Policy di Gestione del Rischio ICT e di Sicurezza

Consiglio di Amministrazione del 20/02/2024

Indice

1. PREMESSA

L'evoluzione normativa e regolamentare, come conseguenza della necessità di sviluppare una regolamentazione più armonizzata all'interno dell'Unione Europea, e il ruolo del sistema informativo quale strumento di primaria importanza per il conseguimento degli obiettivi strategici e operativi degli intermediari, pongono sempre maggiore attenzione ai sistemi di identificazione e gestione dei rischi informatici.

L'attività di controllo e gestione dei rischi informatici, è in continua evoluzione ed aggiornamento sia in considerazione delle modifiche del contesto normativo che dei continui cambiamenti esogeni ed endogeni del business di riferimento.

Scopo del presente documento è fornire una descrizione dei principi e del modello adottati da Flowe (in seguito anche la Società) in tema di Gestione del Rischio ICT e di sicurezza.

In particolare, con la presente Policy, si intende disciplinare gli aspetti organizzativi, operativi e metodologici in materia di Rischio ICT e di sicurezza.

1.1 Contesto di riferimento

Le indicazioni normative di settore[1], in particolare derivanti dalle "EBA Guidelines on ICT and security risk management" e dalle "Disposizioni di Vigilanza per gli istituti di pagamento e gli istituti di moneta elettronica" di Società d'Italia, invitano le imprese a formalizzare il quadro di riferimento per la determinazione della propensione al rischio ICT e di sicurezza e le politiche di governo e il processo di gestione di tale rischio, assicurandone l'applicazione e procedendo al loro riesame periodico per garantirne l'efficacia nel tempo. La responsabilità primaria è attribuita agli Organi aziendali, ciascuno secondo le rispettive competenze.

In tale contesto, il presidio del Rischio ICT e di sicurezza è affidato alle competenti funzioni aziendali, con presidi adeguati nelle strutture di primo, secondo e terzo livello. La definizione delle policy di controllo e gestione di tale rischio ricade sotto la Responsabilità della Funzione Risk Management[2], in outsourcing presso la Banca (che unitamente alla Funzione Compliance per gli aspetti di conformità ed alla Funzione Antiriciclaggio per gli aspetti AML costituisce la 2° linea di difesa, entrambe in outsourcing presso la Capogruppo). Il presidio di primo livello è attribuito all'Unità Organizzativa IT Operation Security & Governance[3] e, in generale, alla *perspective* Product Development & IT Services, nel cui ambito è collocata. Un ruolo importante è inoltre affidato ai Responsabili di unità organizzative (anche detti Utenti Responsabili), referenti chiave per la valutazione delle potenziali perdite derivanti da minacce tecnologiche e di sicurezza.

Il documento disciplina principi e responsabilità di controllo e gestione dei rischi informatici e di sicurezza sia nei processi ordinari e di funzionamento, sia nei processi di change, tipici delle attività di carattere progettuale. Le previsioni contenute all'interno del presente documento sono applicate sia durante le attività periodiche di analisi dei rischi informatici, sia nelle iniziative di sviluppo di nuovi progetti o a fronte di rilevanti modifiche del sistema informativo.

[1] Maggiori dettagli sulle normative di riferimento sono presenti al capitolo 9 Normativa di riferimento

[2] Flowe ha nominato un responsabile del Risk Management che si avvale, per lo svolgimento delle attività di controllo, della omologa funzione della Capogruppo, in base ad un apposito contratto di outsourcing. Per semplicità, nel seguito del documento, con Funzione Risk Management si intende l'Unità Operational Risk Management della Funzione Risk Management della Capogruppo, che svolge le attività di controllo del rischio informatico illustrate nel presente documento in accordo e sotto la supervisione del responsabile della Funzione Risk Management di Flowe.

[3] L'Unità Organizzativa IT Operation Security & Governance di Flowe si avvale della collaborazione del Settore IT Security della Capogruppo, in base ad apposito contratto di outsourcing

1.2 Ambito del documento

Il presente documento definisce le regole di governo e le politiche di gestione dei rischi da adottare da Flowe in qualità di Società del Gruppo Mediolanum, in conformità alle disposizioni normative vigenti e al framework metodologico in uso presso la Capogruppo Società Mediolanum S.p.A. e trasmesso alle società controllate.

Nello specifico, questo documento ha l'obiettivo, all'interno del quadro di riferimento delineato in precedenza, di:

- individuare i principi generali di governance del Rischio ICT e di sicurezza;
- dettagliare i compiti e le responsabilità delle entità organizzative coinvolte;
- definire i modelli di riferimento per l'individuazione dei rischi informatici;
- assicurare la conformità con i requisiti espressi dalle Autorità di Vigilanza in materia di rischi informatici;
- fornire una definizione di Rischio ICT e di Sicurezza e dotare la Società di un glossario di riferimento per le tematiche relative alla gestione dei rischi informatici.

Il processo di gestione dei rischi ICT e di sicurezza è pienamente integrato e allineato con il processo di gestione dei rischi della Società. Tutte le unità organizzative della Società sono chiamate, a vario titolo, a supportare il processo di controllo e gestione dei rischi informatici, ciascuna nei limiti della propria competenza ed in funzione del grado di esposizione ai fattori di rischio e in relazione all'attività svolta.

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

Con riferimento alla "Policy di Conglomerato sulle modalità di redazione, approvazione, diffusione ed aggiornamento della Normativa Interna" il presente documento costituisce il primo livello della piramide documentale richiamata nello schema seguente.

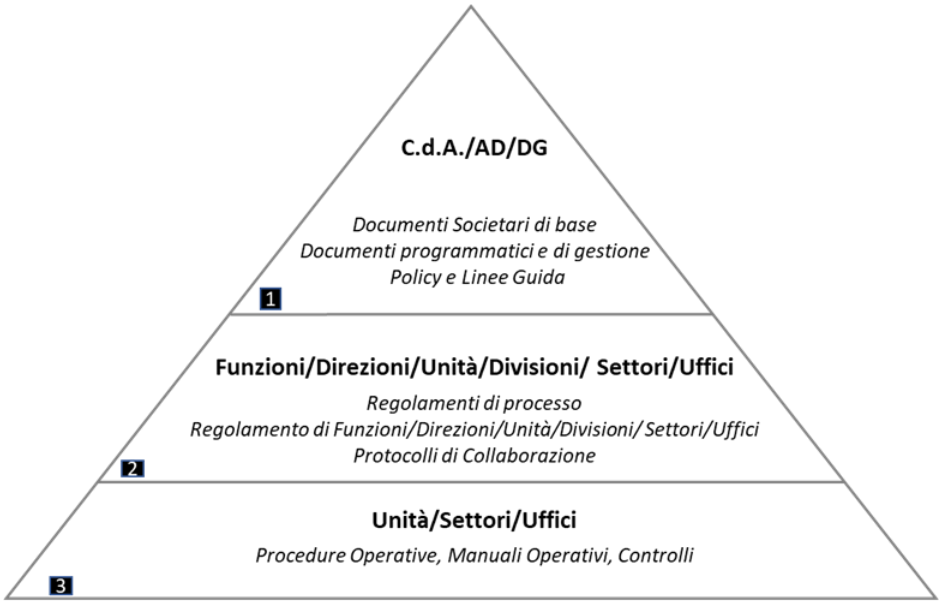

Figura 1: Modello della normativa interna di riferimento

1.3 Principi Generali

Flowe, in conformità alla normativa vigente, definisce il Rischio ICT e di Sicurezza come:

"il rischio di incorrere in perdite economiche, di reputazione e di quote di mercato in relazione all'utilizzo di tecnologia dell'informazione e della comunicazione (Information and Communication Technology – ICT) dovuto a violazione della riservatezza, carente integrità dei sistemi e dei dati, inadeguatezza o indisponibilità dei sistemi e dei dati o incapacità di sostituire la tecnologia dell'informazione (ICT) entro ragionevoli limiti di tempo e costi in caso di modifica dei requisiti del contesto esterno o dell'attività (agility), nonché i rischi di sicurezza derivanti da processi interni inadeguati o errati o da eventi esterni, inclusi gli attacchi informatici o un livello di sicurezza fisica inadeguata".

