



## **Comitato Gestione Rischi del 16-05-2017**

**Piano di Mitigazione,  
monitoraggio delle azioni di mitigazione in corso  
e KRI**

**Direzione Chief Risk Officer  
GRUPPOMONTEPASCHI**



**MONTE  
DEI PASCHI  
DI SIENA**  
BANCA DAL 1472

## **Nuovo Piano di mitigazione :**

- ☐ Il processo
- ☐ Temi principali dello Scenario 2016
- ☐ Interventi individuati

## **Monitoraggio delle azioni di mitigazione in corso:**

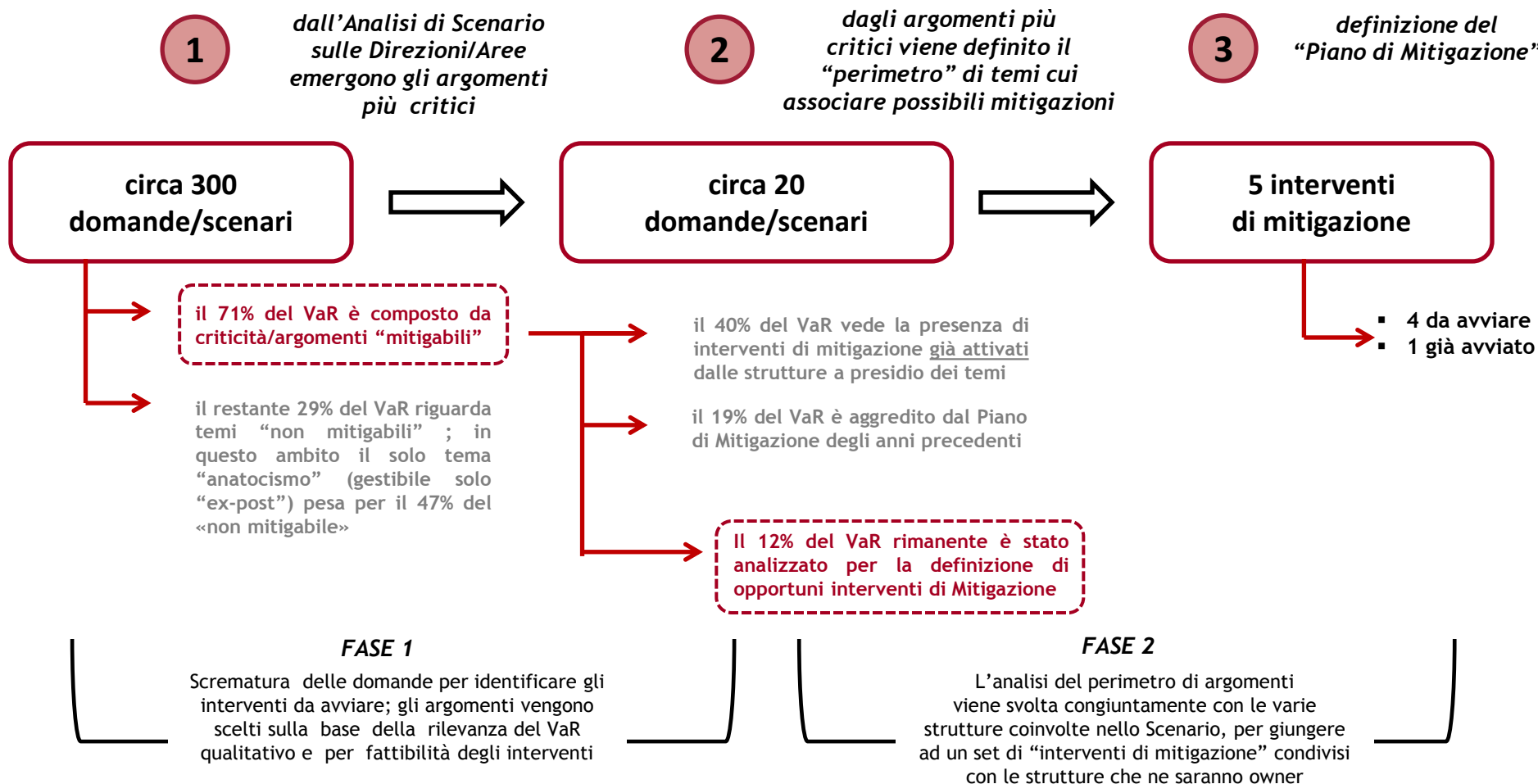
- ☐ Piano di Mitigazione Rischi Operativi - SAL al 31/03/2017
- ☐ Piano di Mitigazione Rischi Informatici - SAL al 31/03/2017

