



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

Gestione ATM

Rapporto n. 2018_63

Siena,

Direzione Chief Audit Executive
Area Revisione Specialistica
Servizio ICT & Operational Audit

La revisione, prevista nell'ambito della pianificazione annuale per il 2018, è stata svolta da team congiunti dei settori "ICT Audit" e "Operational Audit" ed è stata indirizzata a valutare l'adeguatezza del sistema dei controlli, il disegno dei processi e la conformità delle prassi alla normativa interna, per quanto riguarda:

- i processi decisionali, operativi e di monitoraggio relativi alla distribuzione degli ATM;*
- la gestione dell'operatività degli ATM;*
- i processi esternalizzati di caricamento valori, di installazione/manutenzione del parco ATM.*

È stata, inoltre, esaminata l'infrastruttura informatica alla base del funzionamento degli ATM, comprese le soluzioni di sicurezza fisica e logica messe in atto per la prevenzione e rilevazione di frodi.

La revisione ha interessato le seguenti strutture:

- il "Servizio Digital Banking e ATM" ("Funzione Commerciale"), per i processi distributivi degli ATM;*
- il "Servizio Cash Management, ATM e Logistica" ("Funzione Logistica"), per la gestione operativa degli ATM e la relazione contrattuale con B.T.V. S.p.A. e Basilichi S.p.A., outsourcer, rispettivamente, per i servizi di caricamento valori e di installazione/manutenzione del parco ATM;*
- il "Servizio Sicurezza Logica e Continuità Operativa" ("Funzione Sicurezza Logica Banca") e il "Servizio Sicurezza Fisica ed Assicurazioni" ("Funzione Sicurezza Fisica Banca"), per gli elementi afferenti la sicurezza logica e fisica degli ATM;*
- il "Servizio Sicurezza Informatica e BCM" del COG ("Funzione Sicurezza Informatica COG"), per l'analisi delle soluzioni dei presidi di sicurezza logica e delle frodi sugli sportelli ATM;*
- il "Servizio Bancassurance e Monetica" del COG ("Funzione Monetica"), per il ciclo di vita delle applicazioni in ambito ATM;*
- il "Servizio Assisted Banking" del COG ("Funzione Assisted Banking"), per gli approfondimenti relativi all'incidente intercorso durante la revisione;*
- il "Servizio Sistemi Tecnologici" del COG ("Funzione Sistemi"), per la sicurezza delle reti e del software installato sugli ATM.*

Sono stati anche effettuati accessi presso gli outsourcer interessati dall'attività, in particolare Basilichi per i processi di configurazione ed installazione, monitoraggio e manutenzione.

La revisione è stata svolta mediante:

- colloqui con i referenti delle Strutture interessate e osservazione in loco delle prassi agite;*
- esame della normativa e della documentazione operativa correlata;*
- verifiche a campione.*

Overview

ANAGRAFICA INTERVENTO

Intervento: Gestione ATM

Obbligatorietà: NO

Unità auditata/e:

Servizio Cash Management, ATM e Logistica - Naldini Stefano
 Servizio Digital Banking e ATM - Peruzzi Rossano
 Servizio Sicurezza Fisica ed Assicurazioni - Interligi Luigi
 Servizio Sicurezza Logica e Continuità Operativa - Festucci Carlo
 COG/Servizio Bancassurance e Monetica - Barbieri Fabio
 COG/Servizio Assisted Banking – Terranova Enrica
 COG/Servizio Sicurezza Informatica e BCM - Rosa Pablito
 COG/Servizio Sistemi Tecnologici - Bandini Paolo

Tipologia di intervento: settoriale – in loco

Date open meeting: 16/2/2018, 19/2/2018, 21/2/2018, 7/3/2018

Date exit meeting: 4/6/2018, 19/6/2018, 22/6/2018

Responsabili Audit Team:

- Monti Andrea (CIA, CISA) - (Operation)
- Scaccia Michela (CISA) - (IT)

Audit Team:

- Fei Luca
- Giannetti Claudio
- Parrini Isabella
- Volpi Antonio

ESITO INTERVENTO

GRADE COMPLESSIVO INTERVENTO

Rating 1 (VERDE)	Rating 2 (GIALLO)	Rating 3 (ARANCIONE)	Rating 4 (ROSSO)
---------------------	----------------------	-------------------------	---------------------

La scala di valutazione si articola su quattro livelli a criticità crescente: Rating 1 (VERDE), Rating 2 (GIALLO), Rating 3 (ARANCIONE), Rating 4 (ROSSO).

FATTORE CAUSALE	DISTRIBUZIONE DEI GAP PER RILEVANZA		
	ALTA	MEDIA	BASSA
Risorse	-	-	-
Processi	-	1	-
Sistemi	1	6	-
Totale	1	7	0

PRECEDENTI INTERVENTI DI REVISIONE (SE ESISTENTI)

AMBITO INTERVENTO	PERIODO DELLA VERIFICA	N. RAPPORTO	GRADE INTERVENTO
Audit degli apparati e dell'architettura ATM del Gruppo	10/02-23/04/2009	159/2009	Parzialmente favorevole

ORGANI DESTINATARI DEL PRESENTE AUDIT

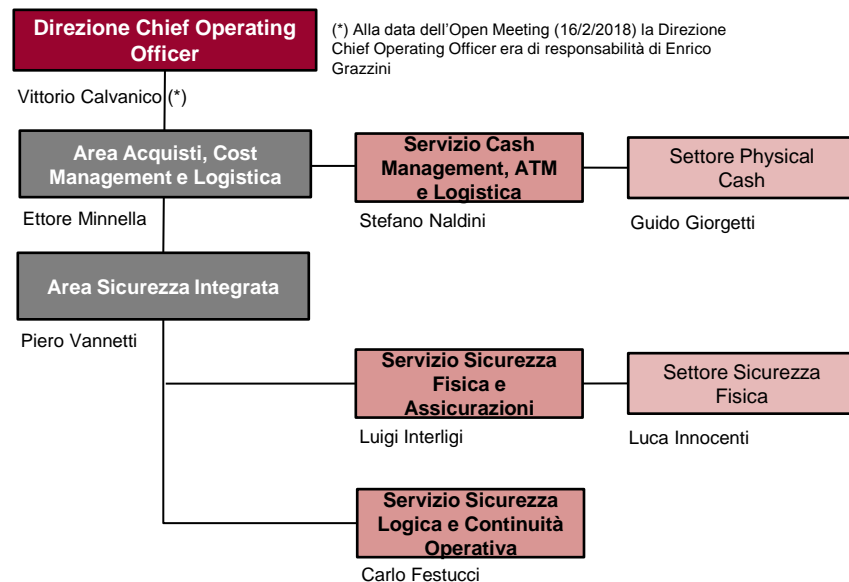
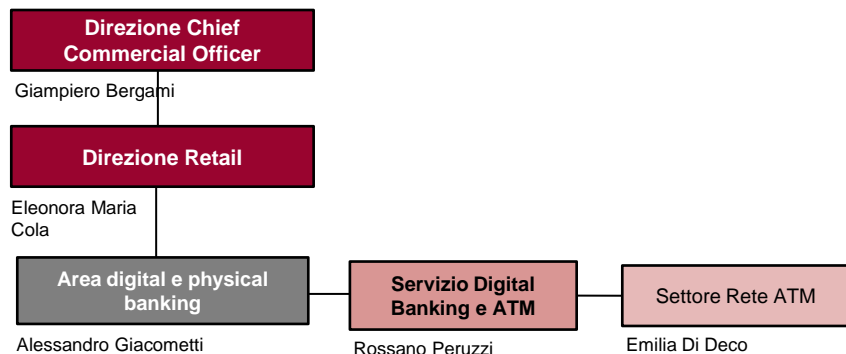
LEGAL ENTITY	ORGANO DESTINATARIO
BMPS	Presidente del CdA
BMPS	Amministratore Delegato
BMPS	Collegio Sindacale
BMPS	Comitato Rischi
COG	Presidente del CdA, Presidente CS (*), AD

