Linee Guida per la gestione del Rischio ICT e di sicurezza

INDICE

PRINCIPALI CONTENUTI NORMATIVI ED INFORMATIVI

La Circolare Banca d'Italia n. 285/2013 "Disposizioni di vigilanza per le banche" descrive nella Parte Prima (Recepimento in Italia della CRD IV) - Titolo IV (Governo societario, controlli interni e gestione dei rischi) - Capitolo 4 i requisiti di carattere generale per lo sviluppo e la gestione del **Sistema Informativo** da parte degli intermediari.

Il Gruppo Montepaschi assegna i compiti della **Funzione di controllo dei rischi ICT e di sicurezza** come definita dalla Circolare 285/2013[1] alla funzione di **Controllo dei Rischi** (Chief Risk Officer) e alla funzione di **Conformità alle norme** (Compliance) in relazione ai ruoli, alle responsabilità e alle competenze proprie di ciascuna delle due funzioni.

Le Linee Guida definiscono il quadro di riferimento organizzativo e metodologico adottato dal Gruppo per l'esecuzione del processo di "Gestione del Rischio ICT e di sicurezza" per quanto di responsabilità e competenza della funzione di **Controllo dei Rischi**.

A tale scopo, il Gruppo Montepaschi con il presente documento prevede:

- la definizione del modello organizzativo di riferimento, con l'identificazione dei ruoli e delle responsabilità esercitati nell'ambito del processo di gestione dei rischi ICT e di sicurezza, ivi compresa la predisposizione della documentazione da sottoporre agli Organi aziendali;
- la definizione del quadro di riferimento metodologico per l'identificazione, l'analisi, la valutazione, il monitoraggio, la comunicazione dei rischi ICT e di sicurezza ed il loro mantenimento entro i limiti della propensione al rischio definiti dalla banca.

[1] Circolare Banca d'Italia n. 285, Titolo IV, Capitolo 4 – Sistema Informativo: Sezione II – Governo, organizzazione e controlli del sistema informativo (punto 4 – La funzione di controllo dei rischi ICT e di sicurezza) e Sezione III – La gestione del rischio ICT e di sicurezza.

ASPETTI GENERALI

La Circolare n. 285 di Banca d'Italia, recante le "Disposizioni di vigilanza per le banche", pone una serie di requisiti di carattere generale per lo sviluppo e la gestione del sistema informativo da parte degli intermediari[2]. Tra questi, la Circolare definisce i requisiti riguardanti l'implementazione di un complessivo quadro di riferimento organizzativo e metodologico per l'esecuzione del processo di gestione dei rischi ICT e di sicurezza e ne attribuisce compiti e responsabilità di gestione e supervisione ad una Funzione di controllo di secondo livello[3].

Il Gruppo Montepaschi, come riportato nella Policy di Gruppo in materia di Sistema dei Controlli Interni, assegna i compiti della **Funzione di controllo di secondo livello dei rischi ICT e di sicurezza**, alla funzione aziendale di **Controllo dei Rischi** ed alla funzione aziendale di **Conformità alle norme (Compliance)**, in relazione ai ruoli, alle responsabilità e alle competenze proprie di ciascuna delle due Funzioni.

Le Linee Guida per lag*Gestione del Rischio ICT e di sicurezza* definiscono il quadro di riferimento organizzativo e metodologico per la gestione del rischio ICT e di sicurezza adottato dal Gruppo.

I **controlli di primo livello**, come definiti nella Policy di Gruppo in materia di Sistema dei Controlli Interni, relativamente ai rischi ICT e di sicurezza sono garantiti dalla funzione **Information Technology** e dalla funzione **Information Security**, responsabili della definizione e dell'attuazione di procedure, presidi e controlli adeguati alla mitigazione del rischio. In ogni caso, tutte le Funzioni aziendali ed il personale del Gruppo, nonché i fornitori terzi, sono responsabili primari dell'attività di prevenzione del rischio ICT e di sicurezza, attraverso la corretta applicazione delle procedure, dei presidi e dei controlli istituiti per la mitigazione del rischio.