## **KRI :**

- ☐ KRI di rischio operativo
- ☐ KRI di rischio informatico

# Nuovo Piano di Mitigazione: il processo

A partire dalle evidenze di criticità emerse nella fase di “**identificazione dei rischi operativi**” (Analisi di Scenario) è stato definito un set di ambiti di miglioramento individuati presso le varie Direzioni, cui far fronte con opportuni “**interventi di mitigazione**”, individuati dalle medesime aree/Direzioni. Al fine di individuare le criticità principali viene calcolato un VaR qualitativo gestionale, che prende in considerazione anche problematiche relative ai rischi di credito, denominate «credit boundary», che non vengono però inserite nel requisito di rischio Operativo poiché già presenti in quello di Credito. I vari interventi sono stati condivisi con le strutture che saranno owner delle azioni di riduzione del profilo di rischio della banca, secondo il processo delineato dalla *Policy in materia di GAP* (doc. 1822). Il processo è così strutturato:



# Nuovo Piano di Mitigazione: temi principali dello Scenario 2016

I temi più rilevanti in termini di rischiosità emersi dall'Analisi di Scenario 2016 sono riportati di seguito.

## Gestione del credito

*Attività non autorizzate in sede di analisi del rischio e concessione del credito*

*Frodi documentali sui mutui*

*Gestione delle garanzie (acquisizione/conservazione, data certa)*

## Condizioni ai clienti

*Anatocismo*

*Usura*

## Finanza

*Change management (errori nel set-up nelle procedure informatiche)*

*Frodi nella negoziazione in conto proprio di strumenti finanziari*

## Mitigazione in corso

è in corso il rafforzamento dei presidi dei rischi operativi connessi all'utilizzo delle delibere post-impianto (in relazione alle evidenze della Dir. CAE), oltre al progetto «Controlli di I livello» ed alla procedura Visti.

sono in corso implementazioni procedurali che prevedono funzionalità automatizzate nel processo di concessione delle restrizioni ipotecarie. Inoltre il Progetto Elise ed il progetto Antifrode possono mitigare gli aspetti critici e migliorare i presidi.

alcuni miglioramenti sono stati ottenuti con il Progetto «Paperless» ed altri aspetti verranno mitigati all'interno dei Progetti «Credit Standard» e «NPL». Ci sono inoltre alcuni interventi in corso relativamente agli Organismi di Garanzia Collettiva.

eventi passati non mitigabili, ma possibili azioni di gestione ex-post. Controlli previsti nell'ambito del progetto «Controlli di I livello».

sono in corso interventi per efficientare i processi di change management .

le attività di controllo in essere risultano adeguate, da prevedere l'integrazione della normativa interna.

## Operazioni con clienti e controparti

*Appropriazioni fraudolente da parte dei dipendenti a danno dei clienti*

*Controparti commerciali - contestazioni per mancato rispetto dei termini contrattuali*

## Operazioni di incasso e pagamento

*Frodi nell'apertura di rapporti di Incassi Commerciali a nuova clientela*

*Clonazione assegni bancari/circolari*

## Altri Ambiti

*Contestazioni per Aumenti di capitale*

*Contenziosi fiscali per errato/mancato adempimento di obblighi fiscali*

*Violazioni alle disposizioni di legge in materia di antiriciclaggio e contrasto al terrorismo*