(*) L'attività rientra tra quelle svolte dalla Capogruppo in qualità di Funzione di Audit esternalizzata del Consorzio



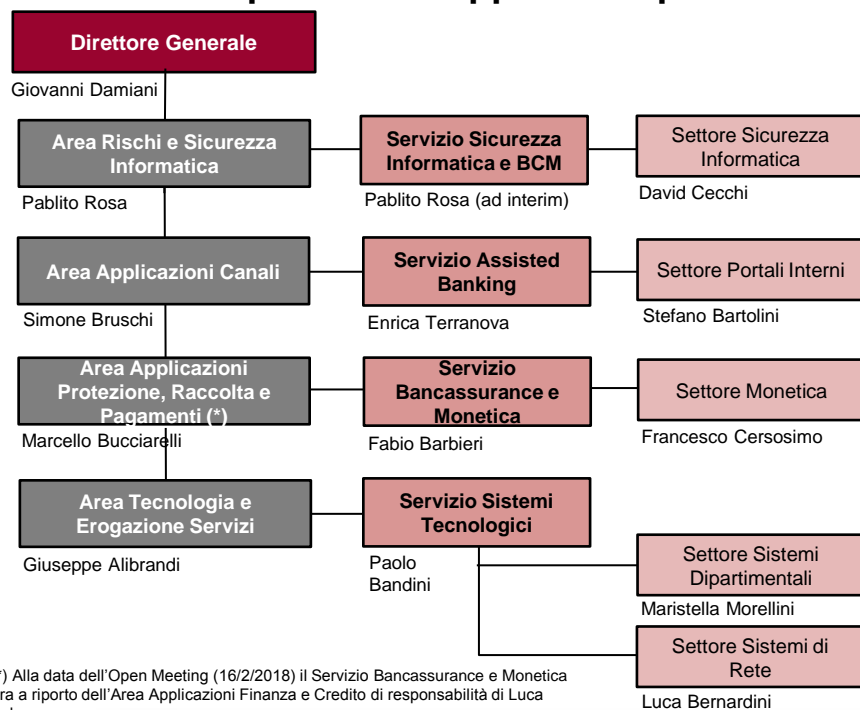
Organigramma Strutture Auditate

BMPS - Capogruppo bancaria



(*) Alla data dell'Open Meeting (16/2/2018) la Direzione Chief Operating Officer era di responsabilità di Enrico Grazzini

Consorzio Operativo Gruppo Montepaschi



(*) Alla data dell'Open Meeting (16/2/2018) il Servizio Bancassurance e Monetica era a riporto dell'Area Applicazioni Finanza e Credito di responsabilità di Luca Falco



Overview SREP

DISTRIBUZIONE DEGLI OBIETTIVI DI CONTROLLO SREP PER PILLAR E RATING









Pillar	Processo	Numero Obiettivi di controllo	A	B	C	D	NA
Business Model	Presidio canale ATM e Self Banking	0	-	-	-	-	-
	Gestione filiera del contante	0	-	-	-	-	-
	Enterprise Architecture Management	1	-	1	-	-	-
	Change, Release e Deployment Management	0	-	-	-	-	-
	Gestione dei processi operativi di sicurezza logica	0	-	-	-	-	-
	Gestione dei processi operativi di sicurezza fisica	0	-	-	-	-	-
Internal Governance & SCI	Presidio canale ATM e Self Banking	3	2	1	-	-	-
	Gestione filiera del contante	3	2	1	-	-	-
	Enterprise Architecture Management	1	-	1	-	-	-
	Change, Release e Deployment Management	1	-	1	-	-	-
	Gestione dei processi operativi di sicurezza logica	2	-	-	2	-	-
	Gestione dei processi operativi di sicurezza fisica	3	2	1	-	-	-
TOTALE		14	6	6	2	0	0

NOTA: La revisione non prevede obiettivi di controllo sui Pillar «Risk to Capital» e «Risk to Liquidity».

La scala di rating si articola su quattro livelli a criticità crescente ("A", "B", "C", "D"). Lo stato "NA" (Non applicabile) è indicato qualora non è espresso alcun rating sull'Obiettivo di controllo, che seppur selezionato in fase di pianificazione dell'intervento non è stato oggetto di specifica verifica in corso di accertamento



Audit findings

N.	PROCESSO	GAP	RILEVANZA (A/M/B)	FATTORE CAUSALE	RACCOMANDAZIONE	STRUTTURA OWNER	SCADENZA (GG/MM/AA)
1	Gestione dei processi operativi di sicurezza logica	Carenze nei presidi di sicurezza logica sugli apparati ATM	A		Implementare adeguati presidi di sicurezza logica sugli ATM	Area Rischi e Sicurezza Informatica (COG)	31/10/2018
2	Gestione dei processi operativi di sicurezza logica	Carenze nella segregazione delle reti	M		Segregare opportunamente la rete interna della Banca	Servizio Sistemi Tecnologici (COG)	31/01/2019
3	Change, release e deployment management	Attività di deployment svolta da Basilichi in assenza di contratto	M		Ricondurre il deploy all'interno del COG	Servizio Erogazione (COG)	31/12/2018
4	Gestione dei processi operativi di sicurezza logica	Utenze abilitate alla gestione degli apparati ATM non integrate nello strumento accentrato di controllo accessi	M		Automatizzare la gestione delle utenze del dominio ATM	Servizio Sicurezza Informatica e BCM (COG)	30/10/2018
5	Gestione dei processi operativi di sicurezza logica	Utenze dell'applicativo GE.BA non gestite nel rispetto della normativa aziendale	M		Condurre una bonifica delle utenze GE.BA	Servizio Digital Banking e ATM (BANCA)	30/9/2018
6	Enterprise Architecture Management	Mancanza di informazioni necessarie al monitoraggio delle giacenze	M		Implementare le adeguate soluzioni informatiche per il monitoraggio delle giacenze e del superamento del massimale	Servizio Cash Management, ATM e Logistica (BANCA)	28/2/2019
7	Enterprise Architecture Management	Problematica di sicurezza nella funzionalità "cardless" dell'ATM	M		Rendere sicuro il canale di trasmissione delle credenziali dell'utente	Servizio Bancassurance e Monetica (COG)	31/10/2018
8	Enterprise Architecture Management	Assenza di monitoraggio sugli interventi di assistenza di secondo livello svolti da TAS	M		Istituire un'attività di monitoraggio degli interventi tecnici di secondo livello	Servizio Bancassurance e Monetica (COG)	31/10/2018

 Sistemi  Processi  Risorse



Executive Summary (1 di 3)

CONTESTO

Il parco ATM alla data del 31/5/2018 è risultato composto da:

- n. 2.238 apparati installati presso le filiali, di cui il 46% circa dotato di funzionalità "cash in – cash out",
- n. 558 remoti, ovvero posizionati in luoghi diversi dalle filiali ma ad alto potenziale operativo (es. enti, centri commerciali, ecc.), prevalentemente di tipo cash out.

Lo sviluppo del parco ATM, in termini sia di numerosità che di tipologie di macchine, rientra nel più ampio progetto strategico "Banca Più" (cantiere Self Banking), iniziato nel 2017 con l'obiettivo, tra gli altri, di potenziare la rete ATM cash in con l'installazione di almeno un apparato per ogni filiale, e di progressiva migrazione dell'operatività dalla cassa verso gli ATM evoluti.

