Policy in materia di Esternalizzazioni

Consiglio di Amministrazione di Flowe S.p.A. del 21/02/2023

INDICE

1 Premessa

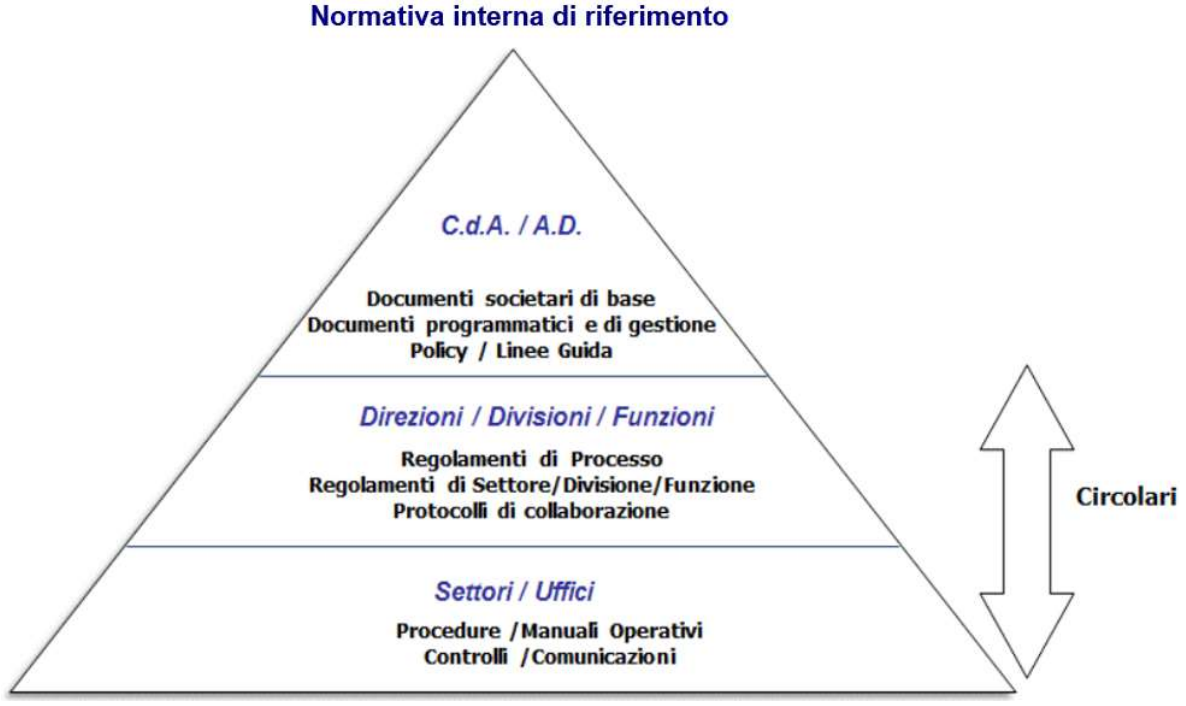
La presente Policy descrive i principi e le regole adottate da Flowe S.p.A. – Società Benefit o Flowe S.p.A. (nel prosieguo anche "Flowe" o "Società"), in qualità di Società facente parte del Gruppo Bancario Mediolanum, in relazione all'esternalizzazione di funzioni aziendali (nuove esternalizzazioni e gestione delle funzioni esternalizzate), in conformità agli "Orientamenti in materia di esternalizzazione" emanati da EBA il 25 febbraio 2019 (EBA/GL/2019/02) ed in ottemperanza alle disposizioni e principi espressi da Banca d'Italia nelle Disposizioni di vigilanza per gli istituti di pagamento e gli istituti di moneta elettronica emesse da Banca d'Italia il 23 luglio 2019.

2 Applicabilità

2.1 Destinatari del Documento

Facendo seguito alla Policy trasmessa da Banca Mediolanum con disposizione di Gruppo, nell'esercizio della funzione di direzione e coordinamento che le compete, è stato predisposto il presente documento, conforme ai principi e alle regole definite dalla Capogruppo che la Società ha recepito secondo le proprie specificità e che trova in essa diretta applicazione, previa approvazione da parte del Consiglio di Amministrazione della Società.

Il presente documento costituisce quindi un primo livello (di vertice) nella piramide riportata nello schema seguente, che raffigura il modello logico della normativa aziendale e richiamata dalla "Policy di Gruppo sulle modalità di redazione, aggiornamento, approvazione e diffusione della normativa interna" recepita da Flowe.



2.2 Responsabilità del Documento

L'aggiornamento e la revisione del presente documento sono di responsabilità della Funzione Risk Management della Banca, che svolge le attività di controllo dei rischi operativi per Flowe S.p.A. sulla base di un contratto di outsourcing, secondo quanto disposto dalla "Policy di Gruppo sulle modalità di redazione, approvazione, diffusione e aggiornamento della Normativa Interna".

Ogni modifica o integrazione sostanziale del Documento deve essere approvata dal Consiglio di Amministrazione della Società su proposta della Funzione Risk Management per cambiamenti di carattere operativo e, coordinandosi con la Funzione Compliance, per cambiamenti di carattere normativo.

2.3 Principi Generali

Si riportano di seguito gli elementi caratterizzanti della Policy coerenti con i requisiti minimi previsti dalle disposizioni di Banca d'Italia[1] in tema di esternalizzazione.

Si precisa che la presente Policy è mirata a normare il processo di esternalizzazione di funzioni aziendali nella loro più ampia accezione: Funzioni Essenziali o Importanti (FEI) e Funzioni Non Essenziali o Importanti (NFEI), ed è finalizzata a presidiare i rischi derivanti dalle scelte effettuate in materia di esternalizzazione e prevede una chiara distinzione in base alla tipologia di attività esternalizzata e alla rilevanza ed importanza all'interno della Società.

In quest'ottica, il presente documento si applica al seguente perimetro:

- casistiche in base alle quali la Società decida di esternalizzare una funzione ritenuta essenziale o importante (FEI) all'interno del Gruppo (attività intra-gruppo) o all'esterno verso fornitori terzi (attività extra-gruppo), previa comunicazione alla Banca d'Italia nella modalità indicata dalle Disposizioni di vigilanza per gli istituti di pagamento e gli istituti di moneta elettronica emesse da Banca d'Italia il 23 luglio 2019;
- casistiche relative a funzioni classificate come NFEI (Funzioni Non Essenziali o Importanti) per le quali il processo decisionale di contrattualistica e gli aspetti concernenti il parco fornitori, il cambio degli stessi o l'inserimento di ulteriori outsourcer per determinate attività segue quanto già normato dalla Procedura Operativa di Gestione della Spesa della Capogruppo. Anche in questo caso l'accordo potrebbe essere concluso all'interno del Gruppo. Particolare rilevanza, assumono gli accordi appartenenti a questo perimetro che, pur non avendo ad oggetto Funzioni Essenziali o Importanti, sono classificati come Esternalizzazioni.

In linea con tale finalità si recepiscono i principi normativi minimi menzionati all'interno delle Disposizioni di vigilanza per gli istituti di pagamento e gli istituti di moneta elettronica emesse da Banca d'Italia il 23 luglio 2019 e dagli Orientamenti EBA del 25 Febbraio 2019 (EBA/GL/2019/02), con riferimento ai quali la Società deve attenersi nella decisione di esternalizzare qualsiasi funzione aziendale.

2.4 Limitazioni

Le Società del Gruppo Bancario, attraverso il ricorso all'esternalizzazione, non possono:

- delegare le proprie responsabilità, né la responsabilità degli Organi Aziendali;
- alterare il rapporto e gli obblighi nei confronti dei clienti nella prestazione dei servizi di pagamento o
- nell'attività di emissione di moneta elettronica;
- mettere a repentaglio il rispetto delle condizioni che la stessa deve soddisfare per poter essere autorizzata all'attività di emissione di moneta elettronica e per conservare tale autorizzazione;
- pregiudicare la qualità del sistema di controllo interno;
- ostacolare la vigilanza.

L'esternalizzazione di compiti operativi delle funzioni aziendali di controllo è ammessa nel rispetto del principio di proporzionalità. Resta ferma la responsabilità degli organi aziendali e del responsabile della funzione esternalizzata per il corretto svolgimento dei compiti esternalizzati.

2.5 Struttura del Documento

Il presente documento risulta articolato nei seguenti capitoli, oltre ai primi due di carattere introduttivo:

- **Capitolo 3 – Definizioni**: descrizione delle principali definizioni adottate nell'ambito del presente documento;
- **Capitolo 4** – **Ruoli e Responsabilità**: descrizione dei ruoli e delle responsabilità delle funzioni di controllo e delle principali unità organizzative coinvolte nel processo di valutazione di una funzione esternalizzata;
- **Capitolo 5** – **I principi in tema di esternalizzazione**: definizioni ed esempi di esternalizzazione, funzione essenziale o importante, sub-esternalizzazione, ecc.;

[1] Disposizioni di vigilanza per gli istituti di pagamento e gli istituti di moneta elettronica emesse da Banca d'Italia il 23 luglio 2019.

- **Capitolo 6** – **Processi di gestione di esternalizzazione**: descrizione dei processi di gestione di nuove esternalizzazioni (sia FEI che non) e successivo monitoraggio;
- **Capitolo 7** – **Quadro normativo di riferimento;**
- **Capitolo 8** – **Allegato.**

3 Definizioni

3.1 Definizione dei termini utilizzati

Di seguito, si riportano le principali definizioni adottate nell'ambito del presente documento:

A. Organo con Funzione di Supervisione Strategica (OFSS): l'Organo aziendale a cui – ai sensi del Codice civile o per disposizione statutaria – sono attribuite le funzioni di indirizzo e/o supervisione della gestione dell'impresa. Ciascuna Società del Gruppo individua, nell'ambito della propria regolamentazione interna, il proprio OFSS; Flowe individua tale Organo nel Consiglio di Amministrazione;

B. Organo con Funzione di Gestione (OFG): l'Organo aziendale o i componenti di esso a cui – ai sensi del Codice civile o per disposizione statutaria – spettano o sono delegati compiti di gestione corrente, intesa come attuazione degli indirizzi deliberati nell'esercizio della funzione di supervisione strategica. Ciascuna Società del Gruppo individua, nell'ambito della propria regolamentazione interna, il proprio OFG; Flowe individua tale Organo nell'Amministratore Delegato;

C. Organo con Funzione di Controllo (OFC): l'Organo aziendale che vigila sull'osservanza delle norme di legge, regolamentarie e statutarie, sulla corretta amministrazione, sull'adeguatezza degli assetti organizzativi e contabili della Società. Ciascuna Società del Gruppo individua, nell'ambito della propria regolamentazione interna, il proprio OFC; Flowe individua tale Organo nel Collegio Sindacale;

D. Esternalizzazione: un accordo di qualsiasi forma tra la Società e un fornitore di servizi, interno o esterno al Gruppo, in base al quale quest'ultimo svolge un processo, un servizio o un'attività che sarebbe altrimenti svolto dalla Società. Le Società del Gruppo Bancario che procedono ad esternalizzare una funzione applicheranno questa definizione avendo a riferimento il proprio perimetro di servizi ed attività;

E. Esternalizzazione Infra-Gruppo: l'affidamento di un processo/ servizio o un'attività propria della Società o altra Società del Gruppo Bancario all'interno del Conglomerato;

F. Esternalizzazione Extra-Gruppo: l'affidamento di un processo/ servizio o un'attività propria della Società o altra Società del Gruppo Bancario verso fornitori esterni al Conglomerato;

G. Funzione: qualsiasi processo, servizio o attività;

H. Funzione Aziendale: l'insieme dei compiti e delle responsabilità assegnate per l'espletamento dell'operatività aziendale (processo, servizio o attività) ed incardinati presso una specifica struttura organizzativa. Le strutture organizzative e le relative responsabilità sono disciplinate nell'ambito della normativa interna della Società e delle Società del Gruppo Bancario.

I. Funzione essenziale o importante (FEI): funzione della Società per la quale è verificata almeno una delle seguenti condizioni:

   - un'anomalia nella sua esecuzione o la sua mancata esecuzione possono compromettere gravemente:
     - i suoi risultati finanziari o la solidità o la continuità dei suoi servizi di pagamento o dell'attività di emissione di moneta elettronica;
     - la capacità di conformarsi nel continuo alle condizioni e agli obblighi derivanti dalla sua autorizzazione o agli obblighi previsti dalla disciplina di vigilanza;
     - costituire un pregiudizio per il regolare funzionamento del sistema dei pagamenti;
   - riguarda funzioni relative ad attività sottoposte a riserva di legge, nella misura in cui la prestazione di tali attività richiede l'autorizzazione da parte di un'autorità di vigilanza;
   - sono esternalizzati compiti operativi delle funzioni di controllo interno, a meno che la valutazione non stabilisca che la mancata esecuzione della funzione esternalizzata o

un'esecuzione inadeguata della stessa non avrebbe un impatto negativo sull'efficacia della funzione di controllo interno.