## Mitigazione in corso

è stata rivista la normativa interna e sono in corso alcuni interventi per rafforzare i controlli. Numerose sono le iniziative sulla filiera Private.

il tema si considera presidiato, c'è una costante attenzione nella gestione di questa tipologia di contestazioni.

alcuni aspetti verranno mitigati all'interno delle progettualità previste in ambito credito.

le mitigazioni rientrano nel Progetto «Digitalizzazione Assegni»

mitigazioni non attuabili sui precedenti aumenti di capitale.

le criticità pregresse sono state risolte ed il tema si considera presidiato.

il nuovo servizio Digital Banking favorirà la raccolta dei questionari mancanti; è anche in corso la sistemazione delle posizioni ex Consumit. Opportuno un rafforzamento dei presidi di Widiba.

## Nuovo Piano di Mitigazione: interventi individuati

In seguito alle analisi di Scenario, in condivisione con le singole direzioni/aree, è stato individuato un set di 5 gap che possono essere “aggrediti” con opportuni interventi di mitigazione, secondo interventi individuati dalle stesse aree interessate, con scadenza dicembre 2017. Per l’ultimo punto (leasing immobiliare) sono già stati attivati gli interventi di mitigazione. Sulla base della direttiva in materia di Gestione dei Rischi Operativi il piano viene presentato al Comitato Gestione Rischi per l’approvazione.

argomento	ambito	intervento	owner	worst case scenario
<b>Gestione del credito</b>	ritardi nelle varie fasi di recupero, carenze nella conservazione della documentazione, ritardi nell’adozione di misure finalizzate alla regolarizzazione delle posizioni anomale e/o classificazione delle posizioni a sofferenza	analisi degli scostamenti dagli obiettivi sui principali indicatori a budget (flussi a default, cura del default) per individuare le principali cause ed incrementare l’efficacia delle azioni di mitigazione	Dir CLO (Ser. Credit Control Unit)	500k (frequenza attesa: 3 volte al mese)
<b>Antiriciclaggio</b>	violazione delle disposizioni di legge in materia di antiriciclaggio	rafforzamento del presidio in materia di controlli per renderli coerenti all’operatività di Banca Widiba, in ragione di alcuni casi di mancata/errata segnalazione di operatività sospetta da parte dei promotori finanziari	Widiba (Compliance Antiriciclaggio)	2 mln (frequenza attesa: 2 volte all'anno)
<b>Frodi nella negoziazione in conto proprio di strumenti finanziari</b>	frodi esterne subite nella negoziazione in conto proprio di strumenti finanziari (operazioni con strumenti finanziari utilizzati al fine di posticipare il concretizzarsi di perdite, truffe realizzate secondo lo schema Ponzi, ecc.)	integrazione della normativa in materia di finanza proprietaria esplicitando espressamente il divieto di porre in essere operazioni della fattispecie, richiedendone l’esplicita presa visione da parte degli operatori	Area Finanza Tesoreria e Capital Management	8 mln (frequenza attesa: 1 volta ogni 10 anni)
<b>Procedure informatiche</b>	malfunzionamento dei sistemi, degrado delle performance delle piattaforme utilizzate, mancato aggiornamento dei dati o loro indisponibilità in tempi utili allo svolgimento dell’attività in occasione di specifiche operazioni rilevanti	implementazione di una procedura di back up che estragga dai portafogli Murex le posizioni in titoli lunghe/corte, procedura alternativa a FDWH ai fini del presidio e della corretta gestione della liquidità	MPS CS (Uff. Government & Money Market)	2 mln (frequenza attesa: 1 volta all' anno)
<b>Leasing immobiliare</b>	perdite subite in seguito ad errori nella fase di acquisizione degli immobili di proprietà/ripossessati e/o nella fase di vendita	emanazione di testi normativi che dettino nuove norme ai fini di fornire un ulteriore e più efficiente presidio al rischio	MPS L&F	2 mln (frequenza attesa: 1 volta ogni 2 anni)

