MONTE DEI PASCHI DI SIENA
BANCA DAL 1472

ALLEGATO n.5

Relazione sul Sistema Avanzato di Gestione e Misurazione del Rischio Operativo (AMA)

Anno 2017

INDICE

In conformità con quanto previsto dalla normativa di riferimento, si forniscono i risultati dell'attività di audit svolta sul Sistema Avanzato di Gestione e Misurazione del Rischio Operativo per l'esercizio 2017.

Il presente documento costituisce allegato della Relazione della Direzione Chief Audit Executive sull'attività svolta e valutazione del sistema dei controlli – anno 2017.

1. Eventi quantitativi e qualitativi con impatto sul modello AMA

Il sistema avanzato di misurazione dei rischi operativi (Advanced Measurement Approach – AMA) per la determinazione del requisito patrimoniale è adottato all'interno delle società bancarie e strumentali del Gruppo da Banca Monte dei Paschi di Siena, MPS Capital Services Banca per le Imprese, MPS Leasing & Factoring e Consorzio Operativo Gruppo Montepaschi. Riguardo invece alle controllate estere (MPS Banque, MPS Belgio) e alle società Widiba e MP Fiduciaria, rientranti nel perimetro di consolidamento, viene adottato il metodo base.

Il requisito patrimoniale ammonta al 31/12/2017 a circa €mio 801, in incremento rispetto al dato registrato nel 2016 (pari a 678 €mln). La tabella seguente riporta il dettaglio per classe di rischio del requisito regolamentare consolidato del Gruppo BMPS.

Classe di Rischio	Requisito Patrimoniale sui Rischi Operativi 31/12/2017
Frodi interne	230.867.552
Frodi esterne	38.548.049
Rapporti di impiego e sicurezza sul lavoro	23.695.458
Clienti prodotti e prassi operative	379.385.273
Danni a beni materiali	2.265.069
Interruzioni operatività e sistemi	14.246.182
Esecuzione, consegna, gestione dei processi	99.979.382
Totale perimetro AMA	788.986.964
Contributo società non AMA	11.936.138
Totale Metodo AMA	800.923.102

Nel corso del 2017 i principali eventi impattanti in termini quali-quantitativi l'applicazione del sistema avanzato di misurazione dei rischi operativi hanno riguardato i seguenti ambiti:

- implementazione delle azioni correttive richieste da BCE, e comunicate al Gruppo MPS con la lettera del 02/02/2017[1], riguardanti l'estensione della profondità storica dei dati interni da 5 a 10 anni, l'adozione di una metodologia di scaling dei dati esterni e la rivisitazione del perimetro dei dati esterni finalizzata a migliorare la corrispondenza tra le sottoclassi DIPO e le classi di rischio interne del framework AMA della Banca[2]. Le sopracitate modifiche metodologiche hanno portato a un incremento del requisito patrimoniale (+9,6% rispetto al requisito di fine 2016);
- messa in produzione delle nuove metodologie a partire dal calcolo del requisito relativo al 30/06/2017, anche in seguito al parere favorevole espresso in data 18/07/2017 dalla Funzione di Convalida in merito alle rettifiche apportate al codice che implementa il nuovo modello;

[1] Si fa riferimento alle azioni di mitigazione richieste a seguito dell'Internal Model Investigation IMI-42 svolta nel periodo 07/09/2015 - 25/09/2015 e finalizzata a verificare sia il corretto recepimento delle modifiche evolutive al modello interno richieste da Banca d'Italia (lettera del 19/01/2015) sia i relativi impatti sul capitale regolamentare.

[2] Dal 30/06/2017 sono stati introdotti i dati della sottoclasse DIPO ET4.2 "Pratiche operative o di mercato improprie" nella classe "ET4 Anatocismo" e i rimanenti dati del DIPO ET4 (ad eccezione delle revocatorie) nella classe interna "ET4 Cause".