J. Funzioni aziendali di controllo (FAC): nell'ambito delle Funzioni Essenziali o Importanti, definite al punto precedente, si definiscono Funzioni Aziendali di Controllo le seguenti:

- la funzione di conformità alle norme (Compliance);
- la funzione di controllo rischi (Risk Management);
- la funzione di revisione interna (Internal Auditing);
- la funzione Antiriciclaggio;

K. Fornitore di servizi (outsourcer): soggetto terzo (identificato sia all'interno che all'esterno del Gruppo) che svolge, in tutto o in parte, una funzione esternalizzata nell'ambito di un accordo di esternalizzazione;

L. SLA (Service Level Agreement): accordo formalizzato contrattualmente tra la Società e un fornitore di un servizio atto a esplicitare i livelli di servizio (ad esempio, natura, qualità, tempistiche) che devono essere rispettati nel rapporto di fornitura. Tale accordo dovrebbe includere precisi obiettivi di performance, quantitativi e qualitativi, per la funzione esternalizzata;

M. Sistema informativo: insieme delle risorse tecnologiche e informative (ad esempio, hardware, software, dati, documenti elettronici, reti telematiche) e delle relative risorse umane, interconnessioni, processi/modelli organizzativi destinati al loro governo;

N. Servizi cloud: Servizi forniti tramite cloud computing, ossia un modello che consente l'accesso in rete diffuso, conveniente e su richiesta a un gruppo condiviso di risorse elettroniche configurabili (ad esempio reti, server, memorie, applicazioni e servizi), che possono essere forniti e messi a disposizione rapidamente con minimo impegno gestionale o interazione con il fornitore del servizio;

O. Due Diligence: è definita *due diligence* il complesso di attività organizzate finalizzate alla raccolta ed alla verifica, mirata ed analitica, di informazioni effettuate nei confronti dei fornitori;

P. Sub-esternalizzazione: una situazione in cui il fornitore di servizi nell'ambito di un accordo di esternalizzazione trasferisce ulteriormente una funzione esternalizzata a un altro fornitore di servizi (qui definito sub-fornitore);

Q. Funzione di Esternalizzazione: la funzione responsabile della gestione e supervisione dei rischi connessi agli accordi di esternalizzazione nell'ambito del sistema dei controlli interni dell'ente e della manutenzione e supervisione del registro delle esternalizzazioni;

R. Funzione Richiedente: è la funzione aziendale *owner* del processo che ne propone l'esternalizzazione e avvia il processo di valutazione. In caso di approvazione della proposta di esternalizzazione, è la funzione responsabile del processo in outsourcing e ne assicura idoneo presidio e controllo attraverso il Referente Contrattuale (che generalmente è il responsabile del Centro di Responsabilità) e il Referente Operativo; fornisce, inoltre, alle funzioni di controllo l'opportuna informativa sull'andamento dell'esternalizzazione;

S. Referente per le Attività Esternalizzate (RAE) / Responsabile operativo dei servizi affidati in outsourcing: per le Società del Gruppo Bancario diverse da Banca Mediolanum, qualora previsti, sono i responsabili del controllo di singole funzioni esternalizzate, dotati di adeguati requisiti di professionalità e identificati all'interno della Società che esternalizza. Nello specifico, i RAE presidiano le attività e i servizi svolti in outsourcing dalle funzioni di controllo della Banca (in caso di Esternalizzazione Infra-Gruppo) e relazionano almeno annualmente il Consiglio di Amministrazione della Società che esternalizza sui risultati delle attività di verifica svolte; Flowe ha identificato un RAE in materia di Antiriciclaggio, Compliance e Risk Management e un RAE in materia di Internal Auditing in due Amministratori indipendenti e non esecutivi della Società. Invece, il Responsabile operativo dei servizi affidati in outsourcing presidia e relaziona almeno annualmente il Consiglio della società in relazione alle attività esternalizzate al di fuori del Gruppo e a quelle diverse dalle funzioni di controllo affidate alla Capogruppo;

T. Referente Contrattuale: è il soggetto formalmente individuato quale interlocutore del fornitore per tutti gli aspetti connessi con gli adempimenti contrattuali "generali" quali a titolo esemplificativo e non esaustivo:

- pianificazione del servizio in termini di volumi e livelli di servizio (SLA);

- modalità di svolgimento del servizio;
- verifiche periodiche sull'andamento del servizio (Comitati Tecnici o incontri periodici con il fornitore per la discussione degli SLA);
- rilevazione anomalie e gestione contenzioso operativo con il fornitore;

U. Responsabile Operativo dei servizi affidati in outsourcing: è il soggetto designato formalmente al controllo del corretto svolgimento delle attività operative affidate in outsourcing alla Capogruppo e ai fornitori esterni al Gruppo Mediolanum, verificando il rispetto dei livelli di servizio concordati e relazionandosi con i referenti contrattuali e/o operativi per la raccolta delle informazioni necessarie. Flowe ha identificato e nominato il Responsabile dell'unità Organization & Business Continuity quale Responsabile Operativo dei servizi affidati in outsourcing;

V. Referente Operativo: è il soggetto designato formalmente al monitoraggio, controllo e presidio della funzione esternalizzata, dev'essere comunicato al Fornitore e, in assenza di una specifica designazione del Referente Operativo, questi viene identificato nel Referente Contrattuale. Tra i suoi principali compiti rientrano:

- definizione e monitoraggio nel continuo del rispetto degli SLA, segnalando ai fornitori (outsourcers) eventuali problematiche operative;
- aggiornamento del Referente Contrattuale sull'andamento ordinario della funzione esternalizzata;
- attivazione in caso di discontinuità della funzione segnalata dal fornitore;
- interazione con il Fornitore in merito a richieste di intervento ordinarie in caso di disservizi, segnalazioni di discontinuità della funzione (es. scioperi, assenza, problemi di continuità operativa) di carattere contingente;
- trasmissione periodica al Responsabile Operativo dei servizi affidati in outsourcing delle informazioni relative all'andamento del rapporto con il fornitore e necessarie alla redazione della "Rendicontazione sulle attività di verifica svolte sull'operato delle Funzioni operative esternalizzate".

In alcuni casi, ad esempio per attività esternalizzate alla Capogruppo, il Referente Operativo può coincidere con il Responsabile Operativo dei servizi affidati in outsourcing della Società.

W. Registro delle Esternalizzazioni: registro delle informazioni concernenti tutti gli accordi di esternalizzazione;

X. Scheda di valutazione delle Esternalizzazioni: allegato A della presente policy costituita da 5 sezioni:

- Sezione A: da compilare a cura della Funzione Richiedente per specificare se la Funzione può essere classificata come esternalizzazione o acquisto;
- Sezione B: da compilare a cura della Funzione Richiedente;
- Sezione C: da compilare a cura della Funzione Richiedente al fine di indicare i motivi, gli obiettivi, il perimetro, i costi, i benefici, i rischi, la durata, i potenziali conflitti di interesse, la strategia di uscita e i fornitori alternativi con riferimento alla Funzione che si intende esternalizzare e se è prevista la possibilità di sub-esternalizzazione;
- Sezione D: da compilare a cura della Funzione Compliance e Risk Management per specificare se la Funzione può essere classificata come Funzione Essenziale o Importante;
- Sezione E: da compilare a cura della Funzione Compliance e Risk Management per esprimere, rispettivamente, il proprio parere formale e la valutazione dei rischi, anche con riferimento ai termini di efficacia temporale dell'accordo di Esternalizzazione con il Fornitore di servizi (outsourcer) ed alle eventuali comunicazioni dovute a Banca d'Italia;

Y. Risorsa ICT: un bene dell'azienda afferente all'ICT che concorre alla ricezione, archiviazione, elaborazione, trasmissione e fruizione dell'informazione gestita dalla Banca;

Z. Sistemi ICT: ICT adottata come parte di un meccanismo o di una rete di interconnessione a supporto delle operazioni della Banca e delle Società appartenenti al Gruppo;

AA. Servizi ICT: i servizi forniti dai sistemi ICT a uno o più utenti interni o esterni. Tali servizi comprendono ad esempio: servizi di inserimento, archiviazione, elaborazione e comunicazione di dati, ma anche servizi di monitoraggio, di supporto alle attività e alle decisioni aziendali;

BB. Principali servizi ICT: i servizi nell'ambito degli accordi che richiedono l'autorizzazione del Consiglio di Amministrazione come da Regolamento del Processo di Gestione della Spesa di Flowe.

4 Ruoli e Responsabilità

La Banca, nell'ambito del proprio ruolo di coordinamento, può definire strategie generali di esternalizzazione, a cui tutte le Società del Gruppo Bancario si conformano. Le singole Società del Gruppo Bancario possono definire specifiche strategie di esternalizzazione, nell'ambito del complessivo disegno definito dalla Capogruppo.

Il processo di gestione e controllo in materia di esternalizzazione è in ogni caso governato dall'Organo con Funzione di Supervisione Strategica (di seguito, alternativamente "OFSS") di ciascuna Società del Gruppo. Spetta all'Organo con Funzione di Gestione (di seguito, anche "OFG") di ciascuna Società del Gruppo assicurare la corretta applicazione della presente Politica, nonché delle strategie definite dall'OFSS.

L'Organo con Funzione di Controllo (di seguito, alternativamente "OFC") di ciascuna Società del Gruppo vigila sul corretto funzionamento e osservanza del modello organizzativo e gestionale adottato dalla stessa. L'OFC della Capogruppo, inoltre, supervisiona sulla complessiva tenuta e osservanza del modello definito dalla presente Politica, per il Gruppo nella sua interezza.

4.1 Funzioni Aziendali di Controllo

Gli esiti delle verifiche effettuate dalle Funzioni Aziendali di Controllo, nonché le rispettive valutazioni sulla complessiva esposizione al rischio da parte delle Società del Gruppo e del Gruppo nel suo complesso, sono periodicamente portati a conoscenza dei competenti Organi aziendali, al fine di garantire a questi ultimi la piena conoscenza e governabilità dei fattori di rischio derivanti dalle strategie di esternalizzazione adottate.

A. Funzione Risk Management

Flowe ha affidato alla Capogruppo Banca Mediolanum la gestione delle attività di Risk Management sulla base del contratto di servizi stipulato tra le due Società. La Funzione Risk Management, nel modello organizzativo della Società, ricopre il ruolo di Funzione di Esternalizzazione[2] ed è quindi responsabile della gestione e supervisione dei rischi connessi agli accordi di esternalizzazione nell'ambito del sistema dei controlli interni dell'ente e della manutenzione del registro delle esternalizzazioni.

Relaziona annualmente il Consiglio di Amministrazione della Società in merito alle funzioni esternalizzate e garantisce la standardizzazione del modello di gestione delle esternalizzazioni definito nella presente policy e il presidio del processo di esternalizzazione, monitorando e condividendo i relativi cambiamenti con tutti gli attori responsabili delle singole attività in ambito.

La Funzione Risk Management è inoltre responsabile, della gestione e della manutenzione del registro delle esternalizzazioni che viene alimentato dalla stessa Funzione Risk Management, per le informazioni di propria pertinenza, e dalle altre Funzioni coinvolte nel processo di gestione e monitoraggio delle esternalizzazioni.

La Funzione Risk Management viene coinvolta dalla Funzione Richiedente nel processo di gestione di tutte le nuove esternalizzazioni (sia di quelle che possono essere considerate Funzioni Essenziali o Importanti che non), per analizzare preventivamente i possibili rischi operativi, reputazionali e, di concerto con la Funzione Compliance, quelli di non conformità connessi con l'esternalizzazione e l'individuazione degli eventuali presidi da porre in essere.

La Funzione Risk Management è chiamata, in particolare, ad esprimere una propria valutazione dei rischi in merito all'esternalizzazione delle attività aziendali per tutte le esternalizzazioni (non solo per le Funzioni Essenziali o Importanti). Tale valutazione deve considerare anche i rischi associati a eventuali sub-esternalizzazioni.

È, inoltre, compito della Funzione Risk Management predisporre ed inviare a Banca d'Italia la comunicazione prevista dalle Disposizioni di vigilanza per gli istituti di pagamento e gli istituti di moneta elettronica emesse da Banca d'Italia il 23 luglio 2019, dopo l'approvazione da parte degli organi competenti e almeno 60 giorni prima di darne corso, o nei tempi eventualmente diversamente stabiliti dalle Autorità di Vigilanza competenti, con riferimento all'esternalizzazione di Funzioni Essenziali o Importanti o di controllo, e, in aggiunta, inviare alla

[3]Nel seguito del documento quando si fa riferimento alla Funzione Risk Management viene, salvo diversamente precisato, inteso il suo ruolo di Funzione di Esternalizzazione.

competente Autorità di Vigilanza l'informativa eventualmente prevista per le esternalizzazioni che riguardano servizi in cloud, secondo le modalità ed i termini stabiliti dalla normativa di riferimento della Società tempo per tempo vigente.

La Funzione Risk Management viene coinvolta dalla Funzione Richiedente, altresì, anche nel processo di monitoraggio di un'esternalizzazione già esistente al fine di valutare se, eventuali variazioni di perimetro della funzione esternalizzata, o di sub-fornitori, potrebbero modificare i possibili rischi (operativi, reputazionali, di non conformità) connessi con l'esternalizzazione e i presidi posti in essere ed eventualmente modificare la classificazione dell'accordo, di concerto con la Funzione Compliance ove necessario.

B. Funzione Compliance

Flowe ha affidato alla Capogruppo Banca Mediolanum la gestione delle attività di Compliance sulla base del contratto di outsourcing stipulato tra le due Società. La Funzione Compliance viene coinvolta obbligatoriamente dalla Funzione Richiedente nel processo di gestione e monitoraggio delle esternalizzazioni che possono essere considerate Funzioni Essenziali o Importanti.

In tutti gli altri casi il coinvolgimento, su richiesta della Funzione Richiedente o della Funzione Risk Management, è facoltativo ed è finalizzato a fornire un supporto alla classificazione dell'accordo come esternalizzazione (FEI o NFEI) o come acquisto.

Laddove coinvolta, nei termini sopraindicati, la Funzione analizza i possibili rischi di non conformità e gli eventuali conflitti di interesse connessi con l'esternalizzazione e individua gli eventuali presidi da porre in essere. Il risultato dell'analisi è riportato in un parere nella Scheda di valutazione delle esternalizzazioni allegata alla presente Policy.

La Funzione Compliance viene coinvolta dalla Funzione Richiedente, altresì, anche nel processo di monitoraggio di un'esternalizzazione già esistente (sia FEI che NFEI) al fine di valutare se eventuali variazioni di perimetro della funzione esternalizzata potrebbero modificare i possibili rischi di non conformità, connessi con l'esternalizzazione ed eventualmente modificare la classificazione dell'accordo.