## **Nuovo Piano di mitigazione :**

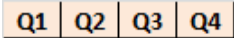
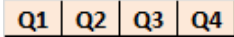
- ☐ Il processo
- ☐ Temi principali dello Scenario 2016
- ☐ Interventi individuati

## **Monitoraggio delle azioni di mitigazione in corso:**

- ☐ Piano di Mitigazione Rischi Operativi - SAL al 31/03/2017
- ☐ Piano di Mitigazione Rischi Informatici - SAL al 31/03/2017

## **KRI :**

- ☐ KRI di rischio operativo
- ☐ KRI di rischio informatico

Ambito	Mitigazione	Chiusura	Owner
Frodi nell'erogazione di mutuo, soprattutto di tipo documentale (falsificazione dati, ecc.)	Rafforzamento dei controlli con implementazione di strumenti di fraud-detection in ambito documentale (gap RM_2016_00003)	31/03/2017 Rischedul. 31/12/2017 	<b>BMPS</b> - Direzione Erogazione e Governo del Credito
Attività fraudolente o non autorizzate compiute da promotori finanziari	Rafforzamento dei processi di controllo: revisione dei controlli di 1° e 2° livello, modifiche applicativi, incremento di alert presso la struttura manageriale di rete (gap RM_2016_00006)	31/03/2017 Rischedul. 29/12/2017 	<b>Widiba</b> - Controlli Promozione Finanziaria e Operational Risk Management



# Piano di mitigazione Rischi Informatici - SAL al 31/03/2017

Al 31/03/2017 il piano di mitigazione dei rischi informatici superiori alla soglia RAS comprendeva 6 interventi relativi a risorse COG. Tali interventi fanno riferimento a 9 asset ICT ed al macro ambito della Sicurezza Logica. <sup>1</sup>

Asset/ambito ICT	Nr. Asset	Mitigazione	Scadenza	SAL 31/03/2017	Owner	Contributor
Anagrafe Operativa Gruppo	1	Gestione profili abilitativi: integrazione trx NCHI con sistema controllo accessi (gap RM_2016_00013)	30/04/2017 Q1 Q2 Q3 Q4	 CHIUSO 11/04	BMPS - Servizio Anagrafe Generale e Indagini	COG - Settore Anagrafe e Condizioni
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	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
CAI - Centrale Allarmi Interbancaria (segnalazioni allarmi su assegni/carte)	1	Livelli di servizio: adozione strumenti di monitoraggio corretto funzionamento (gap RM_2016_00010)	31/07/2017 Q1 Q2 Q3 Q4	 RIPIANIFICATO (EX 31/03)	BMPS - Servizio Finanziamenti e Prodotti Transazionali Retail	COG - Servizio Multicanalità Clienti Interni
CLM - Channel e Liquidity Management (gestione accentrata della liquidità della Banca)	1	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	 RIPIANIFICATO (EX 31/01)	BMPS - Servizio Liquidità Operativa	COG - Servizio Finanza COG - Servizio Sicurezza IT
Applicazioni estero domestico (5 applicazioni: anticipi, tesoreria, bonifici, rimesse imp/exp, estero sconto)	5	Obsolescenza applicativa: studio fattibilità sostituzione con soluzione di mercato e/o incorporazione funzionalità in settoriali Italia (gap RM_2017_00001)	31/03/2018 <sup>2</sup> Q1 Q2 Q3 Q4		BMPS - Staff Supporto Operatività Rete Estera	COG - Servizio Sistemi Referenziali

- Per l'applicazione APP0000494 SAG - Swift Alliance Gateway sono stati valutati rischi di livello "Alto" che devono essere validati 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.
- E' previsto che gli interventi finalizzati a ricondurre il rischio entro il livello «Medio» termineranno il 31/03/18, anche se il gap ha scadenza 30/09/2018.

