



## **Relazione annuale sul Rischio Informatico**

### **Gruppo Montepaschi – Anno 2016**

*Prodotto da:* Servizio Rischi Operativi e Reputazionali – Settore Rischi Informatici  
*Autore:* Emilio Longo  
*Approvato da:* Benedetta Mazzolli  
*Data:* 28 febbraio 2016  
*Stato:* Definitivo

Sommario

<b>1</b>	<b>PREMESSA.....</b>	<b>3</b>
<b>2</b>	<b>EXECUTIVE SUMMARY .....</b>	<b>5</b>
<b>3</b>	<b>MODELLO ORGANIZZATIVO PER LA GESTIONE DEL RISCHIO INFORMATICO .....</b>	<b>7</b>
<b>4</b>	<b>RISK APPETITE STATEMENT E PROPENSIONE AL RISCHIO INFORMATICO .....</b>	<b>10</b>
<b>5</b>	<b>METODOLOGIA DI ANALISI DEL RISCHIO INFORMATICO .....</b>	<b>11</b>
5.1	METODOLOGIA – ANALISI TOP LEVEL .....	11
5.2	METODOLOGIA – ANALISI LOW LEVEL .....	13
5.3	METODOLOGIA – ANALISI DELLA SICUREZZA INFORMATICA .....	15
<b>6</b>	<b>PERIMETRO E GRANULARITÀ DELL’ANALISI DEL RISCHIO INFORMATICO .....</b>	<b>17</b>
6.1	PERIMETRO – ANALISI TOP LEVEL .....	17
6.2	PERIMETRO – ANALISI LOW LEVEL .....	18
<b>7</b>	<b>RISULTATI DELL’ANALISI DEL RISCHIO INFORMATICO .....</b>	<b>19</b>
7.1	RISULTATI – ANALISI TOP LEVEL.....	19
7.2	RISULTATI – ANALISI LOW LEVEL.....	21
7.2.1	<i>Analisi Low Level sui sistemi di pagamento via internet .....</i>	<i>23</i>
7.3	RISULTATI – ANALISI DELLA SICUREZZA INFORMATICA .....	24
<b>8</b>	<b>PIANO DI MITIGAZIONE DEL RISCHIO INFORMATICO .....</b>	<b>24</b>
<b>9</b>	<b>MONITORAGGIO DEI KEY RISK INDICATOR INSERITI NEL RAS .....</b>	<b>26</b>
<b>10</b>	<b>PIANO DI ATTIVITÀ PER IL 2017 .....</b>	<b>27</b>
<b>11</b>	<b>CONCLUSIONI .....</b>	<b>28</b>
	<b>ALLEGATI .....</b>	<b>30</b>

## **1 Premessa**

Il sistema informativo rappresenta uno strumento fondamentale per il conseguimento degli obiettivi strategici e operativi delle Banche, in considerazione del valore delle informazioni gestite e della criticità dei processi aziendali che dipendono da esso. Per tale motivo, la Banca d'Italia ha ritenuto necessario emanare una disciplina organica in materia di sviluppo e gestione del Sistema informativo, esposta nella Circolare n. 285/2013.<sup>1</sup>

La Circolare definisce il *"rischio informatico"* 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).*

Tra i requisiti posti dalla Circolare vi è l'adozione di un modello organizzativo e di un processo strutturato per la gestione del rischio informatico, finalizzato ad identificare, valutare, trattare, documentare e monitorare i rischi connessi all'utilizzo delle tecnologie informatiche. E' richiesto, infatti, che siano forniti agli Organi apicali ed alle Funzioni aziendali preposte, gli elementi di giudizio necessari per il governo del rischio informatico, coerentemente con i principi, le politiche e le linee guida adottate per la determinazione della propensione al rischio a livello di Gruppo (Risk Appetite Statement, RAS).

Al fine di ottemperare alle prescrizioni regolamentari, il Gruppo Montepaschi ha avviato, nel secondo semestre del 2014, un programma di adeguamento volto a dare esecuzione a tutti gli interventi richiesti di carattere organizzativo e procedurale.

Nel corso del 2015, il Servizio Rischi Operativi e Reputazionali ha emanato la Policy in materia di Metodologia di Analisi del Rischio Informatico ed ha creato al proprio interno un Settore dedicato al controllo del rischio informatico. E' stato inoltre costituito all'interno del Consorzio Operativo di Gruppo (d'ora in poi anche "COG"), il Servizio IT Risk Management, che opera quale nucleo di controllo specializzato delle risorse informatiche sviluppate e gestite dal Consorzio stesso, con riporto funzionale al Servizio Rischi Operativi e Reputazionali della Capogruppo.

A giugno 2016 analoga funzione di controllo è stata costituita anche in Banca Widiba, al fine di presidiare il rischio informatico relativo al suo sistema di Front-end multicanale.

Sempre nel 2016, è stato condotto un progetto di affinamento della metodologia di IT risk management, basato su best practice di mercato, al fine di rendere l'analisi e la gestione del rischio informatico maggiormente strutturata e atta a garantire miglior organicità delle rilevazioni sul sistema informativo aziendale, nel rispetto dei dettami normativi. Tale impostazione metodologica, recepita nella nuova Direttiva di Gruppo in materia di Gestione del Rischio Informatico emanata a settembre 2016 (documento 1030D02045), prevede la conduzione in parallelo di due tipologie di analisi:

---

<sup>1</sup> Circolare Banca d'Italia n. 285/2013, Parte prima, Titolo IV, Capitolo 4 – Sistema Informativo.

- Un'analisi di alto livello (di seguito "Top Level") finalizzata a rappresentare la situazione di rischio complessiva dell'ICT sulla base di Key Risk Indicator (KRI), ovvero indicatori di rischio che misurano nel continuo una serie di eventi tecnologici e di processo, raffrontati su scale di misurazione definite a livello di Gruppo;
- Un'analisi di dettaglio (di seguito "Low Level") finalizzata alla valutazione prospettica, in termini di probabilità qualitative, degli eventi di rischio informatico che possono colpire i singoli asset ICT (applicazioni, infrastrutture) in esercizio, condotta su un perimetro selezionato annualmente.

In aggiunta, nel 2016 è stata condotta un'analisi di rischio specifica sulla Sicurezza Informatica del COG, con il supporto metodologico di una Società di consulenza esterna, al fine di verificare l'adeguatezza delle azioni concordate per la mitigazione del rischio di livello "Alto" evidenziato nella Relazione sul rischio informatico relativa al 2015.<sup>2</sup>

Il 26/9/2016 il CdA ha inoltre approvato la costituzione della Commissione Risorse ICT Trasversali per l'esercizio del ruolo di "Utente Responsabile" nella gestione del rischio informatico sulle risorse informatiche di natura trasversale rispetto alle diverse funzioni di business, dando contestualmente mandato all'AD di definirne le funzioni partecipanti, i ruoli, le responsabilità ed i meccanismi di funzionamento. La Commissione è stata quindi costituita nel gennaio 2017.<sup>3</sup>

La presente Relazione descrive le risultanze del ciclo di analisi e trattamento del rischio informatico relativo all'anno 2016 ed è volta a fornire agli Organi aziendali informativa sulla situazione del rischio informatico del Gruppo Montepaschi e sullo stato di implementazione delle relative misure di mitigazione.

Come richiesto dalla Circolare Banca d'Italia n. 285/2013, la presente Relazione è sottoposta all'approvazione dell'Organo con funzione di gestione della Capogruppo, che ne informa l'Organo con funzione di supervisione strategica. Quest'ultimo, nell'ambito del proprio ruolo e delle responsabilità sulla materia, approva la sintesi della Relazione.

Si precisa che, in accordo con la direttiva Direttiva di Gruppo in materia di Gestione del Rischio Informatico (D1030D02045), la "Relazione sul Rischio Informatico del Consorzio Operativo di Gruppo – Anno 2016" è già stata approvata dal Comitato dei Consorziati del Consorzio Operativo di Gruppo in data 7 marzo 2017 e la "Relazione sul Rischio Informatico di Banca Widiba – Anno 2016" è stata approvata dal CdA di Widiba in data 8 febbraio 2017.

---

<sup>2</sup> Relazione approvata dal CdA del 25 febbraio 2016.

<sup>3</sup> Regolamento n.1 - Organizzazione della Banca MPS pubblicato il 17 gennaio 2017 (documento 1030D00751 v. 75).

## **2 Executive Summary**

L'ambito dell'analisi del rischio informatico coperto dalla presente Relazione comprende sia gli asset ICT sviluppati e gestiti dal COG (664 asset), sia quelli gestiti direttamente da Banca Widiba, corrispondenti al sistema di Front-end multicanale della Banca (10 asset).

Il Risk Appetite Statement (RAS) approvato dal CdA per il 2016, ha stabilito che il rischio informatico non debba superare il livello "Medio", con riferimento alla scala qualitativa a 5 livelli prevista dalla Metodologia di Gruppo ("Molto Alto", "Alto", "Medio", "Basso", "Molto Basso").

L'analisi di rischio "Top Level", basata sulla misurazione di Key Risk Indicator (KRI), non ha evidenziato, sul piano complessivo, livelli di rischio superiori alla soglia di propensione definita nel RAS.

In particolare, per l'85% degli ambiti applicativi e infrastrutturali gestiti dai Settori del COG il livello di rischio è stato valutato come "Basso" o "Molto Basso". E così pure è stata valutata "Bassa" la rischiosità complessiva del sistema di Front-end multicanale gestito da Banca Widiba.

L'analisi Top Level ha però indicato anche alcune aree di miglioramento, corrispondenti ai seguenti 6 Settori del COG (il 15% di 40 Settori analizzati) che presentano un livello di rischio "Medio":

- Settore Pagamenti e Portafoglio;
- Settore Sistemi di Rete;
- Settore Finanza Proprietaria;
- Settore Finanza Titoli Compravendita;
- Settore Risparmio Gestito;
- Settore Anagrafe e Condizioni.

Le anomalie osservate hanno riguardato principalmente: gli incidenti sugli asset ICT, i change in emergenza, le modifiche ai dati eseguite direttamente sui data base in produzione, i progetti in ritardo. Le evidenze fornite dai singoli KRI sono state condivise con i Responsabili dei Settori al fine di inquadrare le motivazioni degli andamenti e condividere le azioni di miglioramento da realizzare, seppure non obbligatorie per il rispetto dei limiti fissati nel RAS.

A complemento dell'analisi Top Level, è stata condotta un'analisi di dettaglio ("Low Level") finalizzata alla valutazione prospettica, in termini di probabilità qualitative, degli eventi di rischio informatico che possono colpire i singoli asset ICT in esercizio. Tra i controlli applicati in sede di analisi sono stati integrati i requisiti posti dall'EBA – European Banking Authority in materia di sicurezza dei pagamenti tramite internet, divenuti obbligatori con decorrenza dal 30 settembre 2016.

Per quanto riguarda il COG, l'analisi Low Level è stata condotta su un perimetro di 144 asset su un totale di 664 presenti in inventario: gli asset sono stati selezionati incrociando una serie di fattori indicativi del loro livello di criticità rispetto al rischio informatico e costituiscono la prima tranche di un piano concordato con

la Direzione del COG e approvato dal CdA <sup>4</sup>, che prevede di concludere, nell'arco di un triennio, l'analisi di rischio sugli asset ICT in esercizio.

Il 7% degli asset ICT del COG inseriti nel perimetro di analisi (10 su 144), ha evidenziato un livello di rischio prospettico valutato "Alto" ed ha richiesto l'attivazione di specifiche iniziative di mitigazione. Per uno di questi asset, l'applicazione APP0000494 - SAG - Swift Alliance Gateway, la valutazione come rischio "Alto" costituisce una proposta, da validarsi a cura della neo-costituita Commissione risorse ICT trasversali. Le relative azioni di mitigazione sono state comunque avviate d'iniziativa da parte del COG.

Al 31/12/2016, oltre ai predetti 10 asset ICT con rischio "Alto" individuati nel corso del 2016, ne rimanevano altri 3 con rischio "Alto" individuati a fine 2015, le cui mitigazioni sono in fase di realizzazione (APP0000766 - Centrale Allarme Interbancaria, APP0000760 - Channel & Liquidity Manager e APP0000048 - PEF - Pratica Elettronica di Fido; per quest'ultima applicazione la mitigazione si è chiusa il 31/1/2017).

La Sicurezza Informatica del Consorzio è stata oggetto di un'analisi di rischio specifica, condotta con il supporto metodologico di una Società di consulenza esterna. L'analisi ha confermato che questo rimane un ambito di particolare attenzione, in ragione dell'evoluzione continua delle minacce e della scoperta di nuove vulnerabilità tecnologiche e per la presenza di gap strutturali, emersi nella precedente Relazione sul Rischio Informatico relativa al 2015. Per riportare il rischio su un livello "Medio", il Consorzio ha definito, a settembre 2016, un piano di interventi di breve termine, integrativo rispetto a quello formalizzato a inizio 2016 e denominato "Monte più Sicuro". Tutte le attività previste per il 2016 sono state svolte.

La Sicurezza informatica costituisce un'area di attenzione anche per Banca Widiba: le sessioni di ethical hacking <sup>5</sup> condotte a ottobre del 2016 e l'analisi del rischio Low Level su tutte e 10 le componenti del suo sistema di Front-end hanno, infatti, rilevato la presenza di alcuni rischi di livello "Medio", riconducibili a vulnerabilità rispetto ad attacchi dall'esterno e accessi indebiti. Le mitigazioni delle vulnerabilità individuate attraverso l'attività di ethical haking sono state prontamente avviate e saranno completate al più tardi entro il 31 marzo 2017. Le altre iniziative progettuali che Widiba ha pianificato per il 2017 riguardano il potenziamento delle misure antifrode e dei monitoraggi di sicurezza, nonché lo svolgimento di nuove sessioni di penetration test e vulnerability assessment.

---

<sup>4</sup> Obiettivo definito nella Relazione sul Rischio Informatico relativa al 2015, approvata dal CdA del 25 febbraio 2016.

<sup>5</sup> Attività di verifica condotte da società esterne specializzate, che utilizzano tecniche e scenari d'attacco reali per individuare eventuali vulnerabilità nella sicurezza di reti e applicazioni, simulando le possibili conseguenze nel caso esse siano scoperte e sfruttate da un hacker.

Segue resoconto dei risultati raggiunti a fronte delle attività programmate per il 2016:<sup>6</sup>

Piano di attività per il 2016	Risultati raggiunti
Proseguimento delle analisi sulle risorse informatiche in produzione.	✓ Completata analisi del rischio su: <ul style="list-style-type: none"> <li>• 144 asset ICT gestiti dal Consorzio</li> <li>• 10 asset ICT gestiti da Widiba</li> </ul>
Predisposizione del piano di mitigazione complessivo del rischio informatico, alimentato dagli interventi di mitigazione di tipo tecnologico, organizzativo o procedurale, approvati dagli Utenti Responsabili.	✓ Al 31/12/2016 il piano comprende 8 interventi di mitigazione di rischi che eccedono i limiti fissati dal RAS, con diverse scadenze fino a luglio 2017. Di questi: 7 interventi fanno riferimento a 12 asset ICT, mentre l'ultimo riguarda la sicurezza logica COG.
Avvio dell'analisi del rischio sui progetti di sviluppo e di modifica rilevante del sistema informativo.	✓ Eseguita analisi sui seguenti major changes: <ul style="list-style-type: none"> <li>• progetto Swap data center (inversione del ruolo dei data center di Siena e Firenze);</li> <li>• progetto Digital banking (sviluppo nuovo internet banking clientela privati).</li> </ul>
Adeguamento delle normative di processo impattate dal processo di gestione del rischio informatico.	✓ Analizzati testi normativi da integrare; formalizzazione nel 2017.
Implementazione di una nuova applicazione a supporto dell'analisi del rischio informatico.	✓ Realizzato primo prototipo, utilizzato per analisi rischio 2016 su asset ICT in esercizio.
Completamento, a cura di Area Organizzazione, dell'attività di individuazione degli Utenti Responsabili delle risorse informatiche.	✓ Utente Responsabile individuato per 614 asset ICT gestiti dal Consorzio o da Widiba, pari al 91% del totale; in corso attività per formalizzare assegnazione su ultimi 60 asset. ✓ Costituita Commissione risorse ICT trasversali presso la Capogruppo.
Monitoraggio del rischio informatico tramite i Key Risk Indicator definiti nel RAS.	✓ Monitoraggio effettuato con cadenza mensile.

**Figura 1 – Piano di attività programmate per il 2016 e risultati raggiunti**

Per quanto riguarda il 2017, l'obiettivo è di proseguire l'analisi del rischio su una seconda tranches di asset ICT in esercizio gestiti dal Consorzio Operativo di Gruppo e attuare una serie di iniziative progettuali per il rafforzamento del modello di gestione del rischio informatico, finalizzate principalmente a consolidare il presidio sui major change e garantire l'allineamento della metodologia, dei controlli e del processo alle nuove guidelines EBA in materia di SREP (Supervisory Review and Evaluation Process), attualmente in fase di consultazione.<sup>7</sup>

### 3 Modello organizzativo per la gestione del rischio informatico

Il modello organizzativo adottato dal Gruppo Montepaschi per la gestione del rischio informatico è definito dalla Direttiva 1030D02045 e individua nell'Area Risk Management - Servizio Rischi Operativi e Reputazionali la Funzione di controllo del rischio informatico a livello di Gruppo prevista dalla Circolare

<sup>6</sup> Attività definite nella Relazione sul Rischio Informatico relativa al 2015, approvata dal CdA del 25 febbraio 2016.

<sup>7</sup> Documento EBA/CP/2016/14 del 6 ottobre 2016: Guidelines on ICT Risk Assessment under the Supervisory Review and Evaluation process (SREP). Consultation Paper

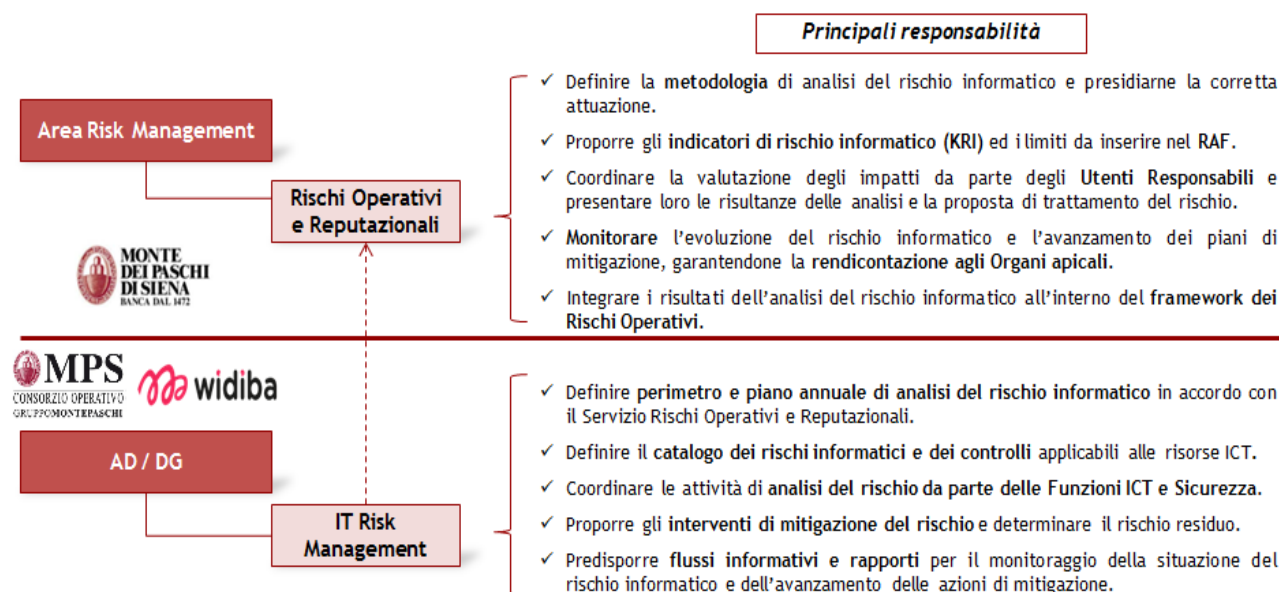
Banca d'Italia n. 285/2013.

Per presidiare opportunamente il processo di gestione del rischio informatico, è stato stabilito di costituire una Funzione di gestione del rischio informatico presso le Società del Gruppo che sviluppano e gestiscono risorse informatiche:

- il Servizio IT Risk Management, presso il Consorzio Operativo di Gruppo (costituito a maggio 2015);
- l'Ufficio IT Risk Management, presso Banca Widiba (costituito a giugno 2016).

Tali Funzioni operano quale nucleo di controllo specializzato delle risorse informatiche sviluppate e gestite della Società di appartenenza. Per garantirne l'indipendenza, esse dipendono gerarchicamente dalla Direzione della propria Società e riportano funzionalmente al Servizio Rischi Operativi e Reputazionali della Capogruppo.

La seguente figura descrive le responsabilità attribuite alle predette Funzioni.



**Figura 2 – Principali responsabilità delle Funzioni di controllo e di gestione del rischio informatico**

Il modello organizzativo prevede inoltre il ruolo dell'Utente Responsabile, figura da identificare per ciascun sistema o applicazione, che concorrere al processo di analisi del rischio informatico sulle risorse di propria competenza, accettandone formalmente il rischio residuo. Il ruolo di Utente Responsabile è stato formalizzato anche nel Regolamento n. 1 della Capogruppo e viene attribuito, a cura dell'Organizzazione, alla Funzione aziendale che, per prevalenza di interesse a livello di Gruppo, può rappresentare gli utenti di una data risorsa informatica nei rapporti con la Funzione ICT.



Ai fini dell'individuazione dell'Utente Responsabile, si distinguono le seguenti tipologie di risorse informatiche:

- Le applicazioni di business, che realizzano un insieme di funzionalità a supporto dell'esecuzione dei processi aziendali, sono assegnate ad una specifica Funzione di business.
- Le piattaforme di sicurezza, poste a protezione dell'integrità fisica e logica del sistema informativo e della riservatezza dei dati gestiti, sono di competenza della Funzione Sicurezza.<sup>8</sup>
- Le risorse c.d. "ITxIT", utilizzate esclusivamente dalla Funzione ICT a supporto dei propri processi operativi<sup>9</sup> e non collegate direttamente ai processi di business. Per tali asset l'Utente Responsabile è individuato all'interno della Funzione ICT.
- Le risorse ICT trasversali, per le quali non è possibile individuare una Funzione aziendale prevalente, ove il ruolo di Utente Responsabile viene esercitato collegialmente da apposita Commissione costituita a inizio del 2017 presso la Capogruppo<sup>10</sup>.

La figura dell'Utente Responsabile è stata individuata per 614 asset ICT gestiti dal Consorzio o da Widiba, pari al 91% del totale. Segue tabella con la ripartizione degli asset per tipologia.

<b>Tipologia di risorse ICT</b>	<b>Utente Responsabile (UR)</b>	<b>Nr. Asset</b>	<b>% su totale</b>
Applicazioni di business	Funzione Business	424	63%
Piattaforme di sicurezza	Funzione Sicurezza	21	3%
Risorse ITxIT	Funzione ICT	40	6%
Risorse ICT trasversali	Commissione Risorse ICT Trasversali	129	19%
<i>subtotale asset ICT con UR individuato</i>		<b>614</b>	<b>91%</b>
Risorse in via di assegnazione	da finalizzare	60	9%
<b>Totale</b>		<b>674</b>	<b>100%</b>

**Tabella 1 – Asset ICT gestiti dal Consorzio o da Widiba: ripartizione per tipologia di risorsa e di Utente Responsabile.**

<sup>8</sup> Ad esempio: controllo accessi, sicurezza perimetrale, monitoraggio eventi di sicurezza, prodotti antivirus, etc..

<sup>9</sup> Ad esempio: analisi e sviluppo del software; change management; gestione dell'inventario delle risorse; etc.

<sup>10</sup> Regolamento n.1 - Organizzazione della Banca MPS pubblicato il 17 gennaio 2017 (documento 1030D00751 v. 75).

Gli Utenti Responsabili individuati sono 109. Segue tabella con la ripartizione per Società di appartenenza.

<b>Società</b>	<b>Nr. Utenti Responsabili</b>	<b>Nr. Asset</b>
BMPS	80	412
WIDIBA	9	18
MPSCS	10	15
COG	10	40
<b>totale</b>	<b>109</b>	<b>485</b>

**Tabella 2 – Utenti Responsabili degli asset gestiti dal Consorzio o da Widiba: ripartizione per Società di appartenenza.**

## 4 Risk Appetite Statement e propensione al rischio informatico

Il livello di propensione al rischio informatico, ovvero il livello massimo di rischio che il Gruppo Montepaschi intende assumere, viene stabilito annualmente nell’ambito del Risk Appetite Statement (RAS).

Il livello di propensione al rischio informatico è stato definito con riferimento alla scala qualitativa a 5 livelli prevista dalla Metodologia di Gruppo (“Molto Alto”, “Alto”, “Medio”, “Basso”, “Molto Basso”).

In particolare, il RAS di Gruppo per il 2016 ha stabilito che il rischio informatico non debba superare il livello “Medio”. Pertanto, qualora il rischio potenziale sia valutato su un livello “Alto” o “Molto alto”, secondo il quadro metodologico definito dalla Direttiva 1030D02045, dovranno essere prontamente individuate misure di mitigazione idonee a contenerlo entro i limiti fissati nel RAS.

Nel RAS è stato inoltre previsto il monitoraggio di due KRI – Key Risk Indicator con l’obiettivo di intercettare tempestivamente nuovi segnali di deterioramento (early warning), da approfondire e indirizzare prima che il rischio si manifesti in un impatto negativo per il Gruppo

<b>Ambito</b>	<b>KRI</b>	<b>Soglia di attenzione</b>
<b>Incidenti sulle risorse informatiche</b>	<b>Numero mensile di incidenti</b> per singola risorsa informatica	10 incidenti mensili, per le <b>applicazioni a supporto di processi critici</b> ai fini della <b>Business Continuity</b> 30 incidenti mensili per le <b>altre applicazioni</b> 200 incidenti mensili per la <b>rete TLC</b>
<b>Frodi sulla clientela Internet Banking</b>	<b>% clienti IB che hanno subito perdite</b> a seguito di transazioni fraudolente, calcolata su base annua	0,01% (1 cliente ogni 10.000)

**Figura 3 – Indicatori rischio informatico monitorati nell’ambito del RAS – Risk Appetite Statement**

## **5 Metodologia di analisi del rischio informatico**

L'impostazione metodologica è definita dalla Direttiva di Gruppo in materia di Gestione del Rischio Informatico (documento 1030D02045) e prevede la conduzione in parallelo di due tipologie di analisi:

- Un'analisi di alto livello (di seguito "Top Level") al fine di rappresentare la situazione di rischio complessiva dell'ICT. Tale analisi si basa su Key Risk Indicator (KRI), ovvero su indicatori di rischio che misurano nel continuo una serie di eventi tecnologici e di processo, raffrontati su scale di misurazione definite a livello di Gruppo.
- Un'analisi di dettaglio (di seguito "Low Level") condotta sui singoli asset ICT e finalizzata alla valutazione prospettica, in termini di probabilità su scala qualitativa, degli eventi di rischio informatico che possono colpire l'asset e provocare un impatto negativo per il Gruppo. Tale analisi si focalizza su un perimetro di asset selezionati annualmente e si basa sul catalogo dei rischi informatici definito a livello di Gruppo.<sup>11</sup>

In considerazione del fatto che la Relazione sul rischio informatico del 2015 aveva evidenziato un rischio di livello "Alto" sulla sicurezza logica del Consorzio, è stata inoltre svolta un'analisi specifica in tale ambito, con l'obiettivo di valutare l'adeguatezza delle azioni di mitigazione già concordate. L'analisi è stata condotta sulla base di un frame metodologico specifico fornito dalla Società di consulenza Deloitte ERS.

### **5.1 Metodologia – Analisi Top Level**

Come anticipato, ai fini della valutazione complessiva della situazione di rischio del sistema informativo di Gruppo si è proceduto alla misurazione di una serie indicatori di rischio (KRI), così come suggerito dagli standard internazionali in ambito rischio informatico (ISO27005, COBIT5 for Risk).

I KRI sono indicatori basati su dati osservabili che permettono di tracciare l'evoluzione del profilo di rischio informatico e fungono da sistema di primo allarme (*early warning*), per cogliere situazioni di anomalia che richiedono analisi più approfondite e interventi tempestivi, prima che il rischio si manifesti in un impatto negativo per il Gruppo.

In particolare, i KRI devono consentire il monitoraggio delle seguenti dimensioni di analisi:



- la capacità della Funzione ICT di evadere le richieste del Business tramite progetti, nei tempi previsti;

---

<sup>11</sup> Il catalogo dei rischi informatici rappresenta l'insieme degli scenari e degli eventi di rischio, delle vulnerabilità e dei controlli (misure di protezione e mitigazione) ad essi collegati, che devono essere valutati per l'analisi di tipo Low Level.

- il grado di allineamento dell'ICT alle best practice di Settore e ai dettami normativi, sia interni che esterni;
- i livelli di disponibilità e affidabilità degli asset ICT;
- i livelli di sicurezza delle applicazioni ICT.

Nella tabella che segue sono elencati i KRI utilizzati per l'analisi del rischio 2016 sulle risorse informatiche gestite, rispettivamente, dal Consorzio e da Banca Widiba. A ciascun KRI è stato assegnato un grado di rilevanza su scala qualitativa, tradotto in un peso percentuale, tenendo conto dell'affidabilità dei dati che alimentano i KRI e della loro significatività nella rappresentazione del livello di rischio per le due Società.