- rimozione delle perdite "credit boundary" dal database dei rischi operativi a partire dal 30/06/2017[3]. In linea con quanto previsto dall'art. 322 b) della CRR, il Gruppo MPS ha segnalato a BCE, con una notifica ex ante (lettera del 24/04/2017), la rimozione di tali perdite dalla base dati di calcolo del requisito essendo queste già trattate a fronte del rischio di credito;
- riassetto organizzativo di Capogruppo: le modifiche apportate in diverse strutture della Banca (es. riorganizzazione del Chief Lending Officer) hanno determinato impatti nelle attività di Risk Self Assessment e di Analisi di Scenario;
- accantonamenti a Fondo Rischi e Oneri che subiscono un forte incremento nell'ultimo trimestre riconducibile sia all'attività di segnalazione della clientela per l'operatività in diamanti (76,5 €mln), sia alle contestazioni relative gli aumenti di capitale passati (59€mln).

2. Dettaglio delle attività di audit

I risultati delle attività svolte hanno confermato il rispetto dei requisiti e delle condizioni di idoneità previste per l'utilizzo a fini regolamentari del metodo avanzato. I principali interventi di audit eseguiti durante l'anno 2017 hanno riguardato diversi ambiti impattanti sul modello e/o sui processi. Di seguito si riportano gli interventi obbligatori condotti sul processo di Operational Risk Management da parte della Direzione Chief Audit Executive e delle funzioni di internal audit locale delle società rientranti nel perimetro validato e i principali rapporti condotti presso la Capogruppo con impatti sui rischi operativi.

N. rapporto	*Descrizione*	*Grade*
Rapporti di Revisione delle funzioni di internal audit delle Società del perimetro		
187/2017	**Banca MPS** Revisione Convalida AMA	Rating 1 - Verde
16/2017	**Consorzio Operativo di Gruppo** Revisione Interna del Processo di Operational Risk Management	Rating 1 -Verde
18/2017	**MPS Capital Services Banca per le Imprese** Revisione Interna del Processo di Operational Risk Management	Rating 1 - Verde
9/2017	**MPS Leasing & Factoring** Processo di Operational Risk Management	Rating 2 - Giallo
Rapporti di Revisione specialistici della Direzione Chief Audit Executive		
41/2017	*Disponibilità Sistemi e Livelli di Servizio*	Rating 2 - Giallo
42/2017	*Issuing carte di debito e prepagate (aspetti operativi ed amministrativi)*	Rating 3 - Arancione
44/2017	*Verifiche implementazioni Remedial Actions BCE (RA #12 e RA #13 – OSI-2015-34-35)*	Rating 3 - Arancione
45/2017	*Archivio Unico Informatico IT*	Rating 2 -Giallo
102/2017	*Attività di Ethical Hacking sulle component infrastrutturali ed applicative del Sistema Informativo di Gruppo*	Rating 3 - Arancione
103/2017	*MPS – Antifrode*	Rating 3 - Arancione
104/2017	*Rilasci Applicazioni IT*	Rating 3 - Arancione
114/2017	*Commissioni attive nel bilancio d'esercizio – composizione e rappresentazione contabile (commissioni percepite dalle Società Assicurative)*	Rating 3 - Arancione

[3] Comunicazione ex ante a BCE con la lettera del 24/04/2017.

154/2017	*Gestione Cause Legali*	Rating 3 - Arancione
164/2017	*Attività di Ethical Hacking sulle component infrastrutturali ed applicative del Sistema Informativo della Filiale di New York*	Rating 2 - Giallo
167/2017	*Anagrafe Operativa di Gruppo*	Rating 2- Giallo
168/2017	*Usura – Calcolo TEG*	Rating 2 - Giallo
182/2017	*Processo di Gestione degli adempimenti prescrittivi in materia di Trasparenza bancaria*	Rating 2 - Giallo

Positive risultano essere le attività di presidio e controllo poste in essere dalla funzione di Convalida e dalla funzione di Risk Management, quest'ultima responsabile dello sviluppo quantitativo del modello avanzato di misurazione del rischio operativo. Elementi di attenzione sono invece emersi nella fase di gestione del rischio.