## **Nuovo Piano di mitigazione :**

- ☐ Il processo
- ☐ Temi principali dello Scenario 2016
- ☐ Interventi individuati

## **Monitoraggio delle azioni di mitigazione in corso:**

- ☐ Piano di Mitigazione Rischi Operativi - SAL al 31/03/2017
- ☐ Piano di Mitigazione Rischi Informatici - SAL al 31/03/2017

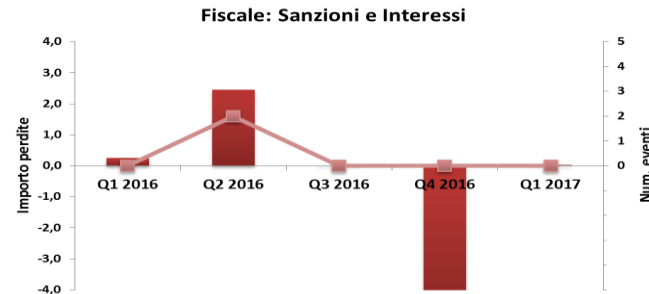
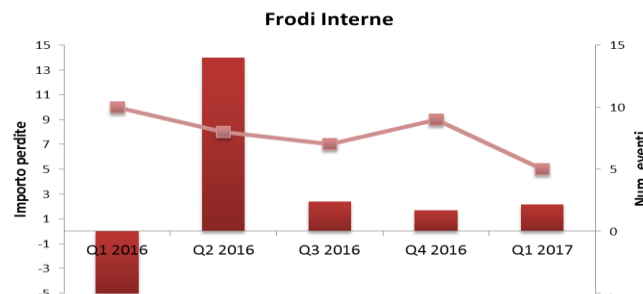
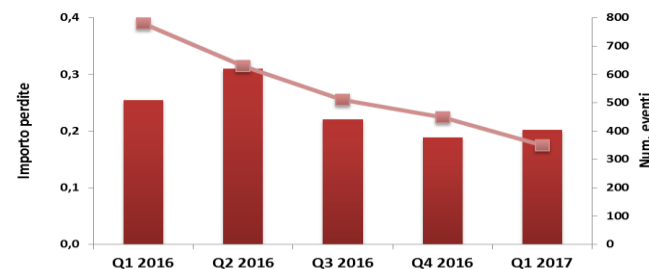
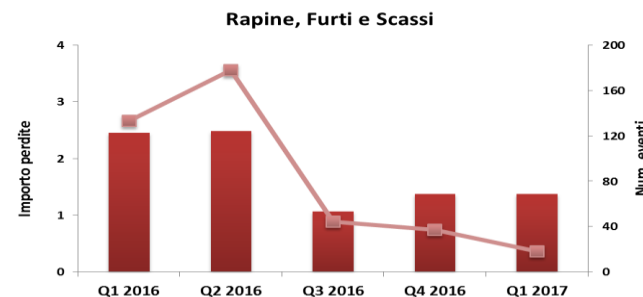
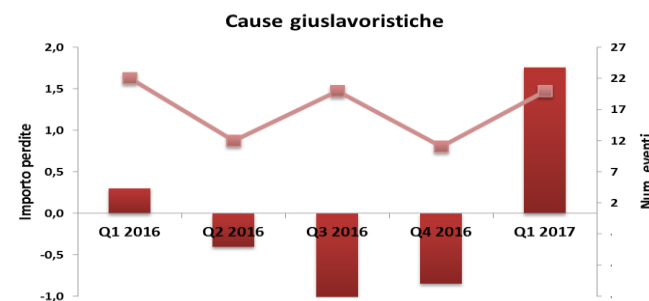
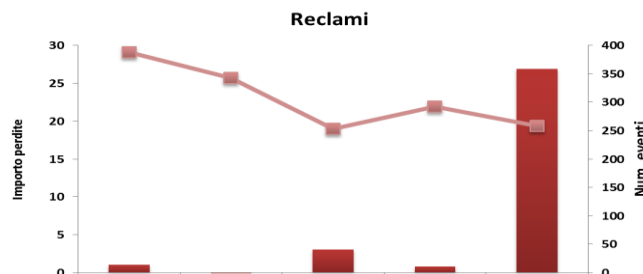
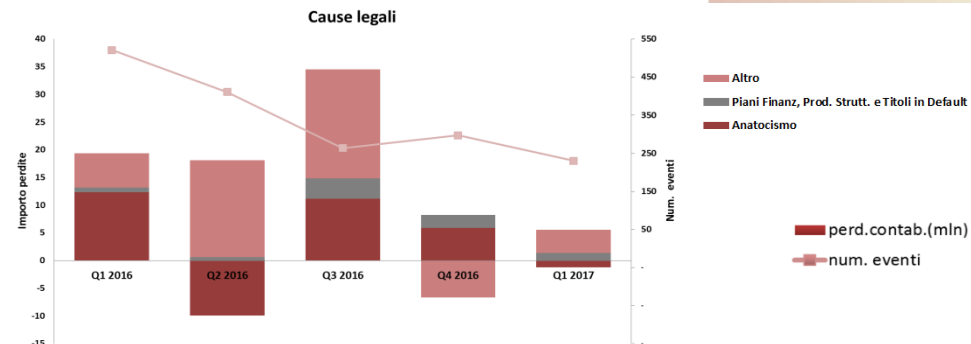
## **KRI :**