		 <b>MPS</b> <small>CONSORZIO OPERATIVO GRUPPO MONTEPASCHI</small>		 <b>widiba</b>	
ID	KRI	Rilevanza	%	Rilevanza	%
PRJ	Somma pesata dei progetti conclusi in ritardo, in rapporto al totale dei progetti rilasciati nel periodo in esame.	Media	15%	Media	15%
GAP	Somma pesata dei rilievi attivi su asset ICT, censiti dalle Funzioni di Controllo nell'applicativo Rigam	Media	15%	Media	15%
RFC	Numero dei change in emergenza, in rapporto al totale dei change rilasciati nel periodo in esame	Media	15%	Media	15%
INC	Somma pesata degli incidenti ICT, in rapporto al numero degli asset ICT	Molto Alta	25%	Molto Alta	30%
JOB	Numero delle elaborazioni batch andate in errore nel periodo in esame, in rapporto al numero degli asset ICT	Media	15%	Non applicabile al Front-end Widiba	-
CA	Numero asset ICT non collegati al controllo accessi centralizzato e/o privi di sistema di Single Sign-On	Molto Bassa	5%	Molto Bassa	5%
CHD	Numero di change eseguiti direttamente sui dati in produzione	Bassa	10%	Non applicabile al Front-end Widiba	-
FR	Numero di clienti Internet Banking che hanno subito perdite a seguito di transazioni fraudolente, in rapporto al totale dei clienti attivi	Non considerato in quanto non applicabile a tutti i Settori del COG	-	Alta	20%

**Tabella 3 – Analisi Top Level: indicatori di rischio informatico (KRI)**

Per ogni KRI è stata quindi costruita una scala di valutazione secondo range numerici, ai quali sono stati associati corrispondenti livelli di rischio, secondo la scala qualitativa a 5 livelli prevista dalla Metodologia di Gruppo ("Molto Alto", "Alto", "Medio", "Basso", "Molto Basso").

Le soglie delle scale di valutazione dei singoli indicatori sono state identificate tenendo in considerazione due criteri: il valore target fissato per l'indicatore in questione e l'andamento storico registrato

dall'indicatore stesso negli anni precedenti.

Il risultato di rischio finale espresso dall'insieme dei KRI è ottenuto eseguendo la media ponderata dei risultati di ogni singolo KRI (sulla base dei pesi percentuali associati ai KRI).

Il periodo di osservazione dei KRI è stato annuale (Gennaio - Dicembre 2016).

Per ogni altro dettaglio sulle modalità di calcolo degli indicatori, sulle fonti informative utilizzate e sulla costruzione delle scale di valutazione, si rimanda alle Relazioni predisposte, rispettivamente, dal Servizio IT Risk Management del Consorzio e dall'Ufficio IT Risk Management di Banca Widiba (in allegato).

## **5.2 Metodologia – Analisi Low Level**

L'analisi di rischio Low Level è svolta a livello di singolo asset ICT ed è finalizzata alla valutazione prospettica, in termini di probabilità su scala qualitativa, degli eventi di rischio informatico che possono colpire l'asset e provocare un impatto negativo per il Gruppo.

Annualmente, il Servizio Rischi Operativi e Reputazionali definisce il perimetro degli asset in esercizio da sottoporre ad analisi, in accordo con le Funzioni di gestione del rischio del Consorzio e di Widiba. Per il ciclo di analisi 2016, gli asset sono stati selezionati sulla base di indicatori di criticità rispetto al rischio informatico, tenendo anche conto degli esiti delle analisi condotte in materia di gestione della business continuity (per maggiori dettagli sui criteri di selezione si rinvia al paragrafo 6.2).

La metodologia di analisi Low Level prevede una fase iniziale di identificazione degli eventi di rischio informatico applicabili all'asset oggetto di analisi, tra quelli previsti all'interno del catalogo dei rischi definito a livello di Gruppo.

L'applicabilità degli eventi di rischio all'asset e la loro probabilità di accadimento (su scala qualitativa) sono valutate dalla Funzione ICT, nel corso di interviste condotte dalle Funzioni di gestione del rischio del Consorzio e di Widiba. In particolare, le valutazioni sono basate sugli esiti di un questionario utilizzato per rilevare la presenza o assenza di una serie di controlli (misure di protezione e mitigazione) che il catalogo associa ai singoli eventi di rischio informatico, nonché sulle serie storiche a disposizione su malfunzionamenti e incidenti di sicurezza. La probabilità è stimata rispetto alla scala qualitativa a 5 livelli prevista dalla Metodologia di Gruppo ("Molto Alto", "Alto", "Medio", "Basso", "Molto Basso").

Gli eventi di rischio, a loro volta, sono aggregati in scenari di rischio.<sup>12</sup> La probabilità qualitativa dello scenario di rischio è attribuita secondo la logica del worst case (ogni scenario eredita la probabilità maggiore associata ad uno o più eventi che lo costituiscono). Segue elenco degli scenari di rischio analizzati per l'anno 2016.

---

<sup>12</sup> Per "scenario di rischio" si intende un insieme di eventi di rischio omogenei per tipologia o per effetti sul business.

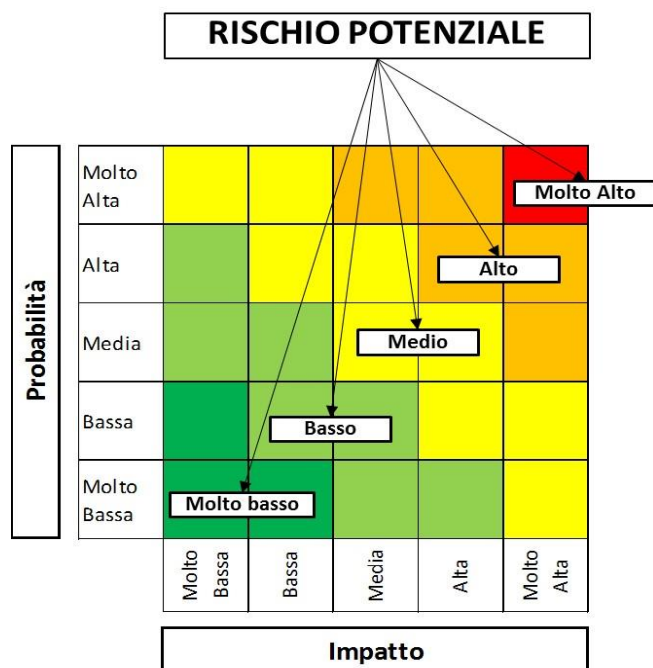
<b>Scenari di rischio</b>
Rischi legati a <b>carenze di expertise</b> o abilità delle <b>risorse ICT</b> nel supporto all'operatività dei sistemi
Rischi legati all' <b>errata esecuzione</b> di operazioni da parte di personale interno
Rischi legati ai <b>fornitori</b>
Rischi legati ad <b>anomalie o degrado</b> dell'asset a <b>causa di change</b> gestito non correttamente
Rischi legati ad <b>anomalie o degrado</b> dell'asset in <b>produzione</b>
Rischi legati a <b>blocchi</b> dell'asset a <b>causa di change</b> gestito non correttamente
Rischi legati a <b>blocchi</b> dell'asset in <b>produzione</b>
Rischi legati a <b>danneggiamento o perdita delle informazioni</b> a causa di <b>eventi accidentali</b>
Rischi legati a <b>danneggiamento o perdita delle informazioni</b> a causa di <b>intenti malevoli</b>
Rischi legati ad <b>accesso indebito o divulgazione delle informazioni</b>
Rischi legati a <b>furto o smarrimento</b> di <b>apparati mobili</b> contenenti informazioni riservate
Rischi legati a <b>malware ed attacchi logici</b>

**Tabella 4 – Analisi Low Level: elenco degli scenari di rischio**

Gli impatti sono valutati per ogni scenario di rischio, tramite un questionario somministrato agli Utenti Responsabili che traduce gli scenari di rischio informatico in domande sui potenziali effetti negativi dal punto di vista del business.

Il questionario distingue quattro tipologie di impatto: economico/operativo; reputazionale/commerciale; normativo e strategico. Le valutazioni sono effettuate secondo la scala qualitativa a 5 valori ("Molto Alto", "Alto", "Medio", "Basso", "Molto Basso") e sono aggregate a livello di scenario secondo la logica del worst case (ogni scenario eredita l'impatto maggiore tra le quattro tipologie considerate). L'attività di raccolta dei questionari è svolta direttamente dalla Funzione di controllo del rischio informatico della Capogruppo.

Il rischio informatico è quindi valutato come la combinazione tra la probabilità di accadimento degli scenari di rischio e il loro impatto stimato per il Gruppo Montepaschi, entrambi espressi su scala qualitativa, secondo quanto definito nella matrice di seguito rappresentata.



**Figura 4 – Analisi Low Level: matrice di valutazione del livello di rischio informatico**

Il livello di rischio finale per ogni singolo asset è ottenuto aggregando i rischi sugli scenari, secondo la logica del worst case (l'asset eredita il valore di rischio maggiore relativo ad uno o più scenari che lo costituiscono).

Per i livelli di rischio superiori alla soglia di propensione definita nel RAS – Risk Appetite Statement del Gruppo Montepaschi (cfr. paragrafo 4) l'Utente Responsabile è obbligato a mitigare il rischio per ricondurlo entro il limite stabilito. Secondo i propri obiettivi, l'Utente Responsabile può pure decidere di mitigare un rischio pari o inferiore alla soglia di propensione, selezionando, in un'ottica di bilanciamento tra costi e benefici, ulteriori misure di mitigazione "discrezionali".

### 5.3 Metodologia – Analisi della Sicurezza Informatica

La Relazione sul Rischio Informatico relativa all'anno 2015 aveva individuato un rischio di livello "Alto" riguardo ai processi operativi e i presidi della sicurezza logica del Consorzio Operativo di Gruppo. A fronte di tale valutazione è stato formalizzato, ad inizio 2016, un piano di interventi di mitigazione (alcuni in corso o già pianificati dal COG per il 2016), denominato "Monte Più Sicuro" e segnalato con la formalizzazione di uno specifico gap.<sup>13</sup>

<sup>13</sup> *Codice Rigam RM 2016 00008.*

Per valutare l'adeguatezza delle azioni di mitigazione già concordate, il Servizio IT Risk Management del COG ha condotto un'analisi specifica sul macro ambito della sicurezza informatica, avvalendosi del supporto della Società di consulenza Deloitte ERS, la quale ha fornito un frame metodologico specifico ed ha partecipato alla conduzione delle interviste alle Funzioni Sicurezza del Consorzio e della Capogruppo.

Nella tabella di seguito sono presentati i quattro scenari presi in considerazione, a ognuno dei quali sono stati associati una o più minacce di sicurezza, a loro volta riconducibili ad un totale di 38 minacce di dettaglio.

Scenario	Minaccia	Descrizione
<b>Attacchi logici</b>	<b>Malware</b>	Include le minacce legate a codice malevolo (viruses / worms, trojan horses / rootkits, botnet clients)
	<b>Hacking</b>	Include le minacce relative ad attacchi DoS, utilizzo di credenziali non autorizzato, scanning / intercettazione della rete, modifiche al sito web / al software / alle informazioni, furto di credenziali, etc.
	<b>Minacce sociali</b>	Include le minacce che utilizzano l'utente finale come veicolo per un attacco ai sistemi/informazioni (spoofing del sito, phishing, spam, etc.) e relative alla disclosure non autorizzata, accidentale o deliberate di informazioni aziendali.
<b>Utilizzo improprio e/o errori</b>	<b>Utilizzo improprio</b>	Include le minacce relative ad utilizzo non autorizzato/non consono dei sistemi informatici, sottrazione di software/informazioni di business.
	<b>Errori e malfunzionamenti</b>	Include le minacce legate ad errore utenti finali / staff tecnico, malfunzionamento HW / SW, effetti non desiderati derivanti da modifiche.
<b>Incidenti di sicurezza fisica</b>	<b>Accessi fisici e furti/perdite</b>	Include le minacce relative ad accessi fisici non autorizzati e furti/perdita di dispositivi.
<b>Interruzione del business</b>	<b>Minacce ambientali</b>	Include disastri naturali, danneggiamenti, interruzione di corrente / comunicazioni esterne.

**Tabella 5: Analisi Sicurezza Informatica: elenco degli scenari di rischio e delle minacce di sicurezza**

Le analisi relative alla robustezza dei controlli in essere, finalizzate alla valutazione del livello di probabilità in termini qualitativi di ciascuna minaccia di dettaglio, sono state svolte in modalità self-assessment guidata, con il supporto di un questionario ove sono stati censiti circa 400 controlli previsti da best practice e standard internazionali in ambito sicurezza (NIST, ISO27001, ISF SoGP).

Il livello di rischio associato a ciascuna minaccia di dettaglio è stato valutato come combinazione tra la probabilità di accadimento e il relativo impatto (quest'ultimo desunto da un benchmark del settore banking a livello mondiale). Le valutazioni su probabilità, impatto e rischio sono espresse rispetto ad una scala qualitativa a 5 livelli ("Molto Alto", "Alto", "Medio", "Basso", "Molto Basso"). L'aggregazione dei rischi sulle minacce e sugli scenari è stata effettuata secondo la logica del worst case.

Le analisi sono state condotte nel periodo Giugno-Luglio 2016. Per ogni altro dettaglio sulla metodologia si rimanda alla Relazione predisposta dal Servizio IT Risk Management del Consorzio (in allegato).



## **6 Perimetro e granularità dell'analisi del rischio informatico**

L'ambito dell'analisi del rischio informatico comprende:

- 664 asset ICT gestiti dal Consorzio Operativo di Gruppo così come censiti nel proprio inventario APM - Application Portfolio Management.
- 10 asset ICT gestiti direttamente da Banca Widiba, corrispondenti al sistema di Front-end multicanale della Banca.<sup>14</sup>

Sono inclusi anche gli asset ICT gestiti in outsourcing da terzi fornitori del Consorzio o di Widiba.

### **6.1 Perimetro – Analisi Top Level**

L'analisi Top Level permette di indagare il livello di rischio degli asset ICT ad un livello aggregato, corrispondente ai diversi ambiti applicativi e infrastrutturali in cui si articola il sistema informativo.

In particolare, gli indicatori di rischio (KRI) sono stati misurati per gli ambiti corrispondenti alle seguenti entità organizzative:

- 40 Settori del Consorzio che hanno in gestione asset ICT, con riferimento all'insieme degli asset e delle attività di competenza di ogni Settore.<sup>15</sup> Non sono stati considerati:
  - i Settori del Consorzio a cui non sono associati asset ICT o che svolgono mansioni di staff o di tipo gestionale;
  - i Settori del Servizio Sicurezza IT per il quale, come detto, è stata adottata una metodologia di analisi specifica (cfr. paragrafo 5.3).
- la Funzione ICT di Banca Widiba, con riferimento al sistema di Front-end multicanale sviluppato e gestito in autonomia dalla Banca, visto nel suo insieme e considerato come un unico ambito.

---

<sup>14</sup> Le principali componenti del sistema di Front-end di Banca Widiba sono: il sito internet della Banca, il portale dei promotori finanziari, il sistema a supporto delle attività del media center (chiamate inbound/outbound) ed il portale interno a supporto delle attività di post-vendita. Il sistema di Back-End di Banca Widiba è invece gestito dal Consorzio Operativo di Gruppo ed è assimilabile, dal punto di vista dell'analisi del rischio informatico, a quello di Banca MPS.

<sup>15</sup> L'elenco dei Settori oggetto di analisi è contenuto all'interno della Relazione predisposta dal Servizio IT Risk Management del Consorzio (in allegato).

## **6.2 Perimetro – Analisi Low Level**

L'analisi Low Level viene condotta su un perimetro di asset ICT in esercizio selezionati all'inizio di ogni ciclo annuale.

Per quanto riguarda gli asset ICT gestiti dal Consorzio, per il 2016 sono stati selezionati 144 asset su un totale di 664 censiti all'interno dell'inventario APM. Di questi:

- 123 asset sono applicazioni, per le quali il ruolo di Utente Responsabile è esercitato da una specifica Funzione aziendale;
- 21 asset sono classificati come risorse ICT trasversali, per le quali il ruolo di Utente Responsabile è esercitato collegialmente dai partecipanti ad una Commissione costituita presso la Capogruppo (cfr. paragrafo 3).

I 144 asset selezionati costituiscono la prima tranche di un piano triennale di analisi degli asset in produzione gestiti dal Consorzio. In particolare, nella Relazione sul Rischio Informatico relativa all'anno 2015 l'Area Risk Management della Capogruppo e la Direzione Generale del Consorzio hanno concordato l'obiettivo di concludere, nell'arco di un triennio, l'analisi di rischio sugli asset ICT in esercizio.

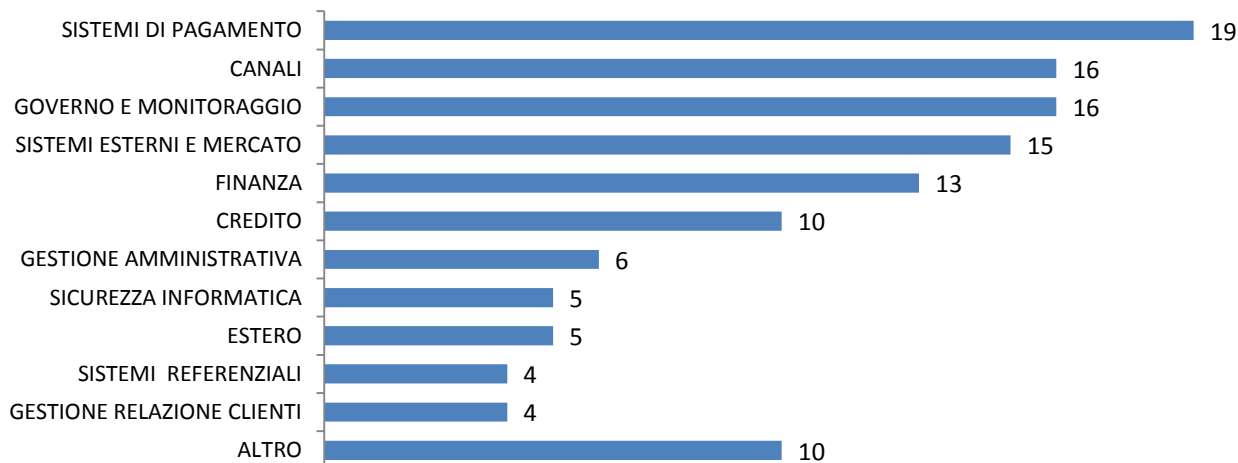
Le applicazioni inserite nel perimetro sono state selezionate incrociando i seguenti due fattori indicativi del loro livello di criticità rispetto al rischio informatico:

1. Innanzitutto, sono state considerate le valutazioni espresse dalle Funzioni di business in merito agli asset ICT che presentano un elevato livello di criticità potenziale:
  - valutazioni di impatto espresse dagli Utenti Responsabili degli asset ICT, a fronte di scenari di compromissione della riservatezza, integrità e disponibilità dei dati gestiti dagli asset;
  - valutazioni sugli asset critici ai fini della business continuity, laddove gli asset supportino uno dei processi individuati come critici nell'ambito del processo di gestione della continuità operativa;
  - analisi di scenario dei Rischi Operativi, laddove gli asset rientrino in uno degli ambiti di business valutati come maggiormente critici dal punto di vista delle perdite potenziali.
2. In seconda battuta, le valutazioni di cui al punto 1. sono state incrociate con una serie di indicatori rivelatori della presenza di anomalie e vulnerabilità sui singoli asset:
  - numero dei gap attivi sull'asset;
  - numero di change in emergenza richiesti per l'asset;
  - somma pesata degli incidenti IT sull'asset;
  - sistema di controllo degli accessi all'asset, centralizzato o meno;
  - esposizione dell'asset su Internet o Extranet.

Da ultimo, il perimetro è stato completato inserendo le applicazioni per le quali gli Organi di Vigilanza hanno richiesto lo svolgimento di analisi specifiche.

Segue la ripartizione delle applicazioni per area funzionale, secondo la tassonomia ABILab.

**Perimetro 2016: ripartizione applicazioni secondo la tassonomia ABILab**



**Figura 5 - Perimetro di analisi 2016: ripartizione applicazioni Consorzio per area funzionale (tassonomia ABILab)**

Le risorse ICT trasversali inserite in perimetro sono state selezionate dal Servizio IT Risk Management del Consorzio in modo da garantire una copertura omogenea delle diverse componenti tecnologiche (tecnologia, sistemi di base, middleware applicativo e tecnologico).

Per quanto riguarda gli asset ICT gestiti da Banca Widiba, l'analisi Low Level ha riguardato tutte le 10 applicazioni e funzionalità applicative che costituiscono il sistema di Front-end della Banca, ivi comprese le componenti gestite da terzi fornitori in outsourcing.

## **7 Risultati dell'analisi del rischio informatico**

Nei paragrafi che seguono si riassumono le evidenze più significative dell'analisi del rischio 2016, rappresentative della situazione del rischio informatico del Gruppo Montepaschi. Per altri dettagli si rimanda alle Relazioni predisposte, rispettivamente, dal Servizio IT Risk Management del Consorzio e dall'Ufficio IT Risk Management di Banca Widiba (in allegato).

### **7.1 Risultati – Analisi Top Level**

L'analisi Top Level, eseguita tramite l'osservazione degli indicatori di rischio (KRI), ha permesso di valutare il livello di rischio dei diversi ambiti applicativi e infrastrutturali in cui si articola il sistema informativo di Gruppo, corrispondenti ai Settori del Consorzio e alla Funzione ICT di Widiba che li hanno in gestione.

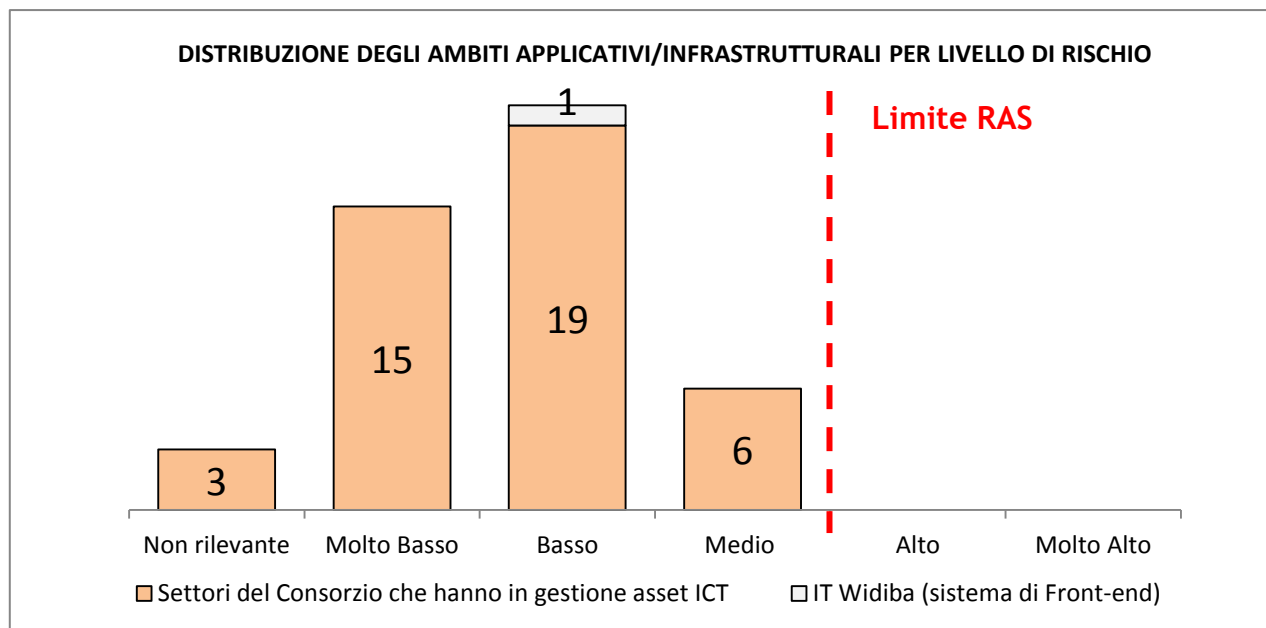


Figura 6 – Distribuzione entità organizzative che gestiscono asset ICT per livello di rischio informatico

#### Consorzio Operativo di Gruppo

L'analisi Top Level non ha evidenziato alcun rischio di livello "Alto" o "Molto alto", eccedente la soglia di propensione stabilita nel RAS di Gruppo.

Vi sono tuttavia alcuni ambiti che presentano un livello di rischio "Medio" e che corrispondono ai seguenti 6 Settori del Consorzio (pari al 15% dei 40 Settori analizzati):

- Settore Pagamenti e Portafoglio;
- Settore Sistemi di Rete;
- Settore Finanza Proprietaria;
- Settore Finanza Titoli Compravendita;
- Settore Risparmio Gestito;
- Settore Anagrafe e Condizioni.

Le anomalie osservate hanno riguardato principalmente: gli incidenti sugli asset ICT, i change in emergenza, le modifiche ai dati eseguite direttamente sui data base in produzione, i progetti in ritardo. Le evidenze fornite dai singoli KRI sono state condivise con i Responsabili dei Settori al fine di inquadrare le motivazioni degli andamenti e condividere le azioni di miglioramento da realizzare, seppure non obbligatorie per il rispetto dei limiti fissati nel RAS.

In generale, si segnala un andamento virtuoso dei Settori nel corso del 2016, con molti dei KRI che presentano un significativo trend discendente rispetto all'anno precedente: batch in errore (-40%), change sui dati in produzione (-48%), change in emergenza (-76%) e progetti in ritardo (-11%). Questo grazie ad una importante iniziativa manageriale, che ha posto come obiettivo la minimizzazione di questi indicatori.

### Banca Widiba

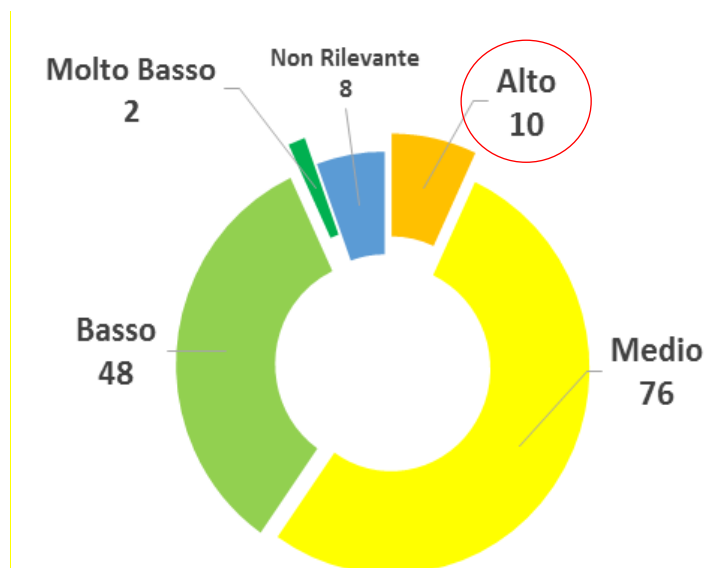
Il rischio relativo al sistema di Front-end multicanale di Banca Widiba è stato valutato complessivamente “Basso”.

Tra i KRI monitorati, solo quello che rileva i Gap aperti dalle Funzioni di controllo ha fatto segnare un livello di rischio “Medio”. In particolare, le sessioni di ethical hacking condotte da una società esterna su richiesta della Funzione Audit di Capogruppo, hanno evidenziato una serie di vulnerabilità rispetto agli attacchi esterni per le quali Banca Widiba ha proceduto allo sviluppo ed all’attivazione delle relative mitigazioni. È previsto che tutte le mitigazioni saranno completate al più tardi entro il 31 marzo 2017.

## **7.2 Risultati – Analisi Low Level**

### Consorzio Operativo di Gruppo

L’analisi Low Level è stata svolta su un perimetro dei 144 asset ICT gestiti dal Consorzio. Segue la ripartizione per livello di rischio emerso dall’analisi:



**Figura 7 – Ripartizione asset ICT gestiti dal Consorzio per livello di rischio informatico (analisi Low Level, perimetro 2016)**

Per 10 asset ICT (il 7% del campione analizzato) il livello di rischio è stato valutato “Alto”, ovvero superiore alla propensione al rischio informatico stabilita dal Gruppo Montepaschi per il 2016. Per uno di questi, l’applicazione APP0000494 - SAG - Swift Alliance Gateway, la valutazione come rischio “Alto” costituisce una proposta, da validare a cura della Commissione risorse ICT trasversali.

Nella tabella che segue, per ognuno degli asset sono evidenziati gli scenari di rischio di livello “Alto” (come combinazione di impatto e probabilità dello scenario, espressi in termini qualitativi secondo la metodologia

descritta al paragrafo 5.2).