Si può, pertanto, definire l'IT Risk Management come il processo dedicato all'identificazione, misurazione, monitoraggio e gestione del rischio ICT e di sicurezza, nel rispetto delle linee di indirizzo del Sistema dei Controlli Interni, definite dal Consiglio di Amministrazione.

Tale obiettivo generale si declina nei seguenti obiettivi specifici:

- determinare la propensione al rischio ICT e di sicurezza;
- identificare e valutare il profilo di rischio ICT e di sicurezza esistente per ciascun asset ICT/processo in perimetro;
- assicurare che tutti i rischi ICT e di sicurezza assunti o assumibili siano individuati, analizzati, misurati, monitorati, gestiti, comunicati e mantenuti entro i limiti della propensione al rischio ICT e di sicurezza della Società;
- supportare le scelte strategiche fornendo una valutazione dei rischi informatici insiti in nuove iniziative, cambiamenti rilevanti, etc.;
- progettare e realizzare interventi volti a ridurre, trasferire e/o mitigare i rischi informatici;
- diffondere la cultura della gestione del rischio all'interno della società e favorire comportamenti e scelte consapevoli e coerenti;
- dotarsi di un sistema di gestione dei rischi informatici con ruoli e responsabilità chiaramente definiti, prevedendo supporto e coordinamento con le altre unità.

Propensione al Rischio ICT e di sicurezza

La propensione al rischio ICT e di sicurezza è definita come una componente della più ampia propensione al rischio della Società e rappresenta il massimo Rischio ICT che la Società intende assumere per il perseguimento dei suoi obiettivi strategici.

Nell'ambito delle valutazioni di rischio ICT e di sicurezza oggetto della presente Policy è, definita ed annualmente approvata dal Consiglio di Amministrazione una **soglia di propensione al rischio ICT e di sicurezza qualitativa**, utilizzata per individuare le soglie di accettabilità o non accettabilità del rischio ICT e di sicurezza stesso.

2. APPLICABILITÀ

2.1 Destinatari del documento

Il presente documento, approvato dal Consiglio di Amministrazione, trova diretta applicazione all'interno della Società.

I principi definiti si applicano a tutte le Unità organizzative della Società incluse nel perimetro di intervento ed in particolare a tutti i soggetti (personale interno/esterno, outsourcer, etc.) coinvolti nelle attività di gestione del sistema informativo aziendale.

2.2 Responsabilità del documento

La presente Policy è aggiornata dalla Funzione Risk Management, con cadenza almeno annuale, ed è sottoposta all'esame ed all'approvazione del Consiglio di Amministrazione di Flowe.

3. DEFINIZIONI

Campagna: attività di analisi dei rischi effettuata su un perimetro di asset ICT e processi in esercizio, in un determinato periodo di tempo. La campagna è caratterizzata dalla durata del periodo e dal perimetro di asset ICT e processi oggetto di analisi.

Controlli sui rischi e sulla conformità (c.d. "controlli di secondo livello"): l'insieme dei controlli, anche detti presidi, che hanno l'obiettivo di assicurare, tra l'altro:

- la corretta attuazione del processo di gestione dei rischi;
- il rispetto dei limiti operativi assegnati alle varie funzioni;
- la conformità dell'operatività aziendale alle norme, incluse quelle di autoregolamentazione.

Le Funzioni preposte a tali controlli sono distinte da quelle produttive: esse concorrono alla definizione delle politiche di governo dei rischi e del processo di gestione dei rischi.

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.

Fornitore di servizi (outsourcer): soggetto terzo (identificato sia all'interno che all'esterno del Gruppo) che realizza, in tutto o in parte, un processo, un servizio o un'attività esternalizzata nell'ambito di un accordo di esternalizzazione.

Funzioni Aziendali di Controllo: le Funzioni identificate come tali dalla normativa di settore vigente; a titolo esemplificativo e non esaustivo, rientrano in tale categoria le Funzioni di Internal Audit, Risk Management, Compliance e Antiriciclaggio.

Progetto ICT (ICT Project): qualsiasi progetto, o parte di esso, in cui i sistemi e i servizi ICT sono modificati, sostituiti, dismessi o implementati e previsto dal piano Strategico ICT. I progetti ICT possono far parte di più ampi programmi ICT o di trasformazione aziendale.

Propensione al rischio informatico: massimo Rischio Informatico che la Società intende assumere per il perseguimento dei suoi obiettivi strategici.

Utente Responsabile: la figura aziendale identificata per ciascun sistema o applicazione che ne assume formalmente la responsabilità in rappresentanza degli utenti e nei rapporti con le Unità Organizzative preposte allo sviluppo e alla gestione tecnica.

Rischio ICT e di Sicurezza: il rischio di incorrere in perdite economiche, di reputazione e di quote di mercato in relazione all'utilizzo di tecnologia dell'informazione e della comunicazione (Information and Communication Technology – ICT) dovuto a violazione della riservatezza, carente integrità dei sistemi e dei dati, inadeguatezza o indisponibilità dei sistemi e dei dati o incapacità di sostituire la tecnologia dell'informazione (ICT) entro ragionevoli limiti di tempo e costi in caso di modifica dei requisiti del contesto esterno o dell'attività (agility), nonché i rischi di sicurezza derivanti da processi interni inadeguati o errati o da eventi esterni, inclusi gli attacchi informatici o un livello di sicurezza fisica inadeguata.

Rischio ICT e di Sicurezza Potenziale: il rischio ICT e di sicurezza a cui la Società è esposta prima dell'applicazione delle misure di attenuazione individuate nel processo di analisi dei rischi.

Rischio ICT e di Sicurezza Residuo: il rischio ICT e di sicurezza a cui la Società è esposta una volta applicate le misure di attenuazione individuate nel processo di analisi dei rischi.

Sistema dei controlli interni:

Il sistema dei controlli interni è costituito dall'insieme delle risorse, delle strutture organizzative, delle regole e delle procedure per assicurare il conseguimento delle strategie aziendali e dell'efficacia ed efficienza dei processi aziendali, della salvaguardia del valore delle attività e della protezione dalle perdite, dell'affidabilità e integrità delle informazioni contabili e gestionali, della conformità delle operazioni con la legge, la normativa di vigilanza e di sorveglianza sul sistema dei pagamenti e le disposizioni interne dell'istituto.

Nel sistema dei controlli interni rientrano le strategie, le politiche, i processi e i meccanismi riguardanti la gestione dei rischi a cui l'istituto è o potrebbe essere esposto e per determinare e controllare il livello di rischio tollerato. In questo contesto, la gestione dei rischi include le funzioni di individuazione, assunzione, misurazione, sorveglianza e attenuazione dei rischi.

Strutture Operative: tutte le Unità Organizzative previste dalla Relazione sulla Struttura Organizzativa, diverse dalle Funzioni Aziendali di Controllo.

4. RUOLI E RESPONSABILITÀ

Di seguito si riportano i ruoli e le responsabilità dei principali attori coinvolti nell'ambito del processo di Governance e valutazione del Rischio ICT e di Sicurezza.

Consiglio di Amministrazione

Il Consiglio di Amministrazione (di seguito CdA) nel suo ruolo di Organo con funzione di supervisione strategica, presiedendo gli aspetti di IT Governance, è il responsabile ultimo per il processo decisionale e di controllo del Sistema Informativo della Società, al fine di ottimizzare l'uso degli Asset ICT a supporto della strategia aziendale. Con specifico riguardo all'attuazione della propria responsabilità per la supervisione del processo di analisi e gestione dei Rischi ICT e di Sicurezza, il CdA è chiamato dalla normativa ad assumere le seguenti responsabilità:

- approva la presente policy di gestione del rischio ICT e di sicurezza (ad ogni aggiornamento) e il Rapporto sintetico sulla situazione del rischio ICT e di sicurezza (prodotto con frequenza annuale);
- approva il quadro di riferimento organizzativo e metodologico per la gestione del Rischio ICT e di Sicurezza, promuovendo l'opportuna valorizzazione dell'informazione sul rischio tecnologico all'interno della Società e l'integrazione con i sistemi di misurazione e gestione dei rischi (in particolare quelli operativi, reputazionali e strategici). Il quadro di riferimento è rivisto almeno annualmente, anche alla luce dell'esperienza acquisita durante la sua attuazione e il suo monitoraggio, in un'ottica di continuo miglioramento;
- assicura che il sistema di governo e controllo dei Rischi ICT e di Sicurezza sia costantemente adeguato, anche in termini di dimensionamento qualitativo e quantitativo del personale e di risorse finanziarie disponibili, alle esigenze operative della Società e dei processi di gestione dei Rischi ICT e di Sicurezza e per l'attuazione della strategia ICT;
- approva la soglia di propensione al rischio ICT e di Sicurezza;
- è informato in maniera chiara e tempestiva, e in ogni caso con cadenza almeno annuale, sulla situazione di Rischio ICT e di Sicurezza rispetto alla propensione al rischio, inclusi i risultati della valutazione dei rischi;
- è informato circa l'avvio e l'avanzamento dei progetti ICT, considerati singolarmente o in forma aggregata e in funzione delle loro dimensioni e importanza e dei rischi ad essi associati, su base periodica e, se del caso, all'occorrenza.