Nell'ambito e in linea con gli obiettivi di suddetto progetto, nel 2017 sono stati acquistati e installati n.406 cash in.

A novembre dello stesso anno, sfruttando una disponibilità di budget Capex residua da altre progettualità, le funzioni Commerciale e Logistica, in accordo con l'AD, hanno deciso di anticipare l'acquisto di n. 1.020 ATM, che nel corso del 2018 sarebbero serviti sia per la sostituzione degli apparati obsoleti, sia per raggiungere gli obiettivi di copertura del progetto Banca Più. La decisione è stata poi rivista a fine 2017 quando, in un'ottica di maggior attenzione ai costi e di maggiore cautela dal punto di vista gestionale, il numero degli apparati da acquistare è stato ridotto a 500 (di cui 300 per il programma Banca Più).

AMBITO COMMERCIALE

Alla Funzione Commerciale compete l'elaborazione del piano distributivo, lo sviluppo delle nuove funzionalità ed il monitoraggio delle performance degli apparati.

Il piano distributivo, ovvero l'identificazione delle filiali su cui effettuare l'installazione di nuovi ATM, prevede l'identificazione di un primo elenco di possibili installazioni effettuato sulla base di fattori quali il numero di operazioni di prelievo e versamento rilevate nell'anno, il numero dei clienti, dei conti correnti e delle carte emesse. Segue poi un'analisi di fattibilità svolta congiuntamente con la Funzione Immobiliare, che tiene conto delle caratteristiche del sito e quelle degli ATM a magazzino.

Per il 2019, visto il residuo numero di filiali ancor non coperte da ATM cash in, si dovrà anticipare la valutazione degli aspetti logistici/immobiliari e solo dopo procedere all'acquisto di ATM aventi caratteristiche idonee ai siti identificati.

AMBITO LOGISTICO

Alla Funzione Logistica compete il governo e la gestione operativa degli ATM, il loro mantenimento in esercizio e l'elaborazione del piano di sostituzione degli apparati obsoleti.

I servizi afferenti al ciclo di vita degli apparati ATM (gestione del magazzino, attivazione e messa in esercizio, assistenza, manutenzione e monitoraggio) sono esternalizzati sul fornitore Basilichi e regolati da un contratto stipulato nel 2009 con il Consorzio Operativo Gruppo Montepaschi (di seguito "COG").

Nel 2015, allo scopo di razionalizzare il presidio operativo, il contratto è stato ceduto dal COG alla Banca e contestualmente è stata creata, all'interno della Funzione Logistica, la figura dell' "ATM Manager", punto di riferimento unico per la rete commerciale e la Direzione Generale, che da allora coordina efficacemente il processo di installazione/sostituzione degli apparati e monitora puntualmente la relazione con l'outsourcer Basilichi.



Executive Summary (2 di 3)

AMBITO LOGISTICO

Nel corso degli anni il contratto con Bassilichi è stato oggetto di rinnovi per ragioni non strettamente correlate al mondo ATM ma connesse al consolidamento della *partnership* commerciale con Bassilichi, prorogando la scadenza, senza possibilità di disdetta, fino al 2025.

Alcuni contenuti del contratto non risultano più rispondenti all'attuale contesto operativo, le condizioni economiche potrebbero essere riviste in linea con le attuali condizioni di mercato, e il sistema delle penali dovrebbe essere rafforzato rispetto al complessivo valore contrattuale (attualmente €43K vs €mln 13 annui).

La cessione del contratto dal COG alla Banca ha trasferito a quest'ultima il governo di alcune attività legate al mondo IT e svolte dal fornitore. Benché efficacemente presidiate dalla Funzione Logistica, l'installazione delle macchine, la manutenzione, l'assistenza e monitoraggio non sono più infatti attività in carico al COG, che, secondo le strategie aziendali, ha invece il compito istituzionale di gestire in un'ottica accentrata e di Gruppo i sistemi informativi ed i relativi servizi.

Per quanto riguarda la gestione del contante, l'attività di caricamento valori nelle apparecchiature ATM remote è affidata all'outsourcer B.T.V, le cui prestazioni vengono monitorate dalla Funzione Logistica e sono risultate adeguate nel rispetto di quanto previsto contrattualmente.

Sempre nell'ambito della gestione del contante, si segnala che le filiali non dispongono dell'informativa sulla giacenza di denaro presente negli apparati cash in e che non viene segnalato il superamento del massimale stabilito per ciascun apparato, con il rischio anche di subire perdite economiche derivanti da rapine di importi superiori al tetto stabilito (gap n. 6).

ACQUISTO PARCO ATM

Nel corso del 2017, per supportare i piani di sviluppo del progetto strategico Banca Più, la Funzione Acquisti, in sinergia con le Funzioni Commerciali, Logistica e Immobiliare, è stata impegnata nello svolgimento di gare competitive per l'acquisto delle nuove apparecchiature, interessando i maggiori player tecnologici sul mercato.

Per mettere a terra la decisione del Novembre 2017 di anticipare l'acquisto di n. 1.020 ATM, da ricevere e capitalizzare entro la fine dell'anno, la Funzione Acquisti ha preso immediati impegni con i fornitori per poter dare il via alla produzione/personalizzazione degli apparati. Tali impegni sono poi risultati in parte disattesi nel Dicembre 2017, quando è stato deciso di dimezzare l'investimento e quindi il numero delle macchine ordinate. In particolare la Banca non ha dato corso all'acquisto di 503 ATM dal fornitore NCR, con il quale, alla data di pubblicazione del presente rapporto, la Funzione Acquisti sta gestendo un'attività di mediazione finalizzata a trovare un accordo commerciale ed evitare un contenzioso.

PRESIDI DI SICUREZZA FISICA

Le misure di sicurezza fisica, necessarie per la salvaguardia degli ATM, sono adeguatamente governate dalla Funzione Sicurezza Fisica, sebbene l'operatività sia distribuita su più Funzioni della Banca. La Funzione ha stabilito uno standard contenente specifiche e dettagliate indicazioni circa i presidi di sicurezza fisica da adottare, in funzione del livello di rischio cui sono esposti i singoli ATM; l'analisi di rischio è stata effettuata e viene mantenuta dalla stessa Funzione. Tale standard non è pubblicato in normativa, ma risulta comunque diffuso a tutte le strutture che si occupano dell'installazione degli ATM (ATM Manager e Funzione Immobiliare), le quali agiscono in conformità allo stesso.

Gli interventi effettuati nel 2017 e quelli pianificati per il 2018 sono stati finalizzati a ricondurre tutti gli ATM di filiale ad un livello di rischio basso/medio-basso. Il progetto di messa in sicurezza degli ATM non comprende quelli remoti, per i quali la sicurezza fisica è demandata all'ente ospitante ed è compresa nel canone di affitto degli spazi.



Executive Summary (3 di 3)

SICUREZZA
LOGICA ED
INFRASTRUTTU
RA IT

Importanti carenze di sicurezza sono state rilevate nella gestione delle utenze relative ai software operanti sulle macchine ATM. Si rileva in particolare l'assenza di standard tecnici ai quali attenersi per l'assegnazione dei diritti di accesso ad utenti e applicazioni, che risultino strettamente limitati alle reali esigenze operative, nonché di verifiche atte ad assicurare che tali standard vengano rispettati (gap 1).