ID Asset	Nome Asset	Scenario di rischio	Impatto	Probabilità	Rischio
APP0000415	<b>Esterio Anticipi Valutari</b>	Rischi legati a carenze di expertise o abilità delle risorse IT nel supporto all'operatività dei sistemi	Alto	Alta	Alto
		Rischi legati a blocchi del software a causa di Change gestito non correttamente	Alto	Alta	Alto
APP0000425	<b>Esterio Tesoreria Accentrata</b>	Rischi legati a carenze di expertise o abilità delle risorse IT nel supporto all'operatività dei sistemi	Molto Alto	Alta	Alto
		Rischi legati all'errata esecuzione di operazioni da parte di personale interno	Molto Alto	Media	Alto
		Rischi legati ad anomalie o degrado del software a causa di Change gestito non correttamente	Alto	Alta	Alto
		Rischi legati a blocchi del software a causa di Change gestito non correttamente	Molto Alto	Alta	Alto
		Rischi legati a blocchi del software in produzione	Molto Alto	Media	Alto
APP0000430	<b>Esterio Bonifici</b>	Rischi legati a blocchi del software a causa di Change gestito non correttamente	Molto Alto	Media	Alto
APP0000434	<b>Esterio Rimesse Imp/Exp</b>	Rischi legati a carenze di expertise o abilità delle risorse IT nel supporto all'operatività dei sistemi	Alto	Alta	Alto
		Rischi legati a blocchi del software a causa di Change gestito non correttamente	Alto	Alta	Alto
APP0000435	<b>Esterio Sconto</b>	Rischi legati a carenze di expertise o abilità delle risorse IT nel supporto all'operatività dei sistemi	Alto	Alta	Alto
APP0000872	<b>Nodo CBI (*)</b>	Rischi legati a blocchi del software a causa di Change gestito non correttamente	Alto	Alta	Alto
APP0000465	<b>CBI (*)</b>	Rischi legati a blocchi del software a causa di Change gestito non correttamente	Alto	Alta	Alto
APP0000920	<b>Gari Gold TFM</b>	Rischi legati ad accesso indebito o divulgazione delle informazioni	Molto Alto	Media	Alto
APP0000526	<b>AOG - Anagrafe Operativa Gruppo</b>	Rischi legati a malware ed attacchi logici	Molto Alto	Alta	Alto
Proposta di valutazione rischio "Alto" da validare a cura della Commissione risorse ICT trasversali					
APP0000494	<b>SAG - Swift Alliance Gateway</b>	Rischi legati ad accesso indebito o divulgazione delle informazioni	Molto Alto	Alta	Alto
		Rischi legati a malware e attacchi logici	Molto Alto	Media	Alto

(\*) Nel corso dell'analisi è emerso che le applicazioni APP0000872 - Nodo CBI e APP0000465 - CBI individuano le medesime funzionalità, seppure censite separatamente all'interno dell'inventario APM del Consorzio.

**Tabella 6 – Asset ICT gestiti dal Consorzio con livello di rischio "Alto"**

Le raccomandazioni sono state presentate agli Utenti Responsabili degli asset e le relative azioni di mitigazione sono state concordate e pianificate con il COG (cfr. paragrafo 8).

Al 31/12/2016, oltre ai predetti 10 asset ICT con rischio “Alto” individuati nel corso del 2016, ne rimanevano altri 3 con rischio “Alto” individuati a fine 2015, le cui mitigazioni sono in fase di realizzazione.

#### Banca Widiba

Per quanto riguarda le 10 applicazioni e funzionalità applicative che costituiscono il sistema di Front-end di Banca Widiba, non sono stati rilevati rischi di livello “Alto” o “Molto Alto”.

Per 6 dei 10 asset ICT di Widiba, l’analisi Low Level ha evidenziato la presenza di alcuni rischi con livello massimo pari a “Medio”. Caratteristica comune è l’esistenza di rischi dovuti a cancellazione/modifica dei dati, sia per eventi incidentali, sia con scopi malevoli. La mitigazione di questi rischi è affidata a soluzioni di back-up dei dati, segregazione della rete e tracciatura delle operazioni nel rispetto delle prescrizioni normative.

#### *7.2.1 Analisi Low Level sui sistemi di pagamento via internet*

Con il 16° aggiornamento della Circolare Banca d’Italia n. 285/2013, datato 17 maggio 2016, sono stati recepiti nell’ordinamento italiano gli “Orientamenti in materia di sicurezza dei pagamenti tramite internet” emanati dall’Autorità Bancaria Europea (European Banking Authority – EBA).

Le nuove disposizioni sono diventate obbligatorie per le Banche dal 30 settembre 2016 e si applicano ai seguenti servizi di pagamento via internet:

- Esecuzione dei pagamenti con carta.
- Esecuzione di bonifici.
- Emissione o modifica di mandati elettronici di addebito diretto.
- Trasferimento di moneta elettronica tra due conti di moneta elettronica.

Per tenere conto delle nuove disposizioni è stata definita un’ulteriore check-list di controlli specifici, da utilizzare per l’analisi Low Level dei sistemi di pagamento via internet.

Tra i 144 asset del Consorzio del perimetro 2016, 6 ricadono nell’ambito dei sistemi di pagamento via internet.<sup>16</sup> Per nessuno di essi sono stati rilevati rischi di livello “Alto” o “Molto Alto”.

Per l’asset APP0000947 - CBI - Paskey Aziende Online è stato identificato un rischio “Medio” sullo Scenario 16 - Rischi legati a malware e attacchi logici, a causa della mancanza di misure di strong authentication della clientela per l’autorizzazione delle operazioni dispositive. Il rischio è stato accettato dall’Utente Responsabile in considerazione del fatto che la strong authentication sarà implementata entro fine aprile 2017 e che, nel frattempo, il team antifrode COG ha rafforzato il monitoraggio delle operazioni sospette.

---

<sup>16</sup> APP0000823 - Internet Banking, APP0000874 - E-Commerce, APP0000921 - Tesoweb Enti Online, APP0000946 - Large Corporate Banking, APP0000947 - CBI - Paskey Aziende Online, APP0001064 - Tribunali Online.

### **7.3 Risultati – Analisi della Sicurezza Informatica**

L'analisi del rischio sulla Sicurezza informatica del Consorzio, condotta tra giugno e luglio 2016 con il supporto metodologico della società di consulenza Deloitte ERS (cfr. paragrafo 5.3), ha evidenziato rischi di livello "Alto" riconducibili allo scenario "Attacchi logici" (in particolare su hacking e minacce sociali rivolte agli utenti) e allo scenario "Utilizzo improprio e/o errori" (con particolare riferimento agli errori effettuati da utenti e personale tecnico e ai malfunzionamenti derivanti da carenze nei processi di progettazione, sviluppo, teste e change).

Per la mitigazione dei rischi rilevati, a settembre 2016 è stato definito un piano di interventi di breve termine, integrativo rispetto a quello formalizzato a inizio 2016, denominato "Monte più Sicuro" (cfr. paragrafo 8). Queste ulteriori azioni di mitigazione, insieme agli interventi in corso nell'ambito del progetto "Monte più Sicuro" (completamento previsto entro maggio 2017), permettono di consolidare il rischio sulla Sicurezza Informatica ad un livello "Medio". Tutte le attività previste per il 2016 sono state svolte.

Gli altri due scenari "Incidenti di sicurezza fisica" e "Interruzione del business" sono stati valutati per completezza ma non sono stati oggetto di approfondimento specifico, in quanto hanno rivelato solo alcuni rischi di livello "Medio".

## **8 Piano di mitigazione del rischio informatico**

Nei casi in cui le analisi condotte evidenzino rischi superiori alla soglia di propensione definita nel Risk Appetite Statement (RAS), il Servizio Rischi Operativi e Reputazionali ha segnalato il relativo gap al fine di sollecitare e monitorare la realizzazione degli interventi di mitigazione c.d. "obbligatori".<sup>17</sup>

Alla fine del 2016, il piano di mitigazione dei rischi informatici comprendeva 8 interventi con scadenze previste fino a luglio 2017. Di questi:









- 1 intervento riguarda l'attuazione del progetto "Monte Più Sicuro" per il rafforzamento dei processi e presidi di sicurezza logica del Consorzio;
- gli altri 7 interventi si riferiscono alla mitigazione di rischi "Alti" rilevati su 12 asset ICT gestiti dal Consorzio, di cui 3 individuati a fine 2015 e 9 nel corso del ciclo di analisi 2016.

Su riepilogano di seguito gli interventi in parola, con evidenza dei contenuti della mitigazione, della scadenza di realizzazione prevista, dello stato avanzamento al 31/12/2016 e delle Funzioni owner e contributor.

---

<sup>17</sup> Secondo modi e tempi indicati dai documenti normativi 1030D1822 - Policy in materia di gestione dei GAP segnalati dalle Funzioni con compiti di Controllo e 1030D1959 - Gestione dei GAP segnalati dalle Funzioni di Controllo.



Asset/processo ICT	Nr. Asset (anno analisi)	Mitigazione	Scadenza	SAL 31/12/2016	Owner	Contributor
PEF - Pratica Elettronica di Fido	1 (fine 2015)	Gestione profili abilitativi: integrazione autonomie deliberative con ruoli PaschiPeople (gap IA_2016_00020)	31/01/2017 Q1 Q2 Q3 Q4	 (COMPLETATO)	COG - Servizio Credito	BMPS - Servizio Credit Services
CBI - Corporate Banking Interbancario (gestione flussi CBI)	2 (2016)	Gestione dei change: integrazione nel tool standard distribuzione automatica software	28/02/2017 Q1 Q2 Q3 Q4	 (COMPLETATO)	BMPS - Servizio Prodotti Corporate	COG - Servizio Incassi e Pagamenti
CAI - Centrale Allarmi Interbancaria (segnalazioni allarmi su assegni/carte)	1 (fine 2015)	Livelli di servizio: adozione strumenti di monitoraggio corretto funzionamento (gap RM_2016_00010)	31/03/2017 Q1 Q2 Q3 Q4		BMPS - Servizio Finanziamenti e Prodotti Transazionali Retail	COG - Servizio Multicanalità Clienti Interni
Anagrafe Operativa Gruppo	1 (2016)	Gestione profili abilitativi: integrazione trx NCHI con sistema controllo accessi (gap RM_2016_00013)	31/03/2017 Q1 Q2 Q3 Q4		BMPS - Servizio Anagrafe Generale e Indagini	COG - Settore Anagrafe e Condizioni
Applicazioni estero domestico (5 applicazioni: anticipi, tesoreria, bonifici, rimesse imp/exp, estero sconto)	5 (2016)	Obsolescenza applicativa: studio fattibilità sostituzione con soluzione di mercato e/o incorporazione funzionalità in settoriali Italia (gap RM_2017_00001)	31/03/2017 Q1 Q2 Q3 Q4		BMPS - Staff Supporto Operatività Rete Estera	COG - Servizio Sistemi Referenziali
Gestione processi operativi e presidi di sicurezza logica del Consorzio	n.s.	Sicurezza logica: iniziative progetto «Monte Più Sicuro» (gap RM_2016_00008)	31/05/2017 Q1 Q2 Q3 Q4		COG - Servizio Sicurezza IT	
Gari Gold TFM (gestione della messaggistica finanziaria su rete SwiftNET)	1 (2016)	Gestione profili abilitativi: bonifica utenze, sostituzione con asset «Messaggistica Finanziaria SWIFT» già integrato con controllo accessi (gap RM_2016_00012)	30/06/2017 Q1 Q2 Q3 Q4		BMPS - Servizio Liquidità Operativa	COG - Servizio Incassi e Pagamenti
CLM - Channel e Liquidity Management (gestione accentrata della liquidità della Banca)	1 (fine 2015)	Gestione profili abilitativi: bonifica utenze e attribuzione profili in base al ruolo, accentramento su Funzione Gestione Utenti (gap RM_2016_00011)	31/07/2017 Q1 Q2 Q3 Q4		BMPS - Servizio Liquidità Operativa	COG - Servizio Finanza COG - Servizio Sicurezza IT

**Figura 8 – Piano di iniziative per la mitigazione dei rischi informatici**

Per completezza, si riporta la dinamica registrata nel corso del 2016 nel numero di asset ICT con rischi sopra la soglia RAS, indirizzati dal piano di mitigazioni:

	2016			
	Q1	Q2	Q3	Q4
N. asset ICT con rischi valutati di livello "Alto" o "Molto Alto" (stock a fine periodo)	2	4	4	12

Si precisa che nei report di monitoraggio del RAS il numero riportato di asset ICT sopra soglia a fine 2016 è pari ad 11, in considerazione del fatto che 2 applicazioni, APP0000872 - Nodo CBI e APP0000465 - CBI, individuano le medesime funzionalità, censite due volte nell'inventario APM del Consorzio. Pertanto, a fine 2016 gli asset ICT con rischi sopra soglia risultavano formalmente 12, ma sostanzialmente 11.

Tra gli asset non è stata conteggiata l'applicazione APP0000494 SAG - Swift Alliance Gateway, la cui valutazione di rischio "Alto" (cfr. paragrafo 7.2) rappresenta una proposta che deve essere validata dalla neo-costituita Commissione risorse ICT trasversali. L'applicazione costituisce l'interfaccia per l'invio dei messaggi verso la rete interbancaria SwiftNET ed è stata oggetto, nel corso del 2016, di diversi casi di frode ai danni di banche a livello internazionale. Le azioni di mitigazione, anche in assenza di conferma da parte dell'Utente Responsabile, sono state comunque avviate d'iniziativa da parte del Consorzio Operativo di Gruppo. La data di completamento attesa, per l'ultima delle azioni di mitigazione, è Dicembre 2017.

Con riferimento alla mitigazione dei rischi sulla Sicurezza informatica del Consorzio, a settembre 2016 è

stato definito un piano di azione di breve termine, integrativo rispetto a quello formalizzato a inizio 2016 e denominato "Monte più Sicuro". Tutte le attività previste per il 2016 sono state svolte.

Di seguito si elencano i filoni di intervento indirizzati dal piano integrativo, rimandando per il dettaglio alla Relazione predisposta dal Servizio IT Risk Management del Consorzio (in allegato):

- Protezione informazioni confidenziali (documenti CdA, utenze privilegiate, dati non strutturati).
- Monitoraggio delle minacce e gestione degli incidenti di sicurezza (processo, reportistica).
- Mitigazione vulnerabilità e minacce (sviluppo del software, protezione reti interne).
- Security awareness e training (dedicate al personale tecnico).
- Sicurezza delle terze parti (classificazione e monitoraggio fornitori secondo parametri sicurezza).
- Organizzazione della sicurezza (revisione impianto normativo e organizzazione).
- Policy e normative (classificazione criticità asset, dispositivi mobili, dispositivi removibili).

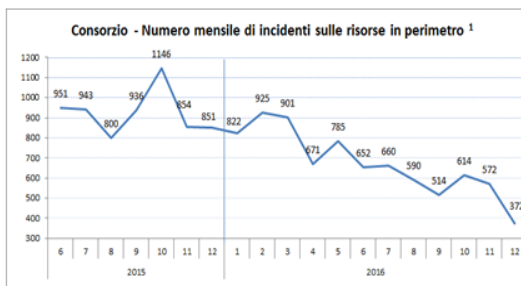
## 9 Monitoraggio dei key risk indicator inseriti nel RAS

I KRI inseriti nel RAS per il 2016 hanno consentito di monitorare l'evoluzione della situazione del rischio informatico nei seguenti ambiti:

- Incidenti sulle risorse informatiche
- Frodi ai danni della clientela internet banking

### Incidenti sulle risorse informatiche

✓ Il numero mensile di incidenti IT sulle risorse gestite dal Consorzio è risultato in costante diminuzione nel corso del 2016 e si colloca oggi su livelli inferiori alle soglie di attenzione definite nel RAF.



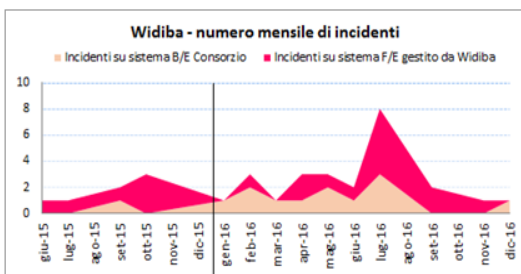
N. risorse con incidenza mensile sopra la soglia di attenzione definita dal RAF <sup>2</sup>

- applicazioni critiche per la business continuity  
- altre applicazioni  
- rete TLC

N. major incident

2016			
Q1	Q2	Q3	Q4
2	-	-	-
1	-	-	-
-	-	-	-
1	2	2	3

✓ Nel corso del 2016, il numero mensile di incidenti IT su Widiba è rimasto su ordini di grandezza comunque contenuti.



N. incidenti con impatto "Alto" <sup>3</sup>

di cui:

- su sistema B/E gestito dal Consorzio  
- su sistema F/E gestito da Widiba

2016			
Q1	Q2	Q3	Q4
3	3	3	2
3	1	1	1
-	2	2	1

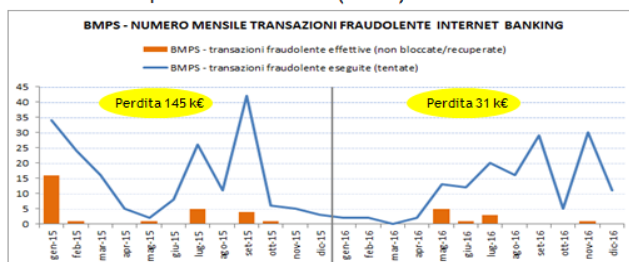
1. Sono esclusi gli incidenti relativi all'informatica periferica (pdf, laptop, stampanti, scanner, server, telefonia, ...).

2. Le soglie di attenzione sono definite in termini di numero incidenti mensili e sono differenziate per tipologia di risorsa informatica: 10 incidenti mensili per le applicazioni critiche ai fini della business continuity, 30 per le altre applicazioni e 200 per la rete TLC.

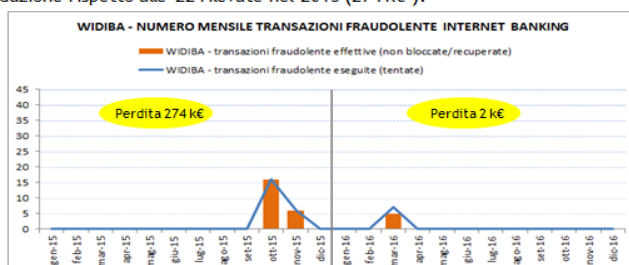
3. Incidenti con impatto "Alto" sulla clientela di Widiba, classificati da Widiba sulla base del numero di segnalazioni ricevute, delle funzionalità coinvolte e della durata del disservizio. I criteri di valutazione differiscono da quelli adottati dal COG per la classificazione dei "major incident".

## Frodi ai danni della clientela internet banking

- ✓ Nel corso del 2016, in BMPS si è ridotto il numero complessivo di tentativi di frode a danno della clientela internet banking (-22% rispetto al 2015). Tale dinamica positiva ha interessato la clientela retail, mentre per il corporate i tentativi di frode sono sensibilmente aumentati (+44% in numero e +400% in volume transato). Grazie anche alle misure antifrode messe in campo, le transazioni fraudolente «effettive» (non bloccate ex ante o recuperate ex post), sono state solo 10 (per una perdita di 31 k€), in ulteriore riduzione rispetto alle 28 del 2015 (145 k€).

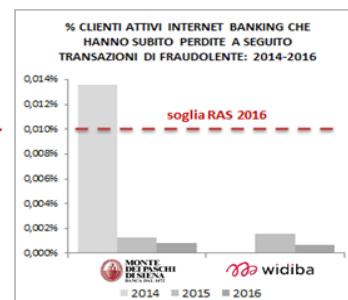


- ✓ Nel corso del 2016, in WIDIBA le transazioni fraudolente che hanno prodotto una perdita per la clientela sono state 5 (2 k€), in riduzione rispetto alle 22 rilevate nel 2015 (274 k€<sup>1</sup>).



1. Relativamente al cliente che ha subito la perdita maggiore (268 k€), WIDIBA ha sporto denuncia alla Polizia Postale per tentativo di truffa ai propri danni.

- ✓ Per entrambe le Banche l'incidenza del fenomeno è risultata significativamente inferiore alla soglia di attenzione definita nel RAS



## 10 Piano di attività per il 2017

Il CdA del 25 febbraio 2016 ha approvato l'obiettivo di concludere, nell'arco di un triennio, l'analisi di rischio sugli asset ICT in esercizio gestiti da Consorzio Operativo di Gruppo.

La prima tranche di 144 asset è stata completata durante il ciclo di analisi 2016.

La selezione della seconda tranche di asset da analizzare nel 2017 sarà effettuata in linea con le nuove guidelines poste da EBA ai fini dello SREP (Supervisory Review and Evaluation Process), attualmente in fase di consultazione, con particolare riferimento all'individuazione dei *material ICT risks that can have a significant prudential impact on the institution's critical ICT systems and services*.<sup>18</sup>

Seguono gli altri, principali filoni di attività programmati per il 2017:

- Consolidamento dell'attività di analisi del rischio sui progetti di sviluppo, modifica rilevante o outsourcing degli asset ICT, nell'ottica di garantire il presidio sui major change che possono

<sup>18</sup> Documento EBA/CP/2016/14 del 6 ottobre 2016: Guidelines on ICT Risk Assessment under the Supervisory Review and Evaluation process (SREP). Consultation Paper.

influenzare il complessivo livello di rischio informatico del Gruppo; formalizzazione della normativa di dettaglio sul processo ed adeguamento delle altre normative impattate (ad esempio, demand management IT).

- Adeguamento della metodologia, dei controlli e del processo di gestione del rischio informatico alle nuove guidelines poste dall'EBA ai fini dello SREP, attualmente in fase di consultazione.
- Presidio sullo stato di avanzamento del piano di mitigazione dei rischi e monitoraggio degli indicatori di rischio.

## **11 Conclusioni**

La presente Relazione costituisce l'informativa annuale agli Organi apicali della Capogruppo in merito alla situazione del rischio informatico del Gruppo Montepaschi, valutata in base al quadro organizzativo e metodologico definiti dalla Direttiva 1030D02045 e in coerenza con le disposizioni della Circolare Banca d'Italia 285/2013.

L'analisi di rischio Top Level, basata su Key Risk Indicator, non ha evidenziato, sul piano complessivo, livelli di rischio superiori alla soglia di propensione definita nel RAS - Risk Appetite Statement.

In particolare, il livello di rischio degli ambiti applicativi e infrastrutturali gestiti dai Settori del Consorzio è stato valutato in grande prevalenza come "Basso" o "Molto Basso". E così pure è stata valutata "Bassa" la rischiosità complessiva del sistema di Front-end multicanale gestito da Banca Widiba.

Le analisi condotte hanno evidenziato comunque la presenza di alcune aree di attenzione che richiedono la focalizzazione del management della Funzione ICT e uno stretto presidio da parte delle Funzioni di controllo e gestione del rischio informatico:

- Per il 15% degli ambiti applicativi e infrastrutturali gestiti da Settori del Consorzio, il livello di rischio è stato valutato "Medio", segnalando l'opportunità per il management di intervenire per correggere le situazioni di anomalia evidenziate dai Key Risk Indicator.
- Per il 7% degli asset ICT del Consorzio inseriti nel perimetro di analisi del 2016 (10 su 144), il livello di rischio prospettico, valutato attraverso l'analisi Low Level, è risultato "Alto" ed ha richiesto l'attivazione di specifiche iniziative di mitigazione. Al 31/12/2016, oltre ai predetti 10 asset ICT con rischio "Alto" individuati nel corso del 2016, ne rimanevano altri 3 con rischio "Alto" individuati a fine 2015, le cui mitigazioni sono in fase di realizzazione.
- La Sicurezza informatica rimane un ambito di particolare attenzione, in ragione dell'evoluzione continua delle minacce e della scoperta di nuove vulnerabilità tecnologiche e per la presenza di gap strutturali, emersi nella precedente Relazione sul Rischio Informatico relativa al 2015. Per riportare il rischio su un livello "Medio", il Consorzio Operativo di Gruppo ha definito, a settembre 2016, un ulteriore piano di interventi di breve termine, integrativo rispetto a quello formalizzato a inizio 2016 e denominato "Monte più Sicuro". Tutte le attività previste per il 2016 sono state svolte.

- La Sicurezza informatica costituisce l'area di maggior attenzione anche per Banca Widiba: le sessioni di ethical hacking e l'analisi del rischio sulle singole componenti del sistema di Front-end hanno infatti rilevato la presenza di rischi di livello "Medio", riconducibili a vulnerabilità rispetto agli scenari di attacco esterno e di accesso indebito. Le mitigazioni delle vulnerabilità individuate attraverso l'attività di ethical haking saranno completate al più tardi entro il 31 marzo 2017. Per il 2017 sono state pianificate iniziative progettuali di potenziamento delle misure antifrode e dei monitoraggi di sicurezza, nonché lo svolgimento di nuove sessioni di penetration test e vulnerability assessment.

Le Funzioni di controllo e gestione del rischio informatico continueranno a garantire il presidio sullo stato di avanzamento del piano di mitigazione dei rischi ed il monitoraggio degli indicatori di rischio, finalizzato ad intercettare tempestivamente nuovi segnali di deterioramento (early warning), da approfondire e indirizzare prima che il rischio si manifesti in un impatto negativo per il Gruppo.

A completamento, nel corso del 2017 saranno attuate una serie di iniziative per il rafforzamento del modello di gestione del rischio informatico, finalizzate principalmente a consolidare il presidio sui major change e garantire l'allineamento alle nuove guidelines EBA in materia di SREP (Supervisory Review and Evaluation Process), attualmente in fase di consultazione.

## **Allegati**

- Relazione sul Rischio Informatico del Consorzio Operativo di Gruppo – Anno 2016
- Relazione sul Rischio Informatico di Banca Widiba – Anno 2016



## Relazione annuale Rischio Informatico

### Consorzio Operativo Gruppo Montepaschi – Anno 2016

<b>PREPARATO DA:</b>		SERVIZIO IT RISK MANAGEMENT Consorzio Operativo Gruppo Montepaschi
<b>DATA PREPARAZIONE:</b>		29 Dicembre 2016

<b>VERIFICATO DA:</b>		
<b>DATA VERIFICA:</b>		

<b>APPROVATO DA:</b>		Comitato dei Consorziati
<b>DATA APPROVAZIONE:</b>		07/03/2017

#### REGISTRO DELLE MODIFICHE

N° Versione	Descrizione	Data Approvazione
0.1	PRIMA STESURA	
0.6	REVISIONE ITRM	
1.1	Versione finale	

#### RIFERIMENTI

Riferimento	Titolo	Codice Risorsa

## Sommario

<b>1</b>	<b>PREMESSA.....</b>	<b>3</b>
<b>2</b>	<b>OBIETTIVI DEL DOCUMENTO E DESTINATARI .....</b>	<b>4</b>
<b>3</b>	<b>EXECUTIVE SUMMARY: PRINCIPALI RISULTANZE.....</b>	<b>5</b>
3.1	ANALISI TOP LEVEL.....	5
3.2	ANALISI LOW LEVEL .....	8
3.3	ANALISI SICUREZZA INFORMATICA.....	10
3.4	RISULTATI COMPLESSIVI DELL'ANALISI.....	11
<b>4</b>	<b>RUOLI E RESPONSABILITÀ .....</b>	<b>13</b>
<b>5</b>	<b>PERIMETRO DI ANALISI .....</b>	<b>16</b>
5.1.1	<i>Cenni metodologici – Analisi Top Level.....</i>	<i>19</i>
5.1.2	<i>Cenni metodologici – Analisi Low Level.....</i>	<i>19</i>
<b>6</b>	<b>ANALISI DEL RISCHIO .....</b>	<b>21</b>
6.1	ANALISI TOP LEVEL.....	22
6.1.1	<i>Modalità di analisi.....</i>	<i>22</i>
6.1.2	<i>Periodo di osservazione e fonti di alimentazione .....</i>	<i>24</i>
6.1.3	<i>Scale e razionali .....</i>	<i>25</i>
6.1.4	<i>Risultati.....</i>	<i>28</i>
6.2	ASSESSMENT LOW LEVEL .....	29
6.2.1	<i>Modalità di analisi.....</i>	<i>29</i>
6.2.2	<i>Risultati.....</i>	<i>30</i>
6.2.3	<i>Risultati complessivi.....</i>	<i>31</i>
6.2.4	<i>Analisi sui Sistemi di pagamento via Internet.....</i>	<i>33</i>
6.3	ASSESSMENT SICUREZZA IT .....	34
6.3.1	<i>Metodologia .....</i>	<i>34</i>
6.3.2	<i>Modalità di conduzione dell'analisi .....</i>	<i>36</i>
6.3.3	<i>Risultati relativi al Servizio Sicurezza IT.....</i>	<i>37</i>
6.4	RACCOMANDAZIONI E CONCLUSIONI .....	39
6.4.1	<i>IT Risk Top Level.....</i>	<i>40</i>
6.4.2	<i>IT Risk Low Level .....</i>	<i>42</i>
6.4.3	<i>Sicurezza IT .....</i>	<i>42</i>



## 1 Premessa

Il sistema informativo rappresenta uno strumento fondamentale per il conseguimento degli obiettivi strategici e operativi delle Banche, in considerazione del valore delle informazioni gestite e della criticità dei processi aziendali che dipendono da esso. Per tale motivo, Banca d'Italia ha ritenuto necessario emanare una disciplina organica in materia di sviluppo e gestione del Sistema informativo, esposta all'interno del Titolo IV, Capitolo 4, 16° Aggiornamento del 16 Maggio 2016 della Circolare 285/2013.

Tra i dettami emanati vi è l'adozione di un modello organizzativo e di un processo strutturato per la gestione del rischio informatico, finalizzato ad identificare, valutare, trattare, documentare e monitorare i rischi connessi all'utilizzo delle tecnologie informatiche. E' infatti richiesto che siano forniti agli Organi Decisionali e alle Funzioni aziendali preposte, gli elementi di giudizio necessari per il governo del rischio informatico, coerentemente con i principi, le politiche e le linee guida adottate per la determinazione della propensione al rischio a livello di Gruppo (Risk Appetite Framework, RAF).

Nel corso del 2016, il Gruppo Montepaschi (di seguito anche il "Gruppo MPS" o "Gruppo") ha avviato un progetto di affinamento della metodologia di IT Risk Management, basata su *best practice* di mercato, al fine di rendere l'analisi e la gestione del rischio informatico maggiormente strutturata e atta a garantire miglior organicità delle rilevazioni sul sistema informativo aziendale, nel rispetto dei dettami normativi.