- ☐ KRI di rischio operativo
- ☐ KRI di rischio informatico

# KRI di rischio operativo

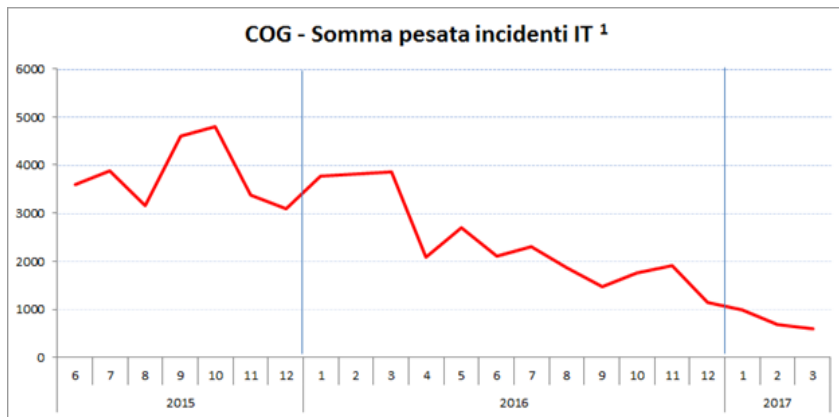
Come ulteriore approfondimento, si riporta l'andamento degli importi osservati e della numerosità degli eventi di perdita rilevati per alcune tipologie di rischio operativo.

- ✓ Nel primo trimestre 2017, si rileva un incremento degli importi osservati, principalmente per accantonamenti su nuovi **Reclami** relativi agli aumenti di capitale passati
- ✓ Nel primo trimestre 2017 si osserva un incremento di fondo rischi a fronte di accantonamenti per 2 nuove cause di ex dipendenti (un ex dirigente e 3 dipendenti ex bav poi esternalizzati) in ambito **Cause giuslavoristiche**.
- ✓ In ambito **Cause Legali** viene confermato il trend in diminuzione sia in numerosità che come importi.
- ✓ Nell'ambito **Rapine, Furti e Scassi**, è confermato il trend in diminuzione osservato negli ultimi trimestri.
- ✓ Si evidenzia il trend in riduzione degli eventi rilevati ed una sostanziale stabilità sulle perdite contabilizzate per **Carte Clonate**.
- ✓ Nell'ambito delle **Frodi Interne** si ha una sostanziale stabilità negli importi e nelle numerosità degli eventi rispetto agli ultimi trimestri.
- ✓ Relativamente al contenzioso **fiscale** non si rilevano perdite contabilizzate nel trimestre.