Amministratore Delegato

L'Amministratore Delegato, nel suo ruolo di Organo con funzione di gestione, essendo incaricato di garantire la completezza, l'adeguatezza, la funzionalità (in termini di efficienza ed efficacia) e l'affidabilità del Sistema Informativo, è in particolare chiamato dalla normativa ad assumere le seguenti responsabilità:

- definisce i ruoli e le responsabilità per la gestione del rischio ICT e di sicurezza, nonché per le relative attività di continuità operativa;

- definisce l'assetto organizzativo, metodologico e procedurale per il processo di analisi del rischio ICT e di sicurezza perseguendo un opportuno livello di raccordo con la funzione di risk management per i processi di stima del rischio operativo;
- assicura che tutto il personale, incluso il personale che riveste ruoli chiave, riceva una formazione adeguata in materia di rischi ICT e di sicurezza, nonché di sicurezza dell'informazione, almeno una volta all'anno o con maggiore frequenza se necessario;
- approva almeno annualmente la valutazione del rischio degli asset ICT, aggregata a livello di processo, e riscontra la complessiva situazione del rischio ICT e di sicurezza in rapporto alla propensione al rischio definita considerando, come minimo, il livello di rischio residuo per i diversi asset ICT a supporto dei processi della Società, lo stato di implementazione dei presidi di attenuazione del rischio, l'evoluzione delle minacce connesse con l'utilizzo di ICT nonché gli incidenti registratisi nel periodo di riferimento;
- approva l'adozione delle eventuali misure alternative o ulteriori di trattamento del rischio da porre in essere nel caso in cui il rischio residuo ecceda la propensione al rischio approvato dal Consiglio di Amministrazione;
- monitora il regolare svolgimento dei processi di gestione e di controllo dei servizi ICT e, a fronte di anomalie rilevate, pone in atto opportune azioni correttive;
- elabora e propone le linee strategiche ed i piani operativi relativi ai periodici budget ed ai progetti di sviluppo strategico, da sottoporre al Consiglio di Amministrazione. Inoltre, approva il piano operativo delle iniziative informatiche, verificandone la coerenza con le esigenze informative e di automazione delle linee di business nonché con le strategie aziendali.

Funzione Risk Management di Banca Mediolanum, sulla base del contratto di servizio in essere:

- definisce e manutiene il framework di controllo e gestione del rischio ICT e di sicurezza, nel rispetto delle linee guida del Consiglio di Amministrazione e delle disposizioni normative vigenti;
- definisce la metodologia di valutazione e gestione del rischio ICT e di sicurezza e ne garantisce la revisione e l'aggiornamento periodico anche considerando le evoluzioni del contesto interno ed esterno (e.g. analisi post-incident, normative esterne, evoluzioni tecnologiche, trend di settore per quanto riguarda minacce, storico incidenti e soluzioni adottate, standard e best practice) in coerenza con i modelli previsti per rischi operativi e reputazionali;
- definisce la periodicità e il perimetro[4] di asset ICT che sono coinvolti in ciascuna campagna;
- richiede all'Unità Organizzativa IT Operation Security & Governance la mappa applicativa aggiornata comprensiva dei collegamenti con le infrastrutture sottostanti;
- riceve dall'ufficio Organization & Business Continuity, che presidia i processi di Business Continuity con il supporto del Business Continuity Office di Banca, l'aggiornamento delle BIA per le verifiche di coerenza con le valutazioni degli impatti derivanti dall'IT Risk Assessment;

[4] Per maggiori dettagli sulla definizione del perimetro degli asset è possibile consultare il Manuale Operativo Metodologia di gestione del rischio ICT e di Sicurezza

- riceve dall'ufficio Organization & Business Continuity, la mappatura dei processi della Società con gli asset a supporto oltre alle valutazioni di riservatezza, integrità e disponibilità dei data asset derivanti dal modello di Data Protection;
- definisce e aggiorna, prima di ogni campagna, i cataloghi utilizzati per le analisi dei rischi (scenari di rischio, presidi di controllo, Key Risk Indicators);
- calcola il valore della probabilità di accadimento con le risultanze derivanti dall'analisi del contesto esterno, dagli incidenti occorsi e dalle valutazioni dei presidi/misure di sicurezza IT;
- esegue test di coerenza periodici su un campione di controlli del framework, al fine di verificarne la corretta esecuzione;
- effettua il monitoraggio, nel continuo, dei valori assunti dai Key Risk Indicators, definiti e raccolti con il supporto dell'Unità Organizzativa IT Operation Security & Governance e del Settore IT Security di Banca Mediolanum, integrandoli nella valutazione finale del rischio ICT e di sicurezza;
- analizza, ove disponibile, la metodologia di analisi del rischio ICT e di sicurezza adottata dagli outsourcer, per definirne le modalità di integrazione nelle valutazioni di probabilità sugli ambiti di competenza;
- supporta l'Utente Responsabile, con il contributo dell'Unità Organizzativa IT Operation Security & Governance, nella definizione di eventuali misure compensative / presidi IT da integrare nei Piani di Trattamento;
- definisce, con il contributo dell'Unità Organizzativa IT Operation Security & Governance, e monitora eventuali piani di rimedio per i controlli con esito non soddisfacente a seguito di test di coerenza sulla loro esecuzione;
- valuta il Rischio Residuo ed i Piani di Trattamento e li propone per accettazione all'Utente Responsabile;
- cura, annualmente e con il supporto dell'Unità IT Operation Security & Governance e del Settore IT Security di Banca Mediolanum, la predisposizione di un Rapporto sintetico sulla situazione del Rischio ICT e di Sicurezza, nonché la Relazione sui rischi legati ai Servizi di Pagamento, da sottoporre al Consiglio di Amministrazione, previa condivisione con la Funzione Compliance per la valutazione inerente agli aspetti di conformità alla regolamentazione;
- monitora costantemente il rischio residuo assunto dall'intermediario e la sua coerenza con gli obiettivi e l'appetito di rischio definiti;
- monitora l'implementazione dei piani di rimedio condivisi;
- rivaluta annualmente la soglia gestionale di propensione al Rischio ICT e di Sicurezza;
- è informata su qualsiasi attività o evento che influenzi in modo rilevante il profilo di rischio della Società, incidenti operativi o di sicurezza significativi, nonché qualsiasi modifica sostanziale ai sistemi e ai processi ICT;
- nel contesto della valutazione dei rischi delle nuove iniziative ICT e sulla base di driver definiti, effettua una verifica di secondo livello, al fine di approfondire e identificare eventuali rischi che lo svolgimento del progetto potrebbe comportare per la Società;
- nel contesto della verifica e dell'accettazione del rischio residuo delle nuove iniziative ICT, effettua una valutazione di secondo livello per assicurarsi che vengano rispettati i

requisiti richiesti per la mitigazione dei rischi identificati. Inoltre, procede a raccogliere l'accettazione del rischio dall'utente Responsabile[5].

Utente Responsabile[6], per gli asset ICT di propria competenza:

- è coinvolto nella valutazione del Rischio ICT e di sicurezza, essendo in particolare responsabile della valutazione degli impatti associati agli Scenari di Rischio ICT;
- accetta il Rischio Residuo ICT e di sicurezza;
- collabora alla definizione dei Piani di Trattamento del Rischio ICT con il Risk Management e con l'Unità Organizzativa IT Operation Security & Governance;
- accetta formalmente i tempi di attuazione del piano di trattamento e i presidi compensativi di tipo organizzativo o procedurale nelle more dell'attuazione;
- è coinvolto, di concerto con la funzione Risk Management, nella fase di accettazione del rischio residuo delle nuove iniziative ICT.