L'impostazione metodologica è definita dalla Direttiva di Gruppo in materia di Gestione del Rischio Informatico (documento 1030D02045) e prevede la conduzione in parallelo di due tipologie di analisi:

- Un'analisi di alto livello (di seguito "Top Level") al fine di rappresentare la situazione di rischio complessiva dell'ICT. Gli elementi su cui si basano le osservazioni sono i Key Risk Indicator (KRI – indicatori di rischio), ovvero metriche che misurano nel continuo una serie di eventi tecnologici e di processo, raffrontati su scale di misurazione definite a livello di Gruppo.
- Un'analisi di dettaglio (di seguito "Low Level") sugli asset ICT (risorse informatiche: applicazioni e infrastrutture) definiti in perimetro di analisi per l'anno 2016, sulla base del catalogo dei rischi del Gruppo MPS.

Le risultanze della prima analisi di alto livello condotta dal Servizio IT Risk Management (di seguito "ITRM") del Consorzio Operativo Gruppo Montepaschi (di seguito anche "Consorzio" o "COG") sono aggregate e rappresentate per Unità Organizzativa (Settore) del Consorzio, al fine di rappresentare agli Organi decisionali e alle Funzioni aziendali preposte la situazione del rischio informatico per le risorse informatiche gestite. I risultati dell'analisi di dettaglio sono, invece, rappresentate per singolo asset ICT.

Al fine di unire le due tipologie di analisi sopra descritte, per ogni Settore del Consorzio, è rappresentata anche la distribuzione dei rischi rilevati sugli asset di propria competenza.

Inoltre, a seguito delle risultanze della Relazione 2015, le quali hanno evidenziato un livello di rischio "Alto" in ambito Sicurezza Informatica, in un'ottica di gestione del rischio informatico e di valutazione e monitoraggio dello stato avanzamento delle azioni di mitigazione concordate, nell'anno 2016 è stata condotta dal Servizio ITRM, un'analisi specifica sulla Sicurezza Informatica, i cui risultati sono descritti nel presente documento. Tale analisi è stata condotta con il supporto metodologico di una società di consulenza esterna, la quale ha partecipato anche alla conduzione degli assessment.

## 2 Obiettivi del documento e destinatari

La presente relazione descrive i risultati ottenuti dall'analisi dei rischi ed è volta a fornire agli Organi Aziendali preposti la rappresentazione della situazione di rischio informatico come previsto dalla Circolare 285 di Banca d'Italia.

Pertanto, i destinatari del presente documento sono:

- *l'Organo con Funzione di Supervisione Strategica*: informato con cadenza almeno annuale sulla situazione di rischio informatico rispetto alla propensione al rischio;
- *l'Organo con Funzione di Gestione*: approva, con cadenza almeno annuale, la valutazione del rischio delle componenti critiche; in tale ambito, riscontra il rapporto sulla situazione complessiva del rischio informatico, con particolare riferimento al livello di rischio residuo per le diverse risorse informatiche, allo stato di implementazione delle misure di mitigazione, nonché alle minacce ed agli incidenti registratisi nel periodo di riferimento. Approva l'adozione di misure alternative o ulteriori di trattamento del rischio, qualora il rischio residuo valutato per una risorsa informatica ecceda la propensione al rischio definita;
- *la Direzione Generale del Consorzio*: approva i risultati di rischio informatico e le eventuali misure di mitigazione proposte sotto forma di raccomandazioni;
- *il Servizio Rischi Operativi e Reputazionali di Capogruppo*: responsabile dello svolgimento dei compiti di controllo di secondo livello del rischio informatico.

Il documento è strutturato nelle seguenti sezioni:

- *Premessa*: introduzione al documento e overview delle attività svolte;
- *Obiettivo del documento e destinatari*: scopo della presente relazione e organi destinatari del documento;
- *Executive Summary*: descrizione delle principali risultanze e raccomandazioni;
- *Ruoli e Responsabilità*: descrizione degli attori coinvolti, dei compiti e delle responsabilità previste;
- *Perimetro di analisi*: ambito di applicabilità dell'analisi e oggetti della valutazione;
- *Il rischio informatico*: definizione di rischio informatico, aspetti metodologici e modalità di conduzione dell'analisi;
- *Valutazione Top Level*: metodologia utilizzata per l'analisi di alto livello, descrizione degli indicatori di rischio, modalità di assessment e rappresentazione dei risultati aggregati per Settore del Consorzio;
- *Valutazione Low Level*: risultati delle analisi di dettaglio condotte sui singoli Asset ICT in perimetro;
- *Rischio Sicurezza Informatica*: focus sulla Sicurezza Informatica concernente la metodologia utilizzata per la conduzione delle analisi, le modalità di raccolta dei dati e la descrizione delle risultanze;
- *Conclusioni*: osservazioni finali, raccomandazioni generali, principali mitigazioni individuate e prossimi passi concordati.
- *Allegati*: documenti a supporto dell'analisi ed evidenze emerse.

### 3 Executive Summary: principali risultanze

#### 3.1 *Analisi Top Level*

L'analisi Top Level consiste nella rilevazione e nella registrazione di eventi occorsi nel periodo in esame e che vanno ad alimentare gli indicatori di rischio (KRI – Key Risk Indicator). Pertanto questa tipologia di valutazione è tipo retrospettivo, ovvero rappresenta l'andamento del Consorzio Operativo di Gruppo nell'ultimo anno passato, secondo le dimensioni di analisi definite.

La valutazione Top Level è stata eseguita sui Settori del Consorzio che hanno in gestione asset ICT (applicazioni e infrastrutture IT), per un totale di 40 Settori. Non sono stati, pertanto, considerati i Settori a cui non sono associati asset o che svolgono mansioni di staff o di tipo gestionale, che sono:

- Settore Antiriciclaggio e Controlli di Conformità
- Settore Compliance
- Settore Gestione Ciclo Passivo
- Settore Organizzazione
- Settore Pianificazione Spesa e Progetti
- Settore Risorse Umane
- Settore Segreteria e Comunicazione Interna
- Settore Innovazione e Prototipazione
- Settore Supporto Utenti
- Settore Monitoraggio Performance IT
- Settore Architettura Reti e Informatica Utente
- Settore Privacy e Business Continuity

Inoltre, pur avendo degli asset in carico, non sono stati valutati tramite gli indicatori Top Level anche i due Settori del servizio Sicurezza IT, per i quali è stata effettuata una valutazione specifica a livello di Servizio (cfr. par. 3.3). Si tratta di:

- Settore Ingegneria di Sicurezza
- Settore Monitoraggio della Sicurezza IT

Per la valutazione Top Level del rischio informatico sono stati utilizzati i seguenti *Key Risk Indicator* (KRI) rilevati a livello di asset e/o per Settore del Consorzio:

1. Percentuale di **BR<sup>19</sup> conclusi in ritardo** rispetto al totale dei rilasciati nel periodo in esame (per Settore) con motivazione «IT» e «Mista», pesati in base alla tipologia (Progetti di Piano Esecutivo, Rilevanti, Altri, Running);
2. Somma pesata dei **rilevi attivi** per Settore, emessi dalle Funzioni di Controllo su asset IT alla data della rilevazione e censiti su RIGAM; sono considerati anche i rilievi ISAE e BCE/JST, anche se non censiti su RIGAM;
3. Numero di **RFC<sup>20</sup> in emergenza** richiesti dal Settore, rispetto al numero degli asset ad esso afferenti, nel periodo in esame;
4. Somma pesata per priorità e per tempo di risoluzione degli **incidenti IT** sugli asset del Settore rispetto al numero degli asset ad esso afferenti;
5. Numero medio di **job batch** schedulati andati in errore nel periodo in esame (terminati in abend) per asset gestiti dal Settore;
6. Numero di applicazioni (asset per Settore) non collegate al **controllo accessi** centralizzato e/o privi di sistema SSO<sup>21</sup>;
7. Numero di **Change eseguiti sui dati** in produzione (transazione GADIS).

La misurazione degli indicatori elencati ha fornito la seguente distribuzione dei Settori del Consorzio per livello di rischio:

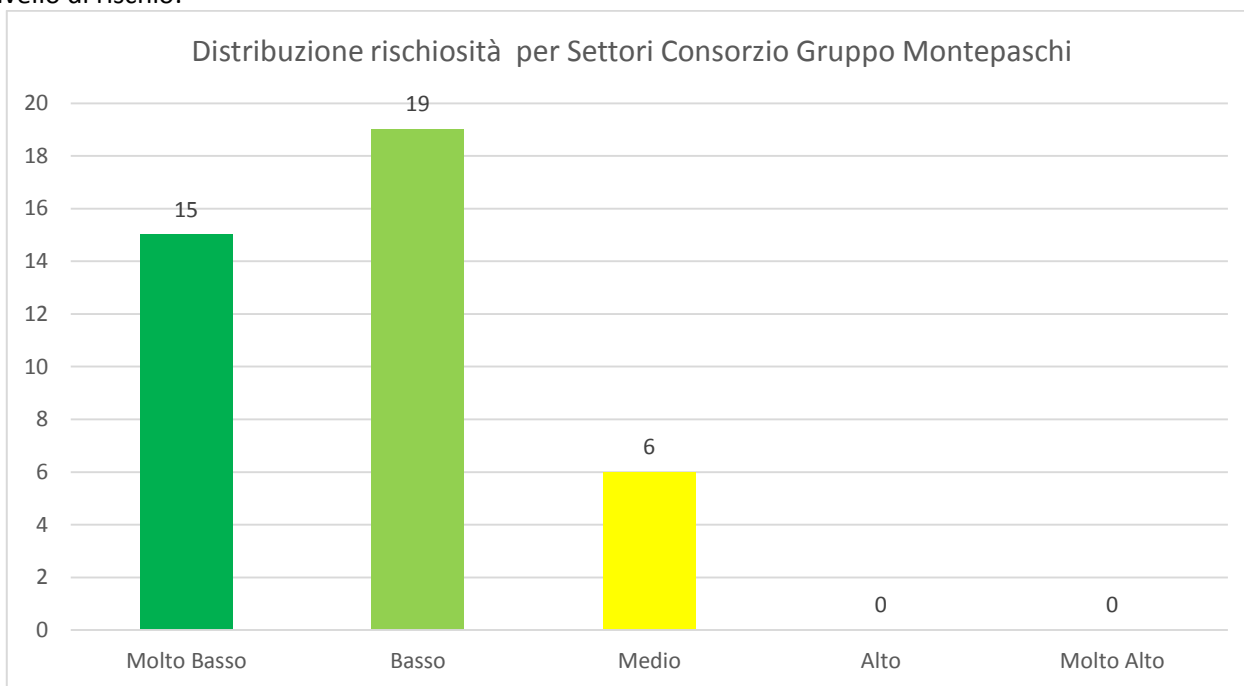


Figura 9: Distribuzione risultati di rischio

I Settori che presentano un livello di rischio “Medio” sono:

<sup>19</sup> BR: Business Requirements

<sup>20</sup> RFC: Request for Change

<sup>21</sup> SSO: Single Sign-On

- Settore Pagamenti e Portafoglio;
- Settore Sistemi di Rete;
- Settore Finanza Proprietaria;
- Settore Finanza Titoli Compravendita;
- Settore Risparmio Gestito;
- Settore Anagrafe e Condizioni.

I dettagli circa i singoli indicatori e le considerazioni per questi sei settori sono illustrati nel paragrafo 6.4.1 relativo a raccomandazioni e conclusioni per l'analisi Top Level.

Per tutti i singoli indicatori sopra soglia sono state individuate azioni di miglioramento da parte dei Responsabili dei rispettivi Settori.

Nella conduzione dell'analisi Top Level, tramite i 7 indicatori di rischio identificati, sono emerse anomalie di carattere generale riconducibili ad alcuni Processi IT del Consorzio. Tali anomalie sono state considerate nell'analisi dalla Funzione IT Risk Management, in accordo con la Funzione Rischi Operativi e Reputazionali e, laddove siano state identificate azioni puntuali di aggiustamento con il Responsabile di Settore, è stata eseguita la revisione del valore del singolo indicatore. Pertanto, sono state avviate azioni di miglioramento sui seguenti ambiti, al fine di migliorare l'affidabilità dei dati che alimentano i KRI:

- *Incident Management*: il processo attuale di Incident Management e lo strumento utilizzato Remedy mostrano alcuni limiti che incidono sulla qualità dei dati e di conseguenza sull'indicatore. L'azione avviata è la redazione del BR 47753 "Studio fattibilità per estensione nuovo modello assistenza al GMPS" che, unitamente ad un percorso di awareness sull'impostazione corretta dei parametri in sede di censimento dell'incidente, dovrebbe portare ad una maggiore qualità dei dati. (ipotesi di chiusura attività: 2Q 2017)
- *Change Management*: il processo attuale di Change Management non consente di gestire correttamente alcune tipologie di change che formalmente risultano di emergenza, ma nei fatti non lo sono. Questo incide sulla bontà dell'indicatore. Per migliorare il processo di Change è stata recentemente acquistata la suite per il SDLC (Software Development Lifecycle) di HP, che prevede l'utilizzo in particolare di due strumenti: ALM (Application Lifecycle Management) per la verifica della bontà dei test e Service Manager per l'inserimento di RFC che, integrato strettamente con ALM, fornirebbe al Change Manager informazioni utili alla decisione relativa all'approvazione o al respingimento di una richiesta. (ipotesi di chiusura attività: 2Q 2017)
- *IT Asset Management*: lo strumento utilizzato mostra alcuni limiti legati alla granularità degli asset e alla possibilità di rivedere alcuni attributi legati all'indicatore CA. Le attività di miglioramento prevedono la formalizzazione di un processo di revisione degli attributi di sicurezza anche in funzione di una deroga formalizzata rispetto allo standard. (ipotesi di chiusura attività: 2Q 2017)

Un maggior dettaglio sulle problematiche e sugli interventi ipotizzati è riportato nel paragrafo 6.4.1.

Si segnala un andamento virtuoso dei Settori, che presentano un forte trend discendente su molti KRI rispetto all'anno precedente: Job (-40%), Change sui dati (-48%), RFC di Emergenza (-76%) e BR in ritardo (-11%). Questo grazie ad una importante iniziativa manageriale, che ha posto come obiettivo la

minimizzazione di questi indicatori, e grazie ad un impegno notevole delle strutture nel garantire il raggiungimento di questo obiettivo.

### **3.2 Analisi Low level**

L'analisi di dettaglio sugli asset nel perimetro 2016 è stata eseguita valutando la probabilità di accadimento degli eventi di rischio sottostanti ad uno o più scenari di rischio, in funzione della presenza o meno di controlli a presidio dell'asset.

Mentre l'analisi Top Level fornisce una rappresentazione del recente passato del Consorzio Operativo di Gruppo, l'analisi Low Level consiste in una valutazione prospettica in termini probabilistici di alcuni eventi di rischio cui la Banca è esposta, descrivendone la possibile situazione futura.

È stato concordato con il Servizio Rischi Operativi e Reputazionali della Capogruppo che, rispetto al totale di 749 asset attivi gestiti dal Consorzio Operativo di Gruppo alla data di definizione del perimetro, il totale degli asset potenzialmente da analizzare era di 674. L'analisi del rischio informatico su questo perimetro sarebbe stata condotta in un programma triennale con definizione annuale del numero e dell'elenco degli asset da analizzare. Questa ipotesi è stata presentata e approvata dal Consiglio di Amministrazione della Banca.

Il perimetro 2016 concordato con il Servizio Rischi Operativi e Reputazionali è stato quindi definito in un primo blocco di 144 asset, ottenuto incrociando i valori di vulnerabilità degli asset misurati secondo KRI e valori di rilevanza degli stessi, espressi secondo i seguenti parametri:

- Criteri di riservatezza, integrità e disponibilità forniti dagli Utenti Responsabili;
- Fattore correttivo "Business Continuity", laddove la risorsa supporti uno dei processi valutati come critici;
- Fattore correttivo espresso dalla Funzione Rischi Operativi e Reputazionali, laddove la risorsa rientri in uno degli ambiti di business individuati come critici.

Per le vulnerabilità si è proceduto a considerare:

- **GAP:** Numero di rilievi attivi sull'asset alla data della rilevazione ed emessi dalle Funzioni Compliance e Internal Audit del Consorzio;
- **CHG:** Numero di change in emergenza richiesti per l'asset;
- **CA:** tipologia di controllo accessi (se centralizzato o meno) alla data della rilevazione;
- **INC:** Somma pesata (dalla gravità) degli incidenti IT sull'asset;
- **INT-EXT:** asset IT raggiungibili tramite Internet o Extranet.

Infine, il perimetro è stato completato inserendo gli asset per i quali è stata richiesta una analisi specifica dagli Organi di Vigilanza.

Le probabilità<sup>22</sup> associate sugli scenari di rischio sono state incrociate con gli impatti stimati dagli Utenti Responsabili delle risorse ICT esaminate e da tale incrocio è stato identificato il valore di rischio potenziale.

---

<sup>22</sup> Le probabilità sono valutate secondo una scala qualitativa come definito in metodologia.

Dall'analisi, i seguenti asset risultano avere un rischio "Alto", ovvero superiore alla propensione al rischio definita dal Gruppo MPS per l'anno 2016:

Asset	Nome	Settore Consorzio
APP0000415	<b>Esteri Anticipi Valutari</b>	Settore Depositi ed Esteri
APP0000425	<b>Esteri Tesoreria Accentrata</b>	Settore Depositi ed Esteri
APP0000430	<b>Esteri Bonifici</b>	Settore Depositi ed Esteri
APP0000434	<b>Esteri Rimesse Imp/Exp</b>	Settore Depositi ed Esteri
APP0000435	<b>Esteri Sconto</b>	Settore Depositi ed Esteri
APP0000465	<b>CBI<sup>23</sup></b>	Settore Pagamenti e Portafoglio
APP0000872	<b>Nodo CBI<sup>5</sup></b>	Settore Pagamenti e Portafoglio
APP0000920	<b>Gari Gold TFM</b>	Settore Pagamenti e Portafoglio
APP0000526	<b>AOG - Anagrafe Operativa Gruppo</b>	Settore Anagrafe e Condizioni

**Tabella 7: Elenco Asset a rischio "Alto"**

Tutti gli asset afferenti al Settore Depositi ed Esteri fanno rilevare rischi riconducibili all'obsolescenza delle applicazioni e allo sviluppo custom, con conseguenti stratificazioni di software che rendono impegnativa l'evoluzione e possono provocare blocchi e degradi prestazionali soprattutto in fase di change. Ciò si rileva anche a causa della carenza di risorse IT con expertise approfondito e documentazione tecnica a supporto. Al fine di mitigare i rischi rilevati, è in corso uno studio di fattibilità su nuove soluzioni applicative al fine di adottare prodotti di mercato, valutando al contempo integrazioni di taluni servizi nei settori Italia. La data di completamento dello studio di fattibilità, concordata con il Servizio Commerciale Esteri e Rete Esteri, è Marzo 2017.

Gli asset "CBI" e "Nodo CBI" presentano un alto rischio di blocchi del software a causa del processo di Change Management non gestito correttamente. La raccomandazione è di integrare l'applicazione nel processo di Change management standard aziendale. Le attività per la mitigazione, concordate con il Servizio Internet Banking e Direct Marketing, si concluderanno entro Febbraio 2017.

L'asset "Gari Gold TFM" presenta rischio alto legato ad accesso indebito e divulgazione di informazioni causata da mancata integrazione con piattaforma IAM e utilizzo di utenze impersonali e password deboli,

<sup>23</sup> Si sottolinea che gli asset relativi a CBI presentano una sovrapposizione di funzionalità, infatti la valutazione ha condotto alla coincidenza dei rischi che sono emersi. Tuttavia, le due applicazioni sono censite separatamente all'interno dello strumento di inventory & asset management (APM), pertanto da un punto di vista metodologico i rischi identificati sono riconducibili ad entrambi gli asset in modo separato; così come segnalato anche dall'Utente Responsabile, si indirizzerà la verifica e l'omogeneizzazione del censimento all'interno dell'APM.

non rispettando gli standard aziendali in materia di gestione degli accessi logici. La raccomandazione è di formalizzare profili e regole di assegnazione delle utenze come previsto da standard aziendale e di rivedere periodicamente le utenze ed i profili abilitativi collegati, rispettando il principio del minimo privilegio. Le attività di mitigazione del rischio, concordate con il Servizio Liquidità Operativa, sono state avviate ed è previsto il completamento entro Giugno 2017.

Infine, “AOG - Anagrafe Operativa Gruppo” presenta rischio alto di accesso indebito; la raccomandazione definita è di provvedere a eliminare le condizioni nel codice che consentono il “by-pass” dei controlli di sicurezza. La mitigazione concordata con il Servizio Anagrafe Generale ed Indagini è stata avviata ed è prevista in chiusura entro Marzo 2017.

Come si è visto, tutte le azioni di mitigazione sono state concordate e pianificate. Pertanto, la fase di mitigazione dei rischi può ritenersi avviata.

Inoltre, esiste una proposta di Rischio Alto per l’asset “SAG - Swift Alliance Gateway”, poiché l’Utente Responsabile (la costituenda Commissione Risorse ICT trasversali) non ha ancora validato formalmente la proposta relativa agli Impatti sui vari scenari di rischio. Qualora questa fosse validata, l’asset rileverebbe un rischio alto di accesso indebito e attacchi logici. Per quanto riguarda il rischio di accesso indebito sarebbe necessario rivalidare le utenze tecniche ed applicative ed i privilegi ad esse assegnate, gestendo le stesse secondo standard aziendale. Inoltre, sarebbe opportuno definire ed assegnare chiaramente i ruoli e gli ambiti di intervento ai vari attori che partecipano al ciclo di vita dell’asset, secondo il principio della separazione dei compiti.

Per quanto riguarda il rischio legato a malware ed attacchi logici si dovrebbero implementare misure di protezione adeguate per gli utenti aventi privilegi amministrativi sulla piattaforma. Inoltre, come da comunicazione della Swift, sarebbe necessario installare l’ultima versione attualmente disponibile.

Le azioni di mitigazione, anche in assenza di decisioni sulla gestione del rischio da parte dell’Utente Responsabile, sono state avviate d’iniziativa da parte della Funzione ICT. La data di completamento attesa, per l’ultima delle azioni di mitigazione, è Dicembre 2017.

### **3.3 Analisi Sicurezza Informatica**

A seguito del risultato dell’analisi dello scorso anno, che individuava un rischio «Alto» per la Sicurezza Informatica, nel periodo GIUGNO-LUGLIO 2016 è stata condotta un’analisi approfondita con il supporto di Deloitte ERS, basata su:

- Una valutazione, mediante intervista<sup>24</sup> al Servizio Sicurezza IT del Consorzio e alla Sicurezza di Capogruppo, della robustezza dei controlli e dell’esposizione al rischio su un set di circa 40 minacce diverse e oltre 400 controlli diversi, raggruppati in domini (combinazione di standard NIST, ISO 27001, ISF SoGP);

---

<sup>24</sup> Condotta da Società di Consulenza esterna con relativi approfondimenti, con supporto della Funzione ITRM



- Un'analisi dell'esposizione intrinseca alle minacce e valutazione degli impatti basata su dati di benchmark del Settore Banking a livello mondiale.

I rischi valutati come "Alti" sono riconducibili allo scenario di attacchi logici e allo scenario di utilizzo improprio e/o errori, con particolare riferimento agli errori potenzialmente effettuati dallo staff utente e tecnico nell'operatività della Banca.

Per la mitigazione dei rischi rilevati è stato definito un piano integrativo rispetto a quello formalizzato ad inizio 2016 denominato "Monte più Sicuro", che ha indirizzato un primo set di azioni da intraprendere nel breve periodo (vedi sezione 6.3 Assessment Sicurezza IT). I dettagli del piano Monte più Sicuro e degli interventi integrativi definiti sono consultabili nell'allegato 1.

Questo ulteriore set di azioni di mitigazione, unito agli interventi portati a termine e previsti all'interno del progetto "Monte più Sicuro" (redatto a seguito dell'assessment 2015) riconducono il rischio sulla Sicurezza Informatica al livello finale "Medio".

### 3.4 Risultati complessivi dell'Analisi

Al fine di comparare i risultati ottenuti dall'analisi Top Level sui settori del Consorzio e i risultati dell'analisi Low Level rilevati sui singoli asset ICT, è stata predisposta la seguente tabella che riporta la distribuzione dei rischi prospettici degli asset gestiti dal Settore e il rischio basato sullo storico dell'ultimo anno del Settore stesso.

	Analisi Top Level				Analisi Low Level					
Settore	Rischio informatico del Settore (KRI periodo 1 GEN-31 DIC 2016)	Numero Asset in Perimetro 2016	Numero Totale Asset Settore	%	Non Rilevante	Molto Basso	Basso	Medio	Alto	Molto Alto
Settore Architettura di Processi IT	Molto Basso	0	5	-	-	-	-	-	-	-
Settore Architettura di Sviluppo	Molto Basso	0	7	-	-	-	-	-	-	-
Settore Architettura Enterprise e Esecutiva	Molto Basso	2	11	18%	-	-	-	2	-	-
Settore Architettura Sistemi	Molto Basso	0	1	-	-	-	-	-	-	-
Settore Erogazione Applicativa Online	Molto Basso	1	2	50%	1	-	-	-	-	-
Settore Erogazione Applicativa Batch	Molto Basso	0	0	-	-	-	-	-	-	-
Settore Gestione del Cambiamento	Molto Basso	0	4	-	-	-	-	-	-	-
Settore Informatica Utente	Molto Basso	1	15	7%	-	-	-	1	-	-
Settore Sistemi Centrali	Basso	2	39	5%	2	-	-	-	-	-
Settore Sistemi di Rete	Medio	2	23	9%	-	-	1	1	-	-
Settore Sistemi Dipartimentali	Basso	11	28	39%	3	1	4	3	-	-
Settore Capacity e Ottimizzazione	Molto Basso	1	4	25%	-	-	1	-	-	-
Settore Monitoraggio e	Molto Basso	0	3	-	-	-	-	-	-	-

	Analisi Top Level				Analisi Low Level					
Settore	Rischio informatico del Settore (KRI periodo 1 GEN-31 DIC 2016)	Numero Asset in Perimetro 2016	Numero Totale Asset Settore	%	Non Rilevante	Molto Basso	Basso	Medio	Alto	Molto Alto
Automazione										
Settore Ingegneria di Sicurezza	Medio	2	7	29%	-	-	-	2	-	-
Settore Monitoraggio della Sicurezza IT	Medio	4	18	22%	-	-	-	4	-	-
Settore Bilancio	Basso	2	12	17%	-	-	2	-	-	-
Settore Conformità	Basso	5	20	25%	1	-	-	4	-	-
Settore Rischi	Molto Basso	5	31	16%	-	-	2	3	-	-
Settore Segnalazioni	Molto Basso	2	16	13%	-	-	-	2	-	-
Settore Controllo di Gestione e Reporting	Basso	1	21	5%	-	-	-	1	-	-
Settore Data Warehouse	Molto Basso	0	19	-	-	-	-	-	-	-
Settore Qualità dei Dati	Molto Basso	0	3	-	-	-	-	-	-	-
Settore Applicazioni Risorse Umane	Basso	2	16	13%	-	-	1	1	-	-
Settore Acquisti	Basso	0	14	-	-	-	-	-	-	-
Settore Risparmio Gestito	Medio	3	8	38%	-	-	1	2	-	-
Settore Bancassurance	Basso	0	13	-	-	-	-	-	-	-
Settore Incassi	Basso	7	11	64%	-	-	4	3	-	-
Settore Monetica	Basso	10	17	59%	-	-	1	9	-	-
Settore Pagamenti e Portafoglio	Medio	20	34	59%	-	-	5	11	4	-
Settore Contenzioso, Leasing e Factoring	Basso	2	13	15%	-	-	1	1	-	-
Settore Crediti Bancari	Basso	4	24	17%	-	-	-	4	-	-
Settore Credito al Consumo e Specializzato	Basso	10	26	38%	-	1	6	3	-	-
Settore Finanza Proprietaria	Medio	11	30	37%	-	-	3	8	-	-
Settore Finanza Titoli Amministrazione	Basso	1	11	9%	-	-	-	1	-	-
Settore Finanza Titoli Compravendita	Medio	3	8	38%	-	-	3	-	-	-
Settore Portali Interni	Basso	6	27	22%	1	-	2	3	-	-
Settore Sportello	Basso	3	29	10%	-	-	3	-	-	-
Settore Usabilità Applicazioni	Molto Basso	0	7	-	-	-	-	-	-	-
Settore Internet Banking	Basso	9	33	27%	-	-	5	4	-	-
Settore Portali Esterni	Basso	1	3	33%	-	-	-	1	-	-
Settore Anagrafe e Condizioni	Medio	1	11	9%	-	-	-	-	1	-
Settore Depositi ed Estero	Basso	10	47	21%	-	-	3	2	5	-

Tabella 2: distribuzione rischi Asset per Settore

## 4 Ruoli e Responsabilità

Nell'ambito del Gruppo Montepaschi la responsabilità dello svolgimento dei compiti di controllo di secondo livello del rischio informatico è accentrata in Capogruppo, nell'Area Risk Management (Servizio Rischi Operativi e Reputazionali).

Per presidiare opportunamente il processo di gestione del rischio informatico, a maggio 2015 è stato costituito all'interno del Consorzio Operativo di Gruppo il Servizio IT Risk Management. Il Servizio riporta gerarchicamente al Direttore Generale del Consorzio e funzionalmente al Servizio Rischi Operativi e Reputazionali della Capogruppo.