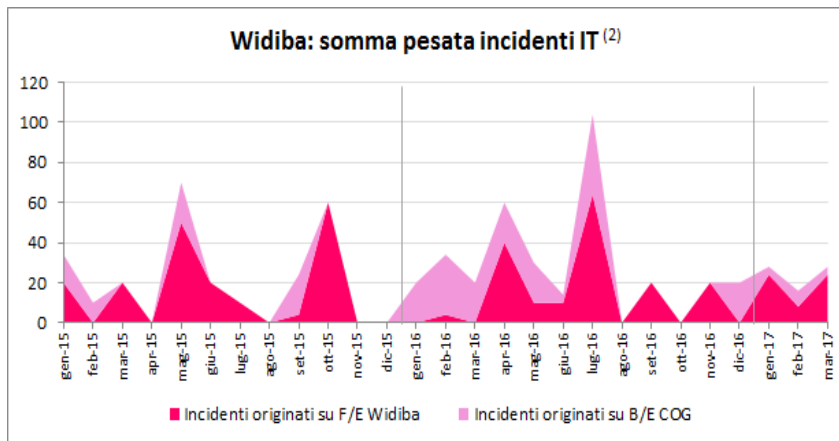


# KRI di rischio informatico: incidenti IT

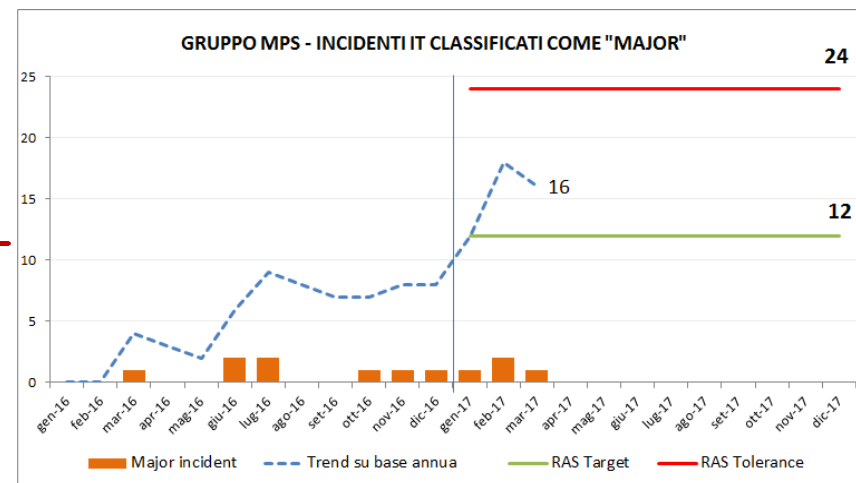
- ✓ La somma pesata degli incidenti IT sulle risorse gestite dal Consorzio, rilevata mensilmente, è in costante diminuzione dal Q2 2016 e si colloca oggi sui minimi della serie storica.



- ✓ La somma pesata degli incidenti IT su Widiba rimane su ordini di grandezza contenuti.



- ✓ Nel corso del 2017 si sono verificati 4 major incident relativi a risorse gestite dal COG. Il dato annualizzato a livello di Gruppo è 16, che si colloca tra il target e la soglia di tolerance.
- ✓ Nessuno degli incidenti ha richiesto la comunicazione alle Autorità.