Di seguito vengono riportate le principali evidenze emerse nel corso delle attività condotte nel 2017, suddivise per identificazione, misurazione, gestione e controllo/monitoraggio dei rischi operativi.

Identificazione

Il processo di identificazione dei rischi operativi (*Loss Data Collection*) è complessivamente migliorato grazie all'implementazione di alcuni affinamenti evolutivi finalizzati a supportare e semplificare la fase di arricchimento informativo e di caricamento in OpRiskEv dei dati di perdita. Le soluzioni rilasciate presentano ancora dei margini di miglioramento essendo possibile automatizzare alcune azioni proposte dall'applicativo stesso e migliorare la garanzia d'integrità dei dati. Occorre inoltre proseguire con gli interventi di automazione sulla Fonte Cause Legali e valutare la progressiva estensione anche ad altre Fonti Informative rilevanti, a cominciare da "Risorse Umane" che ha come sottostante lo stesso applicativo (MICRA) utilizzato dalla Funzione Legale per la gestione delle cause.

Misurazione

Relativamente alle evolutive poste in essere sul modello di misurazione (estensione serie storiche a 10 anni e introduzione scaling dei dati esterni) sono stati condotti specifici approfondimenti, nell'ambito delle attività di audit, finalizzati a valutare la completezza e l'adeguatezza dei controlli svolti dalla Funzione di Convalida. Le analisi hanno confermato la correttezza dell'impatto del nuovo modello sul requisito patrimoniale al 30/06/2017 e l'adeguatezza dell'informativa fornita all'Alta Direzione e agli Organi Aziendali da parte della Funzione Risk Management.

A seguito delle modifiche metodologiche introdotte sul modello è stato richiesto alla Funzione di Convalida di introdurre nel «Framework di Convalida Rischi» un nuovo controllo sulla materialità dell'effetto, sui dati di perdita, del tasso d'inflazione. Poiché quest'ultimo assume valori consistenti con serie storiche a 10 anni, è stato altresì richiesto alla Funzione Risk Management di quantificare l'impatto anche in termini di requisito patrimoniale e di considerare la possibilità di rivalutare i valori di perdita.

Inoltre, con l'allungamento delle serie storiche a 10 anni è necessario monitorare il peggioramento dei test di indipendenza dei dati (non rispettate le assunzioni per 10 delle 14 serie di frequency). Poiché l'indipendenza è condizione necessaria affinché i dati di frequency appartengano ad una stessa distribuzione di probabilità, è stato richiesto alla Funzione Risk Management di valutare metodi alternativi per rendere i dati indipendenti verificandone gli impatti in ottica costi/benefici.

Gestione

Sulla base di quanto emerso dagli audit specialistici effettuati nel corso dell'anno sui principali processi operativi di Capogruppo, sono state avviate diverse azioni progettuali sui comparti di business e tecnico informativi che hanno portato ad un parziale miglioramento della macchina operativa. Al fine di incrementare l'efficacia delle azioni di mitigazione/trasferimento/ritenzione del rischio da parte delle funzioni preposte occorre proseguire nelle attività di rafforzamento in corso.

Di seguito sono sintetizzati gli elementi di attenzione più rilevanti emersi sulla componente **macchina operativa** e in alcuni casi le azioni correttive già poste in essere:

- *gestione delle Cause legali*: in assenza di linee guida specifiche per l'aggiornamento di Micra da parte dei legali interni, per alcune cause è stata osservata una carenza documentale e informativa che non consente la puntuale ricostruzione dei procedimenti giudiziari e delle decisioni assunte. Prevale l'utilizzo di fascicoli cartacei che, in assenza di regole definite, sono risultati implementati con modalità differenti, rimesse in buona parte alla sensibilità dei singoli gestori. Sono state rilevate criticità nelle attività di seguimento di alcune cause vinte con rimborso spese, risultate prive di incassi e chiuse dal gestore senza giustificato motivo. Risulta necessaria una normativa di processo che definisca gli adempimenti operativi, di controllo e di rendicontazione da svolgere nell'ambito della gestione delle cause legali. Su tutti questi ambiti sono in corso le azioni correttive previste;
- *processo di gestione degli aspetti contabili di Gruppo: p*er quanto riguarda la *composizione e rappresentazione contabile delle "commissioni attive",* sono stati verificati e sistemati gli algoritmi utilizzati per il calcolo delle commissioni del "ramo danni" e del "ramo vita" ai fini di una puntale comparazione con i dati trasmessi dalla Compagnia Assicuratrice AXA. Risulta invece necessario procedere a sistemare le differenze riscontrate tra le commissioni presenti nei flussi AXA e i calcoli elaborati dall'applicativo "Syfe", ripristinando la corretta contabilizzazione delle commissioni derivanti dal flusso conto/depositi a pacchetto, non in linea con l'operatività standard. Infine, il processo di retrocessione delle commissioni assicurative necessita di essere disciplinato all'interno di una normativa di processo;
- *processo di gestione Patrimonio Artistico*: su tale ambito è stata riscontrata la necessità di efficientare la catalogazione e inventariazione delle opere d'arte restringendo il catalogo ai soli oggetti effettivamente classificabili come opera d'arte. Risulta altresì necessario predisporre una normativa che regolamenti il processo per le operazioni di prestito, concessione in comodato e, tenuto conto del *commitment*[4] di Piano di Ristrutturazione, anche per le operazioni di vendita;
- *processo di gestione degli adempimenti prescrittivi in materia di Trasparenza bancaria*: il processo di "Modifiche unilaterali delle condizioni contrattuali (art. 118 del TUB)" è stato reso maggiormente efficace istituendo ad esempio punti di controllo/feedback che consentono alla Funzione Mercato il pieno presidio dell'intero processo.

Particolare attenzione deve essere invece mantenuta sulla **componente sistemistica** riguardo ai potenziali rischi derivanti da inefficienze operative delle procedure in uso presso la Banca. A tal proposito si evidenzia quanto segue:

[4] Nell'ambito del Piano di Ristrutturazione 2017-2021, la Banca si è impegnata a procedere alla cessione dell'intera collezione d'arte (eccetto le opere sotto il vincolo di pertinenzialità e di altre leggi) rispettando la conformità alla legislazione nazionale in materia e la condizione che il prezzo di vendita sia almeno pari al valore contabile.