La metodologia di IT Risk Management<sup>25</sup> prevede i seguenti ruoli e responsabilità in riferimento alla conduzione dell'analisi del rischio informatico:

L'Utente Responsabile:

- Partecipa al processo di valutazione del rischio informatico relativo alle risorse informatiche nel proprio perimetro di responsabilità, valutando gli impatti associati ai differenti scenari di rischio;
- Riceve gli esiti della valutazione del rischio potenziale e la proposta del piano di trattamento definita dalla Funzione Gestione Rischio Informatico;
- Ingaggia la Funzione ICT per ricevere una prima stima di massima dell'impegno necessario per la realizzazione delle misure di mitigazione;
- Stabilisce, di concerto con la propria linea gerarchica, la misura del rischio residuo da accettare, assumendo l'impegno delle misure di mitigazione "obbligatorie" e selezionando, in un'ottica di bilanciamento ottimale tra costi e benefici, le ulteriori misure di mitigazione "discrezionali";
- Approva i piani di trattamento del rischio, con gli interventi di mitigazione di tipo tecnico, organizzativo o procedurale e le tempistiche di realizzazione;
- Accetta formalmente il rischio residuo delle risorse informatiche di competenza;
- Propone i progetti per la realizzazione delle misure di mitigazione inserite nel piano di trattamento e richiede, anche mediante il ricorso alla propria linea gerarchica, lo stanziamento delle risorse a budget.

Il ruolo di Utente Responsabile viene attribuito alla Funzione aziendale che, per prevalenza di interesse a livello di Gruppo, può rappresentare gli utenti di una data risorsa informatica nei rapporti con la Funzione ICT. L'individuazione dell'Utente Responsabile deve essere condotta nel rispetto dei seguenti criteri:

- Collocazione, per i servizi oggetto di full outsourcing presso società strumentali di Gruppo, all'esterno della Funzione ICT;
- Responsabilità univocamente definita a livello di Gruppo per ciascuna risorsa informatica, applicando il criterio di "prevalenza di interesse";
- Individuazione ad un adeguato livello gerarchico per le risorse informatiche e le applicazioni maggiormente critiche.

---

<sup>25</sup> Cfr. documento 1030D02045 - Direttiva di Gruppo in materia di Gestione del Rischio Informatico.

L'Utente Responsabile viene individuato dalla Funzione Organizzazione, con il supporto della Funzione ICT e della Funzione Rischi Operativi. Per le risorse informatiche di natura trasversale (sia applicazioni di business che infrastrutture ICT) per le quali la Funzione Organizzazione non è in grado di individuare un Utente Responsabile prevalente, tale ruolo viene esercitato collegialmente da apposita Commissione costituita presso la Capogruppo, cui possono essere invitati a partecipare i rappresentanti delle altre Società del Gruppo. Per le piattaforme di sicurezza, il ruolo di Utente Responsabile è esercitato dalla Funzione Sicurezza BMPS/WIDIBA. In deroga al criterio generale, per le risorse di gestione IT, trattandosi di componenti tecnologiche utilizzate dalla sola Funzione ICT a supporto dei propri processi operativi e non direttamente connesse ai processi di business, gli Utenti Responsabili sono individuati all'interno della stessa Funzione ICT.

La Funzione Organizzazione:

- Individua gli Utenti Responsabili delle nuove risorse informatiche, con il supporto della Funzione ICT e della Funzione Rischi Operativi;
- Conferma il ruolo di Utente Responsabile o individua la Funzione cui deve essere ricondotto a seguito degli interventi di revisione della struttura Organizzativa della Capogruppo e delle altre Società del Gruppo.

La Funzione Rischi Operativi:

- Definisce e aggiorna periodicamente la metodologia di gestione del rischio informatico adottata dal Gruppo Montepaschi, in collaborazione con la Funzione Gestione Rischio Informatico, nel rispetto delle normative vigenti ed in coerenza con le best practice;
- Propone gli indicatori di rischio informatico (KRI) da inserire nel Risk Appetite Framework di Gruppo ed i relativi limiti;
- Coordina l'attività di valutazione degli impatti da parte degli Utenti Responsabili e ne verifica la congruità rispetto alle informazioni disponibili ed agli esiti delle analisi condotte in materia di gestione della Continuità Operativa;
- Presidia le attività di analisi e gestione del rischio informatico a livello di Gruppo, verificandone la coerenza con la metodologia definita;
- Condivide con gli Utenti Responsabili i risultati dell'analisi del rischio e la proposta del piano di trattamento, richiedendo ove opportuno il supporto della funzione Gestione Rischio Informatico;
- A fronte di rischi che superano la soglia di propensione definita nel RAF, segnala il relativo GAP per sollecitare la realizzazione delle misure di mitigazione "obbligatorie";
- Integra i risultati dell'analisi del rischio informatico all'interno del framework dei Rischi Operativi di Gruppo;
- Presidia le attività di monitoraggio del rischio informatico complessivo a livello di Gruppo, verificando la completezza, accuratezza, correttezza e coerenza dei flussi informativi e delle valutazioni predisposti dalla Funzione Gestione Rischio Informatico, validandone la reportistica prodotta;
- Con cadenza almeno annuale, sottopone il Rapporto sulla situazione del rischio informatico a livello di Gruppo all'approvazione degli Organi apicali della Capogruppo;
- Successivamente all'approvazione del Rapporto sulla situazione del rischio informatico a livello di Gruppo, invia ai Referenti Locali Rischi Operativi presso le altre Banche del Gruppo operanti in Italia

che non gestiscono direttamente risorse informatiche, un'informativa sulla situazione del rischio informatico rispetto alla propensione al rischio, con focus sulle risorse di cui dette Banche sono utenti prevalenti a livello di Gruppo.

La Funzione Gestione Rischio Informatico:

- Collabora con la Funzione Rischi Operativi all'aggiornamento periodico della metodologia di gestione del rischio informatico;
- Definisce, in collaborazione con la Funzione Rischi Operativi, la tassonomia degli eventi di rischio informatico, gli scenari di rischio informatico ed il catalogo degli indicatori (KRI) da utilizzare per l'analisi del rischio di alto livello ed il monitoraggio nel continuo della situazione del rischio informatico complessivo del Gruppo;
- Definisce il catalogo delle misure di mitigazione raccordandosi ove opportuno con le Funzioni ICT e Sicurezza;
- Definisce, in collaborazione con la Funzione Rischi Operativi, il perimetro ed il piano annuale di analisi e trattamento del rischio;
- Coordina le attività di analisi e trattamento del rischio informatico, determinando il rischio informatico potenziale e quello residuo sulle risorse ICT in perimetro;
- Supporta la Funzione ICT nell'auto-valutazione della probabilità di accadimento degli eventi di rischio informatico;
- Si confronta con le Funzioni ICT laddove ritenga che la valutazione delle probabilità eseguita dalla stessa non risulti coerente rispetto allo stato delle misure di mitigazione o alle evidenze prodotte da altri processi IT (ad es. incident management, problem management, change management, etc.) o dal sistema dei controlli interni (ad es. processi di revisione interna, data governance, assessment sulla sicurezza; etc.). Se necessario, fa escalation lungo la filiera gerarchica fino all'Organo apicale proponendo l'assunzione di un valore di probabilità più coerente;
- Definisce la proposta di trattamento del rischio informatico sulle risorse ICT analizzate, consultandosi con la Funzione ICT e, ove opportuno, con la Funzione Sicurezza;
- Monitora il livello di attuazione degli interventi di mitigazione indicati nei piani di trattamento del rischio rispetto alle scadenze dichiarate;
- Produce, su richiesta o come attività periodica, appositi report e valutazioni qualitative sui risultati delle attività di analisi e trattamento del rischio informatico;
- Monitora nel continuo i Key Risk Indicator e predispone idonei flussi informativi a supporto della Funzione Rischi Operativi per la valutazione della complessiva situazione del rischio informatico e dello stato avanzamento delle iniziative poste in essere nell'ambito del piano di trattamento del rischio;
- Produce con cadenza almeno annuale il Rapporto sulla situazione del rischio informatico relativo alle risorse informatiche gestite direttamente dalla Società di appartenenza, e lo sottopone ai propri Organi apicali, previa validazione della Funzione Rischi Operativi.

La coerenza complessiva del modello organizzativo è garantita attraverso il riporto funzionale della Funzione Gestione Rischio Informatico alla Funzione Rischi Operativi.

La Funzione ICT

- Fornisce l'inventario delle risorse informatiche;

- Esegue l'auto-valutazione della probabilità di accadimento degli eventi di rischio applicabili alle risorse informatiche in esame, prendendo in considerazione il livello attuale di implementazione e di efficacia delle misure di mitigazione definite per quelle risorse (approccio control-based);
- Supporta la fase di trattamento del rischio informatico attraverso l'identificazione delle ulteriori misure di mitigazione da applicare e la stima di massima dell'impegno necessario per la loro realizzazione;
- Esercita il ruolo di Utente Responsabile per le risorse di gestione IT.

#### La Funzione Sicurezza:

- Segue la redazione e l'aggiornamento delle policy di sicurezza e delle istruzioni operative e assicura la coerenza delle misure di mitigazione con le policy approvate;
- Supporta, qualora richiesta, la valutazione della probabilità degli eventi di rischio informatico nonché l'individuazione delle migliori e più opportune misure di mitigazione aggiuntive per il trattamento del rischio.

#### La Funzione Compliance

- Presidia il rischio di non conformità in tema di sistema informativo, svolgendo verifiche e fornendo valutazioni sul rispetto dei regolamenti interni e delle normative esterne in tema di ICT, con la sola eccezione di quanto previsto in materia di organizzazione e metodologia di analisi del rischio informatico.

#### La Funzione Internal Audit:

- Fornisce valutazioni sulla complessiva gestione del rischio informatico;
- Verifica la corretta e ripetuta attuazione dei processi di analisi e gestione del rischio informatico secondo la normativa in vigore.

## 5 Perimetro di analisi

Il perimetro di analisi del rischio informatico per la valutazione Top Level è stato identificato nei Settori del Consorzio che gestiscono asset ICT (applicazioni e infrastrutture IT) costituenti il sistema informativo di Gruppo. Non sono stati pertanto considerati nella misurazione degli indicatori di rischio i Servizi e i Settori del Consorzio privi di asset ICT o che svolgono mansioni di staff o di tipo gestionale all'interno del COG.

Nella tabella seguente sono elencati i Servizi e i Settori, ad essi afferenti, in perimetro di analisi Top Level.

Servizio	Settore
Servizio Architettura Sviluppo e Processi IT	Settore Architettura di Sviluppo
	Settore Architettura di Processi IT
Servizio Architettura Applicativa	Settore Architettura Enterprise e Esecutiva
Servizio Architettura Tecnologica	Settore Architettura Sistemi
Servizio Erogazione Applicativa	Settore Erogazione Applicativa Batch

	Settore Erogazione Applicativa Online
	Settore Gestione del Cambiamento
Servizio Sistemi	Settore Sistemi Centrali
	Settore Sistemi Dipartimentali
	Settore informatica Utente
	Settore Sistemi di Rete
Servizio Monitoraggio e Capacity	Settore Capacity e Ottimizzazione
	Settore Monitoraggio e Automazione
Servizio Bilancio e Conformità	Settore Conformità
	Settore Bilancio
Servizio Rischi e Segnalazioni	Settore Segnalazioni
	Settore Rischi
Servizio Sistemi di Sintesi	Settore Controllo di Gestione e Reporting
	Settore Qualità dei Dati
	Settore Data Warehouse
Servizio Risorse Umane e Acquisti	Settore Applicazioni Risorse Umane
	Settore Acquisti
Servizio Incassi e Pagamenti	Settore Pagamenti e Portafoglio
	Settore Incassi
	Settore Monetica

Servizio	Settore
Servizio Finanza	Settore Finanza Proprietaria
	Settore Finanza Titoli Amministrazione
	Settore Finanza Titoli Compravendita
Servizio Multicanalità Interni	Settore Sportello
	Settore Portali Interni
	Settore Usabilità Applicazioni

Servizio Multicanalità Clienti Esterni	Settore Internet Banking
	Settore Portali Esterni
Servizio Credito	Settore Crediti Bancari
	Settore Credito al Consumo e Specializzato
	Settore Contenzioso, Leasing e Factoring
Servizio Bancassurance e Risparmio Gestito	Settore Bancassurance
	Settore Risparmio Gestito
Servizio Sistemi referenziali	Settore Anagrafe e Condizioni
	Settore Depositi ed Estero

Tabella 3: Elenco dei Servizi e dei Settori in perimetro

L'analisi del rischio informatico di dettaglio è stata eseguita nel periodo Giugno-Dicembre 2016 sulle singole risorse informatiche in esercizio gestite dal Consorzio così come censite nel sistema di asset & inventory management (APM).

È stato concordato con il Servizio Rischi Operativi e Reputazionali della Capogruppo che, rispetto al totale di 749 asset attivi gestiti dal Consorzio Operativo di Gruppo alla data di definizione del perimetro, il totale degli asset potenzialmente da analizzare era di 674. L'analisi del rischio informatico su questo perimetro sarebbe stata condotta in un programma triennale con definizione annuale del numero e dell'elenco degli asset da analizzare. Questa ipotesi è stata presentata e approvata dal Consiglio di Amministrazione della Banca.

Nello specifico, il perimetro dell'assessment 2016 è costituito da un primo blocco di 144 asset, considerando la situazione degli asset IT presenti in APM al 31 Maggio 2016, ottenuto incrociando i valori di vulnerabilità degli asset misurati secondo KRI e valori di rilevanza degli stessi, espressi secondo i seguenti parametri:

- Criteri di riservatezza, integrità e disponibilità, forniti dagli Utenti Responsabili;
- Fattore correttivo "Business Continuity", laddove la risorsa supporti uno dei processi valutati come critici nell'ambito della continuità operativa;
- Fattore correttivo espresso dalla Funzione Rischi Operativi e Reputazionali, laddove la risorsa rientri in uno degli ambiti di business individuati come critici;

Per le vulnerabilità si è proceduto a considerare:

- **GAP:** Numero di rilievi attivi sull'asset alla data della rilevazione ed emessi dalle Funzioni Compliance e Internal Audit del Consorzio;
- **CHG:** Numero di change in emergenza richiesti per l'asset;
- **CA:** tipologia di controllo accessi (se centralizzato o meno) alla data della rilevazione;
- **INC:** Somma pesata (dalla gravità) degli incidenti IT sull'asset;
- **INT-EXT:** asset IT raggiungibili tramite Internet o Extranet.



Infine, il perimetro è stato completato inserendo gli asset per i quali è stata richiesta una analisi specifica dagli Organi di Vigilanza.

Al fine di monitorare i livelli di rischio identificati nel corso dell'analisi del rischio 2015, è stato considerato all'interno del perimetro di analisi 2016 anche il Servizio Sicurezza IT del Consorzio (e non i suoi settori), sul quale è stato eseguito un assessment specifico le cui modalità di conduzione sono descritte nel successivo paragrafo 6.3 (Assessment Sicurezza IT).

#### 5.1.1 Cenni metodologici – Analisi Top Level

Come già anticipato nei precedenti capitoli, ai fini della valutazione complessiva della situazione di rischio del sistema informativo di Gruppo, è stato eseguito un assessment basato sulla misurazione di indicatori di rischio (Key Risk Indicator - KRI), così come anche suggerito dagli standard internazionali in ambito rischio informatico (ISO27005, COBIT5 for Risk), che prevedono il ricorso alla valutazione dei KRI per graduare l'effort della valutazione del rischio informatico.

L'analisi Top Level consiste nella rilevazione e nella registrazione di eventi occorsi nel periodo in esame e che vanno ad alimentare gli indicatori di rischio (KRI – Key Risk Indicator). Pertanto questa tipologia di valutazione è tipo retrospettivo, ovvero rappresenta l'andamento del Consorzio Operativo di Gruppo nell'ultimo anno passato, secondo le dimensioni di analisi definite. I KRI sono parametri che tengono traccia di eventuali cambiamenti nel "profilo di rischio" alimentando nel continuo gli stessi con gli eventi informatici rilevati. Quindi i KRI possono essere considerati una sorta di sistema di primo allarme (*early warning*) per il "profilo di rischio" informatico.

La scelta degli indicatori da utilizzare per le valutazioni di rischio è legata alle peculiarità di ogni organizzazione e può dipendere da fattori interni o esterni quali ad esempio: la dimensione, la complessità, l'ambito di operatività e la strategia.

Il dettaglio degli indicatori è esploso nel paragrafo 6.1.

#### 5.1.2 Cenni metodologici – Analisi Low Level

Mentre l'analisi Top Level fornisce una rappresentazione del recente passato del Consorzio Operativo di Gruppo Montepaschi, l'analisi Low Level consiste in una valutazione prospettica in termini probabilistici di alcuni eventi di rischio cui la Banca è esposta, descrivendone la possibile situazione futura.

Annualmente il Servizio IT Risk Management, in accordo con il Servizio Rischi Operativi e Reputazionali, definisce il catalogo dei rischi, ovvero l'insieme di scenari, eventi, vulnerabilità e controlli che devono essere valutati per l'assessment. Per l'anno 2016, gli scenari di rischio analizzati sono i seguenti:

#### Scenari di rischio

Rischi legati a **carenze di expertise** o abilità delle risorse IT nel supporto all'operatività dei sistemi

Rischi legati all'**errata esecuzione** di operazioni da parte di personale interno

Scenari di rischio
Rischi legati ai <b>fornitori</b>
Rischi legati ad <b>anomalie o degrado</b> dell'asset <b>a causa di Change</b> gestito non correttamente
Rischi legati ad <b>anomalie o degrado</b> dell'asset in <b>produzione</b>
Rischi legati a <b>blocchi</b> dell'asset <b>a causa di Change</b> gestito non correttamente
Rischi legati a <b>blocchi</b> dell'asset in <b>produzione</b>
Rischi legati a <b>danneggiamento o perdita</b> delle informazioni a causa di <b>eventi accidentali</b>
Rischi legati a <b>danneggiamento o perdita delle</b> informazioni a causa di <b>intenti malevoli</b>
Rischi legati ad <b>accesso indebito o divulgazione</b> delle informazioni
Rischi legati a <b>furto o smarrimento</b> di <b>apparati mobili</b> contenenti informazioni riservate
Rischi legati a <b>malware ed attacchi logici</b>

Tabella 4: elenco degli scenari di rischio 2016

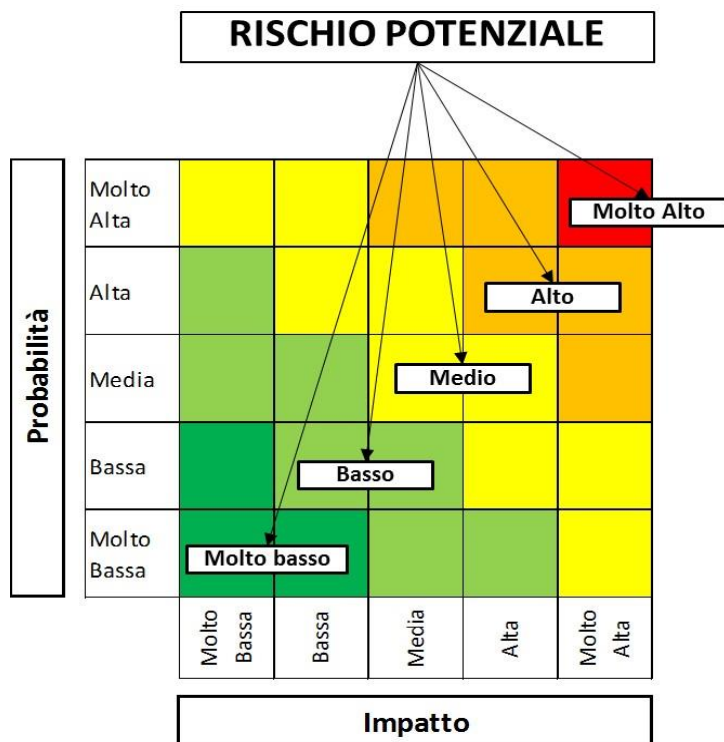
Agli scenari di rischio sono legati gli eventi di rischio a cui si agganciano a loro volta i controlli (misure di protezione esistenti sull'asset).

Gli IT Risk Owner dichiarano la presenza o l'assenza dei controlli per ogni risorsa ICT e valutano le probabilità associate agli eventi per i quali non sono implementati al momento presidi adeguati. Infatti i presidi sono classificati in controlli "chiave" e "non chiave": i primi, per la loro natura, fanno sì che la vulnerabilità sfruttabile da una minaccia sia azzerata impedendo ad un determinato evento di concretizzarsi; i controlli "non chiave" invece contribuiscono ad innalzare o abbassare il livello di protezione sull'asset, influenzando di fatto il valore di probabilità dell'evento, laddove un controllo chiave sia non presente.

Le probabilità sono valutate secondo una scala qualitativa ("Molto Alta", "Alta", "Media", "Bassa", "Molto Bassa") e sono aggregate a livello di scenario secondo la logica del worst case (ogni scenario eredita la probabilità maggiore associata ad uno o più eventi che lo costituiscono).

Gli impatti sono valutati per ogni scenario di rischio, tramite un questionario somministrato agli Utenti Responsabili che traduce gli scenari di rischio informatico in domande sugli effetti negativi dal punto di vista del Business. Il questionario distingue quattro tipologie di impatto: economico/operativo, reputazionale, normativo e strategico. Le valutazioni sono effettuate secondo una scala qualitativa ("Molto Alto", "Alto", "Medio", "Basso", "Molto Basso") e sono aggregate a livello di scenario secondo la logica del worst case (ogni scenario eredita l'impatto maggiore tra le quattro tipologie considerate).

L'incrocio tra impatto e probabilità fornisce il valore di rischio per ogni scenario, come rappresentato dalla matrice seguente:



Il livello di rischio finale per ogni singolo asset è ottenuto aggregando i rischi sugli scenari, secondo la logica del worst case: l'asset eredita il valore di rischio maggiore relativo ad uno o più scenari che lo costituiscono.

Per i valori di rischio superiori alla soglia di propensione definita nel RAF – Risk Appetite Framework dal Gruppo MPS è obbligatoria la gestione del rischio affinché il rischio residuo sia pari o inferiore. L’Utente Responsabile, può anche decidere di mitigare rischio pari o inferiori alla soglia di propensione. Per il 2016 la soglia di propensione è stata fissata sul livello di rischio “Medio” (rischio accettabile dagli Utenti Responsabili).

Il dettaglio delle analisi Low Level è illustrato nel paragrafo 6.2.

## 6 Analisi del Rischio

Il rischio informatico è definito nella sua più ampia accezione, dalla Circolare di Banca d'Italia 285 del 17 dicembre 2013 e suoi aggiornamenti, 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). 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”.

Un rischio può concretizzarsi attraverso un evento specifico che si manifesta attraverso un malfunzionamento delle infrastrutture IT o degli applicativi, un errore nella conduzione dei processi IT o una violazione nei sistemi di sicurezza della Banca.

A seconda della tipologia di evento che si concretizza possono verificarsi effetti sia sulla componente di funzionamento (sistema informativo a supporto del Business) sia sulla componente strategico-evolutiva (disallineamento dalle aspettative del Business).

## 6.1 Analisi Top Level

### 6.1.1 Modalità di analisi

Come già anticipato nei precedenti capitoli, ai fini della valutazione complessiva della situazione di rischio del sistema informativo di Gruppo, è stato eseguito un assessment basato sulla misurazione di indicatori di rischio (Key Risk Indicator - KRI), così come anche suggerito dagli standard internazionali in ambito rischio informatico (ISO27005, COBIT5 for Risk), che prevedono il ricorso alla valutazione dei KRI per graduare l'effort della valutazione del rischio informatico.

Per la valutazione Top Level del rischio informatico del Gruppo MPS sono stati utilizzati i seguenti Key Risk Indicator (KRI):

ID	KRI	Rilevanza	%	U.O./Asset	Alimentazione
PRJ	Somma pesata del numero di progetti rilasciati in ritardo nel Settore IT con motivazione «IT» e «Mista» diviso per il totale pesato dei progetti rilasciati dal Settore. Il peso varia in base alla tipologia (Progetti di Piano Esecutivo, Rilevanti, Altri, Running).	Media	15%	U.O.	Estrazione dei BR (Progetti da Business Requirements) in stato avanzamento «Rilasciato On time» e «Rilasciato Delay» dal sistema di PPM (Project Portfolio Management) con indicazione delle responsabilità del ritardo; sono considerati i progetti in ritardo a causa IT e a causa “mista” (ovvero ICT e Business in concomitanza).
GAP	Somma pesata dei rilievi attivi per Settore, emessi dalle Funzioni di Controllo su asset IT, alla data della rilevazione e censiti su RIGAM; sono considerati anche i rilievi ISAE e BCE/JST, anche se non censiti su RIGAM.	Media	15%	U.O.	Estrazione dal sistema di GRC dei rilievi classificati per emittente e destinatario (Settore) e stato di risoluzione. Sono considerati i gap sugli Asset ICT “attivi” alla data, ovvero i gap ancora non sanati dal Settore di competenza.
RFC	Numero di Change in emergenza richiesti dal Settore, rispetto al numero degli asset ad esso afferenti, nel periodo in esame.	Media	15%	Asset	Estrazione dal sistema di Change management dell'elenco delle richieste di Change in emergenza del Settore.
INC	Somma pesata per priorità e per tempo di risoluzione degli incidenti IT sugli asset del Settore rispetto al numero degli asset ad esso afferenti.	Molto Alta	25%	Asset	Estrazione da strumento di Incident Management Remedy dei ticket classificati come «incidenti» nel periodo in esame, risolti da strutture specialistiche COG o da fornitori esterni, diversi da help desk e back office,

ID	KRI	Rilevanza	%	U.O./Asset	Alimentazione
					associati direttamente all'asset, con livello di priority assegnata pari a «Media» o superiore. Estrazione dei tempi di risoluzione per gli incidenti major e critici.
JOB	Numero medio di job batch schedulati andati in errore nel periodo in esame (terminati inabend per asset gestiti dal Settore).	Media	15%	Asset	Estrazione da Gestione Flussi Job Batch terminati inabend.
CA	Numero di applicazioni (asset per Settore) non collegate al controllo accessi centralizzato e/o privi di sistema SSO.	Molto Basso	5%	Asset	Dati derivanti dal censimento delle applicazioni eseguito dal Consorzio circa i sistemi di controllo accessi centralizzato e sistema di SSO (Single Sign-On).
CHD	Numero di Change eseguiti sui dati in produzione.	Basso	10%	U.O	Dati relativi alle modifiche effettuate sui dati in ambiente di produzione tramite transazione GADIS.

Tabella 5: Indicatori di rischio valutati

A ciascun KRI è stato assegnato un grado di rilevanza su scala qualitativa, associato ad un peso percentuale, tenendo conto dell'affidabilità dei dati che alimentano la metrica e dell'importanza dell'indicatore nella rappresentazione del livello di rischio informatico.

I sette KRI sopra elencati consentono il monitoraggio delle seguenti dimensioni di analisi:

- La capacità dell'ICT nell'evadere le richieste del Business tramite progetti, nei tempi previsti;
- Il grado di allineamento dell'ICT alle best practice di Settore e ai dettami normativi sia interni che esterni;
- I livelli di disponibilità e affidabilità degli Asset ICT;
- I livelli di sicurezza delle applicazioni ICT.

Gli indicatori sono stati rilevati per Unità Organizzativa (Settore); gli indicatori che identificano metriche rilevabili a livello di asset ICT (es. numero di Change in emergenza) sono stati aggregati a livello di Settore, dimensionando il valore del KRI rispetto al numero di asset ICT gestiti dal Settore stesso.

Ad ogni indicatore di rischio è stata assegnata una scala di valutazione secondo range numerici, ai quali sono stati associati dei corrispondenti valori di rischio, secondo la seguente scala qualitativa prevista dalla metodologia di IT Risk Management:

- Molto Basso;
- Basso;
- Medio;
- Alto;

- Molto Alto.

Le soglie sono state identificate tenendo in considerazione due criteri: il valore obiettivo fissato dal Consorzio per l'indicatore in questione e l'andamento storico registrato dall'indicatore stesso. Nel primo caso il valore obiettivo coincide con il valore "Basso" della scala di rischio associata al KRI; nel secondo caso l'andamento medio registrato è stato fatto coincidere con il valore "Medio" della scala di rischio associata al KRI. Infine i range sono stati costruiti in modo da avere pari ampiezze tra di loro per singolo indicatore e secondo scale lineari crescenti. Ai KRI per i quali non siano state rilevate occorrenze per Settore o per Asset ICT (mancata valorizzazione della metrica) è stato assegnato valore zero, corrispondente ad un valore di rischio "Non Rilevante".

Il risultato di rischio finale ottenuto per ogni Settore del Consorzio è ottenuto eseguendo la media ponderata (in base ai pesi percentuali di rilevanza associati ai KRI) dei risultati di ogni singolo KRI.

#### *6.1.2 Periodo di osservazione e fonti di alimentazione*

Il periodo di osservazione, ovvero di alimentazione dei KRI per la redazione della presente relazione, è di un anno: **da Gennaio 2016 a Dicembre 2016**.

Per ogni KRI sono state definite le fonti dei dati di alimentazione di cui si fornisce la descrizione di seguito.