Product Development & IT Services:

- promuove, ispirandosi a criteri di funzionalità, efficienza e sicurezza, in linea con i piani strategici aziendali e con l'evoluzione degli scenari tecnologici, la gestione e lo sviluppo dei Sistemi Informativi e di comunicazione della Società;
- assicura la chiara attribuzione dei compiti e delle responsabilità in capo alle unità organizzative in cui è strutturata, che costituiscono la 1° linea di difesa aziendale per il rischio informatico e di sicurezza;
- nel contesto della valutazione dei rischi delle nuove iniziative progettuali ICT, supervisiona le valutazioni relative alla realizzazione del progetto in termini di costi, attività, architetture, infrastrutture.

IT Operation Security & Governance, avvalendosi del supporto del Settore IT Security della Banca, ove previsto dal contratto di servizi in essere:

- definisce il quadro di riferimento metodologico e di controllo di primo livello per il presidio e per il governo del rischio informatico e di sicurezza, condividendolo con le strutture della Società interessate;
- supporta la funzione Risk Management nell'attività di rivalutazione annuale della propensione gestionale al Rischio ICT;
- verifica che le Policy e i presidi di sicurezza IT e le procedure operative siano mantenute aggiornate rispetto alle normative generali, di settore, alle indicazioni della Capogruppo e che siano coerenti con le Policy approvate;
- supporta la Funzione Risk Management per la raccolta e l'aggiornamento periodico della mappatura degli asset ICT di interesse per l'ICT Risk, nonché per la pianificazione delle interviste con gli IT Risk Control Owner;

[5] Nel caso in cui non sia presente un Utente Responsabile, l'accettazione del rischio residuo dell'iniziativa è in carico, a seconda del tipo di progetto, allo Sponsor del Progetto o al Leadership Team.
[6] L'Utente Responsabile può essere individuato, in caso di Asset in outsourcing, nella figura del Referente per l'Attività Esternalizzata

- garantisce l'applicazione delle policy di sicurezza nello sviluppo delle soluzioni IT e raccoglie l'evidenza delle misure di sicurezza implementate;
- effettua, nella figura dell'IT Risk Control Owner, la valutazione dei presidi di competenza ICT che contribuiscono alla definizione della probabilità di accadimento degli scenari di Rischio ICT, fornendo inoltre i dati storici degli incidenti informatici;
- raccoglie dagli outsourcer, tramite la compilazione della scheda "Modulo sulle caratteristiche del trattamento e misure di sicurezza" o idonea documentazione alternativa, le valutazioni sui presidi del rischio ICT;
- verifica l'adozione delle misure prese per rimediare alle carenze riscontrate nel processo di Valutazione del Rischio ICT e di sicurezza;
- supporta la Funzione Risk Management, nella fase di Trattamento e nella definizione di misure compensative / alternative da integrare nei Piani di Trattamento;
- fornisce, alla funzione Risk Management, i dati utili e necessari per il calcolo degli indicatori di rischio ICT;
- in accordo con la Direttiva (UE) 2015/2366 (PSD2) del Parlamento Europeo, svolge analisi del rischio ICT di dettaglio per i servizi di pagamento con il coinvolgimento della Funzione Risk Management;
- monitora, nel continuo, l'evoluzione delle minacce IT, ne aggiorna l'elenco e lo condivide con la Funzione Risk Management con cadenza almeno annuale;
- nel contesto della valutazione dei rischi delle nuove iniziative ICT, provvede all'identificazione ed all'esportazione dei requisiti di sicurezza mandatory da rispettare durante l'intero ciclo di vita del progetto e valuta le risposte fornite dal PM/Product Owner in merito alla loro implementazione.

Funzione Internal Audit, di Banca Mediolanum, sulla base del contratto di servizio in essere:

- riesamina, secondo un approccio basato sul rischio, tutte le attività e le unità organizzative relative all'ICT e alla sicurezza in modo indipendente e fornisce garanzie oggettive circa la conformità alle policy, alle procedure e ai requisiti esterni;
- definisce e aggiorna regolarmente il piano di audit, compresa la modalità di esecuzione e la frequenza degli audit, che rifletta e sia proporzionato ai rischi della Società, compresi quelli riferiti all'ICT e alla sicurezza.

Funzione Compliance, di Banca Mediolanum, sulla base del contratto di servizio in essere.

La Funzione Compliance è responsabile del processo di verifica della conformità alle norme e presiede la gestione dei rischi di non conformità alle norme, secondo un approccio risk based. Alla Funzione competono attività di consulenza specialistica, ai fini della valutazione del rischio di conformità, il costante monitoraggio del contesto normativo esterno (alert normativo), la valutazione dell'impatto delle normative (gap analysis) sui processi aziendali, le verifiche di adeguatezza (attraverso l'identificazione di proposte di modifiche, anche organizzative e procedurali, derivanti anche da gap analysis, valutazioni e pareri) e di funzionamento di assetti e processi aziendali atte a prevenire la violazione di norme imperative o di

autoregolamentazione e il monitoraggio dell'adozione delle misure correttive proposte. Nell'ambito della presente policy, inoltre, la Funzione Compliance supporta l'Utente Responsabile, qualora necessario, per la compilazione delle domande relative all'assoggettamento dell'asset ICT ai requisiti normativi da essa presidiati.

Funzione Antiriciclaggio, di Banca Mediolanum, sulla base del contratto di servizio in essere:

- supporta l'Utente Responsabile, qualora necessario, per la compilazione delle domande relative all'assoggettamento dell'asset ICT ai requisiti normativi e antiriciclaggio.

IT Risk Control Owner[7], per gli asset ICT di propria competenza:

- contribuisce alla valutazione del rischio ICT e di sicurezza, essendo responsabile della valutazione di efficacia dei presidi di controllo di propria competenza;
- può essere coinvolto nella definizione e applicazione di eventuali misure compensative / presidi IT da integrare nei Piani di Trattamento.

Outsourcer:

- fornisce le sue valutazioni sui presidi del rischio ICT e di sicurezza tramite compilazione della scheda "Modulo sulle caratteristiche del trattamento e misure di sicurezza" o idonea documentazione alternativa. Tali valutazioni vengono integrate nel calcolo della probabilità di accadimento dei vari scenari di rischio correlati agli asset ICT esternalizzati dalla società.

Organization & Business Continuity

- cura la manutenzione del framework organizzativo, attraverso l'aggiornamento di assetti e processi e collaborando con i process owner per una adeguata formalizzazione degli stessi;
- effettua l'assessment periodico dei processi aziendali, con particolare riguardo a quelli critici in ottica continuità operativa, tracciando gli attori, gli strumenti (Asset, Euda, ecc.), gli outsourcer e i fornitori rilevanti;
- definisce il modello di Data Protection per la classificazione dei requisiti di Riservatezza, Integrità e Disponibilità degli asset ICT, e ne supporta la rilevazione tramite assessment che coinvolgono gli utenti di riferimento;
- cura le iniziative di sviluppo organizzativo e trasformazione digitale dei processi aziendali, previa valutazione di costi – benefici delle specifiche iniziative di automazione.

[7] Il Control Owner corrisponde a ciascun referente/ufficio individuato come accountable dello specifico presidio e conseguentemente ha il compito di valutare l'efficacia del presidio stesso.

Market Product Owner

- è responsabile dell'analisi e della prioritizzazione degli interventi e della loro pianificazione in un orizzonte temporale che garantisca il raggiungimento degli obiettivi definiti dal Leadership Team al quale propone la roadmap di sviluppo per opportuna validazione e aggiornamento;

- recepisce i requisiti delineati dall'unità organizzativa IT Operation Security & Governance e le eventuali indicazioni da parte della funzione Risk Management, da indirizzare durante lo svolgimento di un progetto o dello sviluppo di una feature, e ne monitora l'implementazione.

