Rapporto sintetico sulla situazione del Rischio Informatico
Anno 2016

Direzione Chief Risk Officer

GRUPPO**MONTEPASCHI**

MONTE DEI PASCHI DI SIENA
BANCA DAL 1472

Il rischio informatico e le disposizioni di vigilanza

- ✓ 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.

- ✓ La Circolare di Banca d'Italia **n. 285/2013** 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)**.

- ✓ Con cadenza almeno annuale viene predisposta una **Relazione** che descrive le risultanze delle analisi ed il trattamento del rischio informatico, 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 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 di Gruppo in materia di Gestione del Rischio Informatico (D1030D02045)

  - la **"Relazione sul Rischio Informatico del Consorzio Operativo di Gruppo – Anno 2016"**, predisposta dal Servizio IT Risk Management del COG *, è stata **approvata dal Comitato dei Consorziati del Consorzio Operativo di Gruppo in data 7 marzo 2017**
  - la **"Relazione sul Rischio Informatico di Banca Widiba – Anno 2016"**, predisposta dall'Ufficio IT Risk Management di Widiba *, è stata **approvata dal CdA di Banca Widiba in data 8 febbraio 2017**.

(*) Struttura che riporta funzionalmente al Servizio Rischi Operativi e Reputazionali di Capogruppo.

Metodologia di analisi del rischio informatico

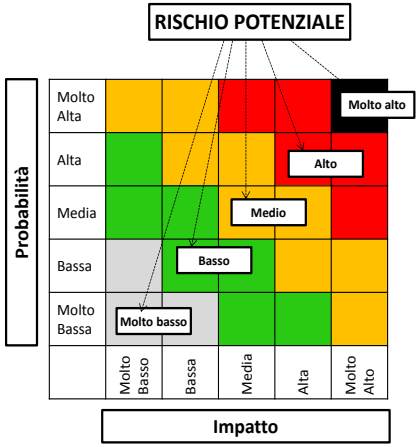
L'impostazione metodologica definita dalla Direttiva di Gruppo in materia di Gestione del Rischio Informatico (documento 1030D02045) prevede la conduzione in parallelo di **due tipologie di analisi**:

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.

		MPS CONSORZIO OPERATIVO GRUPPOMONTEPASCHI		widiba	
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%

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 scenari 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**.

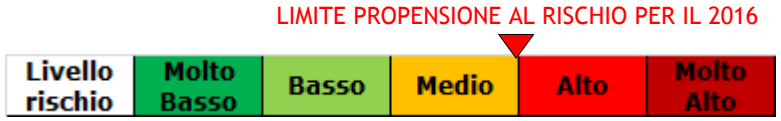
Il livello di rischio è valutato come combinazione tra la probabilità di accadimento degli scenari di rischio e il loro impatto, entrambi espressi sulla scala qualitativa prevista dalla Metodologia di Gruppo:



✓ In considerazione del fatto che la **Relazione sul rischio informatico del 2015** aveva evidenziato un **rischio "Alto" sulla sicurezza logica del Consorzio**, nel corso del 2016 è stata 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 fornito dalla Società di consulenza Deloitte ERS.

Risk Appetite Statement (RAS) e propensione al rischio informatico per l'anno 2016

- ✓ Il **livello di propensione al rischio informatico**, ovvero il livello 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 2016 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

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

Perimetro di analisi del rischio informatico per l'anno 2016

✓ Il Sistema Informativo di Gruppo comprende:

- **664 asset ICT gestiti dal Consorzio Operativo di Gruppo**, censiti nell'inventario APM.
- **10 asset ICT gestiti direttamente da Banca Widiba**, corrispondenti al sistema di Front-end multicanale della Banca.

✓ 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.