Il **rischio ICT e di sicurezza** è definito dalla Circolare 285/2013 come il rischio di incorrere in perdite dovuto alla violazione della riservatezza, carente integrità dei sistemi e dei dati, inadeguatezza o indisponibilità dei sistemi e dei dati o incapacità di sostituire la tecnologia dell'informazione (IT) entro ragionevoli limiti di tempo e costi in caso di modifica dei requisiti del contesto esterno o dell'attività (agility), nonché i rischi di sicurezza derivanti da processi interni inadeguati o errati o da eventi esterni, inclusi gli attacchi informatici o un livello di sicurezza fisica inadeguata. Nella rappresentazione integrata dei rischi aziendali a fini prudenziali (ICAAP), tale tipologia di rischio è considerata, secondo gli specifici aspetti, tra i rischi operativi, reputazionali e strategici.

Il processo di gestione dei rischi ICT e di sicurezza deve essere pienamente integrato e allineato con il processo di gestione dei rischi della Banca. L'obiettivo del processo è di fornire agli Organi ed alle figure aziendali con responsabilità decisionali sul governo del rischio ICT e di sicurezza, gli elementi di giudizio necessari alla sua gestione coerentemente con i limiti della propensione al rischio stabiliti nel **RAF** (**Risk Appetite Framework**) della Banca.

[2] Circolare Banca d'Italia n. 285, Titolo IV, Capitolo 4 – Sistema Informativo.
[3] Circolare Banca d'Italia n. 285, Titolo IV, Capitolo 4 – Sistema Informativo: Sezione II – Governo, organizzazione e controlli del sistema informativo (punto 4 - *La funzione di controllo dei rischi ICT e di sicurezza*) e Sezione III – La gestione del rischio ICT e di sicurezza.

La metodologia di gestione del rischio ICT e di sicurezza comprende l'insieme delle regole e delle procedure volte a:

- identificare, analizzare e valutare i rischi ICT e di sicurezza cui la Banca è esposta;
- monitorare l'evoluzione dei rischi e l'efficacia delle misure di attenuazione dei rischi;
- comunicare i rischi agli Organi ed alle figure aziendali facoltizzati alla loro gestione.

I rischi ICT e di sicurezza sono identificati considerando gli eventi, o serie di eventi collegati, che possono comportare conseguenze negative sull'integrità, la performance, la disponibilità, la continuità, la riservatezza e l'autenticità dei dati gestiti dal sistema informativo, dei processi aziendali o dei servizi offerti alla clientela, o che possono pregiudicare la capacità di evoluzione dei sistemi ICT. Eventi di rischio omogenei per tipologia di minaccia e per effetti sui sistemi IT e sulle informazioni trattate sono raggruppati all'interno di "scenari di rischio". La valutazione del rischio ICT e di sicurezza è quindi effettuata combinando la stima della probabilità di accadimento degli eventi/scenari di rischio e quella dell'impatto negativo che ne deriva per il Gruppo in termini di perdite economiche, di reputazione e di quote di mercato.
Il processo di gestione del rischio ICT e di sicurezza riguarda le iniziative di sviluppo e modifica rilevante del sistema informativo, nonché le risorse informatiche già in esercizio.

Il modello organizzativo adottato per la gestione del rischio ICT e di sicurezza formalizza il ruolo di **Utente Responsabile**, figura aziendale identificata per ciascun sistema ICT che ne assume formalmente la responsabilità in rappresentanza degli utenti e nei rapporti con le Funzioni preposte allo sviluppo e alla gestione tecnica[4]. L'Utente Responsabile partecipa al processo di analisi del rischio ICT e di sicurezza e accetta formalmente le misure di attenuazione dei rischi ed il rischio residuo.