Leadership Team:

- nel rispetto degli indirizzi e delle linee strategiche definite dal Consiglio di Amministrazione e dall'Amministratore Delegato, è responsabile della definizione del piano strategico della Società all'interno del quale vengono definite i progetti cosiddetti "strategici" volti a garantire il raggiungimento degli obiettivi di business definiti;

- nel caso in cui non sia presente un Utente Responsabile o uno sponsor di progetto, verifica e accetta il rischio residuo delle nuove iniziative ICT. monitora l'implementazione dei requisiti delineati dall'unità organizzativa IT Operation Security & Governance e le eventuali indicazioni da parte della funzione Risk Management.

5. MODELLO DI RISCHIO ICT E DI SICUREZZA

Gli elementi che costituiscono il modello di rischio ICT e di Sicurezza sono definiti sulla base della normativa di riferimento, di best practices di settore e in modo coerente con le metodologie di analisi dei rischi operativi, reputazionali e strategici della Società.

La gestione del Rischio ICT e di Sicurezza si poggia sulle tre linee di difesa di seguito riportate:

- la prima linea di difesa è costituita dalla *perspective* Product Development & IT Services e, in particolare, dall' dall'Unità Organizzativa, ad essa appartenente, IT Operation Security & Governance, che definisce, implementa e verifica la efficacia delle misure di attenuazione dei rischi ICT e di sicurezza per i propri ambiti di competenza, che coinvolgono a tal fine i referenti di business responsabili degli asset ICT e/o dei processi dalle stesse supportati nella definizione e valutazione delle misure di attenuazione dei rischi;
- la seconda linea di difesa è costituita dalle Funzioni Risk Management e dalla Funzione Compliance della Capogruppo, ciascuna per gli ambiti di competenza. La funzione Risk Management è responsabile del monitoraggio e del controllo dei rischi ICT e di sicurezza e garantisce che i rischi ICT e di sicurezza siano individuati, misurati, valutati, gestiti, monitorati, segnalati e mantenuti entro i limiti della propensione al rischio dell'istituto finanziario; la Funzione Compliance è responsabile della gestione dei rischi di non conformità alle norme;
- la terza linea di difesa è costituita dalla Funzione Internal Audit, che verifica l'efficacia e l'efficienza dei processi ICT, valutando l'adeguatezza dei controlli di primo e secondo livello.

L'analisi e valutazione dell'esposizione al rischio ICT e di sicurezza è condotta dalla Funzione Risk Management attraverso l'"ICT Risk Assessment".

Di seguito, viene riportata una rappresentazione grafica del framework ICT Risk Assessment[8].

[8] Per maggiori dettagli è possibile consultare il Manuale Operativo *Metodologia di gestione del rischio ICT e di Sicurezza*

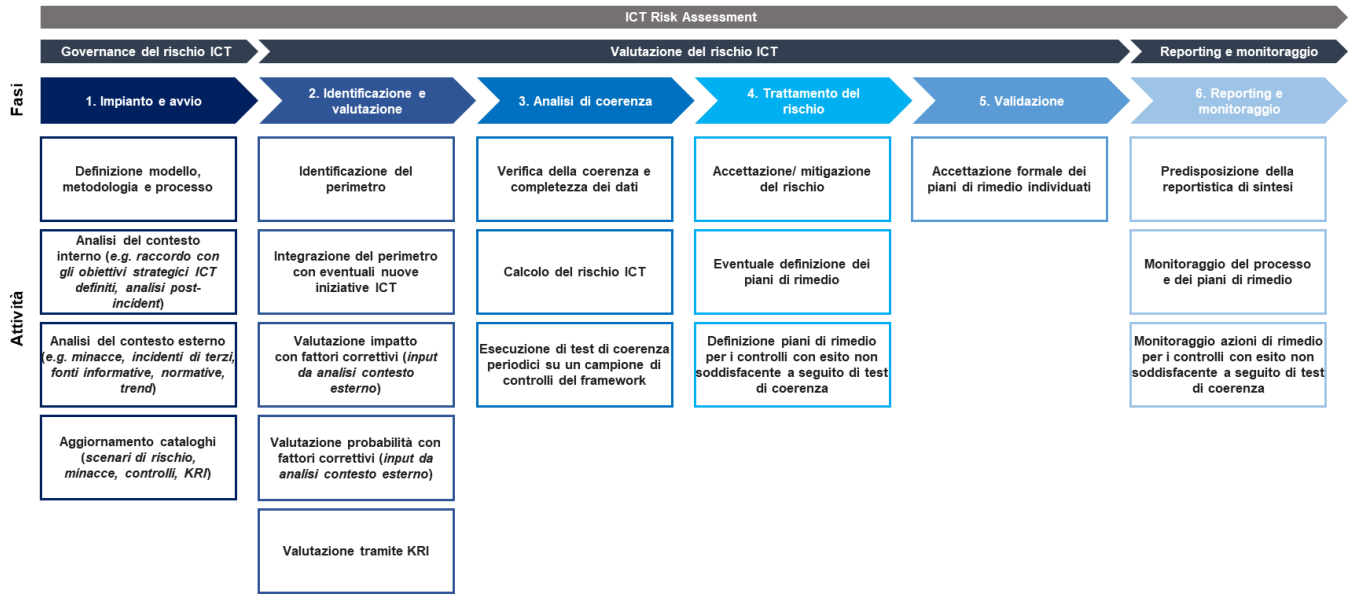

Figura 2 – Schema semplificato del processo di ICT Risk Assessment

Si declina di seguito ciascun elemento rientrante nel processo di analisi e valutazione del rischio ICT e di sicurezza.

5.1 Processo

Il processo è una sequenza strutturata di attività organizzate e interconnesse che vengono svolte, al fine di convertire input specifici in output desiderati, con l'obiettivo di soddisfare un'esigenza del cliente o raggiungere un obiettivo aziendale.

5.2 Asset ICT

Nell'ambito della presente Policy, l'asset ICT è "un bene dell'azienda afferente all'ICT che concorre alla ricezione, archiviazione, elaborazione, trasmissione e fruizione dell'informazione gestita dall'intermediario". L'asset ICT può essere declinato in applicazione o infrastruttura IT.

5.3 Applicazioni

Nell'ambito della presente Policy, per applicazione si intende un sistema riconoscibile dall'utente attraverso un nome ed un'interfaccia con la quale interagisce o, in caso di applicazioni specialistiche, un sistema che eroga delle funzionalità tecniche e/o di utility necessarie all'erogazione delle funzionalità aziendali.

5.4 Infrastrutture IT

L'infrastruttura IT è l'insieme delle componenti infrastrutturali, tra cui i server, unità computazionale base del sistema informativo, che concorrono all'erogazione di una o più applicazioni. Nell'ambito della presente policy, per infrastrutture IT si intendono i raggruppamenti tecnologici forniti dall'Unità Organizzativa IT Operation Security & Governance e mappati con gli applicativi.

5.5 Scenari di Rischio ICT

Gli scenari di rischio ICT rappresentano degli insiemi di minacce raggruppate per caratteristiche comuni (ad esempio attività illecite interne, compromissioni dall'esterno, etc.). I tipici effetti derivanti dall'accadimento delle minacce che compongono gli scenari di rischio sono riferibili a malfunzionamenti, interruzioni dei servizi informatici (inclusi i servizi di pagamento) o alla perdita di integrità, di disponibilità o di riservatezza dei dati da essi trattati.

Le principali caratteristiche di uno Scenario di Rischio ICT sono:

- ciascuna minaccia sottostante lo scenario definito che genera la medesima tipologia di conseguenza per il business in termini di impatto;
- per ciascuno scenario sono identificati dei Presidi IT che mitigano le conseguenze derivanti dal verificarsi dello scenario stesso.

Per l'elenco degli Scenari di Rischio ICT identificati dalla Società, occorre fare riferimento all'

Allegato 1 – Scenari di rischio.

5.6 Libreria dei presidi/misure di sicurezza IT

Nell'ambito più generale del Sistema dei Controlli Interni, ai fini del presente documento si definisce "Presidio/misura di sicurezza IT", un controllo di linea o una misura di sicurezza implementato dalla Società ai fini della mitigazione di uno o più Scenari di Rischio ICT.

I Presidi possono agire sui Rischi ICT nelle seguenti modalità:

- riducendo l'esposizione dell'asset ICT limitando la probabilità di accadimento che la minaccia possa concretizzarsi;
- limitando l'impatto di una minaccia nel caso questa si concretizzi.