- **Progetti in ritardo – PRJ:** estrazione dei BR (Progetti da Business Requirements) in stato avanzamento «Rilasciato On time» e «Rilasciato Delay» dal sistema di PPM (Project Portfolio Management) con indicazione delle responsabilità del ritardo; sono considerati i progetti in ritardo a causa IT e a causa "mista" (ovvero ICT e Business in concomitanza). La rilevanza del Progetto collegato ai BR si ottiene dalla stessa fonte.
- **Numero di rilievi emessi dalle Funzioni di Controllo – GAP:** estrazione dal sistema di GRC dei rilievi classificati per emittente e destinatario (Settore) e stato di risoluzione. Sono considerati i gap sugli Asset ICT "attivi" alla data, ovvero i gap ancora non sanati dal Settore di competenza.
- **Change eseguiti in emergenza – RFC:** estrazione dal sistema di Change management dell'elenco delle richieste di Change in emergenza del Settore.
- **Somma pesata degli incidenti – INC:** estrazione da strumento di Incident Management Remedy dei ticket classificati come «incidenti» nel periodo in esame, risolti da strutture specialistiche COG o da fornitori esterni, diversi da help desk e back office, associati direttamente all'asset, con livello di priority assegnata pari a «Media» o superiore. Estrazione dei tempi di risoluzione per gli incidenti major e critici.
- **Estrazione da Gestione Flussi Job Batch in abend - JOB:** estrazione da Gestione Flussi Job Batch terminati in abend.
- **Controllo Accessi – CA:** dati derivanti dal censimento delle applicazioni in APM eseguito dal Consorzio circa i sistemi di controllo accessi centralizzato e sistema di SSO (Single Sign-On).
- **Change sui dati in produzione – CHD:** dati relativi alle modifiche effettuate sui dati in ambiente di produzione tramite transazione GADIS.

### 6.1.3 Scale e razionali

All'interno del seguente paragrafo sono presentate le scale di valutazione associate ad ogni singolo KRI (secondo le logiche definite nel paragrafo "6.1.1 Modalità di analisi") e i razionali per la definizione delle stesse.

ID	KRI	Molto Basso	Basso	Medio	Alto	Molto Alto
PRJ	<p>Somma pesata del numero di progetti rilasciati in ritardo nel Settore IT con motivazione «IT» e «Mista» diviso per il totale pesato dei progetti rilasciati dal Settore. Il peso varia in base alla tipologia (Progetti di Piano Esecutivo, Rilevanti, Altri, Running).</p> <p>Sono state definite alcune soglie sotto le quali il dato di alimentazione non viene considerato.</p>	<11	11-21	22-32	33-43	≥44
GAP	Somma pesata dei rilievi attivi per Settore, emessi dalle Funzioni di Controllo su asset IT, alla data della rilevazione e censiti su RIGAM; sono considerati anche i rilievi ISAE e BCE/JST, anche se non censiti su RIGAM.	<5	5-29	30-54	55-79	≥80
RFC	Numero di Change in emergenza richiesti dal Settore, rispetto al numero degli asset ad esso afferenti, nel periodo in esame.	<0,35	0,35-0,64	0,65-0,94	0,95-1,24	≥1,25
INC	Somma pesata per priorità e per tempo di risoluzione degli incidenti IT sugli asset del Settore rispetto al numero degli asset ad esso afferenti.	<10	10-34	35-59	60-84	≥85
JOB	Numero medio di job batch schedulati andati in errore nel periodo in esame (terminati inabend per asset gestiti dal	<100	100-399	400-699	700-999	≥1000

ID	KRI	Molto Basso	Basso	Medio	Alto	Molto Alto
	Settore).					
CA	Numero di applicazioni (asset per Settore) non collegate al controllo accessi centralizzato e/o privi di sistema SSO sul totale degli asset del Settore.	<0,2	0,2-0,49	0,5-0,79	0,8-1,19	≥1,2
CHD	Numero di Change eseguiti sui dati in produzione.	<30	30-120	121-210	211-300	≥301

Tabella 6: Scale associate ai KRI

Di seguito si descrivono i razionali utilizzati per la definizione dei range associati alle scale di rischio.

- **Progetti in ritardo – PRJ:** il Consorzio ha fissato l’obiettivo massimo del 21% dei progetti in ritardo. Pertanto tale valore rappresenta il valore di soglia per il rischio “Basso”. Inoltre, la serie storica del 2015 ha evidenziato una media del 25% dei progetti in ritardo all’anno per Settore; tale valore è stato quindi considerato di riferimento per il rischio “Medio”, costituendo di fatto la mediana del range associato a tale valore di rischio. Infine, considerando che il Benchmark di mercato si attesta attorno ad un valore di riferimento del 32% dei progetti IT in ritardo, tale valore è stato fissato come valore di soglia per la fascia di rischio “Media”.

- **Numero di rilievi emessi dalle Funzioni di Controllo – GAP:** i gap sono classificati per rilevanza (“Alta”, “Media”, “Bassa”). Ad ogni valore di rilevanza è associato un peso: “Alta” =10; “Media” =5; “Bassa” = 1, secondo quanto previsto dalle attuali procedure operative di valutazione dei rischi. La definizione delle fasce è stata eseguita considerando due aspetti: i valori assoluti dei gap pesati e la serie di andamento del Consorzio negli ultimi 3 anni.

La definizione delle fasce secondo il criterio dei valori assoluti ha portato a considerare che un Settore, che al momento della rilevazione presenta 10 gap di rilevanza “Alta” (o un punteggio pesato equivalente) debba ricadere nella fascia di rischio “Molto Alto” e, similmente, con meno di un gap di rilevanza “Alta”, debba ricadere nella fascia di rischio “Molto Basso”. Le altre fasce sono state definite di conseguenza, tenendo conto del principio della distribuzione lineare.

Le considerazioni che invece si basano sulla serie storica dell’ultimo triennio hanno evidenziato che il valore pesato dei gap oscilla tra circa 1000 (anno 2014) e circa 200 (anno 2016) passando dal valore intermedio di circa 500 (anno 2015). Di conseguenza, a livello aziendale, tali valori si riconducono nelle seguenti fasce di rischio: 200=“ Basso”; 500 =“ Medio”; 1000 =“ Molto Alto”. La considerazione utilizzata per collegare il livello di rischio del Settore con l’andamento generale del Consorzio è quella della distribuzione media dei gap per Settore che si aggira intorno al 10% del totale. Di conseguenza si considera che, un Settore che ha un punteggio sui gap pari al 10% del



valore misurato a livello aziendale, sia in linea con l'andamento generale e rientri nella fascia di rischio corrispondente a quella più generale del Consorzio. A titolo di esempio, un punteggio di circa 20 ricade all'interno della fascia di rischio "Bassa" ( $200 \times 10\%$ ); un punteggio di circa 50 ricade nella fascia di rischio "Media" ed un punteggio di circa 100 rappresenta un rischio "Molto Alto".

Di conseguenza le fasce di rischio sono state costruite secondo le logiche appena descritte secondo una scala lineare con ampiezza pari a 30.

- **Change eseguiti in emergenza – RFC:** Il Consorzio ha fissato come obiettivo un numero massimo di Change complessivi eseguiti in emergenza pari a 300 all'anno. Gli asset del Consorzio ammontano a circa 600, per cui il numero massimo di Change in emergenza per ogni singolo asset è pari a 0,5 ( $300/600$ ). Di conseguenza, il valore 0,5 coincide con la mediana del range associato al valore "Basso" della scala di misurazione del rischio. Il superamento della soglia di rischio "Basso" avviene all'esecuzione di un numero di RFC in emergenza pari al 30% in più del target ( $0,5 \times 1,3 = 0,65$ ). Un rischio "Molto Alto" si rileva superando del 150% il valore obiettivo.
- **Somma pesata degli incidenti – INC:** - Ad ogni incidente è stato associato un peso. Agli incidenti "Major" e "Critici" è assegnato un punteggio in funzione del tempo di risoluzione. I major risolti entro la prima ora assumono punteggio 40, entro le 4h punteggio 50, oltre le 4h punteggio 60. Gli incidenti critici risolti entro 4h assumono punteggio 15, entro le 8h punteggio 20, oltre le 8h punteggio 25. Le soglie temporali sono ricavate da Best Practice ITIL. Gli incidenti a priority "Alta" e "Media" assumono rispettivamente punteggio 10 e 4. È stato definito come valore di soglia per la fascia di rischio «Alto» il valore pesato degli incidenti pari a 60. Il valore massimo di soglia per il rischio «Molto Basso» è stato considerato pari a 10.
- **Job batch in errore – JOB:** il criterio di calcolo utilizzato è la somma del numero di job batch andati in errore, ovvero terminati in abend, per applicazione del Settore IT, divisa per il numero totale di asset del Settore IT. Il valore obiettivo "Basso" è stato fissato in funzione dell'obiettivo del Consorzio di raggiungere un numero totale all'anno di job batch in abend pari a 100.000 distribuiti su circa 400 asset rilevanti; mentre la fascia di rischio "Medio" è stata fissata in considerazione dell'andamento dei 12 mesi precedenti (240.000 abend).
- **Controllo Accessi – CA:** dalle osservazioni eseguite, solitamente l'assenza di un sistema di SSO (Single Sign-On) e l'assenza di un sistema di autorizzazione centralizzato degli accessi sono tra di loro correlati. Ad un asset che risulti privo di un controllo accessi centralizzato vengono assegnati 1,5 punti, mentre vengono assegnati 0,5 punti nel caso in cui risulti privo di sistema di SSO. Si ritiene quindi che l'assenza di un controllo accessi centralizzato comporti una quota di rischio maggiormente rilevante rispetto ad un sistema SSO. Un asset privo di entrambi i presidi assume quindi punteggio pari a 2. È stato fissato come valore massimo obiettivo un numero pari al 15% delle applicazioni di ogni Settore che presentino entrambe le eccezioni. Pertanto il valore 0,3 ( $0,15 \times 2$ ) rientra all'interno del range relativo al rischio "Basso". La soglia per cui si rileva un rischio "Alto" è stata fissata al valore 40% e la soglia per il rischio "Molto Alto" è fissata a partire dal 60%.
- **Change sui dati in produzione – CHD:** Considerando il trend positivo dell'indicatore si prevede di avere un numero massimo di Change sui dati per Settore a fine anno pari a 65, valore fissato nella fascia di rischio "Basso". La media dell'ultimo anno misurata è pari a 300 che rappresenta il valore limite tra il rischio "Alto" e "Molto Alto".

#### 6.1.4 Risultati

Il presente paragrafo descrive i risultati di rischio ottenuti tramite KRI per i Settori in perimetro. La tabella seguente ne sintetizza gli esiti.

Servizio	Settore	Livello di rischio
Servizio Architettura Sviluppo e Processi IT	Settore Architettura di Sviluppo	Molto Basso
	Settore Architettura di Processi IT	Molto Basso
Servizio Architettura Applicativa	Settore Architettura Enterprise e Esecutiva	Molto Basso
Servizio Architettura Tecnologica	Settore Architettura Sistemi	Molto Basso
Servizio Erogazione Applicativa	Settore Erogazione Applicativa Batch	Molto Basso
	Settore Erogazione Applicativa Online	Molto Basso
	Settore Gestione del Cambiamento	Molto Basso
Servizio Sistemi	Settore Sistemi Centrali	Basso
	Settore Sistemi Dipartimentali	Basso
	Settore informatica Utente	Molto Basso
	Settore Sistemi di Rete	Medio
Servizio Monitoraggio e Capacity	Settore Capacity e Ottimizzazione	Molto Basso
	Settore Monitoraggio e Automazione	Molto Basso
Servizio Bilancio e Conformità	Settore Conformità	Basso
	Settore Bilancio	Basso
Servizio Rischi e Segnalazioni	Settore Segnalazioni	Molto Basso
	Settore Rischi	Molto Basso
Servizio Sistemi di Sintesi	Settore Controllo di Gestione e Reporting	Basso
	Settore Qualità dei Dati	Molto Basso
	Settore Data Warehouse	Molto Basso
Servizio Risorse Umane e Acquisti	Settore Applicazioni Risorse Umane	Basso
	Settore Acquisti	Basso
Servizio Incassi e Pagamenti	Settore Pagamenti e Portafoglio	Medio
	Settore Incassi	Basso

	Settore Monetica	Basso
Servizio Finanza	Settore Finanza Proprietaria	Medio
	Settore Finanza Titoli Amministrazione	Basso
	Settore Finanza Titoli Compravendita	Medio
Servizio Multicanalità Interni	Settore Sportello	Basso
	Settore Portali Interni	Basso
	Settore Usabilità Applicazioni	Molto Basso
Servizio Multicanalità Clienti Esterni	Settore Internet Banking	Basso
	Settore Portali Esterni	Basso
Servizio Credito	Settore Crediti Bancari	Basso
	Settore Credito al Consumo e Specializzato	Basso
	Settore Contenzioso, Leasing e Factoring	Basso
Servizio Bancassurance e Risparmio Gestito	Settore Bancassurance	Basso
	Settore Risparmio Gestito	Medio
Servizio Sistemi referenziali	Settore Anagrafe e Condizioni	Medio
	Settore Depositi ed Estero	Basso

Tabella 7: Risultati Top Level per Settore

Il risultato attribuito al Settore Monitoraggio della Sicurezza IT è stato ricavato dall'analisi specifica condotta sul Servizio Sicurezza IT descritta nel paragrafo 6.3, a cui si rimanda per i dettagli.

I Settori a rischio "Medio" sono sei: Settore Pagamenti e Portafoglio, Settore Sistemi di Rete, Settore Finanza Proprietaria, Settore Finanza Titoli Compravendita, Settore Risparmio Gestito, Settore Anagrafe e Condizioni.

Le considerazioni in merito ai risultati ottenuti, le relative raccomandazioni e le azioni di mitigazione intraprese sono descritti all'interno del paragrafo 6.4.

## 6.2 Assessment low level

### 6.2.1 Modalità di analisi

Come già accennato nel paragrafo 5.1.2 (al quale si rimanda per gli approfondimenti), ogni anno viene rivisto il catalogo dei rischi, ovvero l'insieme di scenari, eventi, vulnerabilità e controlli che devono essere valutati per l'assessment.

Agli scenari di rischio sono legati gli eventi di rischio a cui si agganciano a loro volta i controlli (misure di protezione esistenti sull'asset).

In base ai controlli riscontrati, e/o alla loro efficacia, vengono definite le probabilità di accadimento degli eventi di rischio che, incrociate con gli impatti a livello di scenario, consentono di definire il livello di rischio.

### 6.2.2 Risultati

L'analisi del rischio informatico di dettaglio è stata eseguita nel periodo Giugno-Settembre 2016 sulle singole risorse informatiche in esercizio così come censite nel sistema di asset & inventory management del Consorzio (APM).

Nello specifico il perimetro dell'IT Risk ha riguardato la situazione degli asset IT presenti al 31 Maggio 2016 selezionando le risorse ICT sulla base di criteri specifici e oggettivi di rilevanza per il business e vulnerabilità potenziali.

Nel corso del 2016 sono stati pertanto oggetto di valutazione del rischio informatico 144 asset IT tra applicazioni di business non trasversali (123) e risorse ICT trasversali (21), che costituiscono il primo blocco di 450 asset rilevanti (su un totale di circa 600 gestiti dal Consorzio) che saranno analizzati in 3 anni, come presentato dalla Funzione Rischi Operativi e Reputazionali in Consiglio d'Amministrazione.

Per ciascun asset sono stati completati, tramite interviste:

- Un questionario al Responsabile dell'asset (IT Risk Owner) del Consorzio, che, in base all'applicabilità degli eventi di rischio alla risorsa in esame ha valutato probabilità di accadimento degli eventi in base alla presenza o all'assenza dei controlli, considerando anche le serie storiche a disposizione su malfunzionamenti e incidenti di sicurezza;
- Un questionario di 7 quesiti di Business, collegati agli scenari di rischio, di cui l'Utente Responsabile ha stimato il livello di impatto.

Il dettaglio dei Rischi Alti rilevati è il seguente:

ID Asset	Nome Asset	Rischi	Impatto	Probabilità Max. Scenario	Rischio Max. Scenario
APP0000415	Estero Anticipi Valutari	Rischi legati a carenze di expertise o abilità delle risorse IT nel supporto all'operatività dei sistemi	Alto	Alta	Alto
		Rischi legati a blocchi del software a causa di Change gestito non correttamente	Alto	Alta	Alto
APP0000425	Estero Tesoreria Accentrata	Rischi legati a carenze di expertise o abilità delle risorse IT nel supporto all'operatività dei sistemi	Molto Alto	Alta	Alto
		Rischi legati all'errata esecuzione di operazioni da parte di personale interno	Molto Alto	Media	Alto
		Rischi legati ad anomalie o degrado del software a causa di Change gestito non correttamente	Alto	Alta	Alto

ID Asset	Nome Asset	Rischi	Impatto	Probabilità Max. Scenario	Rischio Max. Scenario
		Rischi legati a blocchi del software a causa di Change gestito non correttamente	Molto Alto	Alta	Alto
		Rischi legati a blocchi del software in produzione	Molto Alto	Media	Alto
APP0000430	Estero Bonifici	Rischi legati a blocchi del software a causa di Change gestito non correttamente	Molto Alto	Media	Alto
APP0000434	Estero Rimesse Imp/Exp	Rischi legati a carenze di expertise o abilità delle risorse IT nel supporto all'operatività dei sistemi	Alto	Alta	Alto
		Rischi legati a blocchi del software a causa di Change gestito non correttamente	Alto	Alta	Alto
APP0000435	Estero Sconto	Rischi legati a carenze di expertise o abilità delle risorse IT nel supporto all'operatività dei sistemi	Alto	Alta	Alto
APP0000465	CBI	Rischi legati a blocchi del software a causa di Change gestito non correttamente	Alto	Alta	Alto
APP0000872	Nodo CBI	Rischi legati a blocchi del software a causa di Change gestito non correttamente	Alto	Alta	Alto
APP0000920	Gari Gold TFM	Rischi legati ad accesso indebito o divulgazione delle informazioni	Molto Alto	Media	Alto
APP0000526	AOG - Anagrafe Operativa Gruppo	Rischi legati a malware ed attacchi logici	Molto Alto	Alta	Alto
<b>PROPOSTE DI RISCHI ALTI DA VALIDARE DA PARTE DELLA COMMISSIONE RISORSE ICT TRASVERSALI</b>					
APP0000494	SAG - Swift Alliance Gateway	Rischi legati ad accesso indebito o divulgazione delle informazioni	Molto Alto	Alta	Alto
		Rischi legati a malware e attacchi logici	Molto Alto	Media	Alto

Tabella 8: Dettaglio Rischi Alti

Il dettaglio complessivo dell'Analisi Low Level per i 144 asset analizzati è consultabile nell'allegato 2.

### 6.2.3 Risultati complessivi

All'interno del presente paragrafo vengono illustrati i risultati delle valutazioni di rischio condotte sui singoli asset in perimetro. Al fine di comparare i risultati ottenuti dall'analisi Top Level sui settori del Consorzio e i risultati dell'analisi Low Level rilevati sui singoli asset ICT, è stata predisposta la seguente tabella che riporta la distribuzione dei rischi prospettici degli asset gestiti dal Settore e il rischio basato sullo storico dell'ultimo anno del Settore stesso:

	Top Level				Low Level					
Settore	Rischio informatico del Settore (KRI periodo 1 GEN-31 DIC 2016)	Numero Asset in Perimetro 2016	Numero Totale Asset Settore	%	Non Rilevante	Molto Basso	Basso	Medio	Alto	Molto Alto
Settore Architettura di Processi IT	Molto Basso	0	5	-	-	-	-	-	-	-
Settore Architettura di Sviluppo	Molto Basso	0	7	-	-	-	-	-	-	-
Settore Architettura Enterprise e Esecutiva	Molto Basso	2	11	18%	-	-	-	2	-	-
Settore Architettura Sistemi	Molto Basso	0	1	-	-	-	-	-	-	-
Settore Erogazione Applicativa Online	Molto Basso	1	2	50%	1	-	-	-	-	-
Settore Erogazione Applicativa Batch	Molto Basso	0	0	-	-	-	-	-	-	-
Settore Gestione del Cambiamento	Molto Basso	0	4	-	-	-	-	-	-	-
Settore Informatica Utente	Molto Basso	1	15	7%	-	-	-	1	-	-
Settore Sistemi Centrali	Basso	2	39	5%	2	-	-	-	-	-
Settore Sistemi di Rete	Medio	2	23	9%	-	-	1	1	-	-
Settore Sistemi Dipartimentali	Basso	11	28	39%	3	1	4	3	-	-
Settore Capacity e Ottimizzazione	Molto Basso	1	4	25%	-	-	1	-	-	-
Settore Monitoraggio e Automazione	Molto Basso	0	3	-	-	-	-	-	-	-
Settore Ingegneria di Sicurezza	Medio	2	7	29%	-	-	-	2	-	-
Settore Monitoraggio della Sicurezza IT	Medio	4	18	22%	-	-	-	4	-	-
Settore Bilancio	Basso	2	12	17%	-	-	2	-	-	-
Settore Conformità	Basso	5	20	25%	1	-	-	4	-	-
Settore Rischi	Molto Basso	5	31	16%	-	-	2	3	-	-
Settore Segnalazioni	Molto Basso	2	16	13%	-	-	-	2	-	-
Settore Controllo di Gestione e Reporting	Basso	1	21	5%	-	-	-	1	-	-
Settore Data Warehouse	Molto Basso	0	19	-	-	-	-	-	-	-
Settore Qualità dei Dati	Molto Basso	0	3	-	-	-	-	-	-	-
Settore Applicazioni Risorse Umane	Basso	2	16	13%	-	-	1	1	-	-
Settore Acquisti	Basso	0	14	-	-	-	-	-	-	-
Settore Risparmio Gestito	Medio	3	8	38%	-	-	1	2	-	-
Settore Bancassurance	Basso	0	13	-	-	-	-	-	-	-
Settore Incassi	Basso	7	11	64%	-	-	4	3	-	-
Settore Monetica	Basso	10	17	59%	-	-	1	9	-	-
Settore Pagamenti e Portafoglio	Medio	20	34	59%	-	-	5	11	4	-
Settore Contenzioso, Leasing e Factoring	Basso	2	13	15%	-	-	1	1	-	-
Settore Crediti Bancari	Basso	4	24	17%	-	-	-	4	-	-

	Top Level				Low Level					
Settore	Rischio informatico del Settore (KRI periodo 1 GEN-31 DIC 2016)	Numero Asset in Perimetro 2016	Numero Totale Asset Settore	%	Non Rilevante	Molto Basso	Basso	Medio	Alto	Molto Alto
Settore Credito al Consumo e Specializzato	Basso	10	26	38%	-	1	6	3	-	-
Settore Finanza Proprietaria	Medio	11	30	37%	-	-	3	8	-	-
Settore Finanza Titoli Amministrazione	Basso	1	11	9%	-	-	-	1	-	-
Settore Finanza Titoli Compravendita	Medio	3	8	38%	-	-	3	-	-	-
Settore Portali Interni	Basso	6	27	22%	1	-	2	3	-	-
Settore Sportello	Basso	3	29	10%	-	-	3	-	-	-
Settore Usabilità Applicazioni	Molto Basso	0	7	-	-	-	-	-	-	-
Settore Internet Banking	Basso	9	33	27%	-	-	5	4	-	-
Settore Portali Esterni	Basso	1	3	33%	-	-	-	1	-	-
Settore Anagrafe e Condizioni	Medio	1	11	9%	-	-	-	-	1	-
Settore Depositi ed Estero	Basso	10	47	21%	-	-	3	2	5	-

Tabella 9: distribuzione rischi Asset per Settore

#### 6.2.4 Analisi sui Sistemi di pagamento via Internet

In data 19 dicembre 2014 l'Autorità Bancaria Europea (EBA – European Banking Authority) ha emesso gli "Orientamenti finali sulla sicurezza dei pagamenti via internet" che sono frutto dall'elaborazione e implementazione delle raccomandazioni BCE del 31 gennaio 2013 e rappresentano "il documento a fronte del quale le banche centrali, nell'esercizio della propria funzione di sorveglianza sui sistemi e sugli strumenti di pagamento, valutano la conformità agli standard di sicurezza dei pagamenti via Internet".

Queste disposizioni sono state recepite e rese obbligatorie per il sistema Bancario italiano dalla Circolare 285/13 di Banca D'Italia nel suo 16° aggiornamento del 17 maggio 2016, con data di decorrenza dell'obbligo di conformità ai requisiti EBA al 30/09/16, e si applicano alle operazioni di pagamento effettuate tramite il canale Internet; in particolare, il perimetro di riferimento è il seguente:

- Esecuzione dei pagamenti con carta;
- Esecuzione di bonifici;
- Emissione o modifica di mandati elettronici di addebito diretto;
- Trasferimento di moneta elettronica tra due conti di moneta elettronica.

Nell'ambito delle attività di valutazione dei rischi informatici, si è tenuto conto di queste disposizioni ed è stata definita una check-list specifica, relativa a controlli ed eventi di rischio afferenti al perimetro dei Sistemi di Pagamento via internet.

Rispetto al totale di 144 asset in perimetro di analisi per l'anno 2016, gli asset che rientrano nei Sistemi di pagamento via internet sono 6. Si tratta di:

- APP0000823 - Internet Banking

- APP0000874 - E-Commerce
- APP0000921 - Tesoweb Enti Online
- APP0000946 - Large Corporate Banking
- APP0000947 - CBI - Paskey Aziende Online
- APP0001064 - Tribunali Online

Di conseguenza, per questi asset l'analisi ha comportato la verifica dei controlli specifici di cui sopra, oltre ovviamente ai controlli normali per la verifica dei rischi IT. I rischi emersi su questi asset, per gli scenari specifici applicabili ai sistemi di pagamento via internet, sono i seguenti:

- Per l'asset APP0000947 - CBI - Paskey Aziende Online risulta un rischio Medio sullo Scenario 16 (Rischi legati a malware ed attacchi logici). Questo rischio è stato rappresentato all'Utente Responsabile ed è stata definita la mitigazione più appropriata ai fini della riduzione del livello di rischio.
- Negli altri sei asset, sempre sullo Scenario 16, il livello di rischio rilevato è Basso per le APP0000155 e APP0001064 e Molto Basso per le rimanenti. Non sono previste azioni di mitigazione per questi rischi.

### 6.3 Assessment Sicurezza IT

L'Assessment condotto sulla Sicurezza IT ha avuto l'obiettivo di fornire una vista di insieme sui rischi associati alle principali minacce di sicurezza informatica a cui la Banca è esposta, fornendo al contempo una indicazione sulla robustezza del sistema dei controlli interni posti a mitigazione dei rischi stessi. La natura di tale assessment non intendeva essere esaustiva o di dettaglio in quanto ha privilegiato l'ottenimento di una panoramica complessiva in tempi particolarmente contenuti.

#### 6.3.1 Metodologia

La metodologia adottata per l'analisi dei rischi di sicurezza si compone di quattro fasi sequenziali che consentono di valutare il rischio associato alle minacce di sicurezza in funzione della relativa probabilità di accadimento e dell'impatto sulla Banca in termini di riservatezza, integrità e disponibilità.

- **Fase 1 - Individuazione scenari e minacce di sicurezza**

Gli scenari oggetto di analisi sono quattro, ognuno dei quali associato ad una o più minacce di sicurezza, a loro volta riconducibili ad un totale di 38 minacce di dettaglio. La tabella seguente fornisce l'elenco degli scenari e delle minacce di sicurezza per le quali è stato determinato il rischio associato.

Scenario <sup>26</sup>	Minaccia	Descrizione
Attacchi logici	Malware	Include le minacce legate a codice malevolo (viruses / worms, trojan horses / rootkits, botnet clients).

<sup>26</sup> Gli scenari "Incidenti di sicurezza fisica" e "Interruzione del business" sono stati valutati per completezza, sebbene non siano state previste analisi di approfondimento specifiche.



	<b>Hacking</b>	Include le minacce relative ad attacchi DoS, utilizzo di credenziali non autorizzato, scanning / intercettazione della rete, modifiche al sito web / al software / alle informazioni, furto di credenziali, etc.
	<b>Minacce sociali</b>	Include le minacce che utilizzano l'utente finale come veicolo per un attacco ai sistemi/informazioni (spoofing del sito, phishing, spam, etc.) e relative alla disclosure non autorizzata, accidentale o deliberate di informazioni aziendali.
	<b>Utilizzo improprio e/o errori</b>	Include le minacce relative ad utilizzo non autorizzato/non consone dei sistemi informatici, sottrazione di software/informazioni di business.
	<b>Errori e malfunzionamenti</b>	Include le minacce legate ad errore di utenti finali / staff tecnico, malfunzionamento HW / SW, effetti non desiderati derivanti da modifiche.
	<b>Incidenti di sicurezza fisica</b>	Include le minacce relative ad accessi fisici non autorizzati e furti/perdita di dispositivi.
	<b>Interruzione del business</b>	Include disastri naturali, danneggiamenti, interruzione di corrente / comunicazioni esterne.

Tabella 10: Scenari e minacce di sicurezza

#### • Fase 2 – Valutazione dei controlli

A ciascuna minaccia sono associati uno o più controlli, la cui adozione ed efficacia consentono di ridurre l'esposizione "inerente" alla minaccia per la Banca e pertanto la probabilità di accadimento della stessa. In funzione del relativo livello di attuazione sul perimetro della Banca, i controlli sono valutati secondo una scala a cinque valori: "in nessun caso"; "in pochi casi"; "in metà dei casi"; "nella maggior parte dei casi"; "in tutti i casi".

I controlli sono raggruppati in specifici domini di analisi (e.g. Security Governance, Access Management, Incident Management) e, in funzione della rilevanza che hanno all'interno di ciascun dominio, sono distinti in controlli chiave e controlli secondari.

La robustezza dei controlli associati alla singola minaccia è calcolata come somma pesata delle valutazioni dei controlli chiave (50%) e dei controlli secondari (50%).

#### • Fase 3 – Assessment delle minacce

Ciascuna minaccia è caratterizzata da un livello di esposizione «inerente» ed un impatto su riservatezza, integrità e disponibilità, entrambi calcolati sulla base di benchmark di settore. Inoltre, ai fini del calcolo del rischio, a ciascuna minaccia sono associati una probabilità di accadimento e un impatto complessivo della minaccia.