L'analisi del rischio ICT e di sicurezza è effettuata con il concorso dell'**Utente Responsabile**, della funzione **Information Technology**, della funzione **Controllo dei rischi operativi in ambito ICT e di sicurezza**, della funzione **Information Security** e, ove opportuno, della funzione di **Conformità alle norme** (**Compliance**) e della funzione **Revisione Interna** (**Internal Audit**), secondo le metodologie e le responsabilità definite dal presente documento e nel rispetto delle rispettive responsabilità e competenze aziendali. Nel caso di risorse informatiche gestite in outsourcing/cloud da fornitori esterni al Gruppo, nell'analisi sono coinvolti anche il fornitore ed il **Referente per le attività esternalizzate** (**RAE**).
Nella gestione del rischio ICT e di sicurezza, la funzione di **Conformità alle norme** (**Compliance**) presidia il rischio di non conformità sul sistema informativo, fornendo valutazioni sul rispetto delle normative esterne e dei regolamenti interni in materia e svolgendo controlli di secondo livello (Parte Prima, Titolo IV, Cap. 4, della Circolare n. 285 di Banca d'Italia) nell'ambito delle responsabilità attribuite dalla normativa interna in materia di Gestione del rischio di non conformità.

[4] La definizione è fornita dalla Circ. 285/2013 Titolo IV - Capitolo 4 – Sezione I – Punto 3 – *Definizioni*.

In particolare, le responsabilità della Funzione Compliance risiedono nella definizione e nell'aggiornamento del complessivo processo di gestione del rischio di non conformità relativo al sistema informativo, ed in tal senso, negli ambiti ICT e sicurezza. In Banca MPS, le attività della Funzione Compliance si ripartiscono nelle componenti di:

- «advisory», che:
  - identifica nel continuo le norme in materia applicabili al Gruppo ed i relativi rischi di non conformità che impattano sui processi aziendali, valutandone gli impatti anche in termini di potenziali sanzioni e danni reputazionali;
  - valida i documenti di normativa interna inerenti a: sistema informativo, sicurezza informatica, continuità operativa, sistemi di pagamento, esternalizzazioni e servizi ICT forniti da Terze Parti; verifica i profili di conformità per i contratti di servizi ICT forniti da Terze Parti ed esternalizzazioni.
- «controlli di conformità», che effettua controlli di secondo livello su processi o funzioni operative per le quali assumono rilievo i rischi di non conformità in ambito ICT e Sicurezza, eseguendo verifiche di compliance anche on-site presso strutture operative.

MODELLO DI GESTIONE DEL RISCHIO ICT E DI SICUREZZA

OBIETTIVI

Il Gruppo Montepaschi riconosce il valore della gestione del rischio ICT e di sicurezza nel conseguimento degli obiettivi individuati dal Piano Strategico, quale strumento a garanzia dell'efficacia ed efficienza delle misure di protezione delle risorse ICT e dei servizi forniti agli utenti interni o esterni. Promuove pertanto una metodologia fondata su una visione olistica delle funzioni aziendali, dei processi di business supportati dal sistema informativo, delle minacce afferenti alle risorse ICT, delle loro vulnerabilità e delle misure di mitigazione dei rischi.

Le misure di mitigazione sono graduate in funzione della classificazione di criticità delle risorse ICT e del livello di propensione al rischio ICT e di sicurezza stabilito nell'ambito del RAF (Risk Appetite Framework) di Gruppo.

ELEMENTI DEL MODELLO DI GESTIONE DEL RISCHIO ICT E DI SICUREZZA (FRAMEWORK DI RIFERIMENTO)

Generalità

Nei paragrafi che seguono sono descritti sinteticamente gli elementi che compongono il modello di gestione del rischio ICT e di sicurezza adottato dalla funzione aziendale di **Controllo dei rischi** e le relazioni rilevanti tra di essi.

Tali elementi sono definiti in coerenza con gli standard ed i framework definiti a livello internazionali e sulla base di *best practice* del settore.

Funzioni e processi aziendali

Le **funzioni** ed i **processi aziendali** sono componenti del modello di gestione del rischio ICT e di sicurezza in quanto permettono di indirizzare, sulla base del loro livello di criticità, la valutazione degli impatti associati agli scenari di rischio che possono colpire le risorse ICT che li supportano.

Utenti Responsabili

I responsabili delle funzioni aziendali sono gli attori di riferimento per la valutazione degli impatti degli scenari di rischio ICT e di sicurezza e l'assunzione delle decisioni relative al trattamento dei rischi.
Il ruolo di Utente Responsabile è formalizzato nell'ambito dell'Assetto Organizzativo della Banca MPS.