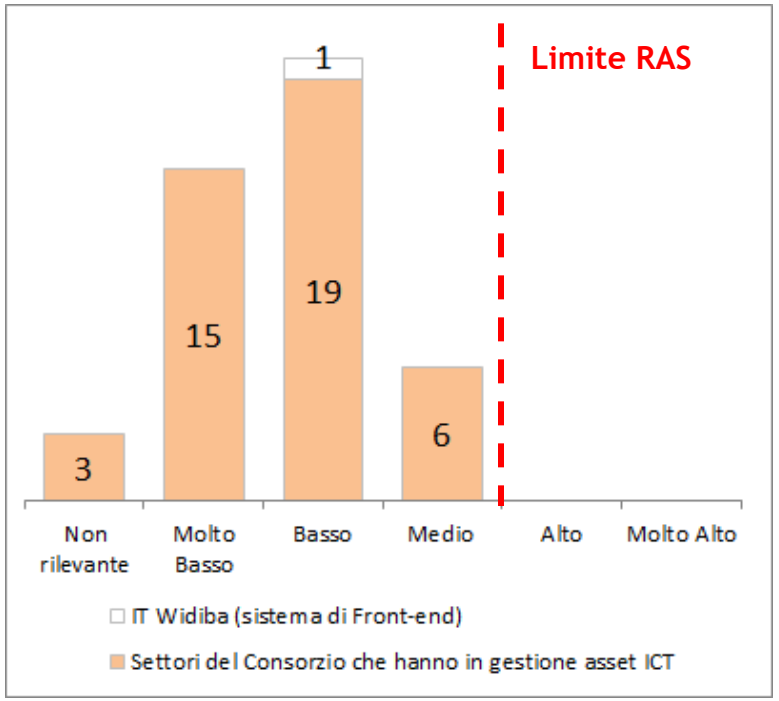
	PERIMETRO ANALISI DEL RISCHIO 2016	
	MPS CONSORZIO OPERATIVO GRUPPOMONTEPASCHI	widiba
Analisi del rischio **"Top Level"**	✓ Gli indicatori di rischio (KRI) sono stati misurati con riferimento agli ambiti applicativi e infrastrutturali corrispondenti a **40 Settori del Consorzio che hanno in gestione asset ICT**. *	✓ Gli indicatori di rischio (KRI) sono stati misurati 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**.
Analisi del rischio **"Low Level"**	✓ Sono stati **selezionati 144 asset ICT** su un totale di 664, sulla base di una serie di fattori indicativi del loro livello di criticità. 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 da apposita Commissione costituita presso la Capogruppo.	✓ L'analisi Low Level ha riguardato **tutte e 10 le applicazioni e funzionalità applicative** che costituiscono il sistema di Front-end multicanale di Banca Widiba.

(*) Non sono stati considerati i Settori del Servizio Sicurezza IT per il quale è stata adottata una metodologia di analisi specifica.

Risultati analisi del rischio «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.

Distribuzione ambiti applicativi e infrastrutturali per livello di rischio



MPS CONSORZIO OPERATIVO GRUPPOMONTEPASCHI

- ✓ L'analisi Top Level **non ha evidenziato alcun rischio eccedente la soglia di propensione stabilita nel RAS di Gruppo**.
- ✓ Vi sono alcuni ambiti che presentano un **rischio "Medio"** e che corrispondono ai seguenti **6 Settori** del COG (il 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 anomale osservate hanno riguardato principalmente: gli incidenti, i change in emergenza, le modifiche ai dati eseguite direttamente in produzione, i progetti in ritardo.
- ✓ Le evidenze fornite dai KRI sono state condivise con i Responsabili dei Settori al fine di inquadrare le motivazioni degli andamenti e condividere le azioni di miglioramento, seppure non obbligatorie per il rispetto dei limiti fissati nel RAS.

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 su richiesta della Funzione Audit hanno evidenziato una serie di **vulnerabilità rispetto agli attacchi esterni**, per le quali **Banca Widiba ha avviato immediatamente le relative mitigazioni**. È previsto che tutte le mitigazioni 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 ethical hacking.