- *sicurezza logica*: l'attività di verifica periodica di Ethical Hacking ha interessato le componenti infrastrutturali e applicative relative alla piattaforma Digital Banking di Gruppo e quelle relative alla filiale di New York. Per quanto riguarda la piattaforma Digital Banking, a seguito dell'attività di audit, sono stati resi maggiormente efficienti gli strumenti di intercettazione delle intrusioni sull'applicazione allo scopo di assicurare, in caso di attacco, una reattività della Banca in linea con i requisiti di sicurezza. Inoltre, sono stati implementati gli opportuni controlli e configurazioni al fine di sanare le vulnerabilità applicative riscontrate migliorando il livello di sicurezza dell'applicazione web. Relativamente alla filiale di New York la verifica delle componenti infrastrutturali e applicative del sistema informativo ha rilevato la necessità di aggiornare alcuni software degli apparati di rete in modo da rimuovere le vulnerabilità riscontrate;
- *gestione dei rilasci di nuove applicazioni IT*: sono stati implementati controlli maggiormente efficaci per il rilascio del software in produzione vincolando il rilascio stesso alla presenza di test UAT e inibendo l'utilizzo della funzionalità di forzatura per il superamento del test (consentendola soltanto a casi eccezionali). Sono state definite regole precise per stabilire le condizioni di chiusura lato IT di un BR, è stata implementata una migliore gestione all'interno dei sistemi delle informazioni riguardanti la relazione tra deliverables del BR e richieste di cambiamento software nonché è stato formalizzato l'assenso definitivo delle funzioni di business al rilascio in produzione del software. Su tali ambiti sono ancora in corso le azioni di rafforzamento e presidio;
- *gestione delle Frodi Informatiche sul servizio Digital Banking:* sono necessarie alcune iniziative per una adeguata gestione del processo (elaborazione di un Piano di interventi per prevenire, rimuovere e monitorare gli eventi di frode; definizione di uno scambio di flussi informativi inerenti gli eventi di sicurezza logica). Al fine di migliorare la sicurezza logica degli accessi agli applicativi è stato definito uno specifico profilo abilitativo per i membri del team antifrode;
- *Procedura Beni:* a seguito dell'attività di verifica, oltre a razionalizzare l'attribuzione dei profili di accesso, è stata inibita la modifica dei dati caricati automaticamente dalla procedura Perizie On Line al fine di assicurare l'integrità delle informazioni caricate e ridurre le possibili malversazioni derivanti da variazioni dei valori di stima per ottenere la concessione di un finanziamento con importo superiore a quello ammissibile. Inoltre, sono stati implementati dei presidi di controllo per verificare l'effettiva acquisizione digitale della documentazione ritenuta necessaria come previsto dal progetto di dematerializzazione;
- *Presidio Archivio Unico Informatico:* l'attività di audit ha portato all'aggiornamento, da parte del COG, dei documenti che descrivono le logiche di alimentazione dell'AUI implementate dai servizi alimentanti. Al fine di uniformare le informazioni decisionali utilizzate per la creazione del flusso di alimentazione dell'AUI sono state rimosse alcune anomalie nelle regole di antiriciclaggio in carico al servizio Cassa e al Servizio Anagrafe. Inoltre, per rimuovere i disallineamenti dei dati anagrafici in AUI sono state riviste le modalità di aggiornamento delle variazioni anagrafiche. Al fine di poter rilevare eventuali anomalie di alimentazione sono stati implementati nuovi controlli di quadratura e sono state poste in essere le azioni necessarie a garantire che tutte le operazioni di "forzata esclusione" siano correttamente segnalate nei controlli SIC;
- *Implementazioni informatiche utilizzate ai fini del calcolo del Tasso Effettivo Globale:* la revisione ha evidenziato la necessità di modificare i programmi affinché la procedura di calcolo del TEG computi, oltre agli oneri a carico del fido in contrattualizzazione, anche tutti quelli a carico dei fidi, della stessa natura, già operativi sul conto corrente;
- *presidio Anagrafe Operativa di Gruppo*: a seguito dell'intervento di audit, per i moduli software che non tracciano i dati aggiuntivi di Log ne è stata assicurata la corretta tracciatura. Sono in corso le attività di mitigazione indirizzate a migliorare la tracciatura dell'operatività svolta sulla base dati "Anagrafe".

Con riferimento alle **attività esternalizzate**, al fine di presidiare la *disponibilità dei sistemi e i Livelli di Servizio* sono stati implementati adeguati controlli (tecnici e di processo) atti a garantire la correttezza dei KPI e degli eventuali "punti penale" prodotti da Fasteweb per il servizio "Rete Dati" fornito.

In merito al Servizio Sportello è stato implementato un monitoraggio maggiormente strutturato e puntuale in modo da evidenziare con prontezza eventuali problematiche sulle applicazioni di sportello ed è stato definito e implementato un KPI significativo per la misurazione della disponibilità. Infine, è stato implementato un nuovo KPI di disponibilità dell'Infrastruttura tecnologica PaschiFace.

Per quanto riguarda il *processo Issuing carte di debito e prepagate* è emerso che la gestione della nuova piattaforma delle carte prepagate Quickard è stata esternalizzata a Bassilichi Spa senza richiedere a suo tempo un'autorizzazione preventiva al Banca d'Italia, così come previsto dalle disposizioni di vigilanza (Circ. 285/13), e senza redigere un contratto per formalizzare il servizio di gestione, svolto soltanto sulla base dell'accettazione di un'offerta economica. Su tali ambiti di attenzione la struttura si è attivata per finalizzare le azioni correttive richieste e procedere alla richiesta di autorizzazione alla BCE (effettuata in data 14/11/2017).