Risorse Informatiche

Sono considerate **risorse informatiche** tutte le componenti tecnologiche hardware e software che supporto le operazioni della Banca ed erogano servizi ICT agli utenti interni o esterni.
Le risorse informatiche sono poste sotto la gestione e il controllo della funzione **Information Technology** e della funzione **Information Security**. Tutte le risorse informatiche sono censite in apposito **inventario**.

Fattori di Rischio

L'analisi dei fattori di rischio è basata definizione di una tassonomia di **minacce**, che costituiscono le cause potenziali degli eventi di rischio ICT e di sicurezza. Le minacce possono essere Interne ed Esterne e differenziate per la presenza o meno di intenzionalità. Inoltre, le minacce possono essere raggruppate in differenti categorie (ad esempio: attacchi cyber dall'esterno, azioni di insider malevoli, attacchi fisici, malfunzionamenti dei sistemi, errori umani, negligenze, carenze di processo, eventi naturali, etc.).

Scenari di rischio

Per **scenario di rischio ICT e di sicurezza** si intende la descrizione di un possibile accadimento di eventi di rischio omogenei per la tipologia di minaccia che li origina a seguito dei quali potrebbero osservare effetti negativi sull'attività ordinaria, sulla sicurezza delle risorse informatiche e delle informazioni trattate, sulla capacità di rispettare gli obiettivi posti dal business o dal contesto normativo.

Impatto degli scenari di rischio

Per **impatto** si intende la conseguenza negativa per il Gruppo Montepaschi, in termini di perdite economiche, di reputazione e di quote di mercato, causata dal manifestarsi degli scenari di rischio sulle risorse informatiche. L'impatto viene valutato in termini potenziali, seguendo un approccio worst-case.

Misure di mitigazione del rischio

Per **misure di mitigazione** si intendono i controlli ed i presidi di natura tecnologica, organizzativa, procedurale, direttiva e formativa, finalizzata ridurre il livello di esposizione e/o di vulnerabilità delle risorse informatiche rispetto alle minacce (rischio inerente), limitando la probabilità di accadimento degli eventi di rischio, ovvero la possibilità che da essi si origini un impatto negativo o la sua entità.

La funzione **Controllo dei rischi operativi in ambito ICT e di sicurezza** verifica la presenza ed il continuo funzionamento delle misure di mitigazione dei rischi inerenti e, anche sulla base di controlli definiti da standard e framework internazionali e dalle best practice di settore, identifica i livelli di rischio residuo.

Esposizione e vulnerabilità delle risorse

L'**esposizione** di una risorsa informatica rispetto ad una minaccia indica che la risorsa, in funzione delle proprie caratteristiche e del posizionamento nell'architettura del sistema informativo, è potenzialmente raggiungibile dalla minaccia. In questi casi, la minaccia ed i possibili eventi/scenari di rischio ad essa associati sono definiti "applicabili".

La **vulnerabilità** di una risorsa informatica rappresenta una condizione di debolezza, carenza o difetto nella progettazione, implementazione, configurazione, protezione o gestione operativa della risorsa, compresi la sua obsolescenza e il mancato aggiornamento secondo le prescrizioni del fornitore, che possono essere sfruttati dalla minaccia e determinare l'accadimento degli eventi di rischio e un impatto negativo per il Gruppo.

Probabilità degli eventi di rischio

La **probabilità di accadimento** di un evento di rischio ICT e di sicurezza è la frequenza su base annua con cui si stima che l'evento possa verificarsi sulle risorse informatiche oggetto di analisi e causare un impatto negativo per il Gruppo.

La valutazione di probabilità è un giudizio esperto espresso da figure dotate di elevate conoscenze sulle risorse informatiche analizzate e sulle minacce cui sono esposte. Una accurata stima della probabilità di accadimento degli eventi di rischio richiede, infatti, competenze specifiche per valutare l'efficacia delle misure di mitigazione in essere ed il livello di esposizione e di vulnerabilità delle singole risorse rispetto alle diverse minacce, oltre che la disponibilità di

informazioni e statistiche sugli incidenti operativi e di sicurezza informatica accaduti in Banca e su quelli osservati a sistema.