C. <u>Funzione Internal Audit</u>

Flowe ha affidato alla Capogruppo Banca Mediolanum la gestione delle attività di Internal Auditing sulla base del contratto di servizi stipulato tra le due Società. La Funzione Internal Audit è responsabile di verificare, anche attraverso accertamenti di natura ispettiva, la regolarità delle diverse attività aziendali, incluse quelle esternalizzate, e l'evoluzione dei rischi nella direzione generale della Società. La frequenza delle ispezioni è coerente con l'attività svolta e la propensione al rischio.

4.2 Altre Funzioni

A. Referente per le Attività Esternalizzate

Il RAE, presso le Società del Gruppo Bancario diverse da Banca Mediolanum, presidia le attività e i servizi svolti in outsourcing dalle funzioni di controllo della Banca (in caso di Esternalizzazione Infra-Gruppo), come definito nell'ambito degli appositi SLA, attraverso la rendicontazione semestrale fornita da tali strutture della Banca (Esternalizzazione Infra-Gruppo) attraverso apposite schede di controllo, contenenti i dettagli delle attività svolte dall'outsourcer nel semestre di riferimento. Con riferimento a Flowe, tali schede sono raccolte e trasmesse ai RAE dai responsabili delle Funzioni Aziendali di Controllo della Società.

I risultati dell'attività svolta dall'outsourcer contenuti nella rendicontazione ricevuta sono valutati con riferimento al corretto svolgimento delle attività, al rispetto degli impegni assunti e al livello di qualità del servizio ricevuto, nonché alla rispondenza agli SLA definiti fra le Società.

I RAE relazionano almeno annualmente il Consiglio di Amministrazione della Società che esternalizza, sui risultati delle attività di verifica svolte.

B. Responsabile operativo dei servizi affidati in outsourcing

Il Responsabile operativo dei servizi affidati in outsourcing, presso le Società del Gruppo Bancario diverse da Banca Mediolanum, presidia le attività e i servizi:

- esternalizzati al di fuori del Gruppo, avvalendosi della collaborazione dei rispettivi Referenti Contrattuali e attraverso il monitoraggio periodico (almeno semestrale) degli appositi SLA e, in generale, della reportistica fornita dagli outsourcer;

- affidati alle funzioni non di controllo della Capogruppo, attraverso il monitoraggio degli appositi SLA e la rendicontazione semestrale fornita da tali strutture della Banca in apposite schede di controllo, contenenti i dettagli delle attività svolte dall'outsourcer nel semestre di riferimento.

I risultati dell'attività svolta dagli outsourcer sono valutati con riferimento al corretto svolgimento delle attività, al rispetto degli impegni assunti e al livello di qualità del servizio ricevuto, nonché alla rispondenza ai SLA definiti fra le Società.

Il Responsabile operativo dei servizi affidati in outsourcing relaziona almeno annualmente il Consiglio di Amministrazione della Società che esternalizza sui risultati delle attività di verifica svolte.

C. Funzione Richiedente

È la funzione aziendale che propone di esternalizzare una funzione e avvia il processo di gestione e valutazione inviando la scheda di valutazione delle esternalizzazioni (allegato A della presente policy) compilata in tutte le sezioni di propria competenza, compresa l'indicazione di eventuali sub-fornitori.
In caso di approvazione della proposta di esternalizzazione, è la funzione responsabile del processo in outsourcing e ne assicura idoneo presidio e controllo attraverso il Referente Contrattuale (che generalmente coincide con il responsabile del Centro di Responsabilità) e il Referente Operativo; fornisce, inoltre, alle Funzioni di Controllo e al Responsabile operativo dei servizi affidati in outsourcing, almeno su base semestrale, l'opportuna informativa sull'andamento dell'esternalizzazione.
La Funzione Richiedente è, altresì, responsabile di avviare il processo di monitoraggio di una funzione esternalizzata, inviando la scheda di valutazione delle esternalizzazioni compilata in tutte le sezioni di propria competenza, al fine di verificare, di concerto con la Funzione Risk Management e la Funzione Compliance, se eventuali variazioni di perimetro della funzione esternalizzata, o di sub-fornitori, potrebbero modificare la classificazione dell'accordo.

D. Divisione Acquisti (attività affidata in outsourcing a Banca Mediolanum)

La Divisione Acquisti è responsabile dello sviluppo e della gestione della relazione commerciale con i Fornitori e della standardizzazione dei processi di selezione, negoziazione e formalizzazione degli accordi (in collaborazione con la Divisione Affari Legali e la Divisione Affari Fiscali di Banca Mediolanum).

È responsabile, inoltre, dell'esecuzione del processo di *due diligence* sui potenziali fornitori di servizi, secondo quanto definito nel paragrafo 5.2.

E. Unità Organization & Business Continuity (di Flowe)

L'Unità Organization & Business Continuity di Flowe collabora con la Funzione Risk Management nel presidio del processo sia di nuove esternalizzazioni che del successivo monitoraggio e, in caso di eventuali cambiamenti di processo, aggiorna e condivide le relative modifiche con tutti gli attori responsabili delle singole attività.

Nell'ambito del processo di gestione di una nuova esternalizzazione viene coinvolta obbligatoriamente dalla Funzione Richiedente e si coordina con la Divisione Pianificazione, Controllo e Investor Relations e la Direzione Risorse Umane di Banca Mediolanum per una valutazione Make or Buy sulla base della convenienza economica della esternalizzazione rispetto a soluzioni "in house" e alla luce dell'efficiente impiego di risorse aziendali disponibili presso altre unità organizzative. L'Unità Organization & Business Continuity, ricevuta la scheda di valutazione delle esternalizzazioni, verifica quanto riportato in merito all'analisi che ha condotto.

L'Unità Organization & Business Continuity viene, inoltre, coinvolta per le opportune valutazioni in merito ai piani di continuità operativa del fornitore e per le conseguenti eventuali integrazioni di quelli della società e dei relativi test, ogni volta che l'esternalizzazione riguarda attività operativi critiche in termini di tempo. Per tali valutazioni, può avvalersi del supporto del Business Continuity Office della Capogruppo.

F. Divisione Pianificazione, Controllo e Investor Relations (attività affidata in outsourcing a Banca Mediolanum)

La Divisione Pianificazione, Controllo e Investor Relations collabora con l'Unità Organization & Business Continuity e la Direzione Risorse Umane di Banca Mediolanum nel processo di gestione delle nuove

esternalizzazioni al fine di effettuare un'analisi Make or Buy per stabilire l'effettiva convenienza economica nell'affidare il processo in outsourcing.

G. Direzione Risorse Umane (attività affidata in outsourcing a Banca Mediolanum)

La Direzione Risorse Umane collabora con la Divisione Pianificazione, Controllo e Investor Relations e con l'Unità Organization & Business Continuity di Flowe nel processo di gestione delle nuove esternalizzazioni al fine di effettuare un'analisi Make or Buy per stabilire l'effettiva convenienza economica nell'affidare il processo in outsourcing alla luce dell'efficiente impiego di risorse aziendali disponibili presso altre unità organizzative.

H. Divisione Affari Legali e Divisione Affari Fiscali (attività affidata in outsourcing a Banca Mediolanum)

La Divisione Affari Legali e la Divisione Affari Fiscali collaborano con la Divisione Acquisti di Banca Mediolanum sia nel processo di gestione delle nuove esternalizzazioni che nel successivo monitoraggio, al fine di formalizzare l'accordo con il fornitore di servizi e garantire che i modelli contrattuali siano rispettati.

I. Augmented Intelligence

Supporta la Funzione Richiedente e si coordina con la Funzione Risk Management, sia nel processo di gestione di una nuova esternalizzazione che nel processo di monitoraggio, al fine di identificare, avvalendosi della collaborazione dell'Unità IT Security (in outosurcing presso Banca Mediolanum), le misure di attenuazione dei rischi informatici che il fornitore di servizi deve garantire, per essere conforme a quelle identificate dalla Società.

5 I Principi in tema di esternalizzazione

5.1 Esternalizzazione

La normativa specifica che per esternalizzazione va inteso ogni accordo in qualsiasi forma tra una Società e un fornitore di servizi in base al quale il fornitore realizza, in tutto o in parte, un processo, un servizio o un'attività che altrimenti sarebbe svolta dalla Società.
Per determinare se un accordo con un soggetto terzo (identificato sia all'interno che all'esterno del Gruppo) rientra nella definizione di esternalizzazione, occorre considerare se la Funzione (o parte di essa) esternalizzata a un fornitore di servizi è eseguita su base ricorrente o continuativa dal fornitore di servizi stesso e se tale funzione (o parte di essa) rientrerebbe in genere nell'ambito delle funzioni che sarebbero o potrebbero realisticamente essere svolte da Flowe, anche qualora quest'ultima non abbia svolto tale funzione in passato.
La scelta di ricorrere all'esternalizzazione deve essere presa valutando i possibili scenari di rischio (operativi, strategici, di compliance e reputazionali) collegati all'operazione e delle misure idonee alla mitigazione degli stessi ed alle potenziali ricadute sulla Società.

Flowe, al pari di tutte le Società del Gruppo non considera esternalizzazione, a titolo esemplificativo:

- una funzione che a norma di legge deve essere svolta da un fornitore di servizi, ad esempio la revisione legale dei conti;
- i servizi di informazione sui mercati (ad esempio la fornitura di dati da parte di Bloomberg, Moody's, Standard & Poor's, Fitch);
- le infrastrutture di rete globali (ad esempio MasterCard);
- gli accordi di compensazione e regolamento tra organismi di compensazione, controparti centrali e istituti di regolamento e loro membri;
- le infrastrutture globali di messaggistica finanziaria soggette alla vigilanza delle pertinenti autorità;
- i servizi bancari di corrispondenza;
- l'acquisizione di servizi che altrimenti non sarebbero intrapresi dall'ente o dall'istituto di pagamento (ad esempio, la consulenza di un architetto, pareri legali e rappresentanza legale di fronte a un tribunale e a organi amministrativi, servizi di pulizia, giardinaggio e manutenzione dei locali della

Banca, servizi medici, manutenzione di automobili aziendali, servizi di ristorazione, servizi di distribuzione automatica, servizi amministrativi, servizi di business travel, servizi postali, servizi di receptionist, segreteria e centralino), beni (ad esempio, tessere di plastica, lettori di carte, forniture per ufficio, personal computer, mobilio) o servizi di pubblica utilità (ad esempio, forniture di elettricità, gas, acqua, telefonia).

È importante che gli approcci implementati vertano a contenere, se possibile, il rischio di concentrazione verso specifici fornitori. Questo requisito risulta essere strategico per Flowe e le altre Società del Gruppo al fine di salvaguardare la possibilità di sostituire determinate forniture con altre funzionalmente equivalenti prevedendo adeguate exit strategies. Il rischio di concentrazione può essere determinato dall'utilizzo di fornitori non facilmente sostituibili per la specifica funzione o dalla somma di più accordi con lo stesso fornitore o con fornitori strettamente connessi.
La valutazione dell'esternalizzazione, laddove possibile, deve essere documentata e deve stimare in che misura aumenterebbe o ridurrebbe il rischio operativo facendo uso di dati sulle possibili perdite e sugli scenari.

Inoltre, nel caso in cui l'esternalizzazione fosse relativa ad attività bancaria o nell'ambito dei servizi di pagamento per la cui esecuzione è richiesta l'autorizzazione da un'autorità competente (di uno stato membro), il fornitore deve essere registrato o autorizzato da un'autorità competente o in base alla normativa di riferimento. Nel caso in cui il fornitore fosse situato in uno stato terzo dovrebbe essere verificato, in fase di scelta, il soddisfacimento delle condizioni specifiche previste dalle linee guida (paragrafo 63, EBA/GL/2019/02).

5.2 Due Diligence

Prima di concludere un accordo di esternalizzazione gli enti e gli istituti di pagamento dovrebbero assicurare, nel loro processo di selezione e valutazione, l'idoneità del fornitore di servizi.
Il rispetto di tale requisito viene garantito tramite l'esecuzione del processo di *due diligence* da parte della Divisione Acquisti di Banca Mediolanum.

Nello specifico la due diligence viene svolta:

1. mediante il processo di qualifica ai fini dell'"Albo Ufficiale dei Fornitori" (di seguito AUF);
2. tramite la raccolta di un set ulteriore di informazioni identificate, in particolare, anche in relazione alle attività specifiche oggetto di esternalizzazione.

Per la raccolta e valutazione delle informazioni utilizzate nell'ambito del processo di *due diligence*, la Divisione Acquisti si avvale del supporto del referente contrattuale e delle altre funzioni competenti, in relazione alla tipologia di informazione.

Nel dettaglio, almeno per quanto riguarda le funzioni essenziali o importanti, le analisi svolte hanno l'obiettivo di verificare che il fornitore di servizi abbia:

- la reputazione commerciale, abilità adeguate e sufficienti, la competenza, la capacità, le risorse (ad esempio umane, informatiche, finanziarie), la struttura organizzativa per adempiere ai propri obblighi per tutta la durata dell'accordo;
- le eventuali autorizzazioni o le registrazioni regolamentari necessarie per svolgere la funzione in modo affidabile e professionale.

Ulteriori fattori presi in considerazione nell'effettuare la due diligence su un potenziale fornitore di servizi comprendono, tra l'altro:

- il modello di business, la natura, le dimensioni, la complessità, la situazione finanziaria, la struttura proprietaria e di gruppo del fornitore di servizi;
- le relazioni a lungo termine con i fornitori di servizi già valutati e che prestano servizi per l'ente o l'istituto di pagamento;
- eventuali conflitti di interesse dichiarati dalla funzione che esternalizza o segnalati dal fornitore;
- se il fornitore di servizi è un'impresa madre o una filiazione dell'ente o dell'istituto di pagamento, se rientra nel perimetro di consolidamento contabile dell'ente o se è membro dello stesso sistema di tutela istituzionale al quale appartiene l'ente oppure è controllato da enti che ne fanno parte;
- se il fornitore di servizi è vigilato dalle autorità competenti;
- se il fornitore è situato o eroga l'attività/conserva i dati in paesi terzi.