Le suddette carenze in termini di gestione delle utenze sono risultate peraltro una delle concause dell'incidente informatico che, in data 19 febbraio u.s. ha comportato il blocco di alcuni ATM con un picco massimo di 430 macchine. Infatti, nonostante l'incidente sia stato innescato da un'attività di installazione non autorizzata da parte di un fornitore del COG, contravvenendo agli standard in termini di processo di rilascio in produzione, il blocco delle macchine avrebbe potuto essere evitato se al software fossero state assegnate le sole abilitazioni strettamente necessarie al suo operato e non quelle equivalenti agli amministratori del sistema.

L'incidente è stato gestito in maniera coordinata, tempestiva ed efficace, ma ha tuttavia evidenziato l'assenza di soluzioni strutturate di Continuità Operativa ("BCM") e Disaster Recovery ("DR") in grado di coprire scenari di indisponibilità di componenti distribuite del sistema informativo (ad esempio ATM o postazioni di lavoro nelle filiali), dovuti ad esempio ad errori operativi, come nel caso in oggetto, incidenti di sicurezza o attacchi cyber. Tali scenari, tutt'altro che improbabili, devono essere oggetto di adeguate valutazioni in coerenza con gli obiettivi strategici del Gruppo in tema di continuità operativa e di contenimento dei rischi.

In corso di revisione la Funzione di Audit ha provveduto ad anticipare agli Organi Apicali una nota di dettaglio sulle cause che hanno generato il blocco degli ATM. Tale nota è stata veicolata anche al team ispettivo di Banca d'Italia all'epoca impegnato presso la Banca in una revisione sui Rischi IT.

Relativamente alla sicurezza delle reti informatiche, la possibilità di connessione diretta alla intranet aziendale da parte degli ATM e delle sedi da cui opera il personale Basilichi (gap 2) implica un rischio di accesso non autorizzato che deve essere adeguatamente valutato per poi procedere all'implementazione delle più adeguate misure di segregazione delle reti aziendali.

Dall'esame delle prassi utilizzate per il rilascio di modifiche al software è emerso che l'attività di rilascio in produzione viene effettuata da Basilichi e non dal COG, funzione owner del processo, in assenza di copertura contrattuale (gap 3).

L'analisi delle utenze ha evidenziato carenze nella loro gestione, sia per quanto riguarda quelle di amministrazione delle macchine ATM (gap 4), che di quelle per l'utilizzo dell'applicativo (GE.BA.) deputato alla gestione in accentrato di tutti gli ATM (gap 5).

La modalità operativa che permette ai nostri clienti di accedere agli ATM senza una carta di debito/credito (operatività «cardless») deve essere rafforzata in termini di sicurezza in quanto le credenziali per accedere al servizio (le stesse del Digital Banking) vengono inviate ai server centrali senza l'utilizzo di sistemi di cifratura, esponendo il cliente al rischio di furto delle credenziali (gap 7).

Relativamente infine alla gestione del fornitore TAS (proprietario delle applicazioni deputate al funzionamento del mondo ATM), sono state evidenziate carenze nel monitoraggio degli interventi di assistenza di secondo livello (gap 8).

Si osserva infine che Microsoft cesserà il supporto dei sistemi operativi attualmente installati sugli ATM, XP Windows Embedded e Windows 7, rispettivamente a gennaio 2019 e gennaio 2020. L'utilizzo di sistemi non più supportati espone a rischi di sicurezza e di malfunzionamenti. Benché la tematica risulti già indirizzata dalle strutture tecniche, è necessario quindi mantenere alta l'attenzione sull'argomento.



Agenda

- 1 Contesto di riferimento
- 2 Punti di attenzione
- 3 Focus acquisto straordinario ATM di fine 2017
- 4 Focus Incidente ATM del Febbraio 2018
- 5 Attività di verifica
- 6 Audit findings

Allegati



1 Contesto di riferimento (1 di 2)

Ruoli e responsabilità

Attori Coinvolti	Responsabilità
Servizio Digital Banking e ATM	Processo: Presidio canale ATM e Self Banking <ul style="list-style-type: none"> Elaborazione piano distributivo Sviluppo nuove funzionalità ATM Monitoraggio performance ATM Coordinamento operativo Piano ATM Modelli commerciali ATM
Servizio Cash Management , ATM e Logistica	Processo: Gestione filiera del contante <ul style="list-style-type: none"> Governo e gestione operativa ATM Elaborazione piano sostitutivo Mantenimento in esercizio degli ATM Presidio della relazione contrattuale con gli <i>outsourcer</i> Gestione contante ATM remoti
Servizio Sicurezza Logica e Continuità Operativa	Processo: Gestione dei processi operativi di sicurezza logica <ul style="list-style-type: none"> Strategia e governo dei presidi di Sicurezza Logica
Servizio Sicurezza Fisica e Assicurazioni	Processo: Gestione dei processi operativi di sicurezza fisica <ul style="list-style-type: none"> Governo e gestione dei presidi di Sicurezza Fisica installati sugli ATM Monitoraggio Allarmi
COG Operativo Gruppo Montepaschi	Processi : Enterprise Architecture Management Change Release e Deployment Management Gestione dei processi operativi di sicurezza logica <ul style="list-style-type: none"> Gestione/sviluppo infrastruttura e software ATM Implementazione soluzioni di sicurezza logica e gestione reti
<i>Outsourcer</i>	Attività in full outsourcing <ul style="list-style-type: none"> Basilichi: servizi afferenti il ciclo di vita degli ATM B.T.V.: trasporto e caricamento contanti

ATM MANAGER

Figura creata all'interno del Servizio Cash Management ATM e Logistica:

- ✓ Costituisce punto di riferimento per le tematiche del mondo ATM.
- ✓ Coordina il processo di installazione e sostituzione.
- ✓ Monitora le relazioni con gli *outsourcer*.



1 Contesto di riferimento (2 di 2)

ATM attivi al 31/5/2018 (*)

Tipologia	Nr. ATM	Di cui in Filiale	Di cui remoti
Cash OUT	1.744	1.192	552
Cash IN e EVO	1.052	1.046	6
Totale	2.796	2.238	558

Il parco ATM risulta composto da n. 2.796 apparati, di cui il 37,6% è dotato di funzionalità "cash in – cash out"

I 558 ATM remoti sono costituiti da apparati installati in luoghi ad alto potenziale di operatività, all'interno di enti/aziende/centri commerciali, o presso le filiali, ma non gestiti direttamente dalle stesse.

L'età media del parco ATM è di ca. 6 anni a mezzo, 3 anni per i cash-in e 8 per i cash-out.

Programma Banca più (**)

Lo sviluppo del parco ATM, in termini di numero e tipologie degli apparati e di nuove funzionalità sono tra gli obiettivi del programma strategico Banca Più (cantieri Self Banking)

Nel 2017 sono stati conseguiti i seguenti risultati:

- ☐ installazione di 400 ATM *cash in*, per consentire l'operatività in *self banking* di alcune operazioni di cassa;
- ☐ migrazione di ca. il 45% delle operazioni di versamento dalla cassa agli ATM;
- ☐ avvio nuova funzionalità ATM *cardless* che consente di operare sull'ATM senza la carta.

Per il 2018 sono previsti i seguenti obiettivi

- ☐ installazione di ulteriori 300 apparati cash-in;
- ☐ migrazione del 60% delle operazioni di versamento dalla cassa agli ATM.

Piano ATM 2018 (***)

Il Piano ATM 2018, da completare entro la fine del corrente anno, combina:

- ☐ il piano distributivo delle 300 nuove installazioni del programma Banca Più della Funzione Commerciale;
- ☐ il piano di sostituzione per aggiornamento tecnologico di 260 unità svolto dalla Funzione Logistica.

Al 31/5/2018 sono state eseguite più del 46% delle installazioni complessivamente pianificate.