Nell'analisi del rischio ICT e di sicurezza sono altresì valutati i diversi aspetti pertinenti alla sicurezza informatica, quali ad esempio la gestione degli accessi logici, della sicurezza fisica, la gestione dei log, l'esecuzione dei backup, etc. A tal proposito, nella libreria dei presidi/misure di sicurezza IT[9] è stato inserito un ambito puntuale comprendente le tematiche sopracitate, oltre agli aspetti relativi alla cyber security.

Il framework dei presidi/misure di sicurezza è aggiornato dalla funzione Risk Management, con cadenza almeno annuale, anche in base all'analisi delle nuove minacce svolta nella fase di analisi del contesto interno/esterno, al fine di valutare l'eventuale introduzione di nuovi presidi necessari alla mitigazione di nuove minacce emergenti.

5.7 Impatto IT

L'impatto IT è la conseguenza negativa per la Società, causata dal realizzarsi di una o più minacce di rischio sull'asset ICT, in termini di perdite economiche, di reputazione e di quote di mercato.

[9] L'elenco dei presidi deriva dai principali standard internazionali di settore in tema di sicurezza informatica quali ISO27001, NIST SP 800-53 etc.

Le tipologie di impatto da valutare possono includere:

- **Impatto operativo**, **finanziario** ed **economico**, quali:
    - Maggiori costi, anche figurativi, per ripristinare il servizio, garantirne la continuità, correggere gli errori prodotti, sostituire i beni danneggiati, etc.;
    - Perdite per risarcimento di frodi e danni patrimoniali subiti dalla clientela, penali contrattuali per mancato rispetto dei livelli di servizio contrattualizzati, spese cause legali, sanzioni causate da violazioni di conformità normative vigenti etc.;
    - Mancati ricavi a causa dell'impossibilità di dare seguito alle operazioni disposte dalla clientela di negoziazione titoli, incassi e pagamenti, etc..
- **Impatto reputazionale e commerciale,** con conseguenti danni in termini di: perdita di clientela, riduzione quote di mercato, risonanza mediatica, etc.

L'impatto, nel modello adottato dalla Società, è valutato in termini quali-quantitativi, utilizzando una scala di valori qualitativa associata a range economici.

La stima dell'impatto generato dal concretizzarsi di uno scenario di rischio è effettuata puntualmente per ogni scenario di rischio ICT associabile ad ognuno degli asset ICT in perimetro di analisi e potrebbe tener conto dei fattori correttivi individuati nella fase di "analisi di contesto".

5.8 Probabilità

La probabilità di accadimento è la stima della condizione con cui una minaccia può verificarsi su una o più componenti IT in un determinato periodo di tempo, causando un impatto negativo per la Società.

La probabilità di accadimento di ciascuna minaccia è stimata sulla base dello stato di implementazione dei presidi IT afferenti alla minaccia stessa, considerando altresì la rilevazione degli incidenti avvenuti nel periodo, nonché gli eventuali fattori correttivi individuati nella fase di "analisi di contesto".

5.9 Il Rischio ICT e di Sicurezza

Il Rischio ICT e di Sicurezza, nell'ambito della presente policy, può essere valutato in termini di:

- **Rischio ICT e di sicurezza Potenziale** a cui sono esposti gli asset ICT: rappresenta il livello di Rischio ICT a cui è soggetto un determinato asset ICT o processo, in termini di possibilità di concretizzarsi di uno scenario di rischio ICT, che possa arrecare un danno, in termini di perdita di riservatezza, di integrità e/o di disponibilità del dato, al processo e all'operatività di quest'ultimo;
- **Rischio ICT e di sicurezza Residuo**: rappresenta il rischio stimato a seguito dell'applicazione di contromisure – di tipo tecnico, organizzativo, procedurale o strategico - atte a determinare una riduzione del Rischio Potenziale. La valutazione di tale rischio tiene conto dei presidi di controllo in essere.

5.10 Key Risk Indicators

I Key Risk Indicators (KRI) sono indicatori di rischio finalizzati ad ottenere una valutazione di alto livello relativa all'esposizione al rischio ICT e di sicurezza della Società, nonché a monitorare l'esposizione stessa nel continuo, al fine di identificare eventuali incrementi di rischio determinati da eventi misurabili e oggettivi.

I KRI, oltre che monitorare i livelli di rischio nel continuo, forniscono gli elementi chiave per l'individuazione degli Asset ICT maggiormente esposti al rischio ICT e di sicurezza.

5.11 Criticità dei processi e degli asset ICT a supporto

La Società adotta processi atti ad individuare, stabilire e mantenere aggiornato l'inventario delle proprie funzioni aziendali, dei ruoli e dei processi di supporto per determinare l'importanza e le interdipendenze di ciascuno di essi in relazione ai rischi ICT e di sicurezza. Tali attività vengono svolte anche con l'obiettivo di consentire una corretta classificazione, sotto il profilo della criticità, delle funzioni aziendali, dei processi che le supportano e gli asset ICT.

I processi aziendali sono classificati come critici in base alle tre principali dimensioni, Riservatezza, Integrità e Disponibilità (di seguito anche "RID") e comunque sono tutti quei processi a servizio delle attività dei clienti e/o core business della Società. Tutti gli asset ICT per lo svolgimento di tali processi sono classificati come critici.

La classificazione di criticità dei processi e degli asset ICT a supporto sulle dimensioni citate, Riservatezza, Integrità e Disponibilità, è effettuata con il coinvolgimento degli utenti di business responsabili dei processi (*process owner*) e degli asset ICT a supporto, in coerenza con il processo di "Business Impact Analysis" (BIA)[10].

[10] L'attività di classificazione dei processi in base ai parametri RID sarà svolta a partire dall'esercizio 2025, in attesa della prima implementazione del modello di classificazione da parte della Capogruppo.

6. GESTIONE DEL RISCHIO ICT E DI SICUREZZA

La gestione del rischio è un processo molto articolato che si sviluppa nelle seguenti macro-fasi:

- Governance del Rischio ICT e di Sicurezza;
- Valutazione del Rischio ICT e di Sicurezza;
- Monitoraggio e Reporting.

6.1 Governance del Rischio ICT e di Sicurezza

Il processo di Governance del Rischio ICT ha come obiettivo definire e mantenere aggiornati il modello, la metodologia, il processo e le procedure operative di gestione del Rischio ICT, in relazione ai cambiamenti del contesto, dell'organizzazione e delle strategie IT della Società, ai cambiamenti normativi e all'evoluzione dei rischi tecnologici sul mercato finanziario.

In tale quadro, il processo di Governance del Rischio ICT è di responsabilità della funzione Risk Management che identifica, manutiene e aggiorna nel continuo le seguenti componenti del modello:

- i **ruoli e le responsabilità** dei principali attori che partecipano e supportano lo svolgimento dell'analisi del rischio ICT e di sicurezza**;**
- i **flussi informativi** necessari alle valutazioni di rischio (ad esempio le serie storiche degli incidenti, gli esiti delle valutazioni dei presidi/misure di sicurezza, etc.);
- i **fattori correttivi** ricavati dall'analisi del contesto interno (e.g., analisi post-incident) ed esterno (e.g. standard e best practice, normative, trend di settore, tra cui minacce emergenti e storico incidenti) da includere nella valutazione del rischio ICT al fine di ottenere risultati più attendibili e realistici;
- i **cataloghi** utilizzati per le analisi dei rischi, quali la mappatura degli asset ICT comprendente le informazioni specifiche per ciascun asset ICT nonché le correlazioni tra processi, applicazioni e infrastrutture IT, gli scenari di rischio ICT, la libreria dei presidi/misure di sicurezza IT e la libreria dei Key Risk Indicators.

6.2 Valutazione del Rischio ICT e di Sicurezza

Il processo di Valutazione del Rischio ICT e di sicurezza è gestito e coordinato dalla funzione Risk Management e ha lo scopo di valutare il livello di rischio degli asset ICT, aggregato in ultima istanza a livello di processo, ed attuare, laddove necessario, le misure appropriate di contenimento e gestione del Rischio ICT e di Sicurezza. A tale scopo, il processo è eseguito:

- **annualmente**, per gli asset ICT in perimetro di analisi definito[11];
- **ad evento**, in seguito alla rilevazione di iniziative in grado di impattare significativamente il livello di rischio ICT e di sicurezza dell'asset ICT e/o processo che supporta (es. sviluppo di nuovi progetti e modifiche rilevanti del sistema informativo, monitoraggio derivante dagli indicatori di rischio che evidenzia un rischio residuo superiore rispetto le valutazioni degli utenti).