Inoltre, la Banca e le Società del Gruppo verificano:

- che i fornitori di servizi agiscano in coerenza con valori e codici di condotta;
- in particolare, per quanto riguarda i fornitori di servizi situati in paesi terzi e, se del caso, i relativi subcontraenti, che il fornitore di servizi agisca in modo etico e socialmente responsabile e rispetti le norme internazionali in materia di diritti umani, di protezione dell'ambiente e di condizioni di lavoro adeguate, compreso il divieto del lavoro minorile.

Infine, se l'esternalizzazione comporta il trattamento di dati personali o riservati, sono previste verifiche per accertarsi che il fornitore di servizi adotti misure tecniche e organizzative adeguate a proteggere tali dati.
Una volta completato il processo di *due diligence*, ne viene messo il risultato a disposizione delle funzioni di controllo per il completamento delle relative valutazioni.

5.3 Valutazione dei rischi

La Funzione Risk Management (nel proprio ruolo di Funzione di Esternalizzazione) valuta l'impatto potenziale degli accordi di esternalizzazione in termini di rischio operativo, includendo un'eventuale mancata o inadeguata prestazione dei servizi, compresi i rischi derivanti da processi, sistemi, persone o eventi esterni. La Funzione documenta le analisi effettuate, i relativi risultati e stima in quale misura l'accordo potrebbe aumentare o ridurre il rischio operativo della Società, ricorrendo, se disponibili, all'utilizzo di dati sulle perdite interne ed esterne nell'analisi degli scenari.
La metodologia di valutazione dei rischi operativi (inclusi quelli ICT e legali) e reputazionali applicata è conforme a quelle previste dalla Policy per il controllo e la gestione dei Rischi Operativi e dalla Policy per la gestione del rischio di reputazione. In particolare, è prevista l'identificazione di scenari 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.

Nell'effettuare la valutazione la funzione Risk Management tiene conto:

- delle funzioni, dei dati e dei sistemi interessati dalla esternalizzazione, in relazione alla relativa sensibilità;
- dei presidi di sicurezza e protezione dei dati previsti;
- delle eventuali implicazioni (stabilità politica, sicurezza, legislazione vigente, …) connesse al paese in cui ha sede il fornitore (stato membro UE o esterno), in cui sono prestati i servizi e/o conservati i dati;
- dell'eventualità in cui il fornitore dei servizi appartenga al medesimo Gruppo della società che esternalizza e delle conseguenti potenziali implicazioni.

Inoltre, la valutazione considera costi e benefici attesi dall'accordo di esternalizzazione proposto, anche valutando gli eventuali rischi che possono essere ridotti o gestiti più efficacemente a fronte dei rischi che possono derivare dall'accordo di esternalizzazione, tenendo conto almeno di eventuali rischi di concentrazione e di rischi aggregati derivanti dall'esternalizzazione di diverse funzioni a livello dell'ente.

Qualora l'accordo di esternalizzazione preveda la possibilità che il fornitore di servizi sub-esternalizzi ad altri fornitori di servizi la Funzione, almeno per le Funzioni Essenziali o Importanti, terrà in considerazione i rischi associati alla sub-esternalizzazione, inclusi i rischi associati al luogo in cui ha sede il sub-contraente ed il rischio che lunghe e complesse catene di sub-esternalizzazione riducano la capacità dell'ente di vigilare sulla Funzione Essenziale o Importante o riducano la capacità delle autorità competenti di esercitare un'efficace vigilanza sull'ente stesso.

In caso di esternalizzazione a fornitori di servizi in cloud la valutazione dei rischi, con il supporto delle analisi svolte nella fase di *due diligence*, terrà anche conto dei rischi operativi e delle eventuali limitazioni della sorveglianza per l'impresa, derivanti da:

- il servizio cloud selezionato e i modelli di implementazione proposti;
- la migrazione e/o i processi di implementazione;
- l'interoperabilità dei sistemi e delle applicazioni dell'impresa e del fornitore, in particolare la loro capacità di scambiare informazioni e di utilizzare reciprocamente le informazioni oggetto di scambio;
- la possibile concentrazione all'interno dell'impresa e del settore finanziario dell'UE, causata da più imprese che si avvalgono dello stesso fornitore di servizi cloud o di un piccolo gruppo di fornitori di servizi cloud.

5.4 Esternalizzazione Funzioni Non ICT

A mero titolo esemplificativo e non esaustivo sono considerate da Flowe esternalizzazioni di Funzioni non ICT quelle relative a:

- servizi di pagamento (es. gestione dei conti, gestione del processing delle carte di pagamento, gestione e/o controllo frodi);
- funzioni aziendali di controllo;
- servizi amministrativi e adempimenti di vigilanza (segnalazioni relative alla centrale rischi, segnalazioni di vigilanza, contabilità generale, bilancio, gestione paghe, adempimenti fiscali, attività di middle e back office, archivio documentale digitale o cartaceo);
- attività di rapporti con la clientela (informativa, resoconti, servizi di postalizzazione, call centre, gestione dei reclami);
- altre attività il cui dettaglio è esposto nell'allegato A della presente Policy (scheda di valutazione delle esternalizzazioni).

5.5 Esternalizzazione Funzioni ICT

L'esternalizzazione delle risorse e servizi ICT può assumere diverse forme a seconda del modello architetturale adottato: dall'outsourcing verticale (relativo a determinati processi operativi), all'outsourcing orizzontale di servizi trasversali come la gestione degli apparati hardware (facility management), lo sviluppo e la gestione degli asset ICT, fino al full outsourcing del complessivo sistema informativo aziendale.
Con riferimento all'esternalizzazione di funzioni ICT, Flowe applica un modello in linea con la definizione fornita dalle Autorità di Vigilanza e coerente a quello previsto per le Funzioni non ICT.

Per tutte le esternalizzazioni in ambito ICT nell'accordo scritto tra Flowe e i fornitori di sistemi e servizi ICT devono essere chiaramente definiti e formalizzati i seguenti aspetti:

- le misure di attenuazione dei rischi del fornitore dei servizi, che devono essere conformi con il quadro di riferimento per la gestione del rischio di Flowe, con particolare riguardo a quello ICT e di sicurezza;
- le misure idonee a garantire l'accountability e la ricostruibilità delle operazioni effettuate, almeno con riferimento alle operazioni critiche e agli accessi a dati personali o sensibili;
- l'obbligo per il fornitore di servizi, una volta concluso il rapporto contrattuale e trascorso un periodo di tempo concordato, di eliminare – facendo uso di opportuni strumenti e soluzioni tecniche, debitamente documentati – qualsiasi copia o stralcio di dati personali o sensibili presente su propri sistemi o supporti in ragione dei servizi in precedenza esternalizzati da Flowe, in modo da escludere qualunque accesso successivo da parte del proprio personale o di terzi;
- la ripartizione dei compiti e delle responsabilità attinenti all'attuazione della politica di Information Security di Flowe;
- il raccordo con i ruoli e le procedure di Flowe attinenti al processo di analisi dei rischi ICT e per il sistema di gestione dei dati.

Quando le funzioni, i servizi o i sistemi ICT utilizzati da qualsiasi attività sono esternalizzati, anche a Società del Gruppo, o quando si fa ricorso a fornitori terzi, Flowe presidia l'efficacia delle misure di attenuazione dei rischi definite dal proprio quadro di gestione dei rischi, incluse quelle previste dalla normativa in vigore.
Per garantire la continuità dei servizi e dei sistemi ICT, gran parte dei contratti e degli accordi coi fornitori comprendono:

- misure e obiettivi adeguati e proporzionati in materia di sicurezza dell'informazione, compresi i requisiti minimi di sicurezza informatica, specifiche relative al ciclo di vita dei dati dell'istituto finanziario ed eventuali requisiti relativi alla cifratura dei dati, alla sicurezza di rete e ai processi di monitoraggio della sicurezza, e l'ubicazione dei centri dati;
- procedure di gestione degli incidenti operativi e di sicurezza, tra cui notifica e attivazione dei livelli successivi di intervento.

5.6 Esternalizzazione di Funzioni Essenziali o Importanti

Si definisce esternalizzazione di Funzione Essenziale o Importante (FEI), la cessione a soggetti all'interno del Gruppo o a terzi, di una funzione per cui sia valida almeno una delle seguenti condizioni:

- può essere considerata essenziale o importante per il modello di business della Società e, in particolare, riguardare funzioni operative relative ai servizi di pagamento o all'emissione di moneta elettronica, ovvero riguarda funzioni relative alle principali linee di business e alle funzioni essenziali quali definite all'articolo 2, paragrafo 1, punto 35, e all'articolo 2, paragrafo 1, punto 36, della direttiva 2014/59/UE (BRRD) e individuate dagli enti sulla base dei criteri di cui agli articoli 6 e 7 del regolamento delegato (UE) 2016/778 della Commissione; a meno che la valutazione dell'ente non stabilisca che la mancata esecuzione della funzione esternalizzata o un'esecuzione inadeguata della

stessa non avrebbe un impatto negativo sulla continuità operativa della linea di business principale o della funzione essenziale);
- un'anomalia nell'esecuzione o la mancata esecuzione della funzione esternalizzata potrebbe avere un impatto negativo rilevante sugli attivi, capitale, costi, fonti di finanziamento, liquidità, profitti e perdite della Società;
- un'anomalia nell'esecuzione o la mancata esecuzione della funzione esternalizzata può compromettere gravemente la capacità della Società di conformarsi nel continuo alle condizioni e agli obblighi derivanti dalla sua autorizzazione o agli obblighi previsti dalla disciplina di vigilanza;
- un'anomalia nell'esecuzione o la mancata esecuzione della funzione esternalizzata può compromettere gravemente la solidità o la continuità operativa delle attività svolte dalla Società;
- un'anomalia nell'esecuzione o la mancata esecuzione della funzione esternalizzata può avere impatti significativi sull'esposizione ai rischi operativi, incluso quelli derivanti dall'utilizzo di tecnologie ICT, ai rischi legali e reputazionali della Società;
- la funzione esternalizzata rientra tra le funzioni o attività sottoposte a riserva di legge per il cui svolgimento è necessario che il fornitore sia un soggetto autorizzato da parte di un'autorità di vigilanza;
- l'attività esternalizzata rientra tra i compiti operativi delle funzioni di controllo;
- l'esternalizzazione ha per oggetto il sistema informativo o sue componenti critiche.

5.6.1 Criteri di valutazione per identificare una FEI

Nel valutare se un accordo di esternalizzazione riguarda una funzione essenziale o importante, la Società considera:

- l'esito della valutazione del rischio (in particolare dei rischi operativi, reputazionali, strategici, di compliance, di concentrazione, step in risk, legati alle tecnologie dell'informazione e comunicazione);
- se l'accordo è direttamente collegato ad attività per cui la Società è autorizzata o se riguarda funzioni necessarie allo svolgimento delle attività delle principali linee di business o delle funzioni essenziali;
- il potenziale impatto che un'interruzione dell'esecuzione della funzione esternalizzata o la mancata prestazione del servizio ai livelli di servizio concordati su base continuativa dal fornitore potrebbe avere su:
    - la propria solidità e sostenibilità finanziaria a breve e lungo termine (o su quella del Gruppo);
    - la propria continuità e solidità operativa;
    - i rischi operativi;
    - i rischi reputazionali;
    - la pianificazione del risanamento e della risoluzione della crisi, la possibilità di risoluzione e la continuità operativa in una situazione di intervento precoce, risanamento o risoluzione;
- l'impatto potenziale dell'accordo di esternalizzazione sulla capacità di (i) individuare, monitorare e gestire tutti i rischi; (ii) rispettare tutte le previsioni di legge e tutti gli obblighi normativi; (iii) condurre opportune verifiche di audit sulla funzione esternalizzata;
- l'impatto potenziale sui servizi forniti ai propri clienti;
- le dimensioni e complessità dell'area operativa interessata;
- tutti gli accordi di esternalizzazione, l'esposizione complessiva della Società nei confronti dello stesso fornitore di servizi e il potenziale impatto cumulativo degli accordi di esternalizzazione nella medesima area operativa;
- la possibilità di ampliare (rivedendo o meno) e/o trasferire l'accordo o reintegrare l'attività all'interno della Società;
- la protezione dei dati e l'impatto potenziale di una violazione dell'obbligo di riservatezza o della mancata disponibilità e integrità dei dati relativi alla Società e ai suoi clienti, compreso tra l'altro il rispetto del regolamento (UE) 2016/679.

Inoltre, la scelta di esternalizzare o meno una funzione essenziale o importante dovrebbe tenere conto dell'impatto potenziale in termini di rischi operativi, in particolare legali, ICT, di conformità e reputazionali, e prevedere l'adozione di misure adeguate per mitigare i rischi potenziali individuati, prima di procedere alla sottoscrizione degli accordi di esternalizzazione.

Vanno, inoltre, incluse in tale valutazione considerazioni in merito:

- i rischi associati ai potenziali fornitori (ad esempio, solidità finanziaria, posizionamento sul mercato, fattori di human capital e tassi di turnover, contingency plans e informativa accurata e tempestiva sull'attività svolta, competenza e esperienza, luogo in cui ha sede e legislazione vigente);
- i rischi derivanti da un livello non adeguato di protezione della riservatezza dei dati e di continuità delle attività esternalizzate;

- la qualità dei sub-fornitori eventualmente preventivamente concordati.