Tipologia	Pianificato	Installato
Cash out	60	17
Cash in ed EVO	500	230
Totale	560	247

(*) Dati: Cruscotto ATM al 31/5/2018.

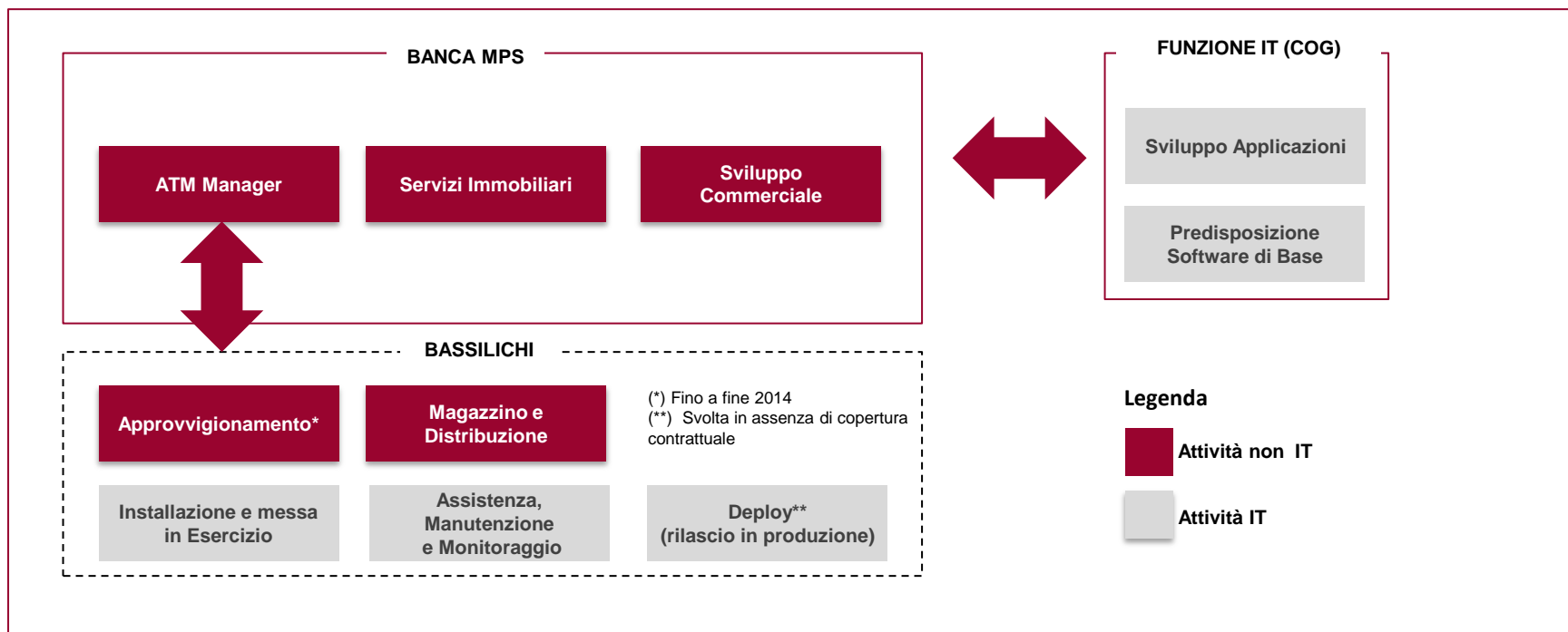
(**) Progetti Direzione CCO - Programma Banca Più – Ipotesi evoluzione 2018 (SAL Febbraio 2018) e STEERING COMMITTEE Maggio 2018

(***) Tavolo ATM



2 Punti di attenzione (1 di 3): modello organizzativo

L'attuale modello organizzativo per la gestione degli ATM è attualmente così costituito:



PUNTO DI ATTENZIONE

- Nel 2015, l'istituzione in BMPS della figura dell'ATM Manager e la contestuale migrazione del contratto con Basilichi dal Consorzio alla Banca ha ridistribuito il governo e la responsabilità di alcune attività legate al mondo dell'IT, in particolare quelle svolte dallo stesso fornitore Basilichi.
- Nell'attuale modello organizzativo le attività di natura IT svolte dal fornitore non risultano infatti più responsabilità del Consorzio che, secondo la strategia aziendale, ha invece il compito istituzionale di gestire i sistemi informativi, nell'ottica della centralizzazione dei servizi informatici a livello di Gruppo.
- La coerenza dell'attuale modello organizzativo dovrà essere rivalutata nel più ampio ambito di definizione delle strategie attualmente in corso sul complessivo assetto della Funzione IT di Gruppo (progetto «Venere»).
- La tematica verrà sottoposta all'attenzione della Direzione Chief Operating Officer.



2 Punti di attenzione (2 di 3): contratto di *outsourcing* con Bassilichi

Contratto Bassilichi: storia e situazione attuale

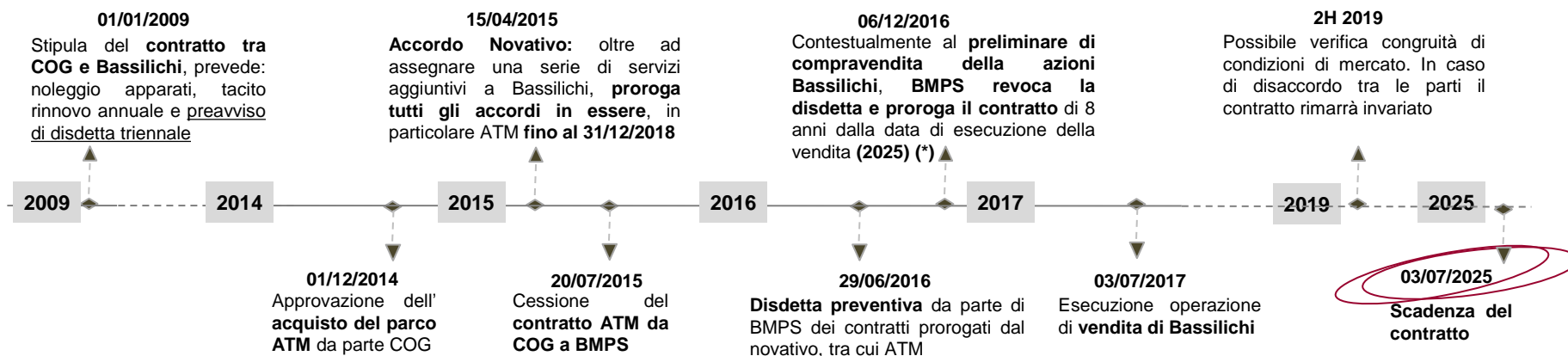
La società Bassilichi fornisce alla Banca i servizi afferenti alla gestione del ciclo di vita degli apparati ATM, in particolare:

- l'approvvigionamento (fino a fine 2014 – successivamente il servizio non è più attivo in quanto le macchine ATM sono diventate di proprietà di BMPS);
- la gestione del magazzino;
- la gestione dei servizi di attivazione e messa in esercizio degli ATM;
- il servizio di assistenza, manutenzione (ordinaria e straordinaria) e il monitoraggio.

Il contratto, ancora in vigore, è stato stipulato l'1/1/2009 e ha scadenza 3/7/2025. L'importo del contratto varia a seconda del numero di ATM; per il 2017 sono stati pagati circa €mln 13.

Nel corso degli anni il contratto è stato oggetto di alcune **estensioni di durata per ragioni non strettamente correlate alla mondo ATM** (es. contratto Novativo, contratto di compravendita relativa alle azioni Bassilichi).