Valutazione del livello di rischio

Si definisce rischio **"inerente"** (o anche "intrinseco") il rischio a cui la Banca è esposta in assenza di qualsiasi misura di mitigazione.
Si definisce, invece, rischio **"residuo"** il rischio a cui la Banca è esposta una volta applicate le misure di mitigazione individuate dal processo di analisi dei rischi.

Sulla base di specifiche regole (matrice di rischio), il Rischio ICT e di sicurezza è rappresentato sulla base della combinazione tra la probabilità di accadimento degli eventi di rischio ed il loro impatto stimato.

Key Risk Indicator

I **Key Risk Indicator (KRI)** sono indicatori quantitativi che rilevano il verificarsi di incidenti, il manifestarsi di anomalie e vulnerabilità tecnologiche, di processo o di sicurezza, o l'evoluzione delle minacce cui è esposto il sistema informativo. I KRI sono misurati sulle singole risorse o, a livello più aggregato, sugli ambiti applicativi e infrastrutturali in cui si articola il sistema informativo e della sicurezza informatica.

I KRI permettono di monitorare nel continuo l'evoluzione del rischio ICT e di sicurezza rispetto a delle soglie di attenzione predefinite e forniscono elementi chiave per l'individuazione di minacce e situazioni di vulnerabilità che richiedono analisi di rischio più approfondite.

I KRI possono essere utilizzati nell'ambito del Risk Appetite Framework per definire i limiti della propensione al rischio ICT e di sicurezza a livello di Gruppo.

METODOLOGIA DI ANALISI

Generalità

La metodologia di analisi del rischio ICT e di sicurezza descrive le regole adottate dalla funzione aziendale di Controllo dei Rischi per l'identificazione, la valutazione ed il monitoraggio dei rischi, sulla base degli elementi del modello descritti nel precedente paragrafo.

La **metodologia di valutazione** prevede la conduzione, in parallelo, di due tipologie di analisi, che si collocano su piani diversi ma tra loro complementari:

1. Un'**analisi di rischio "di dettaglio"** condotta a livello di singole risorse ICT.
2. Un'**analisi di rischio di "alto livello",** effettuata ad un livello più generale e trasversale rispetto a quello delle singole risorse informatiche, finalizzata ad individuare e valutare i rischi ICT e di sicurezza nelle seguenti macro-funzioni in cui si articola la gestione del sistema informativo

Inoltre, il **monitoraggio** nel continuo dell'evoluzione del rischio ICT e di sicurezza e dell'efficacia delle misure di mitigazione viene realizzato attraverso una serie di Key Risk Indicator (KRI), utilizzati per rilevare l'evoluzione del rischio degli ambiti applicativi e infrastrutturali in cui si articola il sistema informativo e della sicurezza informatica. Con cadenza almeno annuale, i risultati forniti dall'analisi di alto livello sono opportunamente integrati con quelli derivanti dall'analisi di dettaglio sulle singole risorse, al fine di ottenere una rappresentazione complessiva e coerente della situazione del rischio ICT e di sicurezza del Gruppo.

TRATTAMENTO E ACCETTAZIONE DEL RISCHIO

L'analisi del rischio ICT e di sicurezza cui sono esposte le risorse informatiche determina il rischio residuo da sottoporre ad accettazione formale dell'Utente Responsabile.

Ove il rischio residuo ecceda la propensione stabilita nel RAF, sono definite dall'Utente Responsabile misure ulteriori di trattamento finalizzate a ricondurre i rischi entro i limiti di propensione, o alternative (es. risk transfer).

Nell'ambito del Sistema dei Controlli Interni, i rischi ICT e di sicurezza che superano i limiti di propensione indicati nel RAF sono segnalati dalla funzione **Controllo dei rischi operativi in ambito ICT e di sicurezza** come "azioni di mitigazione obbligatorie". Alla dichiarazione di chiusura dell'azione di mitigazione, l'analisi del rischio viene aggiornata verificando l'efficacia della mitigazione realizzata ed il conseguente abbassamento del livello di rischio residuo. Il sistema di Risk Reporting Direzionale assicura il monitoraggio delle azioni in corso.

IL REPORTING VERSO L'ORGANO CON FUNZIONE DI SUPERVISIONE STRATEGICA

Il Consiglio di Amministrazione è informato tempestivamente, ed 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, e ne approva il Rapporto sintetico.