Qualora le analisi sopra elencate dovessero evidenziare che l'esternalizzazione è riferita ad una Funzione Essenziale o Importante (FEI) la Società potrà procedere all'esternalizzazione introducendo e contrattualizzando con l'outsourcer gli opportuni presidi di controllo e reportistica che consentano di ridurre i rischi evidenziati.
Le valutazioni devono tener conto del principio di proporzionalità e dell'opportunità di mantenere all'interno delle Società competenze professionali per gestire una transizione tra modelli di sourcing in caso di grave necessità.

5.6.2 Requisiti minimi del contratto di esternalizzazione di una FEI

Nella definizione degli accordi di esternalizzazione di funzioni essenziali o importanti la Società assicura che il contratto sottoscritto con il fornitore definisca:

- una descrizione chiara della funzione esternalizzata che deve essere svolta;
- la data di inizio e, ove applicabile, la data di fine dell'accordo e i termini di preavviso per il fornitore di servizi e per l'ente o l'istituto di pagamento;
- la normativa che disciplina il contratto;
- gli obblighi finanziari delle parti;
- una clausola che indichi se è consentita la sub-esternalizzazione di una funzione essenziale o importante o di parti sostanziali di essa, e in caso affermativo le condizioni previste dagli Orientamenti EBA alle quali la sub-esternalizzazione è soggetta;
- i luoghi (regioni o paesi) in cui sarà svolta la funzione essenziale o importante e/o in cui saranno conservati e trattati i relativi dati, compreso l'eventuale luogo di conservazione, e le condizioni da soddisfare, compreso l'obbligo di informare l'ente o l'istituto di pagamento se il fornitore di servizi propone di cambiare tali luoghi;
- se del caso, le disposizioni riguardanti l'accessibilità, la disponibilità, l'integrità, la riservatezza e la sicurezza dei relativi dati;
- il diritto di effettuare un monitoraggio costante della performance del fornitore di servizi;
- i livelli di servizio concordati, che dovrebbero includere precisi obiettivi di performance, quantitativi e qualitativi, per la funzione esternalizzata, in modo da consentire un monitoraggio tempestivo che consenta di adottare, senza indebiti ritardi, le opportune azioni correttive in caso di mancato raggiungimento dei livelli di servizio concordati;
- gli obblighi di reportistica del fornitore di servizi alla Società, compresa la comunicazione da parte del fornitore di servizi di qualsiasi sviluppo che possa avere un impatto rilevante sulla sua capacità di svolgere efficacemente la funzione essenziale o importante in linea con i livelli di servizio concordati e in osservanza del diritto applicabile e degli obblighi normativi e, se opportuno, gli obblighi del fornitore di servizi di presentare le relazioni della propria funzione di audit interno;
- una clausola che indichi se il fornitore di servizi debba stipulare un'assicurazione obbligatoria contro determinati rischi e, ove applicabile, il livello di copertura assicurativa richiesto;
- i requisiti per l'attuazione e la verifica dei piani di emergenza (c.d. business contingency plan);
- disposizioni che assicurino l'accesso ai dati di cui la Società è titolare, anche nel caso di insolvenza, risoluzione o cessazione dell'attività del fornitore di servizi;
- l'obbligo del fornitore di cooperare con le autorità competenti, incluse le autorità di risoluzione dell'ente o dell'istituto di pagamento, e con altri soggetti da questi designati;
- un chiaro riferimento ai poteri dell'autorità nazionale di risoluzione, in particolare agli articoli 68 e 71 della direttiva 2014/59/UE (BRRD), e una descrizione degli «obblighi sostanziali» del contratto ai sensi dell'articolo 68 della medesima direttiva;
- il diritto illimitato della Società e delle autorità competenti di ispezionare e sottoporre a verifiche di audit il fornitore di servizi;
- i diritti di cessazione così come declinati al par. 13.4 degli Orientamenti EBA in materia di outsourcing;
- in caso di esternalizzazione in cloud, l'obbligo per il fornitore di servizi cloud di sostenere il trasferimento ordinato della funzione esternalizzata, e il relativo trattamento dei dati, dal fornitore stesso e da eventuali sub-fornitori a un altro fornitore di servizi cloud indicato dall'impresa o direttamente all'impresa, nel caso in cui quest'ultima attivi la strategia di uscita;
- eventuali clausole *Resolution Resilient*, oggetto di contrattazione nel caso in cui la normativa che disciplina il contratto sia quella di uno Stato extra UE e l'esternalizzazione riguardi funzioni relative alle principali linee di business e alle funzioni essenziali quali definite all'articolo 2, paragrafo 1, punto 35), e all'articolo 2, paragrafo 1, punto 36), della direttiva 2014/59/UE18.

La Società, inoltre, deve assicurare che il contratto con il fornitore definisca:

- i requisiti di sicurezza dei dati e dei sistemi nell'ambito dell'accordo di esternalizzazione al fine di monitorarne costantemente il rispetto;
- nel caso di esternalizzazione a fornitori di servizi in cloud e/o di altri accordi di esternalizzazione che comportano il trattamento o il trasferimento di dati personali o riservati, che la Società adotta un approccio basato sul rischio con riferimento al luogo (paese o regione) dove sono conservati e trattati i dati e alla sicurezza delle informazioni.

5.6.3 Esternalizzazione di FEI in ambito ICT

Anche le esternalizzazioni di FEI in ambito ICT sono identificate applicando i criteri illustrati al paragrafo 5.5 e sottoposte al modello di gestione e valutazione applicato per le altre funzioni esternalizzate classificate FEI, avendo particolare riguardo ai rischi ICT e alle misure e processi di sicurezza ICT.

5.6.4 Esternalizzazione di Funzioni Aziendali di Controllo

Si precisa che l'esternalizzazione delle Funzioni aziendali di controllo è possibile solo se effettuata all'interno del Gruppo Bancario Mediolanum, tramite l'accentramento alle relative Funzioni Aziendali di Controllo di Capogruppo.

La decisione, da parte di una Società, di esternalizzare funzioni aziendali di controllo all'interno del Gruppo, è consentita dalla normativa, senza porre limiti di carattere dimensionale o di complessità operativa, purché siano rispettati i seguenti criteri:

- deve essere valutata e documentata l'economicità dell'operazione nel continuo a livello di Gruppo (costi, benefici e rischi);
- gli organi aziendali delle Società del Gruppo devono essere consapevoli delle scelte effettuate dalla Capogruppo e devono essere responsabili, in relazione a competenze e sfera di pertinenza, delle strategie e politiche in materia di controlli, favorendone l'integrazione nell'ambito dei controlli di Gruppo.

La normativa delinea, inoltre, specifici requisiti minimi per i referenti di funzioni aziendali di controllo esternalizzate:

- possesso di requisiti di professionalità adeguati;
- riporto gerarchico e funzionale adeguato; in particolare il referente delle funzioni aziendali di controllo è il rappresentante in prima linea nei confronti dell'organo con funzione di supervisione strategica e dell'organo con funzione di gestione;
- indipendenza nel proprio giudizio, non avendo obblighi di responsabilità diretta verso le aree operative sottoposte a controllo, né di riporto gerarchico verso i rappresentanti di quelle aree;
- revoca e nomina dall'organo con funzione di supervisione strategica, dopo aver sentito l'organo con funzione di controllo;
- potere di riferire direttamente agli organi aziendali senza alcuna restrizione o intermediazione.

5.7 Sub-Esternalizzazione

Con riferimento specifico alla "sub-esternalizzazione" (ovvero la possibilità del fornitore di esternalizzare a sua volta, su base ricorrente o continuativa, l'attività oggetto del contratto di esternalizzazione o parte di essa), il rispetto dei principi e delle condizioni per l'esternalizzazione previste dall'Autorità di Vigilanza non deve essere messo a repentaglio.
A tal fine, il contratto con il fornitore di servizi, il quale deve assicurare di supervisionare adeguatamente i sub-fornitori, prevede che eventuali rapporti di sub-esternalizzazione siano preventivamente concordati e autorizzati dalla la Società e siano definiti in modo da consentire il pieno rispetto di tutte le condizioni sopra elencate relative al contratto primario, inclusa la possibilità per l'Autorità di Vigilanza di avere accesso ai dati relativi alle attività esternalizzate e ai locali in cui opera il sub-fornitore di servizi.

Nel caso di sub-esternalizzazione, la Società provvede ad annotarlo nel registro, come specificato nel par. 5.8 della presente policy, almeno per le Funzioni Essenziali o Importanti.

In caso di sub-esternalizzazione di funzioni essenziali o importanti, il contratto deve:

- specificare eventuali tipi di attività che sono esclusi dalla sub-esternalizzazione;
- specificare le condizioni da rispettare nel caso di sub-esternalizzazione;

- specificare che il fornitore di servizi sia tenuto a sorvegliare quei servizi che essa ha sub-esternalizzato per assicurare che tutti gli obblighi contrattuali tra il fornitore di servizi e la Società vengano rispettati in modo continuativo;
- prevedere da parte della Società un'autorizzazione scritta, generale o specifica, al fornitore per la sub-esternalizzazione dei dati;
- includere l'obbligo per i fornitori di informare di qualsiasi sub-esternalizzazione e comunicare ogni cambiamento sostanziale nelle sub-esternalizzazioni;
- assicurare, ove opportuno, che la Società abbia il diritto di opporsi alla sub-esternalizzazione pianificata o alle relative modifiche sostanziali, o che sia necessaria un'approvazione esplicita;
- assicurare che la Società abbia il diritto contrattuale di risolvere l'accordo in caso di sub-esternalizzazione indebita, ad esempio quando la sub-esternalizzazione aumenta notevolmente i rischi o quando il fornitore di servizi sub-esternalizza senza comunicarlo.

La Società acconsente alla sub-esternalizzazione solo se il sub-contraente si impegna a:

- rispettare tutte le leggi, gli obblighi normativi e gli obblighi contrattuali applicabili;
- riconoscere alla stessa gli stessi diritti contrattuali di accesso e di audit previsti per il fornitore di servizi.

5.8 Registro delle Esternalizzazioni

La Banca, coerentemente a quanto previsto nella sezione 11 degli Orientamenti EBA in materia di esternalizzazioni, ha istituito un registro, alimentato autonomamente dalle unità organizzative delle Società e della Capogruppo coinvolte nel processo per i campi di propria competenza, che include tutti gli accordi di esternalizzazione, distinguendo tra FEI e NFEI, comprese le modalità di outsourcing con fornitori di servizi all'interno del Gruppo Bancario.

Il registro include, a titolo esemplificativo e non esaustivo, almeno le seguenti informazioni:

- un numero di riferimento per ogni soluzione di outsourcing;
- la data di inizio e, a seconda dei casi, la data di scadenza o di prossimo rinnovo e/o i termini di preavviso;
- una breve descrizione della funzione in outsourcing, specificando se sono trasferiti dati personali o se la loro elaborazione è affidata a un fornitore di servizi;
- una categoria che riflette la natura della funzione (es. ICT, funzione di controllo), al fine di facilitare l'individuazione delle diverse tipologie di accordi;
- il nome del fornitore di servizi, il numero di registrazione aziendale, l'entità giuridica identificatore (se disponibile), la sede legale ed altri dettagli rilevanti, e il nome della sua Società madre (se presente);
- il paese oi paesi in cui il servizio deve essere effettuato, compresa la posizione (per esempio paese o regione) dei dati;
- l'evidenza se la funzione esternalizzata è considerata essenziale o importante, compresa, se del caso, una breve sintesi dei motivi per cui la funzione in outsourcing/sub-outsourcing è considerata essenziale o importante;
- nel caso di esternalizzazione a un fornitore di servizi di cloud, i modelli di servizi cloud e di distribuzione, vale a dire private/ibrido/comunità pubblica, e la specificità dei dati che si svolgeranno e le posizioni (ossia i paesi o regioni) in cui tali dati saranno essere memorizzate;
- la data della più recente valutazione della criticità o l'importanza della funzione di outsourcing;
- l'evidenza se l'accordo prevede sub-esternalizzazione.

Per le Funzioni classificate come Funzioni Essenziali o Importanti, il registro include almeno le seguenti informazioni aggiuntive:

- i soggetti che si avvalgono dell'esternalizzazione (la Società che esternalizza, la Funzione Richiedente, il Referente Contrattuale, il Referente Operativo);
- se il fornitore di servizi o il fornitore di sub-servizio è parte del gruppo o è un membro del sistema di tutela istituzionale o è di proprietà di enti o istituti di pagamento all'interno del gruppo o è di proprietà di membri di un sistema di tutela istituzionale;
- la data della valutazione dei rischi più recente e una breve sintesi dei principali risultati;
- l'organo decisionale della Banca o della Società che ha approvato l'accordo di esternalizzazione;
- la legge che disciplina il contratto di outsourcing;
- le date dell'audit più recente e il prossimo audit programmato, se del caso;

- se del caso, i nomi dei sub-outsourcer a cui sono affidate parti sostanziali di FEI, compresi il paese in cui sono registrati i sub-contraenti, dove verrà eseguito il servizio e, se del caso, la posizione (ad esempio paese o regione) in cui verranno memorizzati i dati;
- il risultato della valutazione della sostituibilità del fornitore di servizi (il più semplice, difficile o impossibile), della possibilità di reintegrare una funzione essenziale o importante nella Società o dell'impatto dovuto all'interruzione della funzione essenziale o importante;
- l'identificazione dei fornitori di servizi alternativi;
- un campo che indichi se la FEI esternalizzata supporta attività operative che sono critiche in termini di tempo;
- il costo finanziario annuo stimato.

La Banca conserva nel registro la documentazione relativa agli accordi di esternalizzazione cessati e la documentazione di supporto per un periodo di 10 anni. I medesimi criteri di conservazione sono applicati per la documentazione relativa agli accordi di esternalizzazione conclusi dalle altre società del Gruppo Bancario.

Ove richiesto, la Banca mette a disposizione dell'autorità competente il registro completo di tutti gli accordi di esternalizzazione o sezioni di esso, su formato elettronico leggibile.