La valutazione si articola nelle seguenti attività:

[11] Per maggiori dettagli è possibile consultare il Manuale Operativo *Metodologia di gestione del rischio informatico*

- **Valutazione della probabilità di accadimento**: il processo di valutazione della probabilità di accadimento tiene conto degli eventuali fattori correttivi individuati nella fase di "analisi di contesto" e prevede due flussi separati per le Applicazioni e le Infrastrutture:
    - *Applicazioni:* la valutazione dell'efficacia dei presidi IT applicativi permette di definire la probabilità residua per le applicazioni, la quale è integrata, tramite media ponderata, con la valutazione di probabilità derivante dagli incidenti registrati nel periodo di riferimento;
    - *Infrastrutture IT:* prevede la valutazione dell'efficacia dei presidi infrastrutturali e il calcolo della probabilità residua per le infrastrutture.

  Successivamente ai passaggi sopra elencati, le due componenti si combinano nel calcolo della probabilità residua dell'applicazione tramite il calcolo del "worst case" considerando le infrastrutture IT sottostanti l'applicazione come da mappatura definita.

  La valutazione dell'efficacia dei presidi/misure di sicurezza è in capo ai Control Owner, identificati con il supporto dell'Unità Organizzativa IT Operation Security & Governance.
- **Valutazione dell'impatto**: per ciascuna applicazione in perimetro di analisi, l'Utente Responsabile di riferimento è chiamato a valutare l'impatto, sia potenziale moda che reputazionale, sugli scenari di rischio ICT. I valori di impatto potenziale moda sono aggregati con gli impatti reputazionali e in seguito mitigati dall'efficacia dei presidi/misure di sicurezza applicabili alla mitigazione dell'impatto stesso. L'analisi di impatto può tener conto dei fattori correttivi individuati nella fase di "analisi di contesto".
- **Calcolo del Rischio ICT**: la funzione Risk Management verifica la completezza e la coerenza dei dati forniti dagli attori coinvolti; i valori derivanti dai processi di valutazione della probabilità di accadimento e dell'impatto sono combinati nel calcolo del Rischio ICT per Scenario. Successivamente, il profilo di rischio complessivo dell'applicazione oggetto di analisi è calcolato come worst case del rischio residuo di ogni scenario di rischio ICT. Attraverso la mappatura tra asset ICT e processi, viene valutata in ultima istanza la rischiosità dei processi stessi.
- **Valutazione tramite indicatori di rischio (KRI):** i KRI definiti in fase di design sono aggregati secondo logiche di calcolo predefinite in un KRI complessivo (per applicazione). Qualora la valutazione del KRI complessivo risultasse, per tre mesi consecutivi, superiore alla valutazione dell'utente e previa approvazione della funzione Risk Management, il valore di rischio ICT per l'asset applicativo sarebbe sovrascritto dal valore del KRI complessivo nell'ultimo mese in analisi, potenzialmente impattando anche il rischio ottenuto sul/i relativo/i processo/i.
- **Gestione del Rischio Residuo**: obiettivo della fase è l'accettazione formale da parte dell'Utente Responsabile del rischio residuo così come determinato a seguito delle fasi precedenti. Nel caso in cui il rischio ecceda la soglia di tolleranza al rischio definita, risulta necessario identificare le azioni da intraprendere al fine di mitigare il rischio residuo, attraverso l'adozione di ulteriori misure di trattamento da sottoporre all'approvazione dell'Amministratore Delegato. Lo scopo di tale processo è quello di riportare il profilo di rischio dell'applicazione entro i livelli di tolleranza definiti dal Società. L'Utente Responsabile ha, in ogni caso, facoltà di richiedere e collaborare alla definizione di un piano di mitigazione del rischio.

- **Test di coerenza:** la funzione Risk Management effettua annualmente dei test su un campione significativo di controlli del framework al fine di verificarne la corretta esecuzione. L'obiettivo di tale fase è individuare eventuali presidi di controllo/misure di sicurezza che, seppur presenti, non sono sufficientemente implementati/e. In tale ottica, la conseguente definizione di piani di rimedio ha lo scopo di indirizzare eventuali punti di miglioramento del sistema di controllo per gli ambiti oggetto di verifica.

6.3 Reporting e monitoraggio

La predisposizione della reportistica inerente all'esito del Processo di Valutazione del Rischio ICT è in capo alla Funzione Risk Management della Banca che, oltre a condividere con gli Utenti Responsabili, e con la Funzione Compliance, i report di accettazione del rischio residuo, con frequenza annuale, rende disponibile alle funzioni apicali della Società, tra cui l'Amministratore Delegato, la documentazione relativa ai risultati del processo di analisi del rischio ICT e di sicurezza, ogni loro aggiornamento successivo, le assunzioni e le decisioni prese. Da essa è estratto il Rapporto Sintetico sulla Situazione del Rischio ICT e di sicurezza, sottoposto annualmente all'approvazione del Consiglio di Amministrazione, previa condivisione con la Funzione Compliance per la valutazione inerente agli aspetti di conformità alla regolamentazione. Tale Rapporto Sintetico contiene, a titolo esemplificativo, i risultati della campagna annuale di IT Risk Assessment rappresentati sia a livello di asset ICT che di processo, l'analisi del rischio sulle iniziative progettuali, l'andamento degli indicatori di rischio ICT e di sicurezza (KRI), l'andamento incidenti occorsi, gli eventuali piani di rafforzamento definiti per la mitigazione dei rischi individuati.

Inoltre, nel corso dell'intero processo di gestione del rischio, sia annuale che ad evento, la funzione Risk Management, garantisce un'efficace attività di monitoraggio e revisione su tutte le fasi che costituiscono il processo di IT Risk Management, nonché sull'avanzamento delle azioni/misure definite all'interno del piano di rimedio, qualora identificato.

7. VALUTAZIONE RISCHIO ICT E DI SICUREZZA NUOVE INIZIATIVE ICT

Al fine di monitorare e attenuare adeguatamente i rischi derivanti dal proprio portafoglio di progetti ICT, tenendo conto anche dei rischi che potrebbero scaturire dalle interdipendenze tra progetti diversi e dalle dipendenze di più progetti dalle stesse risorse e/o competenze, la Società si è dotata di un processo per la identificazione e gestione dei rischi del progetto in coerenza con le linee guida definite nella Policy di ICT Project Management.

Di seguito si riporta il flusso esplicativo di alto livello contenente i principali attori del processo e gli step necessari che portano al calcolo del profilo di rischio dell'iniziativa.

Identificazione delle priorità di intervento e analisi preliminare dell'iniziativa

Tutte le iniziative vengono prioritizzate e inserite nella roadmap delle iniziative nel rispetto della capacity complessiva disponibile della Società.

I progetti "evolutivi" possono essere proposti da qualsiasi struttura organizzativa in un'ottica di evoluzione e miglioramento continuo dei prodotti e dei servizi di Flowe o del margine a loro associato. Questi progetti vengono analizzati e prioritizzati secondo criteri, rivisti e confermati annualmente sotto la guida dei Market Product Owner.

E', inoltre, svolta la valutazione dei driver propedeutici all'individuazione dei progetti da sottoporre a valutazioni e analisi di rischio del progetto da parte del Risk Management. Il coinvolgimento di tale funzione è, infatti, previsto per le iniziative progettuali più rilevanti, individuate tramite la combinazione di appositi driver, di seguito riportati[12]:

- la realizzazione del progetto prevede una modifica sostanziale del sistema informativo;
- la realizzazione del progetto ha notevole rilevanza economica;
- la realizzazione del progetto ha un impatto significativo su programmi strategici;
- la realizzazione del progetto prevede la presenza di terze parti per servizi ICT a supporto di processi critici;
- la realizzazione del progetto è finalizzata ad attività di adeguamento su input interno (da parte di FAC) o esterno (rilievi da parte dell'Autorità di Vigilanza);
- la realizzazione del progetto prevede l'introduzione di nuovi prodotti o servizi o modifiche rivelanti di prodotti o servizi;
- la realizzazione del progetto prevede l'introduzione di nuovi asset ICT e/o migrazioni di dati per dismissione di sistemi;
- la realizzazione del progetto ICT introduce nuove tecnologie o soluzioni innovative (e.g. AI, RPA, Blockchain);
- la realizzazione del progetto impatta asset ICT che sono risultati fuori soglia, nell'ambito dell'IT Risk Assessment, rispetto al Risk Appetite negli ultimi 12 mesi.