Gli eventi principali che hanno caratterizzato la vita del contratto sono di seguito rappresentati:



(*) In tale ambito vengono contemporaneamente prorogati anche i contratti CBI (Corporate Banking Interbancario) e POS per un valore complessivo di circa €mln 40.

PUNTO DI ATTENZIONE

- Il contratto non può essere disdetto fino al 2025.
- Il contratto è risultato non più attuale nei contenuti e non più competitivo rispetto alle condizioni di mercato (la Funzione Acquisti ha effettuato un'analisi di mercato che ha portato a stimare potenziali saving per circa il 20% dell'importo contrattuale).
- E' previsto un sistema di penali con tetto massimo non significativo rispetto all'importo contrattualizzato (€43K vs €mln13).
- Nonostante i vincoli contrattuali, in un'ottica di continuità commerciale, è opportuno verificare la disponibilità di Nexi-Bassilichi a rivedere almeno le clausole contrattuali più svantaggiose per la Banca.
- La tematica verrà sottoposta all'attenzione della Funzione Acquisti.



2 Punti di attenzione (3 di 3): soluzioni di Continuità Operativa

Per Continuità Operativa del Business (Business Continuity) si intende la possibilità che i processi ritenuti critici dall'Azienda possano mantenere un livello di funzionamento accettabile anche a seguito di incidenti, catastrofici o meno, che colpiscono direttamente o indirettamente l'azienda. Il Piano di Continuità Operativa (PCO) definisce le strategie ed i principi e descrive le procedure per garantire la Continuità Operativa dei processi aziendali critici e sistemici. In tale contesto devono essere analizzati **scenari di emergenza a fronte dei quali predisporre adeguate soluzioni** atte a garantire il ripristino, nei tempi e nei modi ritenuti tollerabili, dei processi impattati.

Piano di Continuità Operativa - Scenari

L'attuale **PCO** della Banca ha soluzioni codificate a fronte di **scenari** di crisi che prevedano un **impatto sui processi svolti in accentrato**

Distruzione o inaccessibilità di strutture nelle quali sono allocate unità operative o apparecchiature critiche

Indisponibilità di personale essenziale per il funzionamento dell'azienda

Indisponibilità dei sistemi informativi

A fronte di questo scenario è definita la soluzione di Disaster Recovery (DR), questa stabilisce le misure tecniche e organizzative per fronteggiare eventi che provochino la indisponibilità dei Centri di Elaborazione Dati (CED). Il piano di DR, finalizzato a consentire il funzionamento delle procedure informatiche rilevanti in siti alternativi a quelli di produzione, costituisce parte integrante del piano di continuità operativa.



Il piano di DR della Banca prende in considerazione lo scenario di indisponibilità del sistema informatico centrale (CED di Firenze), codificando le procedure per il suo ripristino presso il sito alternativo (CED di Siena).

PUNTO DI ATTENZIONE

Le attuali soluzioni di BCM/DR non coprono scenari di crisi che prevedano un impatto diffuso sulle componenti distribuite del sistema informativo (ad esempio ATM o PdL di filiale). Gli avvenimenti recenti (incidente ATM del 19/2/2018, comunicazione CERTFin in merito a vulnerabilità ATM, etc.) hanno dimostrato come tali eventi possano realmente accadere e, pertanto, debbano essere oggetto di adeguate valutazioni in coerenza con gli obiettivi strategici del Gruppo in tema di BCM/DR e di contenimento dei rischi.

La tematica verrà sottoposta all'attenzione della Funzione Sicurezza con il supporto della Funzione Rischi di Capogruppo.



3 Focus acquisto straordinario ATM di fine 2017(1 di 2)

Sfruttando una disponibilità di budget Capex residua da altre progettualità, nel Novembre 2017 le funzioni Commerciale e Logistica, in accordo con l'AD, hanno deciso di anticipare l'acquisto di n. 1.020 ATM che, nel corso del 2018, sarebbero serviti sia per la sostituzione degli apparati obsoleti, sia per raggiungere gli obiettivi di copertura del progetto Banca Più.

L'acquisto, per complessivi € mln 19, prevedeva n. 260 ATM per la sostituzione di apparati obsoleti (esigenza Funzione Logistica) e n.760 ATM (cash-in evoluti) da installare nelle aree self services delle filiali per obiettivi Commerciali rientranti nel Programma Banca Più.

Per poter ricevere e capitalizzare entro la fine dell'anno i 1.024 ATM, la Funzione Acquisti ha preso immediati impegni con i fornitori per poter dare il via alla produzione/personalizzazione degli apparati.

I suddetti impegni sono poi risultati in parte disattesi nel Dicembre 2017, quando l'AD ha deciso di dimezzare l'investimento e quindi il numero delle macchine ordinate, in un contesto di riduzione degli investimenti, di coerenza con le linee guida del Piano Industriale, e di maggior cautela dal punto di vista gestionale.

La Funzione Immobiliare ha in particolare revocato l'impegno di acquisto di 503 ATM verso il fornitore NCR, con il quale, alla data di pubblicazione del presente rapporto, sta tuttora gestendo un'attività di mediazione finalizzata a trovare un accordo commerciale. Al momento non si può ancora escludere il rischio di contenzioso con il fornitore.

Di seguito vengono rappresentati i principali eventi che si sono succeduti a partire del 4Q 2017 al 2Q 2018:

**Inizio novembre
2017**

Viene effettuata, da parte della Funzione Acquisti, una trattativa economica con i tre principali fornitori della Banca (NCR, Wincor e Bassilichi - distributore unico di Hyosung) per l'acquisto di n. 1.020 macchine, con la seguente ripartizione:

- n. 503 ATM di marca NCR;
- n. 412 ATM di marca WINCOR (produttore Diebold-Nixdorf);
- n. 105 ATM di marca HYOSUNG (distribuiti tramite Bassilichi).

**15 novembre
2017**

Viene condiviso con l'AD il conferimento di budget residui da altre progettualità per l'acquisto anticipato dei suddetti ATM (Progetto Condor).

**17 novembre
2017**

La Funzione Acquisti, in data 17/11/2017, anticipa una lettera di impegno all'acquisto dei 1.020 ATM a Bassilichi in qualità di "Main Contractor Multivendor" e due lettere, rispettivamente a NCR e Diebold Nixdorf, in cui si comunicano ai fornitori le intenzioni di acquisto e le modalità di consegna.

Sudette lettere di impegno sono state ritenute necessarie dalla Funzione Acquisti per poter ricevere e capitalizzare gli apparati ATM entro l'anno, trovandosi nell'impossibilità tecnica di effettuare regolare ordine a compimento del ciclo approvativo della spesa in SAP, in quanto:

- era necessario chiedere ai fornitori di avviare subito la produzione, in quanto gli ATM, per poter essere spesi nel 2017, dovevano essere consegnati in magazzino entro fine dicembre e i tempi di produzione richiedevano almeno 6 settimane;
- risultava impossibile avviare l'iter approvativo della spesa in SAP (RdA - Richiesta di Acquisto) in quanto dovevano ancora essere avviate le necessarie attività per dar corso alle variazioni di budget (trasferimenti a saldo zero all'interno del Piano Progetti 2017).



3 Focus acquisto straordinario ATM di fine 2017(2 di 2)

**Fine dicembre
2017**

Regolarizzazione dell'iter autorizzativo in SAP con inserimento di una RdA di importo pari a €mln 18,7 rientrante nell'autonomia dell'AD. L'RdA viene firmata dal Chief Operating Officer e dal VDG, ma rimane sospesa alla firma dell'AD.