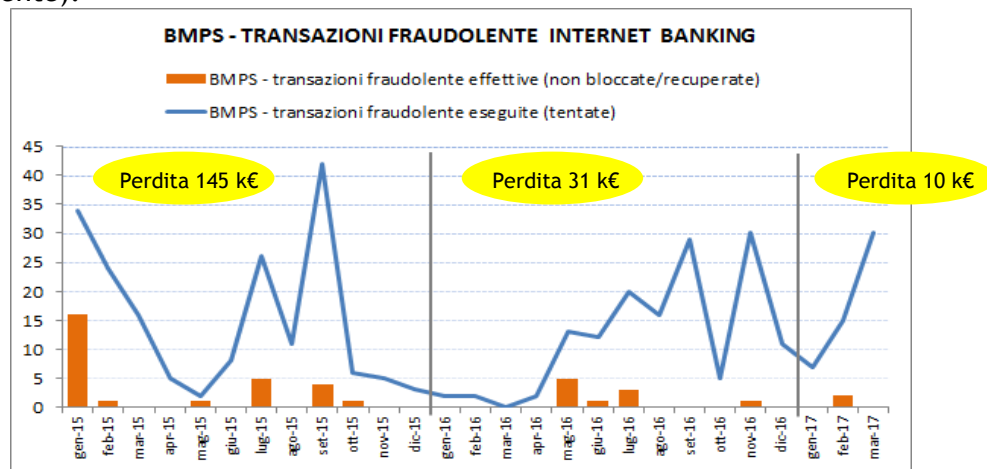


1. I pesi sono attribuiti agli incidenti in funzione del livello di priority assegnato al ticket: «Major» = 60, «Critica» = 20, «Alta» = 10, «Media» = 4, «Bassa» = 1. Sono esclusi gli incidenti relativi all'informatica periferica (pdl, laptop, stampanti, scanner, server, telefonia, ...).
2. I pesi sono attribuiti agli incidenti in funzione del livello di impatto sulla clientela Widiba: Impatto «Alto» = 20, «Medio» = 10, «Basso» = 4. La valutazione del livello di impatto è effettuata da Widiba sulla base del numero di segnalazioni ricevute, delle funzionalità coinvolte e della durata del disservizio. In caso di riclassificazione di un incidente come Major viene attribuito un peso = 60.

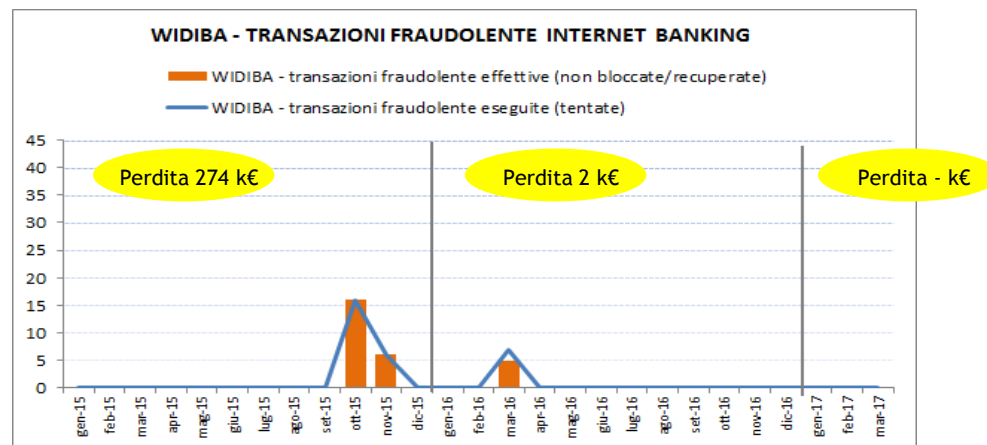
# KRI di rischio informatico: transazioni fraudolente a danno dei clienti internet banking



- ✓ Nel corso del 2017 continuano a registrarsi numerosi tentativi di frode internet banking su clienti Corporate BMPS, efficacemente contrastati dal sistema di monitoraggio antifrode (perdita 4 K€).
- ✓ A marzo 2017 si è registrato un picco di tentativi di frode sui clienti Retail BMPS: tali attacchi, condotti tramite inserimento di malware nel PC del cliente, hanno interessato possessori del vecchio servizio Paskey IB. Anche in questo caso il monitoraggio anti-frode è risultato efficace (l'unica perdita di 6 K€ riguarda la segnalazione di bonifico sospetto autorizzato dalla Filiale senza la conferma del cliente).



- ✓ Nel corso del 2017, WIDIBA non ha registrato tentativi di frode sull'Internet Banking.



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