La probabilità di accadimento della minaccia è funzione dell'esposizione "inerente" della stessa e del livello di vulnerabilità determinato dalle eventuali carenze del sistema di controlli associato (calcolato come "complemento a 100" della robustezza dei controlli), secondo la matrice riportata di seguito.

Overall Vulnerability Rating	Very High	Low	Medium	High	Very High	Very High
		Very Low	Low	Medium	High	Very High
Overall Threat Rating	High	Very Low	Low	Medium	High	Very High
	Medium	Very Low	Low	Medium	Medium	High
	Low	Very Low	Low	Low	Low	Medium
	Very Low	Very Low	Very Low	Very Low	Very Low	Low

Figura 11 – Matrice per il calcolo della probabilità in funzione del livello di esposizione e di vulnerabilità

L'impatto complessivo della minaccia è calcolato considerando il *worst case* tra gli impatti su confidenzialità, integrità e disponibilità.

Come si evince dalla matrice, le dimensioni che caratterizzano le minacce (esposizione, vulnerabilità, probabilità e impatto) sono determinate su una scala a cinque valori: "Molto Alto"; "Alto"; "Medio"; "Basso"; "Molto Basso".

- **Fase 4 – Valutazione del rischio**

Il rischio associato a ciascuna minaccia è calcolato come combinazione dei fattori di probabilità di accadimento ed impatto associati, secondo la matrice riportata di seguito.

Business Impact Rating	Very High	Low	Medium	High	High	Very High
		Low	Low	Medium	High	High
Likelihood Rating	Medium	Very Low	Low	Medium	Medium	Medium
	Low	Very Low	Low	Low	Low	Medium
	Very Low	Very Low	Very Low	Very Low	Low	Low
		Very Low	Low	Medium	High	Very High

Figura 12 - Matrice per il calcolo del rischio in funzione di probabilità e impatto

Come si evince dalla matrice, il rating associato al rischio è determinato su una scala a cinque valori: "Molto Alto"; "Alto"; "Medio"; "Basso"; "Molto Basso".

### 6.3.2 Modalità di conduzione dell'analisi

Le analisi relative alla robustezza dei controlli in essere, finalizzate alla rilevazione del valore di vulnerabilità associato a ciascuna minaccia, sono state svolte in modalità self-assessment guidata, mediante il supporto di un questionario costruito sulla base di best practice e standard internazionali in ambito sicurezza (e.g. NIST, ISO27001, ISF). I controlli presenti nel questionario (circa 400) indirizzano i principali aspetti di sicurezza informatica e delle informazioni, fornendo uno strumento di analisi a 360°, e sono organizzati in 4 macro-domini (security governance, security requirements, security controls, security monitoring and improvement) e 26 domini di dettaglio (e.g. access management, incident management, network management, etc.).

In virtù dell'organizzazione della Banca e della distribuzione delle responsabilità di sicurezza tra il Consorzio e la Capogruppo, sono stati svolti incontri con il Responsabile del Servizio Sicurezza del Consorzio e con un referente del Servizio di Sicurezza Integrata della Capogruppo, al fine di rilevare lo stato di attuazione dei controlli identificati.

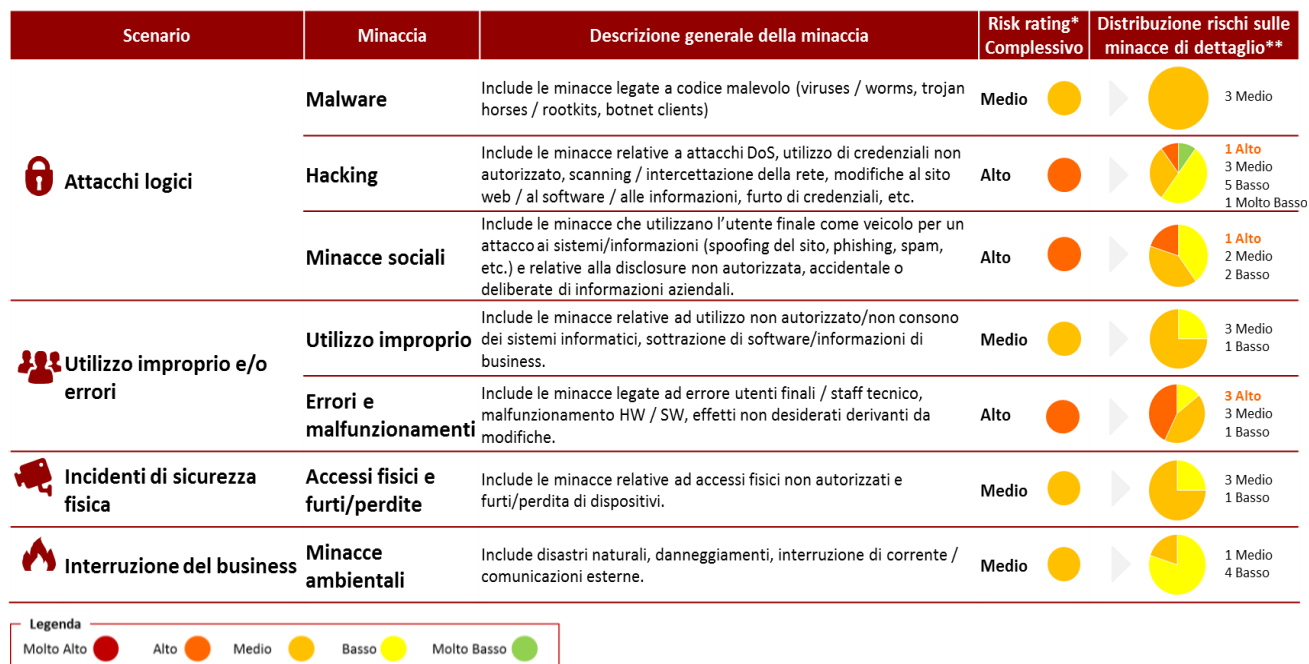
Sebbene l'ownership di alcuni controlli ricada sulla Capogruppo (e.g. governance, sicurezza fisica), il rischio associato agli scenari identificati per il Servizio Sicurezza del Consorzio ne risulta ugualmente influenzato, soprattutto in virtù delle ricadute che hanno sull'attuazione delle misure di sicurezza da parte del Consorzio. A titolo esemplificativo, una scarsa consapevolezza degli utenti finali, sebbene di responsabilità della Capogruppo, ha impatti significativi sul livello di rischio del Consorzio. In tal senso, considerando anche la natura di alto livello di tale assessment, si assume che il livello di rischio risultante sul Servizio Sicurezza sia in gran parte assimilabile al livello di rischio complessivo in materia di Sicurezza delle Informazioni per la Banca.

### *6.3.3 Risultati relativi al Servizio Sicurezza IT*

Dall'analisi effettuata, sia in termini di robustezza dei controlli, sia di rischi potenziali associati, emerge che la sicurezza informatica e delle informazioni è influenzata da gap strutturali accumulati negli anni precedenti. Tale situazione è più evidente in specifiche aree di rischio e, al netto delle iniziative a Piano e degli investimenti già deliberati, richiederà un periodo medio-lungo al fine di attuare l'insieme delle misure previste su tutto il perimetro della Banca. In particolare, considerando la complessità di attuazione di alcune misure correttive, sia in termini organizzativi che tecnologici e di processo, è necessario considerare tempistiche adeguate per mitigare sull'intera organizzazione i rischi emersi.

Nello specifico, dalle analisi effettuate emerge che i rischi valutati come "Alti" per la Banca sono riconducibili allo scenario di attacchi logici e allo scenario di utilizzo improprio e/o errori, con particolare riferimento agli errori potenzialmente effettuati dallo staff utente e tecnico durante l'operatività della Banca.

La tabella seguente illustra il livello di rischio associato a ciascuna minaccia di sicurezza, aggregato secondo la logica del *worst case* (un singolo rischio Alto comporta l'attribuzione del medesimo valore all'intera minaccia di sicurezza).



\* Calcolato considerando il valore massimo di rischio (worst case) riscontrato per le minacce sottostanti  
 \*\* Il dettaglio delle valutazioni per singola minaccia è riportato in Allegato

**Figura 13 – Rischi di sicurezza**

Le considerazioni in merito ai risultati ottenuti, le relative raccomandazioni e le azioni di mitigazione intraprese, sono descritte all'interno del paragrafo 6.4.3. Sicurezza IT

Si riporta di seguito il dettaglio dei risultati rilevati per ciascuno scenario di rischio.

### 6.3.3.1 Attacchi logici

I rischi afferenti allo scenario risultano essere **medio/alti** e sono riconducibili principalmente a vulnerabilità non completamente indirizzabili nel breve e medio periodo. Tra i principali fattori di rischio si evidenziano i seguenti:

- Possibilità di **accesso non autorizzato ai dati confidenziali/sensibili** da parte di **organizzazioni criminali esterne**, attraverso l'utilizzo di malware, tecniche di attacco avanzate (e.g. Advanced Persistent Threat) e/o altre tecniche che sfruttano vulnerabilità eventualmente presenti nei software proprietari e commerciali, aggravata da una potenziale difficoltà e/o mancata tempestività nell'individuazione delle compromissioni e ad una gestione migliorabile delle utenze privilegiate;
- **Diffusione involontaria/dolosa di informazioni sensibili/confidenziali** da parte degli **utenti interni**, dovuta principalmente a un non adeguato utilizzo dei dispositivi mobili personali (BYOD) e ad una scarsa percezione e controllo generale dei rischi di Cyber Security (assenza di formazione/awareness specifica), aggravata dall'assenza di un coinvolgimento diretto degli utenti nei processi di classificazione delle informazioni e conseguente applicazione delle misure di sicurezza opportune;

- Sensibile peggioramento dei **rischi associati ai servizi core verso la Clientela** (e.g. Retail e Corporate Banking) qualora l'iniziativa «Accesso Unico Clienti» dovesse subire rallentamenti e/o riduzioni degli ambiti di intervento.

#### **6.3.3.2 Utilizzo improprio e/o errori**

I rischi afferenti allo scenario risultano essere **medio/alti** e sono riconducibili principalmente a vulnerabilità non completamente indirizzabili nel breve e medio periodo. Tra i principali fattori di rischio si evidenziano i seguenti:

- **Modifiche non autorizzate ai privilegi di accesso**, dovute principalmente ad un non completo e granulare controllo delle credenziali amministrative / privilegiate, seppure inserite nel Piano strategico di sicurezza;
- Sensibile probabilità di **errori** da parte del **personale utente e tecnico**, dovuto alla carenza di processi di formazione, sensibilizzazione, codifica e conoscenza diffusa delle misure di sicurezza da applicare in funzione dei livelli di classificazione dei sistemi e degli asset informativi;
- **Malfunzionamenti o vulnerabilità** applicative dovute ad una mancata sistematicità delle procedure preventive di progettazione (e.g. requisiti/security by design), sviluppo sicuro, Change e testing di sicurezza, anche con riferimento alle attività esternalizzate (estensione misure di sicurezza alle terze parti);
- **Malfunzionamenti hardware**, dovuti ad una inerente elevata probabilità di failure dei sistemi / dispositivi di rete, nonostante risultino presenti le principali misure di mitigazione.

#### **6.3.3.3 Incidenti di sicurezza fisica**

I rischi afferenti allo scenario, sebbene non siano stati oggetto di analisi specifiche, risultano essere per lo più **medi**. Tra i principali fattori di rischio si evidenziano i seguenti:

- Possibilità di **accesso non autorizzato** ai dati confidenziali/sensibili presenti sotto forma di **documentazione cartacea**, dovuta ad un utilizzo assai limitato di misure di sicurezza specifiche (e.g. casseforti, distruggi-documenti);
- Possibilità di accesso non autorizzato a quantità significative di dati presenti su **dispositivi mobili** non adeguatamente protetti (e.g. chiavette USB) e/o non gestiti con la corretta sensibilizzazione da parte degli utenti.

#### **6.3.3.4 Interruzione del business**

I rischi afferenti allo scenario, sebbene non siano stati oggetto di analisi specifiche, risultano essere per lo più **bassi**. Tra i principali fattori di rischio si evidenzia:

- Interruzione del business, dovuta ad una **inerente** elevata probabilità di **danneggiamento dei servizi di comunicazione** (e.g. connessioni internet), con potenziali impatti anche sui servizi core verso Clientela, nonostante risultino presenti le principali misure di mitigazione.

### **6.4 Raccomandazioni e Conclusioni**

All'interno del presente capitolo sono descritte le raccomandazioni fornite dal Servizio IT Risk Management ai referenti dei Settori in perimetro di analisi.

#### 6.4.1 IT Risk Top Level

Le risultanze ottenute tramite l'alimentazione di KRI possono essere ritenute "oggettive", in quanto basate su dati registrati in riferimento agli eventi monitorati su ogni Settore oggetto di analisi, fornendo la situazione relativa all'ultimo anno passato del Consorzio Operativo di Gruppo.

In particolare, il Settore Anagrafe e Condizioni è classificato a rischio "Medio" a causa di valori elevati per quanto riguarda RFC in emergenza e numero di incident; Job, controllo accessi e BR in ritardo rilevano risultati riconducibili ad un valore qualitativo "Medio". Si suggerisce, pertanto, un maggiore presidio dei citati ambiti, in modo da tenere sotto controllo il livello di rischio complessivo del Settore.

Il Settore Sistemi di Rete presenta valore complessivo di rischio "medio" a seguito soprattutto di un valore molto elevato nel KRI incident. Ciò è dovuto alle caratteristiche di trasversalità del Settore nell'erogazione dei Servizi; per tale motivo a questi viene aperto un gran numero di incidenti. Tuttavia, si suggerisce di rivedere i criteri di assegnazione e soprattutto classificazione degli incidenti al Settore, in quanto, a seguito di analisi ed intervista con i relativi referenti, è emerso una non corretta apertura dei ticket (vedi anche raccomandazione di seguito su incident management).

Il Settore Pagamenti e Portafoglio rileva rischio complessivo "medio" generato dai KRI relativi ai BR in ritardo, incident e change sui dati in produzione. Per quanto riguarda i change sui dati in produzione il fenomeno è da attribuirsi ad interventi specifici richiesti ad inizio anno per esigenze di Business; l'indicatore è già in mitigazione in quanto i valori nel corso dell'anno risultano essere in diminuzione.

Si suggerisce inoltre di focalizzare l'attenzione sui progetti in corso in modo da chiudere i BR in carico nei tempi e ridurre il valore relativo dell'indicatore. Infine, si suggerisce un presidio forte sugli incidenti prestando attenzione alla corretta assegnazione e classificazione dei ticket, provvedendo a segnalare eventuali anomalie al gruppo preposto in Consorzio.

Il Settore Finanza Proprietaria presenta valori medi per quanto riguarda i KRI dei change in emergenza e dei BR in ritardo. In questo caso si suggerisce di seguire il processo di change standard aziendale provvedendo, laddove possibile, ad una pianificazione dei rilasci secondo calendario. E' comunque da tenere presente che, date le esigenze specifiche della Banca durante l'anno 2016, alcune operazioni in emergenza sono da considerarsi normali e sono del tutto giustificate soprattutto l'ambito Finanza. Per quanto riguarda i BR in ritardo, si suggerisce di controllare i progetti in carico in modo da rispettare le scadenze, soprattutto in caso di BR rilevanti o presenti nel piano esecutivo della Banca.

Il Settore Finanza Titoli Compravendita fa registrare rischio complessivo "medio" soprattutto a causa del KRI sui change in emergenza. Anche in questo caso, si suggerisce di seguire il processo di change standard aziendale provvedendo, laddove possibile, ad una pianificazione dei rilasci secondo calendario. E' comunque da tenere presente che, date le esigenze specifiche della Banca durante l'anno 2016, alcune operazioni in emergenza sono da considerarsi normali e sono del tutto giustificate soprattutto per l'ambito Finanza.

Infine, per il Settore Risparmio Gestito il valore finale "medio" è imputabile principalmente a change sui dati in produzione e RFC in emergenza. Anche in questo caso, date le esigenze della Banca nel corso del 2016, alcune operazioni sono del tutto giustificate. In ogni caso, si suggerisce di rispettare, laddove

possibile, il processo standard di change management, evitando al contempo interventi sui dati in produzione come richiesto dalla Direzione Generale del Consorzio.

Nella conduzione dell'analisi Top Level, tramite i 7 indicatori di rischio identificati, sono emerse anomalie di carattere generale riconducibili ad alcuni Processi IT del Consorzio. Tali anomalie sono state considerate nell'analisi dalla Funzione IT Risk Management, in accordo con la Funzione Rischi Operativi e Reputazionali e, laddove siano state identificate azioni puntuali di aggiustamento con il Responsabile di Settore, è stata eseguita la revisione del valore del singolo indicatore. Alla luce di questo, sono state avviate alcune azioni al fine di migliorare l'affidabilità dei dati che alimentano i KRI:

- *Incident Management*: il processo attuale di Incident Management e lo strumento utilizzato Remedy non consentono al momento una eventuale "riclassificazione" del livello di priorità di un incidente da parte della struttura che ha in carico l'incident, della "resolution category" o dell'asset associato come origine del problema. Inoltre, molti ticket, seppur correlati ad uno stesso incidente, non risultano essere correttamente aggregati all'interno dello strumento.

Per avviare un percorso che conduca alla mitigazione di queste ed altre criticità è stato redatto il BR 47753 "Studio fattibilità per estensione nuovo modello assistenza al GMPS" che, unitamente ad un percorso di awareness sull'impostazione corretta dei parametri in sede di censimento dell'incidente, dovrebbe portare ad una maggiore qualità dei dati. (data di completamento attesa 2Q 2017)

Si raccomanda inoltre una verifica periodica della qualità dei dati relativi ai ticket per poter fare gli eventuali aggiustamenti necessari in maniera tempestiva.

- *Change Management*: il processo attuale di Change management fa segnalare anomalie relative alla pianificazione dei rilasci dal momento che alcune richieste di modifiche non possono essere correttamente gestite e devono essere fatte come RFC di emergenza: questo dà indicazione di un rischio anche quando il Change è gestito con un presidio dei rischi adeguato. Inoltre, alcuni interventi specifici possono essere eseguiti, per loro natura, solo in ambiente di produzione e, dunque, presentano una rischiosità anche quando sono poste in essere tutte le misure di presidio possibili (ad es. intervento a filiali chiuse, etc.).

Per garantire un miglioramento nella gestione delle RFC, è stata recentemente acquistata la suite per il SDLC (Software Development Lifecycle) di HP, che prevede l'utilizzo in particolare di due strumenti: ALM (Application Lifecycle Management) per la verifica della bontà dei test effettuati nei vari ambienti, in ottemperanza allo standard di sviluppo DEV-OPS, e Service Manager per l'inserimento di RFC che, integrato strettamente con ALM, fornirebbe al Change Manager informazioni su livello della distribuzione, test effettuati e superati, congruenza delle versioni nei vari ambienti, utili alla decisione relativa all'approvazione o al respingimento della richiesta. (data di completamento attesa 2Q 2017)

Oltre a questo, sarebbe opportuno considerare l'introduzione di una nuova categoria di RFC che separi chiaramente il tema dell'urgenza o della attività non nelle finestre previste da quello del rischio potenziale collegato al Change.

- *IT Asset Management*: lo strumento utilizzato mostra alcuni limiti legati alla granularità degli asset censiti, che presentano una forte disomogeneità, e la necessità di rivedere alcuni dati attualmente



contenuti in APM<sup>27</sup>, aggiornando soprattutto le informazioni relative all'indicatore di rischio CA, per il Controllo Accessi. (data di completamento attesa 2Q 2017)

Si segnala un generale andamento virtuoso dei Settori, che presentano un forte trend discendente su molti KRI rispetto all'anno precedente: Job (-40%), Change sui dati (-48%), RFC di Emergenza (-76%) e BR in ritardo (-11%). Questo grazie ad una importante iniziativa manageriale, che ha posto come obiettivo la minimizzazione di questi indicatori, e grazie ad un impegno notevole delle strutture nel garantire il raggiungimento di questo obiettivo.

#### 6.4.2 IT Risk Low Level

Gli Asset che hanno fatto rilevare rischi "Alti" presentano le stesse vulnerabilità riassumibili in:

- Rischi legati a Change management;
- Rischi legati ad expertise del personale;
- Rischi legati ad accesso indebito o divulgazione delle informazioni;
- Rischi legati a malware ed attacchi logici;
- Rischi legati ad operatività del personale.

Tutti gli asset afferenti al Settore Depositi ed Estero fanno rilevare rischi riconducibili all'obsolescenza delle applicazioni e allo sviluppo custom, con conseguenti stratificazioni di software che rendono impegnativa l'evoluzione e possono provocare blocchi e degradi prestazionali soprattutto in fase di change. Ciò si rileva anche a causa della carenza di risorse IT con expertise approfondito e documentazione tecnica a supporto. Al fine di mitigare i rischi rilevati, è in corso uno studio di fattibilità su nuove soluzioni applicative al fine di adottare prodotti di mercato, valutando al contempo integrazioni di taluni servizi nei settoriali Italia. La data di completamento dello studio di fattibilità, concordata con il Servizio Commerciale Estero e Rete Estera, è Marzo 2017.

Gli asset "CBI" e "Nodo CBI" presentano un alto rischio di blocchi del software a causa del processo di Change Management non gestito correttamente. La raccomandazione è di integrare l'applicazione nel processo di Change management standard aziendale. Le attività per la mitigazione, concordate con il Servizio Internet Banking e Direct Marketing, si concluderanno entro Febbraio 2017.

L'asset "Gari Gold TFM" presenta rischio alto legato ad accesso indebito e divulgazione di informazioni causata da mancata integrazione con piattaforma IAM e utilizzo di utenze impersonali e password deboli, non rispettando gli standard aziendali in materia di gestione degli accessi logici. La raccomandazione è di formalizzare profili e regole di assegnazione delle utenze come previsto da standard aziendale e di rivedere periodicamente le utenze ed i profili abilitativi collegati, rispettando il principio del minimo privilegio. Le attività di mitigazione del rischio, concordate con il Servizio Liquidità Operativa, sono state avviate ed è previsto il completamento entro Giugno 2017.

---

<sup>27</sup> APM: Sistema di *inventory & asset management*



Infine, "AOG - Anagrafe Operativa Gruppo" presenta rischio alto di accesso indebito; la raccomandazione definita è di provvedere a eliminare le condizioni nel codice che consentono il "by-pass" dei controlli di sicurezza. La mitigazione concordata con il Servizio Anagrafe Generale ed Indagini è stata avviata ed è prevista in chiusura entro Marzo 2017.

Come si è visto, tutte le azioni di mitigazione sono state concordate e pianificate. Pertanto, la fase di mitigazione dei rischi può ritenersi avviata.

Inoltre, esiste una proposta di Rischio Alto per l'asset "SAG - Swift Alliance Gateway", poiché l'Utente Responsabile (la costituenda Commissione Risorse ICT trasversali) non ha ancora validato formalmente la proposta relativa agli Impatti sui vari scenari di rischio. Qualora questa fosse validata, l'asset rileverebbe un rischio alto di accesso indebito e attacchi logici. Per quanto riguarda il rischio di accesso indebito sarebbe necessario rivalutare le utenze tecniche ed applicative ed i privilegi ad esse assegnate, gestendo le stesse secondo standard aziendale. Inoltre, sarebbe opportuno definire ed assegnare chiaramente i ruoli e gli ambiti di intervento ai vari attori che partecipano al ciclo di vita dell'asset, secondo il principio della separazione dei compiti.

Per quanto riguarda il rischio legato a malware ed attacchi logici si dovrebbero implementare misure di protezione adeguate per gli utenti aventi privilegi amministrativi sulla piattaforma. Inoltre, come da comunicazione della Swift, sarebbe necessario installare l'ultima versione attualmente disponibile.

Le azioni di mitigazione, anche in assenza di decisioni sulla gestione del rischio da parte dell'Utente Responsabile, sono state avviate d'iniziativa da parte della Funzione ICT. La data di completamento attesa, per l'ultima delle azioni di mitigazione, è Dicembre 2017.

#### 6.4.3 Sicurezza IT

Si forniscono di seguito alcune raccomandazioni e punti di approfondimento da considerare nel breve periodo al fine di mitigare ulteriormente (oltre agli interventi già pianificati) il livello di rischio associato alle minacce considerate in ambito Sicurezza informatica.

Ambito	Descrizione soluzione
<b>Protezione delle informazioni confidenziali</b>	Valutazione di una soluzione per la protezione dei dati non strutturati con POC sul campo
	Survey sulle utenze privilegiate (es. domain admin, enterprise admin, etc.) e pilota per l'utilizzo di utenza anonima su CyberArk al posto di utenza personale privilegiata
	Adozione di Dromedary iMeeting per la condivisione sicura dei documenti del Board
<b>Monitoraggio delle minacce e gestione degli incidenti</b>	Formalizzazione ed enforcement del processo di gestione degli incidenti di sicurezza
	Produzione reportistica periodica su incidenti ed eventi di sicurezza
<b>Mitigazione vulnerabilità e minacce</b>	Formalizzazione contenuti per progetto per "Segregazione delle reti interne protette da Firewall", da avviare nel 2017

Ambito	Descrizione soluzione
	Scouting e analisi di fattibilità di prodotti di VA da acquisire e implementare nell'infrastruttura di sicurezza
	Revisione del processo/metodologia/testing di sviluppo sicuro del software per le applicazioni sviluppate internamente (nell'attualità e per il DevOps) e condivisione con le funzioni interessate
<b>Security awareness e training</b>	Definizione del piano di formazione per il personale tecnico e allocazione del budget
	Definizione e somministrazione sessioni di awareness per gli utenti COG in materia di Sicurezza delle Informazioni (es. Sicurezza Applicativa, standard architetturali per la sicurezza, etc.)
<b>Sicurezza delle terze parti</b>	Revisione clausole di sicurezza standard per indirizzare i rischi più elevati
	Introdurre il processo di classificazione dei fornitori anche secondo i parametri di sicurezza, a cui associare specifiche azioni per la mitigazione dei rischi IT
	Monitoraggio terze parti esistenti mediante servizio di Security Vendor Rating da applicare ai fornitori più critici
<b>Organizzazione della sicurezza</b>	Avvio progetto di revisione dell'impianto normativo di sicurezza
	Analisi organizzativa COG per definire attività e competenze richieste alla Sicurezza COG, con relativo piano di chiusura di eventuali gap
	Formalizzare il ruolo di CISO, assegnando responsabilità e poteri appropriati, in coerenza con le altre figure/funzioni già esistenti. Definire chiaramente attività e responsabilità di ASI e di Sicurezza IT in modo da garantire la corretta distribuzione tra le due funzioni
<b>Policy e Normative</b>	Policy e modello di classificazione degli asset (anche semplificato) funzionale a determinare la criticità di un asset (sia per la protezione che per monitoraggio/response)
	Definizione e somministrazione campagna di awareness per gli utenti finali in materia di Sicurezza delle Informazioni
	Policy strutturata per la sicurezza dei dispositivi mobili che consideri anche i device personali (BYOD)
	Policy MPS per la gestione dispositivi removibili

**Tabella 11 - Raccomandazioni**

Questo ulteriore set di azioni di mitigazione, unito agli interventi portati a termine e previsti all'interno del progetto "Monte più Sicuro" (redatto a seguito dell'assessment 2015) riconducono il rischio sulla Sicurezza Informatica al livello finale "Medio".



## Relazione Funzione Gestione Rischio Informatico – Anno 2016

### Approvazione documento

Unità Organizzativa	Referente	Data
Direzione Compliance e Antiriciclaggio	Stefano Delibra	01/02/17
Ufficio IT Risk Management	Stefano Aghini Lombardi	30/01/17

### Storia delle Versioni

N° Versione	Descrizione
1.0	Prima stesura

### Redattori

Unità organizzativa	
Ufficio IT Risk Management	Andrea Paoloni

## 1 Executive Summary

Il Rischio Informatico (di seguito “Rischio IT”) è a pieno titolo inserito tra i rischi operativi, reputazionali e strategici e, come tale, necessita di un adeguato presidio affinché situazioni contingenti o eventuali scenari di rischio siano adeguatamente verificati e mitigati. La stessa Circolare 285 di Banca d’Italia e il documento normativo di Capogruppo (1030D02045) definiscono modelli, ruoli e responsabilità per la corretta gestione del Rischio IT.

Il dominio di applicazione del Rischio IT è costituito da tutte le componenti hardware, software e di rete che compongono le soluzioni tecnologiche asservite al business della Banca.

A partire da quest’anno è stata implementata una nuova metodologia a livello di Gruppo che si basa sull’individuazione di alcuni indicatori (Key Risk Indicator) come segnali da tenere sotto controllo per avere una indicazione di tipo “Top Level” della situazione del Rischio IT, mentre attraverso un’analisi di dettaglio delle singole Funzionalità Applicative (analisi “Low level”) individua le criticità e le relative mitigazioni.

Relativamente ai ruoli, sono stati individuati: i) il *Servizio Rischi Operativi e Reputazionali della Capogruppo con compiti di indirizzo e coordinamento*; ii) l’*Ufficio IT Risk Management della Banca*, con compiti di definizione degli assets e degli scenari di rischio, di supporto alla Funzione IT nell’individuazione dei rischi, di definizione della proposta di mitigazione delle eventuali criticità e monitoraggio del livello di attuazione degli interventi; iii) l’*Utente Responsabile* con compiti valutazione degli scenari di rischio per gli assets di propria responsabilità, approvazione dei piani di mitigazione del rischio e accettazione del rischio residuo; iv) la Funzione IT di riferimento, che si occupa di fornire il quadro dei controlli e dei processi relativi alla gestione informatica della risorsa.