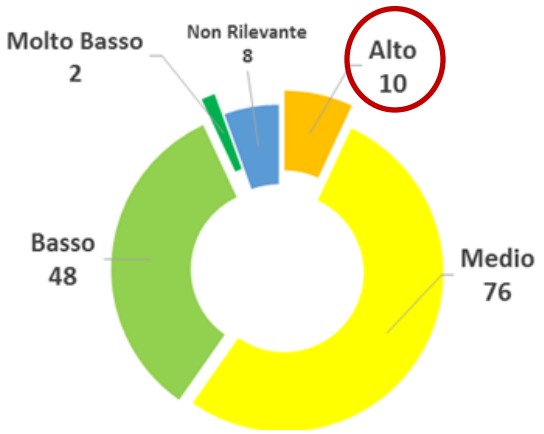
Risultati analisi del rischio «Low Level»

- ✓ L'analisi di rischio Low Level è svolta su un **perimetro di asset ICT** ed è finalizzata alla **valutazione prospettica degli eventi di rischio informatico che possono colpire l'asset** e provocare un impatto negativo per il Gruppo.
- ✓ L'analisi ha considerato anche i **controlli specifici applicabili ai sistemi di pagamento via internet**, in osservanza ai requisiti posti dagli "Orientamenti in materia di sicurezza dei pagamenti tramite internet" emanati dall'EBA, divenuti obbligatori dal 30 settembre 2016.*

MPS CONSORZIO OPERATIVO GRUPPOMONTEPASCHI

- ✓ Per **10 asset ICT** (il 7% dei 144 analizzati) il livello di rischio è stato valutato **"Alto"**, ovvero superiore al limite stabilito nel RAS per il 2016.
- ✓ A questi si aggiungono **altri 3 asset** valutati con rischio «**Alto**» individuati a fine 2015.

Ripartizione dei 144 asset analizzati



- ✓ Le raccomandazioni per la mitigazione dei rischi sono state presentate agli Utenti Responsabili degli asset e le relative iniziative sono state pianificate.
- ✓ 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 (le mitigazioni sono state comunque avviate d'iniziativa da parte del COG).

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.

(*) L'obbligatorietà è stata stabilita dal 16° aggiornamento della Circolare Banca d'Italia n. 285/2013, datato 17 maggio 2016

Risultati analisi del rischio sulla Sicurezza informatica del COG

- ✓ 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**. Ad inizio 2016 il COG, aveva già predisposto un **piano di interventi di mitigazione** denominato "**Monte Più Sicuro**".

- ✓ Nel corso del 2016, al fine di valutare l'adeguatezza delle azioni di mitigazione già avviate, è stata inoltre condotta un'**analisi specifica** sul macro ambito della sicurezza informatica, con il supporto della Società di consulenza Deloitte ERS.

MPS CONSORZIO OPERATIVO GRUPPOMONTEPASCHI

Sicurezza informatica COG - Scenari di rischio analizzati

Scenario	Minaccia	Descrizione
Attacchi logici	Malware	Include le minacce legate a codice malevolo (viruses / worms, trojan horses / rootkits, botnet clients).
	Hacking	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.
	Minacce sociali	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.
Utilizzo improprio e/o errori	Utilizzo improprio	Include le minacce relative ad utilizzo non autorizzato/non consono dei sistemi informatici, sottrazione di software/informazioni di business.
	Errori e malfunzionamenti	Include le minacce legate ad errore di utenti finali / staff tecnico, malfunzionamento HW / SW, effetti non desiderati derivanti da modifiche.
Incidenti di sicurezza fisica	Accessi fisici e furti/perdite	Include le minacce relative ad accessi fisici non autorizzati e furti/perdita di dispositivi.
Interruzione del business	Minacce ambientali	Include disastri naturali, danneggiamenti, interruzione di corrente / comunicazioni esterne.

- ✓ L'analisi del rischio 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 ("Monte più Sicuro").