6 Processi di Gestione di Esternalizzazioni

La scelta di esternalizzare è preceduta dall'analisi "make or buy" condotta/verificata dall'Unità Organization & Business Continuity, su richiesta della Funzione Richiedente, e con la collaborazione della Direzione Risorse Umane e della Divisione Pianificazione, Controllo e Investor Relations di Banca Mediolanum, al fine stabilire l'effettiva convenienza economica nell'affidare il processo in outsourcing.

La scelta di esternalizzare lo svolgimento di determinate funzioni aziendali, in accordo con il principio di proporzionalità legato alle caratteristiche delle attività da esternalizzare, deve rispettare i seguenti processi di gestione delle esternalizzazioni:

- Processo di gestione di una nuova esternalizzazione non in ambito ICT;
- Processo di gestione di una nuova esternalizzazione in ambito ICT;
- Processo di gestione di una nuova esternalizzazione fra Società del Gruppo;
- Monitoraggio esternalizzazioni;
- Processo di rinnovo dei contratti in scadenza;
- Monitoraggio nel continuo;
- Exit strategy e cessazione dell'accordo.

Nel modello adottato da Flowe e dalle altre Società del Gruppo i processi sopra esposti si applicano al contratto principale che disciplina la funzione esternalizzata e che incorpora tutte le singole richieste di acquisto effettuate in una fase successiva.

In ogni caso il processo prevede sempre di:

a. valutare se si tratti o meno di FEI;
b. valutare se sono soddisfatte le condizioni di vigilanza di cui alla sezione 12.1 degli Orientamenti EBA in materia che declinano diversi presidi a seconda del fatto che il fornitore risieda o meno in paesi membri dell'Unione e, in caso non lo siano, che vi siano accordi di cooperazione alla vigilanza;
c. individuare e valutare i rischi ai sensi dei principi esposti al precedente par 5.2 Valutazione dei rischi
d. effettuare una due diligence sul fornitore (processo richiamato al par. 5.2);
e. valutare se il fornitore sia vigilato dalle autorità competenti;
f. individuare e valutare i conflitti di interesse che l'esternalizzazione può generare.

La Funzione Risk Management, unitamente alla Funzione Compliance, è chiamata ad esprimere una propria valutazione anche con riferimento ai termini di efficacia temporale dell'accordo di Esternalizzazione con il Fornitore di servizi (outsourcer) ed alle comunicazioni dovute a Banca d'Italia. Tale valutazione sarà formalizzata nell'ambito della Scheda di valutazione delle Esternalizzazioni – Allegato A, Sezione E.

6.1 Processo di Gestione di una nuova Esternalizzazione non in ambito ICT

La Funzione Richiedente definisce il perimetro (processi, asset e risorse) della funzione che si intende esternalizzare e compila la scheda di valutazione delle esternalizzazioni (allegato A della presente policy) compilando le sezioni di propria competenza:

- Sezione A: per specificare se la funzione può essere classificata come esternalizzazione;
- Sezione B: ulteriori specifiche sulla funzione nell'ottica di definire se l'esternalizzazione possa essere classificata FEI o NFEI;
- Sezione C: per indicare i motivi, gli obiettivi, il perimetro, i costi, i benefici, i rischi, la durata, la strategia di uscita dalla funzione che si intende esternalizzare e se è prevista la possibilità di sub-esternalizzazione e i dati relativi ai sub-fornitori;

La Funzione Richiedente, esclusivamente se la sezione A è stata valorizzata con esternalizzazione, invia la scheda alle seguenti unità organizzative:

- Funzione Risk Management che conduce un'apposita analisi dei possibili rischi connessi con l'esternalizzazione per valutarne l'esposizione ed individuare eventuali presidi aggiuntivi da porre in essere;
- Funzione Compliance per valutare i potenziali conflitti di interesse e rischi di non conformità e le eventuali misure proposte per la loro gestione;
- Unità Organization & Business Continuity di Flowe che, in base a quanto specificato nella sezione C in merito al perimetro, costi e benefici dell'esternalizzazione, verifica quanto riportato in merito all'analisi "make or buy" che ha condotto con la Direzione Risorse Umane e la Divisione Pianificazione, Controllo e Investor Relations di Banca Mediolanum, al fine di stabilire l'effettiva convenienza economica nell'affidare il processo in outsourcing e analizza le eventuali risorse liberate a seguito dell'outsourcing. L'Unità Unità Organization & Business Continuity, oltre all'analisi "make or buy", effettua le proprie valutazioni sui piani di continuità operativa del fornitore, ogni volta che l'esternalizzazione riguarda attività operative critiche in termini di tempo;

- Divisione Acquisti che effettua la redazione della *due diligence* sul fornitore e la rende disponibile e consultabile alle Funzioni Risk Management e Compliance.

Per consentire alle Funzioni Risk Management e Compliance di effettuare le rispettive analisi dei possibili rischi connessi con l'esternalizzazione e la valutazione dei potenziali conflitti di interesse, la Funzione Richiedente, oltre all'allegato A (scheda di valutazione delle esternalizzazioni), invia alle predette funzioni, non appena disponibile, un draft dell'accordo contrattuale con il fornitore e dei relativi allegati tra cui, in particolare, l'idonea documentazione che permette di svolgere, in collaborazione con la Perspective Augmented Intelligence e l'Unità IT Security, l'analisi relativa ai dati e ai sistemi esternalizzati e di definire le misure di protezione adeguate.

La Funzione Richiedente esamina le analisi effettuate dalle predette Funzioni/Direzioni/Divisioni coinvolte nel processo di gestione di un'esternalizzazione e procede con la scelta di esternalizzare o meno, basandosi, oltre che sulle valutazioni delle funzioni precedentemente citate, anche sui seguenti aspetti già espressi nella scheda di valutazione delle esternalizzazioni:

- adesione a politiche e progetti al livello di gruppo;
- riduzione dei costi;
- riduzione Time to Market;
- accesso a migliori servizi/tecnologia/know how;
- focalizzazione sui servizi core;
- migliore qualità del servizio per i clienti;
- flessibilità e scalabilità delle soluzioni;
- più rapido adeguamento al framework normativo;
- migliori standard di sicurezza;
- altro.

La Funzione Risk Management e Compliance completano la scheda di valutazione delle esternalizzazioni con le sezioni di loro competenza:

- Sezione D: per specificare se la funzione può essere classificata come Funzione Essenziale o Importante;
- Sezione E: per esprimere il parere formale di Compliance e la valutazione dei rischi da parte del Risk Management, anche con riferimento ai termini di efficacia temporale dell'accordo di Esternalizzazione con il Fornitore di servizi (outsourcer) ed alle comunicazioni dovute a Banca d'Italia.

6.1.1 Processo di Gestione di una nuova Esternalizzazione non in ambito ICT classificata come FEI

Qualora la funzione esternalizzata fosse classificata come FEI, la Funzione Richiedente deve sottoporre la scelta di procedere all'esternalizzazione al Consiglio di Amministrazione della Società per ricevere l'autorizzazione a procedere e, successivamente alla delibera del Consiglio di Amministrazione della Società, prima di dare avvio all'esternalizzazione, la Funzione Risk Management invia comunicazione alla Banca d'Italia - come indicato nelle Disposizioni di vigilanza per gli istituti di pagamento e gli istituti di moneta elettronica emesse da Banca d'Italia il 23 luglio 2019, ovvero, almeno 60 giorni prima di dar corso all'esternalizzazione, o nei tempi eventualmente diversamente stabiliti dalle Autorità di Vigilanza competenti.

E', inoltre, compito della Funzione Risk Management predisporre alla competente Autorità di Vigilanza l'informativa se l'esternalizzazione FEI riguarda servizi in cloud secondo le modalità ed i termini eventualmente previsti dalla normativa di riferimento tempo per tempo vigente per la Società.

Dopo l'invio della comunicazione alla Banca d'Italia, la Divisione Acquisti prosegue, in condivisione con la Funzione Richiedente, alla negoziazione con il fornitore e, in collaborazione con le Divisioni Affari Legali e Affari Fiscali, completa la formalizzazione dell'accordo e della strategia di uscita, tenuto conto delle indicazioni fornite dalla Funzione Risk Management e dalla Funzione Compliance.

Dopo la formalizzazione, l'accordo di esternalizzazione viene censito dalla Funzione Richiedente nel registro delle esternalizzazioni e ogni unità inserisce i campi di propria competenza.

6.1.2 Processo di Gestione di una nuova Esternalizzazione non in ambito ICT non classificata come FEI

E', inoltre, compito della Funzione Risk Management predisporre alla competente Autorità di Vigilanza l'informativa se l'esternalizzazione NFEI riguarda servizi in cloud, secondo le modalità ed i termini eventualmente previsti dalla normativa di riferimento tempo per tempo vigente per la Società.

La Divisione Acquisti prosegue, in condivisione con la Funzione Richiedente, alla negoziazione con il fornitore e, in collaborazione con le Divisioni Affari Legali e Affari Fiscali, completa la formalizzazione dell'accordo, tenuto conto delle indicazioni fornite dalla Funzione Risk Management e dalla Funzione Compliance.

Dopo la formalizzazione, l'accordo di esternalizzazione viene censito dalla Funzione Richiedente nel registro delle esternalizzazioni e ogni unità inserisce i campi di propria competenza.

6.2 Processo di Gestione di una nuova Esternalizzazione in ambito ICT

Per le esternalizzazioni di attività, servizi o funzioni ICT la Funzione Richiedente applica il medesimo processo descritto al paragrafo 6.1.

6.2.1 Processo di Gestione di una nuova Esternalizzazione in ambito ICT classificata come FEI

In questo caso la Funzione Richiedente compila la scheda di valutazione delle esternalizzazioni (allegato A della presente policy) compilando le sezioni di propria competenza:

- Sezione A: per specificare se la funzione può essere classificata come esternalizzazione in ambito ICT;
- Sezione B: ulteriori specifiche sulla funzione nell'ottica di definire se l'esternalizzazione possa essere classificata FEI o NFEI;
- Sezione C: per indicare i motivi, gli obiettivi, il perimetro, i costi, i benefici, i rischi, la durata, la strategia di uscita dalla funzione che si intende esternalizzare e se è prevista la possibilità di sub-esternalizzazione e i dati relativi ai sub-fornitori.

La Funzione Richiedente invia la scheda alle seguenti unità organizzative:

- Funzione Risk Management che conduce un'apposita analisi dei possibili rischi connessi con l'esternalizzazione per valutarne l'esposizione ed individuare eventuali presidi aggiuntivi da porre in essere;
- Funzione Compliance per valutare i potenziali conflitti di interesse e i rischi di non conformità e le eventuali misure proposte per la loro gestione;
- Unità Organization & Business Continuity di Flowe che, in base a quanto specificato nella sezione C in merito al perimetro, costi e benefici dell'esternalizzazione, verifica quanto riportato in relazione all'analisi "make or buy" che ha condotto con la Direzione Risorse Umane e la Divisione Pianificazione, Controllo e Investor Relations di Banca Mediolanum, al fine di stabilire l'effettiva convenienza economica nell'affidare il processo in outsourcing e analizza le eventuali risorse liberate a seguito dell'outsourcing. L'analisi viene effettuata dove applicabile e nel caso in cui si sta esternalizzando una attività fino a quel momento gestita internamente. L'Unità Unità Organization & Business Continuity, oltre all'analisi "make or buy", effettua le proprie valutazioni sui piani di continuità operativa del fornitore, ogni volta che l'esternalizzazione riguarda attività operative critiche in termini di tempo;
- Divisione Acquisti che effettua la redazione della due diligence sul fornitore (avvio del processo per essere inserito in AUF) e la rende disponibile e consultabile alle Funzioni Risk Management e Compliance.

Per consentire alle Funzioni Risk Management e Compliance di effettuare le rispettive analisi dei possibili rischi connessi con l'esternalizzazione e la valutazione dei potenziali conflitti di interesse, la Funzione Richiedente, oltre all'allegato A (scheda di valutazione delle esternalizzazioni), invia alle predette funzioni, non appena disponibile, un draft dell'accordo contrattuale con il fornitore e dei relativi allegati tra cui, in particolare, l'idonea documentazione che permette di svolgere, in collaborazione con la Perspective Augmented Intelligence e l'Unità IT Security, l'analisi relativa ai dati e ai sistemi esternalizzati e di definire le misure di protezione adeguate.

La Funzione Richiedente esamina le analisi effettuate dalle predette Funzioni/Direzioni/Divisioni coinvolte nel processo di gestione di un'esternalizzazione e procede con la scelta di esternalizzare o meno, basandosi, oltre che sulle valutazioni delle funzioni precedentemente citate, anche sui seguenti aspetti già espressi nella scheda di valutazione delle esternalizzazioni:

- adesione a politiche e progetti al livello di gruppo;
- riduzione dei costi;
- riduzione Time to Market;
- accesso a migliori servizi/tecnologia/know how;
- focalizzazione sui servizi core;
- migliore qualità del servizio per i clienti;
- flessibilità e scalabilità delle soluzioni;
- più rapido adeguamento al framework normativo;
- migliori standard di sicurezza;
- altro.

La Funzione Risk Management e Compliance completano la scheda di valutazione delle esternalizzazioni con le sezioni di loro competenza:

- Sezione D: per specificare se la funzione può essere classificata come Funzione Essenziale o Importante (dato che sarà fornito dalla Funzione Richiedente in base all'applicazione del modello di classificazione dei contratti ICT);
- Sezione E: per esprimere il parere formale di Compliance e la valutazione dei rischi da parte del Risk Management, anche con riferimento ai termini di efficacia temporale dell'accordo di Esternalizzazione con il Fornitore di servizi (outsourcer) ed alle comunicazioni dovute a Banca d'Italia.