Per l’anno 2016 l’Ufficio IT Risk Management ha effettuato l’analisi delle sole Funzionalità Applicative erogate dal sistema di Front-End, ovvero quello sviluppato e gestito in autonomia dalla banca, ivi compresi i servizi acquisiti in outsourcing.

La Funzione IT Risk Management del Consorzio, considerando che il sistema di Back-End di Widiba per questi aspetti è analogo a quello di Banca MPS, ha svolto l’analisi di questa componente, non rilevando alcun rischio sopra soglia per quelle applicazioni di specifico interesse di Banca Widiba, il cui dettaglio verrà presentato al CDA della Capogruppo.

L’analisi *Top Level* ha mostrato che tutti gli indicatori rimangono all’interno delle soglie di attenzione e complessivamente il rischio si attesta ad un valore “Basso”.

Si evidenzia che, su tutta la piattaforma, compresi anche i 225 progetti rilasciati durante l’anno, si sono rilevati solo 25 incidenti totali, tra impatti alti, medi e bassi, in prevalenza riferibili ai servizi prestati dagli outsourcers, a cui sono imputabili tutti gli incidenti di gravità alta. Gli incidenti sono stati sempre risolti in tempi molto rapidi e nel rispetto degli SLA di servizio, hanno provocato disservizi molto lievi alla clientela impattata, comunque molto limitata.

Ai fini dell’analisi *Low Level* sono state individuate dieci componenti, di cui quattro Funzionalità Applicative e sei Applicazioni, tutte assegnate a quattro Utenti responsabili. La differenza tra Funzionalità Applicative e Applicazioni generalmente non è percepita dagli utenti, mentre a livello tecnologico si sostanzia negli aspetti realizzativi, le prime fanno parte di una sola applicazione, le seconde costituiscono da sole vere e proprie applicazioni.

Le risultanze dell'analisi *Low Level* hanno evidenziato la presenza di alcuni rischi con livello massimo pari a "Medio" per quattro Funzionalità Applicative e due delle sei applicazioni, riferiti agli scenari di compromissione dell'integrità dei dati, accesso indebito dall'interno e attacco dall'esterno, mentre le restanti quattro Applicazioni hanno riportato un livello "Basso/Molto Basso".

Tali valori di rischio si mantengono al di sotto della soglia di propensione al rischio definita nel RAF – Risk Appetite Framework dal Gruppo MPS e non richiedono, secondo la policy, lo sviluppo e l'attivazione di interventi specifici di mitigazione sul singolo gap.

Ciò non toglie, tuttavia, che verranno comunque attivate alcune attività di mitigazione ritenute opportune per rafforzare la tutela del patrimonio dei clienti e dell'immagine della Banca. Inoltre, si raccomanda di mantenere un forte coinvolgimento della funzione IT Risk Management nel presidio di nuove progettualità e la necessità di un continuo monitoraggio degli indicatori di rischio e dei relativi scenari.

Nell'ambito delle analisi svolte sono stati considerati e valutati gli esiti degli interventi di Ethical Hacking svolti dalla Funzione di Revisione Interna di BMPS e le criticità rilevate, alcune delle quali immediatamente risolte dalla funzione IT, altre con risoluzione pianificata entro il primo trimestre 2017.

## 2 Generalità

Il sistema informativo rappresenta uno strumento fondamentale per il conseguimento degli obiettivi strategici e operativi delle Banche, in considerazione del valore delle informazioni gestite e della criticità dei processi aziendali che dipendono da esso. Per tale motivo, Banca d'Italia ha ritenuto necessario emanare una disciplina organica in materia di sviluppo e gestione del Sistema informativo, esposta all'interno del Titolo IV, Capitolo 4, XI Aggiornamento del 21 Luglio 2015 della Circolare 285/2013.

Tra i dettami emanati vi è l'adozione di un modello organizzativo e di un processo strutturato per la gestione del rischio informatico, finalizzato ad identificare, valutare, trattare, documentare e monitorare i rischi connessi all'utilizzo delle tecnologie informatiche. E', infatti, richiesto che siano forniti agli Organi Decisionali e alle Funzioni aziendali preposte, gli elementi di giudizio necessari per il governo del rischio informatico, coerentemente con i principi, le politiche e le linee guida adottate per la determinazione della propensione al rischio a livello di Gruppo (Risk Appetite Framework, RAF).

Nel corso del 2016, il Gruppo Montepaschi (di seguito anche il "Gruppo MPS" o "Gruppo") ha avviato un progetto di affinamento della metodologia di IT Risk Management, basata su *best practice* di mercato, al fine di rendere l'analisi e la gestione del rischio informatico maggiormente strutturata e atta a garantire miglior organicità delle rilevazioni sul sistema informativo aziendale, nel rispetto dei dettami normativi.

L'impostazione metodologica è definita dalla Direttiva di Gruppo in materia di Gestione del Rischio Informatico (documento 1030D02045) ed è stata effettuata dall'Ufficio IT Risk Management di Banca Widiba all'interno del perimetro di riferimento per l'anno in corso, rappresentato dalle applicazioni di esclusiva competenza di Banca Widiba, escludendo di conseguenza tutte le applicazioni gestite dal Consorzio Operativo Gruppo MPS (di seguito "COG").

## 3 Metodologia

Il presidio delle normative vigenti, sia istituzionali che interne ha garantito nel corso del 2016 la revisione della metodologia impostata nell'anno precedente, di conseguenza si è confermato il ruolo dell'Area Risk Management (Servizio Rischi Operativi e Reputazionali) come funzione di indirizzo, coordinamento, e controllo di tutta la tematica e oltre al presidio del processo di gestione del rischio informatico. Per raggiungere la conformità con la normativa vigente (cfr. Circolare B.I. 285) è stato costituito all'interno di Banca Widiba l'Ufficio IT Risk Management.

Inoltre si sono rivisti i processi di analisi e di determinazione del valore del rischio a seconda dei vari scenari di accadimento.

### 3.1 Analisi Top Level

Come già anticipato nei precedenti capitoli, ai fini della valutazione complessiva della situazione di rischio del sistema informativo di Gruppo, è stato eseguito un assessment basato sulla misurazione di indicatori di rischio (Key Risk Indicator - KRI), così come anche suggerito dagli standard internazionali in ambito rischio informatico (ISO27005, COBIT5 for Risk), che prevedono il ricorso alla valutazione dei KRI per graduare l'effort della valutazione del rischio informatico.

Per la valutazione Top Level del rischio informatico sono stati arricchiti i *Key Risk Indicator* (KRI) dell'anno scorso, variandone le modalità di calcolo, e a cui ne sono stati aggiunti di nuovi, tutti rilevati a livello di Banca Widiba:

ID	KRI	Rilevanza	Peso %	Alimentazione
PRJ	Percentuale di progetti conclusi in ritardo rispetto al totale dei rilasciati nel periodo in esame	Media	15	Direzione IT e Innovazione Digitale
GAP	Somma pesata dei rilievi attivi, emessi dalle Funzioni di Controllo su asset IT, alla data della rilevazione e censiti su RIGAM	Media	15	Sono considerati i gap sugli Asset ICT "attivi" alla data, ovvero i gap ancora non sanati
RFC	Numero di Fix richiesta dalla banca pesati rispetto al numero dei change rilasciati	Media	15	Direzione IT e Innovazione Digitale
CA	Numero di applicazioni non collegate al controllo accessi centralizzato e/o privi di sistema SSO	Bassa	5	Direzione IT e Innovazione Digitale
INC	Somma pesata per priorità e per tempo di risoluzione degli incidenti IT in rapporto agli asset	Molto Alta	30	Direzione IT e Innovazione Digitale
FR	% di clienti che hanno subito perdite a seguito di transazioni fraudolente	Alta	20	Direzione IT e Innovazione Digitale

Tabella 3: Indicatori di rischio valutati

A ciascun KRI è stato assegnato un grado di rilevanza su scala qualitativa, associato ad un peso percentuale, tenendo conto dell'affidabilità dei dati che alimentano la metrica e dell'importanza dell'indicatore nella rappresentazione del livello di rischio informatico.

I sei KRI sopra elencati consentono il monitoraggio delle seguenti dimensioni di analisi:

- la capacità dell'ICT nell'evadere le richieste del Business tramite progetti, nei tempi previsti;
- il grado di allineamento dell'ICT alle best practice di settore e ai dettami normativi sia interni che esterni;



- i livelli di disponibilità e affidabilità degli Asset ICT;
- i livelli di sicurezza delle applicazioni ICT.

Un periodico processo di revisione manterrà tali KRI adeguati alle specifiche esigenze di Banca Widiba nel corso degli anni.

### 3.2 Analisi Low level

Annualmente l'Ufficio IT Risk Management in accordo con il Servizio Rischi Operativi e Reputazionali definiscono il catalogo dei rischi, ovvero l'insieme di scenari, eventi, vulnerabilità e controlli che devono essere valutati per l'assessment. Per l'anno 2016, gli scenari di rischio analizzati sono i seguenti:

Scenari di rischio
Rischi legati a <b>carenze di expertise</b> o abilità delle risorse IT nel supporto all'operatività dei sistemi
Rischi legati all' <b>errata esecuzione</b> di operazioni da parte di personale interno
Rischi legati ai <b>fornitori</b>
Rischi legati ad <b>anomalie o degrado</b> dell'asset <b>a causa di Change</b> gestito non correttamente
Rischi legati ad <b>anomalie o degrado</b> del asset in <b>produzione</b>
Rischi legati a <b>blocchi</b> dell'asset <b>a causa di Change</b> gestito non correttamente
Rischi legati ad <b>anomalie o degrado</b> dell'asset in <b>produzione</b>
Rischi legati a <b>blocchi</b> dell'asset <b>a causa di Change</b> gestito non correttamente
Rischi legati a <b>blocchi</b> dell'asset in <b>produzione</b>
Rischi legati a <b>danneggiamento o perdita</b> delle informazioni a causa di <b>eventi accidentali</b>
Rischi legati a <b>danneggiamento o perdita delle</b> informazioni a causa di <b>intenti malevoli</b>
Rischi legati ad <b>accesso indebito o divulgazione</b> delle informazioni
Rischi legati a <b>furto o smarrimento</b> di <b>apparati mobili</b> contenenti informazioni riservate
Rischi legati a <b>malware ed attacchi logici</b>

Tabella 6: elenco degli scenari di rischio 2016

Agli scenari di rischio sono legati gli eventi di rischio a cui si agganciano a loro volta i controlli (misure di protezione esistenti sull'asset).

I referenti IT valutano la probabilità degli eventi di rischio.

Le probabilità sono valutate secondo una scala qualitativa ("Molto Alta", "Alta", "Media", "Bassa", "Molto Bassa").

L'analisi di dettaglio sugli asset nel perimetro 2016 è stata eseguita valutando la probabilità di accadimento degli eventi di rischio in funzione della presenza o meno di controlli a presidio dell'asset. Le probabilità associate sugli scenari di rischio sono state incrociate con gli impatti stimati dagli Utenti Responsabili delle risorse ICT esaminate e da tale incrocio è stato identificato il valore di rischio potenziale, come rappresentato dalla matrice seguente:



Per il 2016 la soglia di propensione fissata dal Gruppo MPS è pari al livello di rischio “Medio”, ultimo livello che non richiede interventi di mitigazione.

Per ciascun asset coinvolto nel perimetro sono stati completati, tramite interviste:

- Un questionario al Responsabile dell'asset (IT Risk Owner), che, in base all'applicabilità degli eventi di rischio alla risorsa in esame ha valutato probabilità di accadimento degli eventi in base alla presenza o all'assenza dei controlli, considerando anche le serie storiche a disposizione su malfunzionamenti e incidenti di sicurezza;
- Un questionario di 7 quesiti di Business, collegati agli scenari di rischio, di cui l'Utente Responsabile ha stimato il livello di impatto.

### 3.3 Ruoli e Responsabilità

La metodologia di IT Risk Management<sup>28</sup> prevede i seguenti ruoli e responsabilità in riferimento alla conduzione dell'analisi del rischio informatico:

- *Servizio Rischi Operativi e Reputazionali della Capogruppo*: è informato circa l'esito della raccolta dei dati, approva le scale ed i razionali metodologici per la misurazione dei KRI ed è informato circa l'esito dei risultati di rischio; presidia le attività di analisi e trattamento del rischio informatico, verificandone la coerenza con la metodologia definita; definisce le modalità di integrazione dei risultati dell'analisi del rischio informatico all'interno del framework dei Rischi Operativi, in particolare considerando le fasi di Assessment, Analisi di scenario e definizione del Piano di Gestione dei Rischi Operativi; presidia le attività di monitoraggio del rischio informatico complessivo, verificando la correttezza, accuratezza e tempestività dei flussi informativi predisposti dalla Funzione IT Risk Management e validando la reportistica prodotta.
- *Servizio IT Risk Management*: si occupa della raccolta dei dati per l'alimentazione degli indicatori di rischio, di rappresentare i rischi per Unità Organizzativa e di individuare la proposta di risk mitigation sotto forma di raccomandazioni; definisce in accordo con la Funzione Rischi Operativi e Reputazionali il perimetro ed il piano annuale di analisi; definisce il catalogo dei rischi informatici, degli eventi di rischio IT e degli indicatori ritenuti utili al monitoraggio della situazione di rischio informatico complessivo del Gruppo nel continuo; supporta la Funzione ICT nell'esecuzione dell'auto-valutazione della probabilità di accadimento degli eventi di Rischio innescati da contromisure non soddisfacenti sull'Asset; richiede, nel caso in cui lo ritenga necessario, un confronto con i referenti delle funzioni interessate, laddove la valutazione delle probabilità eseguita dalla Funzione ICT non risulti coerente con la valutazione dei controlli sull'asset o con eventuali gap, rilievi delle funzioni di controllo e risultati assessment di sicurezza condotti, per proporre un valore di probabilità maggiormente coerente con le evidenze emerse; se necessario, inoltre, può eseguire escalation verso il Direttore Generale affinché ne valuti il valore di probabilità più coerente; coordina e svolge le attività di analisi del rischio informatico, determinando il rischio informatico potenziale e residuo sulle risorse ICT in perimetro; definisce, in collaborazione con la Funzione ICT la proposta di trattamento del rischio informatico sulle risorse ICT analizzate; predispone idonei flussi informativi a supporto della Funzione Rischi Operativi e Reputazionali per

---

<sup>28</sup> Cfr documento 1030D02045 - Direttiva di Gruppo in materia di Gestione del Rischio Informatico.

la valutazione della complessiva situazione del rischio informatico; produce con cadenza almeno annuale il Rapporto sulla situazione del rischio informatico.

- **Utente Responsabile:** Partecipa al processo di valutazione del rischio informatico relativo alle risorse informatiche ed ai servizi applicativi nel proprio perimetro di responsabilità, valutando gli impatti associati ai differenti scenari di rischio informatico; supporta l'identificazione delle misure di tipo tecnico, organizzativo o procedurale, per la mitigazione del rischio rilevato; approva i piani di trattamento del rischio, con gli interventi di mitigazione di tipo tecnico, organizzativo o procedurale, e le relative tempistiche di realizzazione; accetta formalmente, per le risorse informatiche di competenza, il rischio residuo valutato attraverso l'attività di analisi del rischio; sponsorizza, anche mediante il ricorso alla propria linea gerarchica, i piani di trattamento del rischio che interessano il proprio perimetro di responsabilità, contribuendo ad assicurare i necessari stanziamenti di budget a copertura degli interventi previsti.
- **Funzione ICT:** offrono supporto nella raccolta dei dati per l'alimentazione degli indicatori di rischio; eseguono l'autovalutazione delle probabilità di accadimento degli eventi di Rischio innescati da contromisure non soddisfacenti sull'Asset; supportano il processo di analisi e trattamento del rischio informatico in tutte le sue fasi per quanto di competenza; implementano e verifica le misure di attenuazione tecniche sulle risorse informatiche all'interno del proprio perimetro e supporta l'identificazione e la valutazione delle eventuali ulteriori misure da applicare.

## 4 Perimetro di analisi

Il perimetro di analisi del rischio informatico per la valutazione Top Level è stato identificato nelle applicazioni che costituiscono il sistema di Front-End di Banca Widiba, ivi compresi i servizi acquisiti in outsourcing. Per il sistema di Back-End l'analisi è svolta dal Consorzio Operativo che produce un analogo documento.

Le applicazioni sono quindi le seguenti:

Nome asset	Tipo	Utente Responsabile	Referente IT
Portale interno	Funzionalità Applicativa	Fabio Ferri	Ufficio Sviluppo e Sistemi
CRM	Applicazione	Fabio Ferri	Full outsourcing a Microsoft
Portale consulenti finanziari	Funzionalità Applicativa	Massimo Giacomelli	Ufficio Sviluppo e Sistemi
Sito internet della Banca	Funzionalità Applicativa	Marco Marazia	Ufficio Sviluppo e Sistemi
PEC	Applicazione	Marco Marazia	Ufficio Sviluppo e Sistemi
SMS e OTP	Funzionalità Applicativa	Marco Marazia	Ufficio Sviluppo e Sistemi
MoviPay	Applicazione	Marco Marazia	Ufficio Sviluppo e Sistemi
Infoprovder	Applicazione	Marco Marazia	Ufficio Sviluppo e Sistemi
Prodotti Office	Applicazione	Daniela Pivato	Ufficio Sviluppo e Sistemi
Posta	Applicazione	Daniela Pivato	Ufficio Sviluppo e Sistemi

Tabella 2: Elenco delle applicazioni in perimetro

## 5 Risultati Analisi del Rischio

Il rischio informatico è definito nella sua più ampia accezione, dalla Circolare di Banca d'Italia 285 del 17 dicembre 2013 e suoi aggiornamenti, 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). 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".

Un rischio può concretizzarsi attraverso un evento specifico che si manifesta attraverso un malfunzionamento delle infrastrutture IT o degli applicativi, un errore nella conduzione dei processi IT o una violazione nei sistemi di sicurezza della Banca.

A seconda della tipologia di evento che si concretizza possono verificarsi effetti sia sulla componente di funzionamento (sistema informativo a supporto del Business) sia sulla componente strategico-evolutiva (disallineamento dalle aspettative del Business).

### 5.1 Analisi Top Level

#### 5.1.1 Risultati analisi top level

Dall'analisi top level risulta un livello di rischio "Basso" e non si evidenziano situazioni critiche in quanto tutti gli indicatori rimangono all'interno delle soglie di attenzione.

Solo una delle applicazioni sottoposte ad analisi non è integrata con il controllo accessi centralizzato (CRM) ma le utenze dell'applicativo sono comunque gestite centralmente dal servizio Gestione Utenti Widiba. La situazione è comunque temporanea in quanto è già previsto il passaggio al SSO (Single Sign On).

Il numero totale di incidenti rilevato durante l'anno è pari a 25, tra impatti alti, medi e bassi e denota una infrastruttura solida ed in grado di garantire un adeguato livello di servizio. Tali incidenti sono in prevalenza riferibili ai servizi prestati dagli outsourcers (Ubiquity, Consorzio Operativo GMPS, Infocert), a cui sono imputabili tutti gli incidenti di gravità alta. Gli incidenti sempre sono stati sempre risolti in tempi molto rapidi e nel rispetto degli SLA di servizio, hanno provocato disservizi molto lievi ad un numero molto ristretto di clienti.

Non si evincono particolari problemi sui tempi di rilascio con 90% dei progetti rilasciati in tempo utile.

Sul lato GAP si nota che il valore del relativo KRI è interamente dovuto all'ultimo Ethical Hacking, effettuato dalla Funzione audit, le cui mitigazioni sono in fase di risoluzione.

Un solo cliente risulta essere stato vittima di una frode internet nel corso del 2016, per un totale di 1.750 euro, ma per cause non imputabili alla banca che pertanto non ha provveduto al rimborso degli importi frodati.

KRI	Risultato	Metodo	Rischio	Interventi
PRJ	10%	Percentuale di progetti conclusi in ritardo rispetto al totale dei rilasciati nel periodo in esame	Molto Basso	

KRI	Risultato	Metodo	Rischio	Interventi
<b>GAP</b>	54	Somma pesata dei rilievi attivi, emessi dalle Funzioni di Controllo su asset IT, alla data della rilevazione e censiti su RIGAM	Medio	Sono in corso alcuni interventi di mitigazione che si concluderanno entro il primo trimestre del 2017
<b>RFC</b>	<10%	Numero di Fix richiesta dalla banca pesati rispetto al numero dei change rilasciati	Molto Basso	
<b>CA</b>	1	Numero di applicazioni non collegate al controllo accessi centralizzato e/o privi di sistema SSO	Molto Basso	
<b>INC</b>	10	Somma pesata per priorità degli incidenti IT in rapporto agli asset	Basso	
<b>FR (*)</b>	0,0007%	% di clienti che hanno subito perdite a seguito di transazioni fraudolente	Molto Basso	

(\*) Il caso si riferisce ad un cliente che è rimasto vittima di una frode a causa di comportamenti impropri nella custodia delle credenziali ed in violazione degli obblighi contrattuali sottoscritti

## 5.2 Analisi low level

### 5.2.1 Risultati analisi low level

All'interno del presente paragrafo vengono illustrati i risultati delle valutazioni di rischio condotte sui singoli asset in perimetro che hanno rilevato un rischio almeno Medio.

Nome Asset	Descrizione Scenario	Rischio Max Scenario
<b>Portale interno (Widitools)</b>	Compromissione dell'integrità dei dati	Medio
	Accesso indebito dall'interno	Medio
	Attacco dall'esterno	Medio
<b>Portale consulenti finanziari (valigetta)</b>	Compromissione dell'integrità dei dati	Medio
	Accesso indebito dall'interno	Medio
	Attacco dall'esterno	Medio
<b>Sito internet della Banca</b>	Compromissione dell'integrità dei dati	Medio
	Accesso indebito dall'interno	Medio
	Attacco dall'esterno	Medio

Nome Asset	Descrizione Scenario	Rischio Max Scenario
PEC	Compromissione dell'integrità dei dati	Medio
	Attacco dall'esterno	Medio
SMS e OTP	Compromissione dell'integrità dei dati	Medio
	Attacco dall'esterno	Medio
Infopvider	Compromissione dell'integrità dei dati	Medio

**Tabella 8: Dettaglio Rischi**

Tutte le altre applicazioni hanno rilevato soltanto rischi “Basso” o “Molto basso”.

Dall’analisi effettuata nessun asset nel perimetro risulta avere un rischio maggiore della soglia di propensione al rischio fissata per l’anno 2016. Tale risultato può essere facilmente compreso in quanto le Funzionalità Applicative, che costituiscono il “core” del Front-End fanno parte di un unico framework in completa gestione della Direzione IT e Innovazione Digitale, che gode di approfondite attenzioni da parte di tutti gli organi aziendali e le Applicazioni sono di fornitori specializzati altamente qualificati di riferimento nel mercato.

Caratteristica comune di tutte le Funzionalità Applicative è la marginale esistenza dei rischi dovuti a cancellazione/modifica dei dati da parte di personale autorizzato, sia per eventi incidentali, sia con scopi malevoli. La mitigazione di questi rischi è affidata a soluzioni di back-up dei dati, segregazione della rete e tracciatura delle operazioni nel rispetto delle prescrizioni della normativa vigente sia interna che istituzionale.

### 5.3 Assessment Sicurezza IT

Nel corso del 2016, allo scopo di consolidare l’infrastruttura software e hardware della Banca sono state effettuate diverse sessioni di Penetration Test e Vulnerability Assessment al fine di individuare e risolvere eventuali criticità. Tali attività sono state commissionate a società esterne ed hanno interessato tutta la componente di Front-End, sia a livello applicativo, sia a livello infrastrutturale.

Sono state riscontrate alcune anomalie e sono state suddivise in due categorie principali in base alla loro criticità: Alta/Media, Bassa. Le criticità appartenenti alla prima categoria hanno avuto un immediato sviluppo delle necessarie contromisure, invece, le criticità appartenenti alla seconda categoria sono state attualizzate nel modello operativo della banca e, in alcuni casi considerato il basso impatto, sono state ricondotte ad una assunzione del rischio da parte della Direzione, mentre per altri si è proceduto allo sviluppo e all’attivazione della relativa mitigazione. È previsto che tutte le mitigazioni saranno completate al più tardi entro il 31/3/2017.

L’esecuzione periodica di suddette attività è una “best practices” nel ciclo di vita di sviluppo del software e di conseguenza verranno replicate anche nel 2017.

### 5.4 Piano di attività 2017

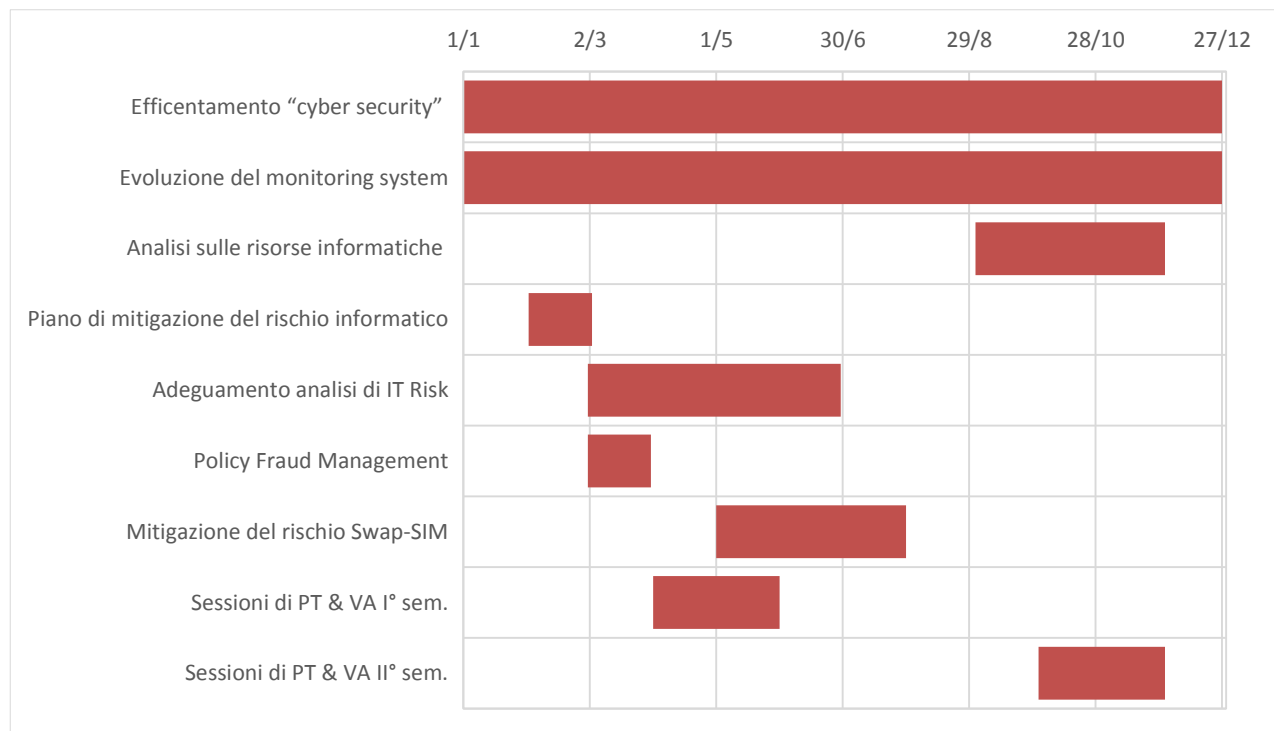
Nel corso dell’anno sono state svolte le principali attività programmate l’anno scorso per la messa a regime del processo di gestione del rischio informatico.

Le attività previste per il 2017, oltre alla continua evoluzione e monitoraggio (KRI) del piano di mitigazione del rischio informatico sono:

- proseguimento delle analisi sulle risorse informatiche in produzione estendendo l'analisi a tutte le risorse della banca
- predisposizione del piano di mitigazione del rischio informatico, alimentato dagli interventi di mitigazione di tipo tecnologico, organizzativo o procedurale, approvati dagli Utenti Responsabili;
- adeguamento e sviluppo delle pratiche di analisi di IT Risk per banca Widiba.

Saranno, inoltre, condotte le seguenti attività cross:

- Definizione di una Policy aziendale per il Fraud Management che fornisca le linee guida per ogni prodotto/servizio offerto dalla Banca alla propria clientela;
- ulteriore efficientamento dei processi "cyber security" (monitoraggio antifrode, monitoraggio uscite, processi sicurezza, alert comportamentali);
- continua evoluzione del monitoring system (attivo in produzione ed attualmente copre due funzioni: monitoraggio sistemi e monitoraggio funzioni);
- sperimentazione di una funzionalità per la mitigazione del rischio di appropriazione indebita di un numero di cellulare (Swap-SIM) con l'operatore telefonico TIM;
- sessioni periodiche di penetration test e vulnerability assessment.





### **5.5 Conclusioni**

I valori del Rischio IT rilevati dall'analisi relativa all'anno 2016 risultano nel complesso di valore "BASSO" e si mantengono al di sotto della soglia di tolleranza definita nel RAF (Risk Appetite Framework) dal Gruppo MPS.

Non richiedono, pertanto, lo sviluppo e l'attivazione di interventi specifici di mitigazione da parte di Widiba, fermo restando che verranno attivate nel 2017 una serie di azioni di mitigazione ritenute opportune per rafforzare la tutela del patrimonio dei clienti e dell'immagine della Banca e si raccomanda di un mantenere un forte coinvolgimento della funzione IT Risk Management nel presidio di nuove progettualità e di assicurare un continuo monitoraggio degli indicatori di rischio e dei relativi scenari.