**11 dicembre
2017**

L'AD, sentita la Funzione Acquisti, la Funzione Logistica e quella Funzione Commerciale, decide di ridurre il numero di ATM da acquistare da 1.020 a 500. I principali motivi di tale scelta riguardano una maggiore attenzione agli impegni economici assunti dalla Banca in un contesto di riduzione degli investimenti, di coerenza con le linee guida del Piano Industriale, e di maggior cautela dal punto di vista gestionale, in quanto l'acquisto di un primo lotto di macchine avrebbe permesso di sondare sul campo i risultati dell'operazione e solo in un secondo momento, qualora tali risultati fossero risultati soddisfacenti, procedere all'acquisto di un secondo lotto per il completamento del progetto.

**27 - 28 dicembre
2017**

Viene respinta dall'AD la RdA originale e dell'AD e viene inserita dalla Funzione Acquisti una nuova RdA per €mln 9,4 finalizzata all'acquisto di n. 500 apparati, così suddivisi:

- n. 105 di marca Hyosung (numero invariato);
- n. 395 di marca Wincor (diminuzione di 17 unità);
- nessuna macchina di marca NCR.

La nuova distribuzione, definita dalla Funzione Acquisti, aveva l'obiettivo di:

- evitare di dover fare un'ulteriore trattativa economica, non possibile nei ristrettissimi tempi richiesti per la chiusura dell'iter e sicuramente peggiorativa per la Banca, e mantenere, almeno per due dei tre fornitori, le quantità per cui era già stato concordato il prezzo in fase di gara;
- ridurre al minimo il rischio di cause legali (di fatto concentrandolo su di un unico fornitore);
- penalizzare il fornitore NCR che la Funzione riferisce avesse all'epoca peggiorato la qualità dell'assistenza tecnica.

L'iter approvativo di ciclo passivo viene concluso al limite del tempo utile per consentire la contabilizzazione a cespiti entro l'anno solare, come prescritto dalle normative di bilancio.

**gennaio - giugno
2018**

La Funzione Acquisti avvia un'attività di mediazione con il fornitore NCR, escluso dall'acquisto, finalizzata alla chiusura bonaria della vicenda. In particolare, la Banca si è resa disponibile all'acquisto di n. 34 macchine, utilizzando parte del budget 2018 originariamente destinato all'installazione delle 1.020 macchine e non abbattuto in fase di definizione delle esigenze.

L'impegno ad acquisto dal fornitore NCR n. 34 macchine non esclude un contenzioso. Alla data di pubblicazione del presente rapporto il fornitore richiede la fornitura di n. 100 ATM entro il 2018 e la conclusione di un accordo commerciale che favorisca per un certo periodo di tempo il mantenimento della quota di mercato di NCR in MPS.



4 Focus incidente ATM del Febbraio 2018

In data 19 Febbraio u.s. si è manifestata un'anomalia tecnica sul parco ATM che causava il blocco di parte delle macchine. Le strutture operative hanno identificato come causa dell'incidente un intervento tecnico effettuato dal fornitore Fabbrica Digitale, a cui Basilichi, ditta appaltatrice per il COG del servizio di Digital Signage¹, ha subappaltato la fornitura del software a supporto (Xuniplay).

Tale intervento, mirato a rimuovere un file di log che generava problemi di spazio sul disco fisso degli ATM, è stato effettuato mediante la distribuzione di un file di configurazione in cui era presente un errore sintattico ed ha causato, sulle sole macchine con sistema operativo Windows XP Embedded (n. 1.456 su 2.758), la cancellazione di alcuni file di sistema. Gli ATM continuavano regolarmente ad erogare il servizio, ma, in caso di riavvio, la macchina si bloccava, richiedendo un intervento tecnico on-site per un nuovo set up. Lo stesso file non ha prodotto invece anomalie sulle macchine con sistema Windows 7.

Il COG e le Funzioni di Governo degli ATM della Banca hanno cooperato al fine di individuare la problematica, ridurne al minimo l'impatto e approntare idonee contromisure nei giorni successivi all'evento. Da subito sono state attuate tutte le misure, tecniche e organizzative, necessarie ad impedire il riavvio programmato degli ATM, riuscendo così a stabilizzare il numero di quelli bloccati. Il picco massimo di disservizio si è raggiunto il 25 febbraio con 430 macchine ferme (15% del totale). Le attività di ripristino complessive sono terminate il giorno 8/3/2018.

Dagli approfondimenti svolti è stato appurato che la distribuzione del file di configurazione è stata svolta da Fabbrica Digitale senza il rispetto delle fasi autorizzative previste dal processo di Change Release e Deployment Management (che governa le modifiche del software in ambiente di produzione), nonostante il COG avesse più volte esplicitato al fornitore tale vincolo, peraltro già rispettato nelle precedenti occasioni. Inoltre, l'operatore di Fabbrica Digitale ha eseguito le modifiche ricorrendo ad una funzionalità di distribuzione di cui il COG non era a conoscenza e che aveva piuttosto chiesto di eliminare.

Si osserva altresì che la cancellazione dei file di sistema che ha determinato il blocco degli ATM non sarebbe comunque stata possibile se alle componenti software installate sulle macchine fossero stati assegnati profili abilitativi circoscritti alle effettive necessità applicative, piuttosto che privilegi di amministratore che, di fatto, rendevano possibile il pieno controllo della macchina.

L'incidente è stato comunicato agli organi apicali ed al CdA della Banca e, in ragione di tale escalation, è stato anche segnalato all'Autorità di Vigilanza in data 26 febbraio 2018. Per maggiori dettagli fare riferimento alla "Relazione Incidente ATM" consegnata al "Collegio Sindacale" ed al "Comitato dei Consorziati" in data 10 Maggio 2018.

¹ Digital Signage è una forma di comunicazione digitale, i cui contenuti vengono mostrati ai destinatari attraverso schermi elettronici appositamente sistemati in luoghi pubblici.

NOTA



L'incidente è stato gestito in maniera coordinata, tempestiva ed efficace, ciò ha permesso di limitare l'impatto sulla Banca.



Assenza in fase progettuale di una dettagliata analisi di sicurezza finalizzata all' "hardening" dei sistemi (**Gap 1**)



Le attuali soluzioni di BCM e DR non coprono scenari di Cyber incident/attack con impatto diffuso sulle componenti distribuite del sistema informativo (ad esempio ATM o PdL di filiale).



5 Attività svolta: premessa

Tenuto conto della complessità della materia e della pluralità di processi interessati e dei soggetti coinvolti, le verifiche sono state effettuate partendo da una rappresentazione che, sulla base del modello del Ciclo di Deming (Plan, Do, Check, Act), definisce un processo logico all'interno del quale sono collocati i processi aziendali (così come formalizzati nell'applicativo ARIS).

I seguenti processi ARIS relativi all'ambito *Supporto* sono stati analizzati limitatamente alla materia trattata nella presente revisione:

- ☐ Gestione filiera del contante,
- ☐ Enterprise architecture management,
- ☐ Change, Release e Deployment Management,
- ☐ Gestione dei processi di sicurezza logica,
- ☐ Gestione dei processi operativi di sicurezza fisica.

Di seguito sono rappresentate in grigio le fasi del processo logico, mentre in rosso sono presentati i processi aziendali.