La Funzione Richiedente deve sottoporre la scelta di procedere all'esternalizzazione al Consiglio di Amministrazione della Società per ricevere l'autorizzazione a procedere e, successivamente alla delibera del Consiglio di Amministrazione, prima di dare avvio all'esternalizzazione, la Funzione Risk Management invia comunicazione, sottoscritta dal legale rappresentante della Società, alla Banca d'Italia come indicato nelle Disposizioni di vigilanza per gli istituti di pagamento e gli istituti di moneta elettronica emesse da Banca d'Italia il 23 luglio 2019, ovvero, almeno 60 giorni prima di dar corso all'esternalizzazione, o nei tempi eventualmente diversamente stabiliti dalle Autorità di Vigilanza competenti.

E', inoltre, compito della Funzione Risk Management predisporre alla competente Autorità di Vigilanza l'informativa se l'esternalizzazione FEI riguarda servizi in cloud secondo le modalità ed i termini eventualmente previsti dalla normativa di riferimento tempo per tempo vigente per la Società.

Dopo l'invio della comunicazione alla Banca d'Italia, la Divisione Acquisti prosegue, in condivisione con la Funzione Richiedente, alla negoziazione con il fornitore e, in collaborazione con le Divisioni Affari Legali e Affari Fiscali, completa la formalizzazione dell'accordo e della strategia di uscita, tenuto conto delle indicazioni fornite dalla Funzione Risk Management e dalla Funzione Compliance.

Dopo la formalizzazione, l'accordo di esternalizzazione viene censito dalla Funzione Richiedente nel registro delle esternalizzazioni e ogni unità inserisce i campi di propria competenza.

6.2.2 Processo di Gestione di una nuova Esternalizzazione in ambito ICT non classificata come FEI

In questo caso la Funzione Richiedente definisce il perimetro (processi, asset e risorse) della funzione che si intende esternalizzare e compila la scheda di valutazione delle esternalizzazioni (allegato A della presente policy) compilando le sezioni di propria competenza:

- Sezione A: per specificare se la funzione può essere classificata come esternalizzazione in ambito ICT;
- Sezione C: per indicare i motivi, gli obiettivi, il perimetro, i costi, i benefici, i rischi, la durata, la strategia di uscita dalla funzione che si intende esternalizzare e se è prevista la possibilità di sub-esternalizzazione e i dati relativi ai sub-fornitori.

La Funzione Richiedente, esclusivamente se la sezione A è stata valorizzata con esternalizzazione, invia la scheda alle seguenti unità organizzative:

- Funzione Risk Management che conduce un'apposita analisi dei possibili rischi connessi con l'esternalizzazione per valutarne l'esposizione ed individuare eventuali presidi aggiuntivi da porre in essere;
- Funzione Compliance per valutare i potenziali conflitti di interesse e i rischi di non conformità e le eventuali misure proposte per la loro gestione;
- Unità Organization & Business Continuity di Flowe che, in base a quanto specificato nella sezione C in merito al perimetro, costi e benefici dell'esternalizzazione, verifica quanto riportato in relazione all'analisi "make or buy" che ha condotto con la Direzione Risorse Umane e la Divisione Pianificazione, Controllo e Investor Relations di Banca Mediolanum, al fine di stabilire l'effettiva convenienza economica nell'affidare il processo in outsourcing e analizza le eventuali risorse liberate a seguito dell'outsourcing. L'analisi viene effettuata dove applicabile e nel caso in cui si sta esternalizzando una attività fino a quel momento gestita internamente. L'Unità Unità Organization & Business Continuity, oltre all'analisi "make or buy", effettua le proprie valutazioni sui piani di continuità operativa del fornitore, ogni volta che l'esternalizzazione riguarda attività operative critiche in termini di tempo;

- Divisione Acquisti che effettua la redazione della due diligence sul fornitore e la rende disponibile e consultabile alle Funzioni Risk Management e Compliance.

Per consentire alle Funzioni Risk Management e Compliance di effettuare le rispettive analisi dei possibili rischi connessi con l'esternalizzazione e la valutazione dei potenziali conflitti di interesse, la Funzione Richiedente, oltre all'allegato A (scheda di valutazione delle esternalizzazioni), invia alle predette funzioni, non appena disponibile, un draft dell'accordo contrattuale con il fornitore e dei relativi allegati tra cui, in particolare, l'idonea documentazione che permette di svolgere, in collaborazione con la Perspective Augmented Intelligence e l'Unità IT Security, l'analisi relativa ai dati e ai sistemi esternalizzati e di definire le misure di protezione adeguate.

La Funzione Richiedente esamina le analisi effettuate dalle predette Funzioni/Direzioni/Divisioni coinvolte nel processo di gestione di un'esternalizzazione e procede con la scelta di esternalizzare o meno, basandosi, oltre che sulle valutazioni precedentemente citate, anche sui seguenti aspetti già espressi nella scheda di valutazione delle esternalizzazioni:

- adesione a politiche e progetti al livello di gruppo;

- riduzione dei costi;
- riduzione Time to Market;
- accesso a migliori servizi/tecnologia/know how;
- focalizzazione sui servizi core;
- migliore qualità del servizio per i clienti;
- flessibilità e scalabilità delle soluzioni;
- più rapido adeguamento al framework normativo;
- migliori standard di sicurezza;
- altro.

La Funzione Risk Management e Compliance completano la scheda di valutazione delle esternalizzazioni con le sezioni di loro competenza:

- Sezione D: per specificare che la funzione non può essere classificata come Funzione Essenziale o Importante (dato che sarà fornito dalla Funzione Richiedente in base all'applicazione del modello di classificazione dei Contratti ICT);
- Sezione E: per esprimere il parere formale di Compliance e la valutazione dei rischi da parte del Risk Management, anche con riferimento ai termini di efficacia temporale dell'accordo di Esternalizzazione con il Fornitore di servizi (outsourcer) ed alle comunicazioni dovute a Banca d'Italia.

E', inoltre, compito della Funzione Risk Management predisporre alla competente Autorità di Vigilanza l'informativa se l'esternalizzazione NFEI riguarda servizi in cloud secondo le modalità ed i termini eventualmente previsti dalla normativa di riferimento tempo per tempo vigente per la Società.

Dopo l'invio della comunicazione alla Banca d'Italia, la Divisione Acquisti prosegue, in condivisione con la Funzione Richiedente, alla negoziazione con il fornitore e, in collaborazione con le Divisioni Affari Legali e Affari Fiscali, completa la formalizzazione dell'accordo, tenuto conto delle indicazioni fornite dalla Funzione Risk Management e dalla Funzione Compliance.

Dopo la formalizzazione, l'accordo di esternalizzazione viene censito dalla Funzione Richiedente nel registro delle esternalizzazioni e ogni unità inserisce i campi di propria competenza.

6.3 Processo di Gestione di una nuova Esternalizzazione Infra-Gruppo

La Funzione Richiedente della Società definisce il perimetro (processi, asset e risorse) della funzione che si intende esternalizzare e compila la scheda di valutazione delle esternalizzazioni (allegato A della presente policy) compilando le sezioni di propria competenza:

- Sezione A: per specificare se la funzione può essere classificata come esternalizzazione;
- Sezione B ulteriori specifiche sulla funzione nell'ottica di definire se l'esternalizzazione possa essere classificata FEI o NFEI;
- Sezione C: per indicare i motivi, gli obiettivi, il perimetro, i costi, i benefici, i rischi, la durata, la strategia di uscita dalla funzione che si intende esternalizzare e se è prevista la possibilità di sub-esternalizzazione e i dati relativi ai sub-fornitori.

La Funzione Richiedente, esclusivamente se la sezione A è stata valorizzata con esternalizzazione, invia la scheda alle seguenti unità organizzative:

- Funzione Risk Management della Società che conduce un'apposita analisi dei possibili rischi connessi con l'esternalizzazione, per valutarne l'esposizione ed individuare eventuali presidi aggiuntivi da porre in essere;
- Funzione Compliance della Società per valutare i potenziali conflitti di interesse e i rischi di non conformità e le eventuali misure proposte per la loro gestione;
- Unità Organization & Business Continuity di Flowe che, in base a quanto specificato nella sezione C in merito al perimetro, costi e benefici dell'esternalizzazione, verifica quanto riportato in merito all'analisi "make or buy" che ha condotto con la Direzione Risorse Umane e la Divisione Pianificazione, Controllo e Investor Relations di Banca Mediolanum, al fine di stabilire l'effettiva convenienza economica nell'affidare il processo in outsourcing e analizza

le eventuali risorse liberate a seguito dell'outsourcing. L'Unità Unità Organization & Business Continuity, oltre all'analisi "make or buy", effettua le proprie valutazioni sui piani di continuità operativa del fornitore, ogni volta che l'esternalizzazione riguarda attività operative critiche in termini di tempo.

Per consentire alle Funzioni Risk Management e Compliance della Società di effettuare le rispettive analisi dei possibili rischi connessi con l'esternalizzazione e la valutazione dei potenziali conflitti di interesse, la Funzione Richiedente, oltre all'allegato A (scheda di valutazione delle esternalizzazioni), invia alle predette funzioni, non appena disponibile, un draft dell'accordo contrattuale con il fornitore e dei relativi allegati tra cui, in particolare, l'idonea documentazione che permette di identificare, in collaborazione con la Perspective Augmented Intelligence e l'Unità IT Security, le misure definite per la protezione dei dati e dei sistemi esternalizzati.

La Funzione Richiedente esamina le analisi effettuate dalle predette Funzioni/Direzioni/Divisioni coinvolte nel processo di gestione di un'esternalizzazione e procede con la scelta di esternalizzare o meno, basandosi, oltre che sulle valutazioni delle funzioni precedentemente citate, anche sui seguenti aspetti già espressi nella scheda di valutazione delle esternalizzazioni:

- adesione a politiche e progetti al livello di gruppo;
- riduzione dei costi;
- riduzione Time to Market;
- accesso a migliori servizi/tecnologia/know how;
- focalizzazione sui servizi core;
- migliore qualità del servizio per i clienti;
- flessibilità e scalabilità delle soluzioni;
- più rapido adeguamento al framework normativo;
- migliori standard di sicurezza;
- altro.

Le Funzioni Risk Management e Compliance completano la scheda di valutazione delle esternalizzazioni con le sezioni di loro competenza:

- Sezione D: per specificare se la funzione può essere classificata come Funzione Essenziale o Importante;
- Sezione E: per esprimere il parere formale di Compliance e la valutazione dei rischi da parte del Risk Management, anche con riferimento ai termini di efficacia temporale dell'accordo di Esternalizzazione con il Fornitore di servizi (outsourcer) ed alle comunicazioni dovute a Banca d'Italia.

6.3.1 Processo di Gestione di nuova Esternalizzazione Infra-Gruppo classificata come FEI

Qualora la funzione esternalizzata fosse classificata come FEI, la Funzione Richiedente deve sottoporre la scelta di procedere all'esternalizzazione al Consiglio di Amministrazione della Società per ricevere l'autorizzazione a procedere.

Successivamente la Funzione Richiedente, per il tramite dell'Amministratore Delegato della Banca, presenta anche una nota informativa al Comitato Rischi e al Consiglio di Amministrazione della Capogruppo.

Successivamente alla delibera del Consiglio di Amministrazione della Società e all'invio della nota informativa presso i comitati Consiliari della Banca, la Funzione Risk Management invia una comunicazione alla Banca d'Italia come indicato nelle Disposizioni di vigilanza per gli istituti di pagamento e gli istituti di moneta elettronica emesse da Banca d'Italia il 23 luglio 2019, ovvero, almeno 60 giorni prima di dar corso all'esternalizzazione, o nei tempi eventualmente diversamente stabiliti dalle Autorità di Vigilanza competenti.

E', inoltre, compito della Funzione Risk Management predisporre alla competente Autorità di Vigilanza l'informativa se l'esternalizzazione FEI riguarda servizi in cloud secondo le modalità ed i termini eventualmente previsti dalla normativa di riferimento tempo per tempo vigente per la Società.

Dopo l'invio della comunicazione alla Banca d'Italia, la Divisione Acquisti prosegue, in condivisione con la Funzione Richiedente, alla negoziazione con il fornitore e, in collaborazione con le Divisioni Affari Legali e

Affari Fiscali, completa la formalizzazione dell'accordo e della strategia di uscita, tenuto conto delle indicazioni fornite dalla Funzione Risk Management e dalla Funzione Compliance.

Dopo la formalizzazione, l'accordo di esternalizzazione viene censito dalla Funzione Richiedente nel registro delle esternalizzazioni e ogni unità inserisce i campi di propria competenza.

6.3.2 Processo di Gestione di una nuova Esternalizzazione Infra-Gruppo non classificata come FEI

E', inoltre, compito della Funzione Risk Management predisporre alla competente Autorità di Vigilanza l'informativa se l'esternalizzazione NFEI riguarda servizi in cloud secondo le modalità ed i termini eventualmente previsti dalla normativa di riferimento tempo per tempo vigente per la Società.

La Divisione Acquisti prosegue, in condivisione con la Funzione Richiedente, alla negoziazione con il fornitore e, in collaborazione con le Divisioni Affari Legali e Affari Fiscali, completa la formalizzazione dell'accordo e della strategia di uscita, tenuto conto delle indicazioni fornite dalla Funzione Risk Management e dalla Funzione Compliance.

Dopo la formalizzazione, l'accordo di esternalizzazione viene censito dalla Funzione Richiedente nel registro delle esternalizzazioni e ogni unità coinvolta inserisce i campi di propria competenza.

