le altre Unità Organizzative con cui interagisce si rinvia alle Policy predisposte per i rischi operativi, ICT e di sicurezza, reputazionali e in materia di esternalizzazioni.

- **Collegio Sindacale** – E' chiamato ad esercitare il proprio ruolo istituzionale di vigilanza anche in relazione all'adeguatezza del framework integrato per la gestione ed il controllo dei rischi e al suo concreto funzionamento.
- **Alta Direzione** – L'Alta Direzione (Amministratore Delegato) partecipa al processo di controllo dei rischi, assumendo la responsabilità di contribuire alla definizione degli indirizzi strategici e gestionali in tema di rischi operativi, seguendo le linee guida definite dal Consiglio di Amministrazione e garantendo risorse e strumenti adeguati agli obiettivi.
- **Funzione Internal Audit** – Effettua un costante controllo finalizzato a verificare l'efficacia e l'efficienza del sistema dei controlli, evidenzia le eventuali mancanze presenti nel sistema, nelle procedure e nelle policy. Inoltre, con frequenza annuale, verifica il sistema di gestione e valutazione del rischio operativo e il processo di classificazione delle linee di attività regolamentari per le società che adottano metodologie di misurazione del requisito patrimoniale a fronte del rischio operativo di tipo standardizzato (tra cui Flowe).
- **Funzione Compliance** – L'implementazione di nuove regolamentazioni afferenti ai rischi non può prescindere dal rispetto della compliance normativa. L'unità si rapporta quindi con la Funzione Risk Management preposta al recepimento e rispetto della stessa per assicurare il dovuto allineamento normativo.
- **Divisione Amministrazione, Contabilità e Bilancio** – La Funzione Risk Management si confronta e collabora con la Divisone in particolare nell'ambito dei processi di controllo e gestione dei rischi operativi.
- **Funzione Antiriciclaggio** – E' responsabile, secondo un approccio risk based, del presidio del rischio di riciclaggio e finanziamento al terrorismo e degli adeguamenti dei processi sull'evoluzione del contesto normativo e procedurale in tale ambito. Sono possibili interrelazione con la Funzione Risk Management per le casistiche che rientrano nell'ambito dei rischi operativi.
- **IT Operation Security & Governance** – Interagisce con le Funzioni Risk Management e Compliance, nell'ambito delle analisi relative al rischio ICT e di sicurezza previste dal framework di controllo e gestione di tali rischi, e in relazione al ricorso a fornitori terzi per i servizi e sistemi ICT.
- **Organization & Business Continuity** – Interagisce con le Funzioni Risk Management in particolare con riferimento ai processi di Business Continuity, Data Governance e in relazione al ruolo svolto nell'ambito del monitoraggio degli outsourcer della società.

6 Il quadro normativo di riferimento

6.1 RIFERIMENTI NORMATIVI

Nel presente capitolo si richiama il contesto normativo nel quale opera il presente Regolamento di processo.

I principali riferimenti normativi alla base del presente documento riguardano:

- “Disposizioni di vigilanza per gli istituti di pagamento e gli istituti di moneta elettronica” di Banca d’Italia del 17 maggio 2016 e successivi aggiornamenti
- Circolare n. 285 del 17 dicembre 2013 - "Disposizioni di vigilanza per le banche" e successivi aggiornamenti
- Regolamento (UE) n. 575/2013 del Parlamento europeo e del Consiglio, del 26 giugno 2013, relativo ai requisiti prudenziali per gli enti creditizi e le imprese di investimento e che modifica il Regolamento (UE) n. 648/2012

6.2 RIFERIMENTI NORMATIVI AZIENDALI

L’operatività della Funzione Risk Management è regolamentata dalla normativa interna pubblicata e costantemente aggiornata nel Data Base aziendale.

Di seguito si riportano i riferimenti relativi ai documenti interni di Flowe, a cui si rimanda per gli opportuni approfondimenti e/o collegamenti rispetto ai contenuti riportati nel presente regolamento. In particolare, le versioni in vigore di:

- Relazione sulla Struttura Organizzativa
- Policy per il controllo e la gestione dei Rischi Operativi
- Policy in materia di esternalizzazioni
- Policy di gestione del Rischio ICT e di sicurezza
- Policy per il controllo del rischio di reputazione