- ✓ **Tutte le attività di mitigazione previste per il 2016 sono state svolte.** Questo permette di consolidare il rischio sulla Sicurezza Informatica ad un livello **"Medio".**

Piano di mitigazione dei rischi informatici

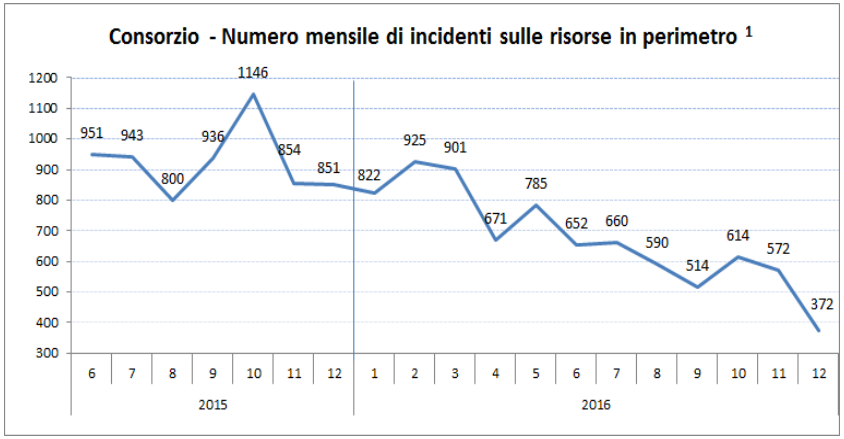
✓ A fine 2016, il piano di mitigazione dei rischi informatici superiori alla soglia RAS comprendeva 8 interventi relativi a risorse del COG, con scadenze diverse fino a luglio 2017. Tali interventi fanno riferimento ai 12 asset ICT valutati con rischio «Alto» ed alla Sicurezza Logica *.

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

(*) Per quanto riguarda l'applicazione APP0000494 SAG - Swift Alliance Gateway, la cui valutazione di rischio "Alto" rappresenta una proposta da validare a cura dalla neo-costituita Commissione risorse ICT trasversali; le mitigazioni sono state comunque avviate d'iniziativa del COG con data di completamento attesa, per l'ultimo degli interventi, a dicembre 2017.

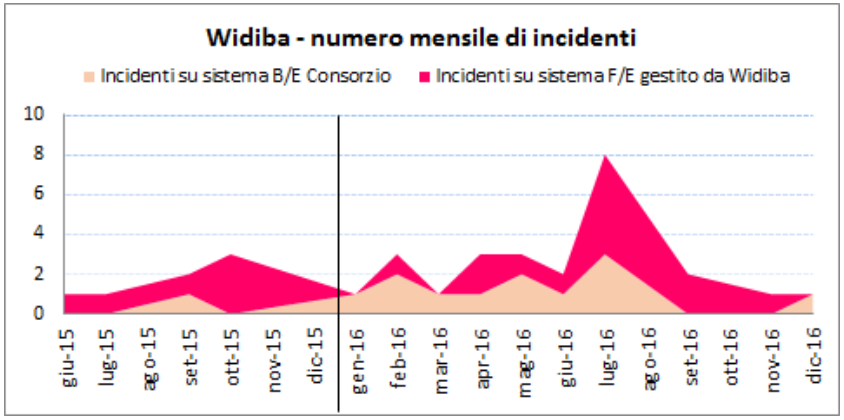
Monitoraggio dei key risk indicator inseriti nel RAS: incidenti IT

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



	2016			
	Q1	Q2	Q3	Q4
N. risorse con incidentalità mensile sopra la soglia di attenzione definita dal RAF 2				
- applicazioni critiche per la business continuity	2	-	-	-
- altre applicazioni	1	-	-	-
- rete TLC	-	-	-	-
N. major incident	1	2	2	3