6.4 Monitoraggio Esternalizzazioni

La normativa specifica che le banche e gli intermediari finanziari che ricorrono all'esternalizzazione di funzioni aziendali presidiano i rischi derivanti dalle scelte effettuate e mantengono la capacità di controllo e la responsabilità sulle attività esternalizzate nonché le competenze tecniche e gestionali essenziali per re-internalizzare, in caso di necessità, il loro svolgimento.
Nello specifico, la Società assicura che siano rispettati i seguenti requisiti minimi richiesti dalla normativa:

- mantenere il possesso delle competenze richieste per garantire un controllo efficace delle funzioni esternalizzate e per gestire i rischi che possono insorgere a seguito dell'esternalizzazione (ivi inclusi i potenziali conflitti di interesse verso i fornitori cui si esternalizza). Al fine di presidiare tale rischio la Società ha individuato il Risk Management come referente per le funzioni esternalizzate;
- effettuare un monitoraggio indipendente del fornitore del servizio per il tramite del Referente Contrattuale e del Referente Operativo o, dove previsto, del Responsabile Operativo dei servizi affidati in outsourcing;
- garantire che l'Organo con Funzione di Gestione (OFG), per la Società individuato nell'Amministratore Delegato, sia debitamente informato delle modifiche rilevanti previste per quanto riguarda i fornitori di servizi ed il potenziale impatto di questi cambiamenti sulle funzioni operative importanti, tra cui una sintesi dell'analisi dei rischi in modo da poter valutare l'impatto di questi cambiamenti; a tal proposito le informative saranno fornite dalla Funzione Risk Management e dal Responsabile Operativo dei servizi affidati in outsourcing con frequenza almeno annuale;
- monitorare il livello di conformità dei fornitori agli obiettivi di sicurezza, alle misure e alle prestazioni previste dalla Società, per il tramite del Referente Contrattuale e del Referente Operativo;

Per le Funzioni Essenziali o Importanti, attraverso il Referente Contrattuale, ovvero, attraverso il Responsabile Operativo dei servizi affidati in outsourcing:

- prende atto dei piani di continuità operativa posti in essere dal Fornitore cui si esternalizza, o richiederne informativa adeguata, al fine di valutarne la consistenza e di integrarli con le soluzioni presenti all'interno della Società;
- identifica, valuta, gestisce e mitiga i rischi connessi dei contratti in corso con il Fornitore;
- è in grado di attivare gli uffici preposti al fine di trasferire le funzioni a fornitori di servizi alternativi o reintegrare internamente la funzione;
- verifica che i dati personali siano trattati dai fornitori in conformità al regolamento UE 2016/679;
- effettua un monitoraggio dell'elenco sub-fornitori, richiedendo ai fornitori la rendicontazione periodica dei sub-appalti in essere.

Nel ciclo di vita di una funzione esternalizzata possono subentrare delle modifiche di perimetro derivanti dall'introduzione/riduzione di attività, servizi o processi, sub-fornitori.

A titolo esemplificativo e non esaustivo si individuano 5 principali casistiche:

- si riduce il perimetro della funzione esternalizzata (es. viene re-internalizzata un'attività) e, di conseguenza, cambia il rischio dell'esternalizzazione e una funzione classificata come esternalizzazione FEI potrebbe essere "declassificata" come esternalizzazione NFEI;
- si estende il perimetro della funzione esternalizzata (es. fornitura di un nuovo servizio) e, di conseguenza, cambia il rischio dell'esternalizzazione e una funzione classificata come NON FEI potrebbe diventare FEI;
- si estende il perimetro di una non esternalizzazione e, di conseguenza, occorre avviare l'iter di gestione di una nuova esternalizzazione (vale quanto descritto nei paragrafi precedenti);
- rinnovi dei contratti in scadenza;
- monitoraggio nel continuo.

6.4.1 Monitoraggio Esternalizzazioni con riduzione di perimetro

Valgono i processi descritti nel paragrafo 6.1, 6.2, 6.3.

La Funzione Richiedente compila le sezioni A, B, C della scheda di valutazione delle esternalizzazioni (al fine di evidenziare la riduzione del perimetro della funzione esternalizzata) e invia la scheda di valutazione delle esternalizzazioni alle Funzioni Risk Management e Compliance per le valutazioni di competenza:

- Funzione Risk Management che conduce un'apposita analisi dei possibili rischi connessi con l'esternalizzazione per valutarne l'esposizione ed individuare eventuali presidi aggiuntivi da porre in essere;
- Funzione Compliance verifica, in collaborazione con la Funzione Risk Management, se sussistono i requisiti normativi per modificare la classificazione da esternalizzazione FEI ad esternalizzazione NFEI.

Per consentire alle Funzioni Risk Management e Compliance di effettuare le rispettive analisi dei possibili rischi connessi con l'esternalizzazione e la valutazione dei potenziali conflitti di interesse, la Funzione Richiedente, oltre all'allegato A (scheda di valutazione delle esternalizzazioni), invia alle predette funzioni, non appena disponibile, un draft dell'accordo contrattuale con il fornitore e dei relativi allegati tra cui, in particolare, l'idonea documentazione che permette di svolgere, in collaborazione con l'Unità IT Security, l'analisi relativa ai dati e ai sistemi esternalizzati e di definire le misure di protezione adeguate.

La Funzione Richiedente, dopo aver ricevuto la scheda compilata con il parere formale di Compliance e la valutazione dei rischi da parte del Risk Management, qualora si renda necessario procedere con la riclassificazione di una FEI, chiede l'approvazione per procedere a classificare la funzione come esternalizzazione NFEI al Consiglio di Amministrazione della Società e, successivamente alla delibera del Consiglio di Amministrazione, la Funzione Risk Management invia un'informativa alla Banca d'Italia come indicato nelle Disposizioni di vigilanza per gli istituti di pagamento e gli istituti di moneta elettronica emesse da Banca d'Italia il 23 luglio 2019.

La Divisione Acquisti prosegue, in condivisione con la Funzione Richiedente, alla negoziazione con il fornitore e, in collaborazione con le Divisioni Affari Legali e Affari Fiscali, completa la formalizzazione dell'accordo, tenuto conto delle indicazioni fornite dalla Funzione Risk Management e dalla Funzione Compliance.

Dopo la formalizzazione del nuovo accordo, la Funzione Richiedente e ogni unità coinvolta aggiornano i campi di propria competenza nel registro delle esternalizzazioni.

6.4.2 Monitoraggio Esternalizzazioni con estensione di perimetro

Valgono i processi descritti nel paragrafo 6.1, 6.2, 6.3.

La Funzione Richiedente compila le sezioni A, B, C della scheda di valutazione delle esternalizzazioni (al fine di evidenziare l'ampliamento del perimetro della funzione esternalizzata) e invia la scheda di valutazione delle esternalizzazioni alle Funzioni Risk Management e Compliance per le valutazioni di competenza:

- Funzione Risk Management che conduce un'apposita analisi dei possibili rischi connessi con l'esternalizzazione per valutarne l'esposizione ed individuare eventuali presidi aggiuntivi da porre in essere;

- Funzione Compliance verifica, in collaborazione con la Funzione Risk Management, se sussistono i requisiti normativi per modificare la classificazione da esternalizzazione NFEI a esternalizzazione FEI.

Per consentire alle Funzioni Risk Management e Compliance di effettuare le rispettive analisi dei possibili rischi connessi con l'esternalizzazione e la valutazione dei potenziali conflitti di interesse, la Funzione Richiedente, oltre all'allegato A (scheda di valutazione delle esternalizzazioni), invia alle predette funzioni, non appena disponibile, un draft dell'accordo contrattuale con il fornitore e dei relativi allegati tra cui, in particolare, l'idonea documentazione che permette di svolgere, in collaborazione con l'Unità IT Security, l'analisi relativa ai dati e ai sistemi esternalizzati e di definire le misure di protezione adeguate.

La Funzione Richiedente, dopo aver ricevuto la scheda compilata con il parere formale di Compliance e la valutazione dei rischi da parte del Risk Management, trattandosi di una Funzione Essenziale o Importante, deve sottoporre la scelta di procedere alla riclassificazione, da NFEI a FEI, dell'esternalizzazione al Consiglio di Amministrazione della Società per ricevere l'autorizzazione a procedere e, successivamente alla delibera del Consiglio di Amministrazione, la Funzione Risk Management invia previa comunicazione alla Banca d'Italia come indicato nelle Disposizioni di vigilanza per gli istituti di pagamento e gli istituti di moneta elettronica emesse da Banca d'Italia il 23 luglio 2019.

La Divisione Acquisti prosegue, in condivisione con la Funzione Richiedente, alla negoziazione con il fornitore e, in collaborazione con le Divisioni Affari Legali e Affari Fiscali, completa la formalizzazione dell'accordo e della strategia di uscita, tenuto conto delle indicazioni fornite dalla Funzione Risk Management e dalla Funzione Compliance.

Dopo la formalizzazione del nuovo accordo, la Funzione Richiedente e ogni unità coinvolta aggiornano i campi di propria competenza nel registro delle esternalizzazioni.

6.4.3 Processo di rinnovo dei contratti in scadenza

Nel caso di rinnovi contrattuali sia relativi alle FEI che alle esternalizzazioni, la Funzione Richiedente compila le sezioni A, B, C della scheda di valutazione delle esternalizzazioni (al fine di evidenziare se eventuali modifiche contrattuali comportino una riduzione o un ampliamento del perimetro della funzione esternalizzata) e invia la scheda di valutazione delle esternalizzazioni alle Funzioni Risk Management e Compliance per le valutazioni di competenza.

Valgono i medesimi processi già descritti nei par. 6.4.1 e 6.4.2.

6.4.4 Monitoraggio nel continuo

Per le esternalizzazioni, in particolare di Funzioni Essenziali o Importanti, il Responsabile Operativo dei servizi affidati in outsourcing presenta con frequenza annuale la relazione sui processi di outsourcing al Consiglio di Amministrazione della Società, al fine di rendicontare le attività di controllo sugli outsourcer relativamente agli SLA e alle eventuali anomalie o criticità emerse nel periodo di monitoraggio.

La relazione, prima di essere presentata alle sedute Consiliari, viene preliminarmente condivisa con la Funzione Risk Management e la Funzione Compliance al fine di assicurare la piena informativa e governabilità dei fattori di rischio attinenti alle FEI.

In ogni caso, sia per le esternalizzazioni di FEI che di NFEI, il Referente Contrattuale comunica al Responsabile Operativo dei servizi affidati in outsourcing, alla Funzione Compliance e alla Funzione Risk Management, con frequenza semestrale, le attività di controllo sugli outsourcer relativamente agli SLA e alle eventuali anomalie o criticità emerse nel periodo di monitoraggio.

Qualora dal monitoraggio nel continuo dovesse emergere una variazione o riduzione del perimetro della funziono esternalizzata, si applicano i processi già descritti nei par. 6.4.1 e 6.4.2.

6.5 Exit Strategy e cessazione dell'accordo

In linea con quanto previsto negli Orientamenti in materia di esternalizzazione emanati da EBA (EBA/GL/2019/02), la redazione in forma scritta, lo sviluppo e aggiornamento di un plan, di competenza del

Referente Contrattuale e previsto almeno per le esternalizzazioni di funzioni essenziali o importanti, in coerenza con la politica di esternalizzazione ed ai piani di continuità operativa, ricomprende:

- la definizione degli obiettivi del piano per il passaggio di consegne;
- l'analisi d'impatto sulle attività aziendali, al fine di individuare, ad esempio, tempistiche e risorse umane e finanziarie per attuarlo;
- l'assegnazione di ruoli, responsabilità e risorse sufficiente per la gestione dei piani di uscita e la transizione delle attività;
- la definizione di criteri efficaci per la transizione delle funzioni e dei dati esternalizzati comprendendo, laddove pertinente, l'eliminazione sicura dei dati dai sistemi del fornitore e di eventuali sub-fornitori;
- la definizione, nell'ambito degli indicatori per il monitoraggio dell'accordo di esternalizzazione, di soglie il cui superamento rappresenti un livello inaccettabile e tale da comportare l'attivazione del piano d'uscita.

Inoltre, in linea con le indicazioni normative, nella definizione della exit strategy, almeno per le funzioni essenziali o importanti, il referente contrattuale tiene conto della possibilità di:

- porre termine agli accordi di esternalizzazione;
- un dissesto del fornitore di servizi;
- il deterioramento della qualità della funzione eseguita e interruzioni effettive o potenziali delle attività causate dall'inadeguata o mancata esecuzione della funzione;
- l'insorgenza di rischi rilevanti per lo svolgimento adeguato e continuativo della funzione.

I piani di uscita, anche in questo caso almeno per le funzioni essenziali o importanti, devono essere esaustivi, documentati e sufficientemente dettagliati.

In caso di applicazione della exit strategy e della conseguente cessazione dell'accordo, la Società può procedere a reintegrare le attività al proprio interno o, in alternativa, trasferire l'accordo presso un altro fornitore di servizi, senza interrompere indebitamente le proprie attività operative, senza limitare il rispetto degli obblighi normativi e senza pregiudicare la continuità e la qualità dei servizi forniti ai propri clienti.

In caso di trasferimento ad un altro fornitore di servizi è necessario avviare il processo di gestione delle esternalizzazioni come descritto nei paragrafi precedenti.

In caso di cessazione dell'accordo, la Funzione Richiedente e ogni unità coinvolta aggiornano i campi di propria competenza nel registro delle esternalizzazioni.

7 Quadro Normativo di Riferimento

I principi e le regole definiti nel presente Documento fanno riferimento al seguente contesto legislativo e regolamentare:

- Disposizioni di vigilanza per gli istituti di pagamento e gli istituti di moneta elettronica emesse da Banca d'Italia il 23 luglio 2019;
- Final Report relativo alle linee guida in materia di accordi di outsourcing pubblicato dall'European Banking Authority (EBA) del 25 Febbraio 2019, in vigore dal 30 Settembre 2019, recepite da Banca d'Italia con la circolare n. 34 del 23 Settembre 2020.

8 Allegato

Si allega la scheda di valutazione dell'esternalizzazione che deve essere compilata dalla Funzione Richiedente per avviare il processo di gestione sia di una nuova esternalizzazione (sia in caso di Funzione Essenziale o Importante che non) che di successivo monitoraggio con variazione del perimetro della funzione esternalizzata.

2022_Flowe_Scheda
di Valutazione dell'Est