Nel caso in cui tutti gli elementi per la valutazione dei driver non fossero disponibili in fase di analisi preliminare può esserne completata la raccolta anche in fasi successive ma, ad ogni modo, prima dell'approvazione del progetto. La valutazione dei driver è svolta, al fine di ingaggiare la funzione Risk Management, dal Market Product Owner di concerto all'Unità

[12] Per la lista completa dei driver si rinvia al documento "Metodologia di gestione del rischio informatico ICT e di sicurezza".

Organizzazione e Business Continuity o dall'Unità stessa per quei residuali progetti (es. di Gruppo) per cui svolge il ruolo di PM.

Valutazione del rischio dell'iniziativa

Tale fase viene attivata nel caso in cui la valutazione dei driver preveda il coinvolgimento della funzione Risk management.

La Funzione Risk Management effettua una verifica di secondo livello in merito ai rischi che insistono sull'iniziativa, affinché ne sia garantita e monitorata la fattibilità/profittabilità nel tempo (e.g. rischi aziendali, rischi di business, rischi tecnici, rischi di gestione di progetti) e il presidio dei rischi ICT e di sicurezza.

Il Risk Management, nell'ambito delle valutazioni di competenza, prende in considerazione le analisi svolte e i requisiti definiti dall'unità organizzativa IT Operation Security & Governance, e con l'eventuale supporto del Settore IT Security della Banca, sulla base delle caratteristiche dell'iniziativa stessa e condivisi con il Market Product Owner / PM di progetto.

L'esito delle analisi della funzione Risk Management è discusso con il Market Product Owner / PM di progetto e il Leadership Team, e possono essere portate all'attenzione delle eventuali ulteriori strutture, anche di Gruppo, e/o al Consiglio di Amministrazione in funzione dell'importanza, della complessità e delle dimensioni degli stessi.

Monitoraggio, Verifica e Accettazione del Rischio residuo

Prevede il monitoraggio, da parte del Market Product Owner / PM, dei requisiti definiti nelle fasi precedenti e le eventuali indicazioni della funzione Risk Management.

Al termine del progetto la funzione Risk Management recepisce informativa dal Product Owner circa l'avvenuta implementazione dei requisiti e l'attuazione delle indicazioni fornite. L'ultima fase del processo prevede la richiesta di accettazione formale del rischio residuo all'Utente Responsabile identificato (Leadership Team / Sponsor del progetto ove non previsto un UR).

8. NORMATIVA DI RIFERIMENTO

Nel presente paragrafo, viene delineato il quadro normativo e degli standard di riferimento per l'individuazione e la definizione dei requisiti minimali di un sistema integrato ed omogeneo di gestione del rischio ICT e di sicurezza.

L'elenco fornito è riportato principalmente allo scopo di richiamare l'attenzione sui principali riferimenti, della normativa generale ed interna aziendale, sui quali si fonda la presente Policy.

Gli elementi principali sono i seguenti:

Normative interne	[1] Policy di Sicurezza [2] Policy in materia di Esternalizzazioni [3] Policy per il controllo e la gestione dei Rischi Operativi [4] Policy per la gestione del rischio di reputazione
Normative esterne	[5] EBA Guidelines on ICT and security risk management - EBA/GL/2019/04 [6] Disposizioni di Vigilanza per gli istituti di pagamento e gli istituti di moneta elettronica, Provvedimenti di Banca d'Italia del 23 luglio 2019 [7] Recommendations for the security of internet payments (emanate dalla BCE nel mese di Gennaio 2013) [8] Payment services (PSD 2) - Directive (EU) 2015/2366 [9] Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)
Standard di riferimento	[10] ISO IEC 31000 - Risk management – Principles and guidelines [11] ISO IEC 27035 - Information technology – Security techniques – Information Security Incident Management [12] ISACA - COBIT 5 For Risk

9. ALLEGATI

9.1 Allegato 1 – Scenari di rischio

Scenario di Rischio	Descrizione scenario	Criticità RID
Indisponibilità dei sistemi informativi	Rischio che i sistemi (i dati e le informazioni presenti / raggiungibili) e/o i servizi IT non siano raggiungibili ed utilizzabili quando richiesto da soggetti autorizzati. Le funzionalità offerte da un sistema / da un servizio IT non sono disponibili alla richiesta di soggetti autorizzati per un periodo coerente alle soglie di tolleranza (RTO) dei processi correlati (di derivazione dalle analisi BIA)	Disponibilità
Degrado della qualità del servizio	Rischio che alcune funzionalità dei sistemi (i dati e le informazioni presenti / raggiungibili) e/o dei servizi IT non funzionino correttamente, a seguito di rallentamenti/ritardi nell'aggiornamento dei dati, comportamenti anomali, malfunzionamenti parziali etc.	-
Compromissione dell'integrità dei dati	Rischio che i dati e le informazioni presenti / raggiungibili tramite l'asset ICT non siano protette da eventuali modifiche volontarie non autorizzate (soggetto esterno / malware / hacker oppure personale interno) del contenuto. Rischio che la modifica illegittima dei dati ne comprometta gli aspetti di accuratezza, completezza, correttezza. Accesso non autorizzato con modifica dei dati.	Integrità
Violazione della riservatezza dei dati	Rischio che i dati e le informazioni presenti / raggiungibili tramite l'asset ICT siano accessibili a soggetti non autorizzati (soggetti esterni/malware/hacker oppure personale interno non autorizzato) con conseguente divulgazione impropria e/o furto di dati. Accesso non autorizzato senza modifica dei dati.	Riservatezza
Perdita di Qualità dei dati	Rischio che i sistemi (i dati e le informazioni presenti / raggiungibili) e/o i servizi IT subiscano modifiche accidentali, errori operativi o anomalie con impatti sulla qualità dei dati (ad esempio dati non corretti o mancanti a valle di un'elaborazione/batch).	-

9.2 Allegato 2 – Impatto

Scala	Impatto
Molto Alta	Perdita pari o superiore a 50.000 euro
Alta	Perdita compresa tra 10.000 euro e 50.000 euro
Media	Perdita compresa tra 2.000 euro e 10.000 euro
Bassa	Perdita compresa tra 500 euro e 2.000 euro
Molto Bassa	Perdita compresa tra la soglia minima di raccolta e 500 euro
Trascurabile	Nullo (Perdita inferiore alla soglia minima di raccolta)

9.3 Allegato 3 – Probabilità di accadimento

Scala	Frequenza stimata di accadimento
Molto Alta	*Da più volte la settimana a più volte al giorno (da superiore a 52 volte l'anno a superiore a 365 volte l'anno)*
Alta	*Da bimensile a più volte la settimana (da 25 a superiore a 52 volte l'anno)*
Media	*Da trimestrale a bimensile (da 5 a 24 volte all'anno)*
Bassa	*Da annuale a trimestrale (da 2 a 4 volte all'anno)*
Molto Bassa	*Da quadriennale a annuale (da 0,26 a 1 volta all'anno)*
Trascurabile	*Da decennale a quadriennale (da 0,10 a 0,25 volte l'anno)*

9.4 Allegato 4 – Matrice di rischio

		Probabilità					
		Trascurabile	**Molto Basso**	**Basso**	**Medio**	**Alto**	**Molto Alto**
Impatto	**Trascurabile**	Trascurabile	Molto Basso	Molto Basso	Basso	Basso	Basso
	Molto Basso	Molto Basso	Molto Basso	Basso	Basso	Medio	Medio
	Basso	Molto Basso	Basso	Basso	Basso	Medio	Alto
	Medio	Basso	Basso	Medio	Medio	Alto	Alto
	Alto	Basso	Medio	Medio	Alto	Alto	Molto Alto
	Molto Alto	Medio	Medio	Alto	Alto	Molto Alto	Molto Alto