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

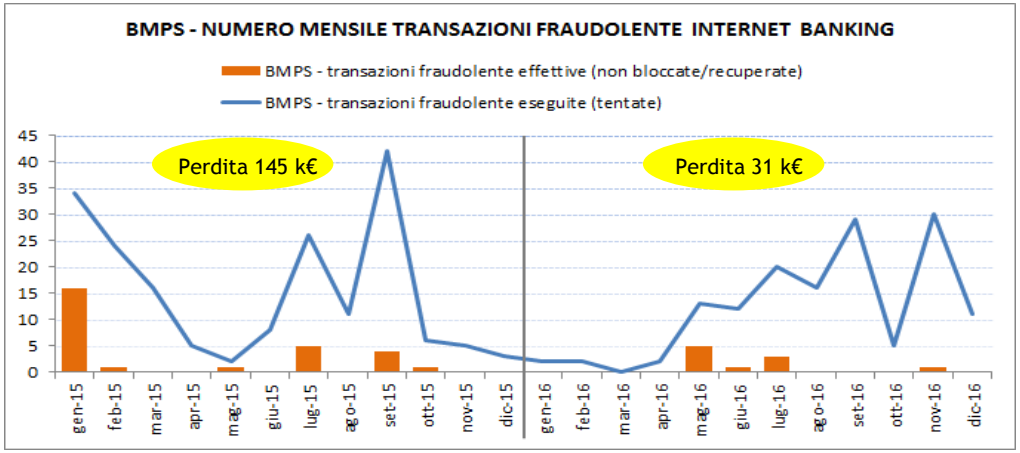


	2016			
	Q1	Q2	Q3	Q4
N. incidenti con impatto "Alto" 3	3	3	3	2
di cui:				
- su sistema B/E gestito dal Consorzio	3	1	1	1
- su sistema F/E gestito da Widiba	-	2	2	1

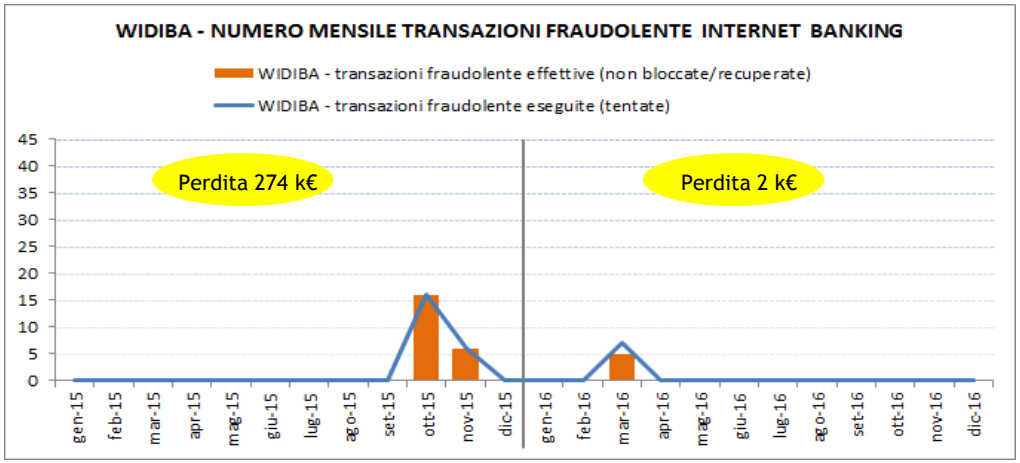
1. Sono esclusi gli incidenti relativi all'informatica periferica (pdl, laptop, stampanti, scanner, server, telefonia, …).
2. Le soglie di attenzione sono definite in termini di numero incidenti mensili e sono differenziate per tipologia di risorsa informatica: 10 incidenti mensili per le applicazioni 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».