Infine, occorre regolarizzare il subappalto a Fruendo Srl, effettuato da Bassilichi, su alcuni processi (prevenzione frodi e gestione reclami sulle carte). In vista del prossimo rinnovo, è stato richiesto di regolarizzare il processo di issuing (la stampa dei PIN), utilizzando fornitori omologati, e assegnare chiaramente la responsabilità dell'istruttoria della pratica di omologazione presso i circuiti. E' necessario revocare le abilitazioni non necessarie e, laddove possibile, razionalizzare i panieri abilitativi, prevedendo periodiche verifiche delle utenze abilitate.

Controllo e Monitoraggio

Gli specifici audit condotti a distanza ed in loco principalmente indirizzati alla verifica della complessiva funzionalità e regolarità nelle varie fasi (*Loss Data Collection, Risk Self Assessment e Analisi di Scenario*) del Processo di Operational Risk Management presso le Società del Gruppo, hanno consentito di valutare positivamente i presidi e la complessiva funzionalità del processo di gestione dei rischi operativi.

Gli unici ambiti di attenzione sono stati rilevati sulla fase di *Loss Data Collection* di MPS Leasing & Factoring, per la quale è stata evidenziata l'esigenza di attivare quanto prima il processo operativo di monitoraggio delle cosiddette Pending Loss[5] e delle Perdite di Contabilità Generale su voci riferibili a esborsi da sentenze legali. Nell'ambito delle attività di *Analisi di Scenario* di MPS Capital Services, è emersa, invece, la necessità di attivare interventi di mitigazione per risolvere le criticità rilevate nell'operatività tipica giornaliera sui mercati finanziari a causa di disfunzioni o rallentamenti nel Sistema IT (malfunzionamenti "real time" di Murex, mancata acquisizione di operazioni di mercato in tempi ragionevoli, sistemi di quotazione market-making obsoleti).

L'azione di follow up rivolta a rimuovere o mitigare le principali criticità evidenziate viene garantita nel continuo attraverso l'utilizzo dell'applicativo RIGAM (Repository Integrato per la Gestione delle Aree di Miglioramento), specifico strumento informatico a supporto della gestione e risoluzione dei gap e delle attività di mitigazione, che riunisce in un unico database tutte le evidenze rilevate dalle funzioni di controllo.

Nel corso del 2017 sono stati completati gli interventi previsti dal Piano di Mitigazione Rischi Operativi, tra i quali si segnala l'integrazione della normativa in materia di finanza proprietaria allo scopo di vietare la negoziazione in conto proprio di strumenti finanziari da parte degli operatori di mercato, ai quali è stato richiesto esplicitamente di

[5] Appostazioni transitorie sui rapporti del servizio partite diverse che possono tradursi in perdite.

prendere visione della normativa. A livello prospettico, per impedire la violazione delle disposizioni di legge in materia di antiriciclaggio, sono stati rafforzati i controlli e potenziate le attività di monitoraggio, in ragione di alcuni casi di mancata/errata segnalazione di operatività sospetta da parte dei promotori finanziari di Widiba. Inoltre, per MPS Capital Services è stata implementata una procedura di back up che estrae dai portafogli Murex le posizioni in titoli lunghe/corte, procedura alternativa a FDWH al fine di presidiare e gestire correttamente la liquidità.

Sono invece previsti entro il primo semestre 2018 alcuni miglioramenti nei criteri di alimentazione degli applicativi allo scopo di garantire la correttezza dei saldi ai fini del presidio e della corretta gestione della liquidità. Ulteriori interventi di mitigazione nel corso del 2018 sono previsti per minimizzare alcuni rischi informatici, quali ad esempio quelli relativi alla revisione degli attuali profili abilitativi di alcuni applicativi a supporto del business e all'implementazione del processo accentrato per la concessione di nuove abilitazioni.