Monitoraggio dei key risk indicator inseriti nel RAS: frodi ai danni dei clienti internet banking

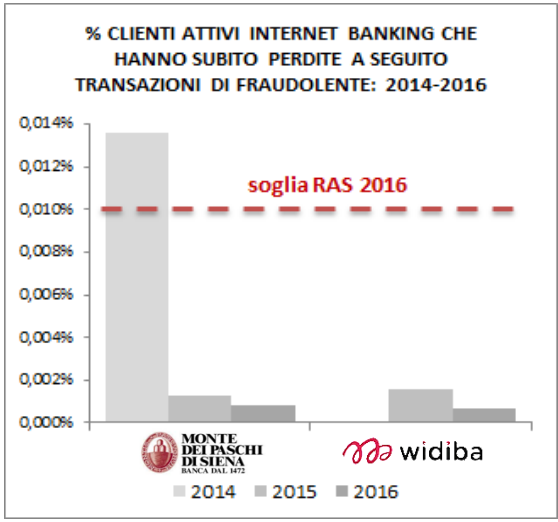
- ✓ Nel corso del 2016, in BMPS si è ridotto il numero complessivo di tentativi di frode a danno della clientela internet banking (-22%). Tale dinamica positiva ha interessato la clientela retail, mentre per il corporate i tentativi di frode sono sensibilmente aumentati (+44% in numero e +400% in volume 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€ *).



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



(*) 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.

Fact checking sul piano di attività programmate per il 2016

✓ Nella Relazione sul rischio informatico del 201S * era stato definito il piano di attività per il 2016; segue il resoconto dei risultati raggiunti:

Piano di attività per il 2016	Risultati raggiunti
Proseguimento delle analisi sulle risorse informatiche in produzione.	✓ Completata analisi del rischio su: • 144 asset ICT gestiti dal Consorzio • 10 asset ICT gestiti da Widiba
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 dei rischi che eccedono i limiti fissati dal RAS, a fronte dei 12 asset valutati con rischio «Alto» ed alla 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: • progetto Swap data center (inversione del ruolo dei data center di Siena e Firenze); • progetto Digital banking (sviluppo nuovo internet banking clientela privati).
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. cfr. allegato 1
Monitoraggio del rischio informatico tramite i Key Risk Indicator definiti nel RAS.	✓ Monitoraggio effettuato con cadenza mensile.

(*) Relazione approvata dal CdA del 25 febbraio 2016.

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*. *

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 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.

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

Allegati

Allegato 1 - Individuazione degli Utenti Responsabili degli asset ICT

- ✓ Come richiesto dalla Circolare Banca d'Italia 285/2013, il modello organizzativo prevede inoltre il ruolo dell'**Utente Responsabile**, figura da identificare **per ciascun sistema o applicazione**, avente la responsabilità di:
  - **concorrere al processo di analisi del rischio informatico** secondo la metodologia di analisi adottata dal Gruppo,
  - **accettare formalmente il rischio residuo**.
- ✓ Il ruolo di Utente Responsabile è stato formalizzato 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 **quattro tipologie di risorse informatiche**:

Applicazioni di business	Le applicazioni di business realizzano un insieme di funzionalità a supporto dell'esecuzione dei processi aziendali. Sono assegnate ad una **specifica Funzione di business**.
Piattaforme di sicurezza	Le piattaforme di sicurezza sono poste a protezione dell'integrità fisica e logica del sistema informativo e della riservatezza dei dati gestiti. Sono di competenza della **Funzione Sicurezza**.
Risorse ITxIT	Le risorse "ITxIT" sono utilizzate esclusivamente dalla Funzione ICT a supporto dei propri processi operativi e non sono collegate direttamente ai processi di business. L'Utente Responsabile è individuato all'interno della **Funzione ICT**.
Risorse ICT trasversali	Per le risorse ICT trasversali, ove non è possibile individuare una Funzione aziendale prevalente, sono assegnate da **apposita Commissione** costituita a inizio 2017 in Capogruppo.

L'Utente Responsabile è stato **individuato per 614 asset ICT** gestiti dal Consorzio o da Banca Widiba, pari al **91% del totale**:

Tipologia di risorse ICT	Utente Responsabile	Nr. asset	*% su totale*
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%*
	subtotale asset ICT con UR individuato	**614**	***91%***
Risorse in via di assegnazione		60	*9%*
	Totale	**674**	***100%***