5 Attività svolta: premessa - legenda degli obiettivi di controllo SREP

Nell'ambito delle attività di verifica sono stati presi in esame i seguenti obiettivi di controllo SREP

- **IG 1.2** - Verificare la presenza una chiara divisione dei poteri e delle responsabilità a tutti i livelli, dalle singole unità organizzative agli organi aziendali. Accertare inoltre che siano chiaramente definite le linee di riporto e il collocamento gerarchico dell'intera struttura organizzativa, nel rispetto del principio di segregation of duties e dei vincoli normativi esistenti (es: collocamento gerarchico delle Funzioni Aziendali di Controllo)
- **IG 2.3** - Verificare che le strategie e le politiche adottate siano comunicate a tutto il personale interessato e che la cultura del rischio sia applicata a tutti i livelli dell'ente
- **IG 2.6** - Verificare che i Responsabili delle diverse linee di business pongano in essere dei controlli efficaci ad identificare, monitorare e segnalare il superamento dei limiti di rischio loro assegnati, agendo in maniera tempestiva nei casi di sfioramento dei limiti di rischio assegnati
- **IG 2.11** Verificare l'esistenza di adeguati e strutturati flussi informativi sia verticali che orizzontali e che gli stessi siano opportunamente codificati
- **IG 6.3** Verificare l'adozione di un set di controlli di linea e la regolare esecuzione da parte delle unità organizzative coinvolte nei processi aziendali
- **IG 7.6** - Verificare che il Gruppo/ la Banca possieda appropriati sistemi IT, infrastrutture e processi in modo da fornire adeguate, tempestive e complete informazioni all'Organo con Funzione di Supervisione Strategica e all'Organo con Funzione di Gestione per l'identificazione dei rischi e per la sorveglianza.
- **BM 7.8** - Verificare che gli interventi IT vengano effettuati in ottica prospettica (sviluppi strategici in tema di IT), sottoponendo i sistemi a un processo di "continuous innovation" e minimizzando gli ostacoli creati dai "legacy systems "

OBIETTIVO

Accertare che i processi decisionali connessi alla installazione dei nuovi ATM siano oggettivi, documentati e che ne sia verificata ex-post l'efficacia.

Obiettivi SREP: IG 1.2, IG 2.11, IG 6.3

PERIMETRO/ METODOLOGIA

- ☐ Interviste, analisi documentale, analisi di dati, osservazione delle prassi
- ☐ Periodo di riferimento: anno 2018

RISCHI IMPATTATI

ID50837: Mancata, non chiara o incompleta definizione degli obiettivi commerciali

ID50453: Rischio che la definizione dei prodotti non sia supportata da un adeguata analisi tecnico e commerciale

VERIFICHE SVOLTE

- a) Analisi del D00751 – Regolamento n. 1 – Organizzazione della Banca MPS, del Catalogo dei Processi e dei documenti normativi connessi

- b) Analisi delle modalità di definizione del piano distributivo ATM e sua esecuzione

ESITI

Le responsabilità connesse con l'attività in esame sono chiaramente assegnate.

In particolare, è attribuito alla Funzione Commerciale il compito di elaborare periodicamente il “piano distributivo di gruppo degli strumenti di self-banking” ed i programmi globali di razionalizzazione della presenza territoriale degli stessi ed eventuali revisioni.

Nel continuo, la Funzione Commerciale è chiamata a presidiare l'esecuzione delle attività necessarie a installare e riallocare/disinstallare gli apparati compresi nel piano distributivo.

Il piano distributivo è, insieme al piano di sostituzione, una delle due componenti del “Piano ATM” e si occupa sostanzialmente di aggiungere nuovi apparati (ampliamento cash-in) e della sostituzione di macchine esistenti con nuove, dotate di maggiori funzionalità (upgrade da cash-out a cash-in).

La definizione del piano distributivo inizia con la determinazione del numero di nuovi apparati da installare, stabilito tenendo conto dei vari progetti che insistono sul mondo ATM, del numero di apparati in magazzino, nonché del budget disponibile per nuovi acquisti e per interventi immobiliari di allestimento delle aree self e esecuzione delle installazioni. Per il 2018, l'obiettivo è stato fissato a 300 installazioni.

Il piano distributivo consiste inizialmente di un elenco teorico di filiali dove la Funzione Commerciale intende installare nuovi apparati.

Tali filiali, tenendo conto degli indirizzi strategici aziendali, sono individuate assegnando alle stesse un target di macchine (assegnazione ideale di numero e tipologia) con calcoli che tengono conto del numero di operazioni di prelievo e versamento rilevate nell'anno solare, nonché dei numeri di clienti, conti correnti e carte.

VERIFICHE SVOLTE

ESITI

Successivamente, dopo un confronto con la Funzione Logistica per analizzare le possibili interferenze con il piano di sostituzione da questa predisposto, viene effettuata, congiuntamente alla Funzione Immobiliare, una prima analisi a tavolino delle planimetrie delle filiali (c.d. "esame desk") per valutare la fattibilità delle installazioni.

I siti per cui le installazioni sono valutate fattibili sono di volta in volta comunicati al c.d. "Tavolo ATM" e, insieme a quelli ricompresi nel piano di sostituzione, entrano nel c.d. "elenco siti", che rappresenta, nella sostanza, il "Piano ATM".

Riguardo all'esecuzione del piano 2018, la Funzione Commerciale, sulla base delle analisi fatte sull'operatività delle filiali, ha individuato n. 456 filiali; questo primo elenco è stato trasmesso (in data 10/11/2017) alla Funzione Immobiliare per svolgere congiuntamente le verifiche di fattibilità.

Delle 456 filiali originarie, alla data del 1/6/2018 è stata richiesta l'installazione per n. 236 apparati (95 ampliamenti e 141 upgrade). Di questi, alla stessa data, sono stati effettivamente installati 90, complessivamente in linea (94%) con la pianificazione di inizio anno.

c) Verifica della coerenza del piano distributivo 2018 con le strategie aziendali

Il piano distributivo 2018 tiene conto degli obiettivi del programma strategico "Banca Più", che inizialmente prevedeva di dotare ogni filiale di un ATM cash-in, al fine di spingere sulla migrazione delle operazioni di cassa verso i canali remoti. Il 2017 si è, in effetti, concluso con il potenziamento della Rete ATM con 400 cash-in, raggiungendo così un parco di 913 ATM, distribuiti in 850 filiali.

Per il 2018 gli obiettivi iniziali del programma sono stati rivisti in un'ottica di rimodulazione degli impegni economici della Banca e di maggior cautela dal punto di vista gestionale, oltre che a seguito delle esperienze del 2017 in ordine alle verifiche sui siti effettuate dalla Funzione Immobiliare, alle problematiche hardware connesse con lo sviluppo delle nuove funzionalità e non ultimo alle capacità di execution della filiera di installazione.

Per il 2018 saranno installati 300 cash-in, con circa 300 filiali che, a fine piano, rimarranno prive di tale apparato.

Tenuto conto di quanto sopra, la Funzione Commerciale ha prodotto inizialmente un primo elenco teorico di 456 filiali, ordinate per priorità, da cui, dopo le verifiche di fattibilità immobiliari, estrarre quelle dove installare effettivamente gli apparati.

Al momento della verifica erano già stati messi in esercizio n.230 ATM evoluti.

VERIFICHE SVOLTE

- d) Analisi delle modalità di funzionamento dei c.d. "Tavolo ATM"

Il "Tavolo ATM" è la sede in cui il piano distributivo ed il piano di sostituzione vengono trasformati da piani "teorici" in decisioni di singole installazioni da effettuare. Si tratta di un gruppo di lavoro informale, che si riunisce settimanalmente, coordinato dalla Funzione Logistica, cui partecipano le funzioni Commerciale, Immobiliare, l'*outsourcer* Basilichi e, a seconda dei casi, la Funzione Sicurezza.

In tale sede vengono discussi i vari aspetti tecnico/logistici connessi all'installazione degli ATM (pianificazione e esito dei sopralluoghi immobiliari, problematiche di sicurezza, etc.) e concordate le relative attività propedeutiche (p.es. sopralluoghi, interventi immobiliari, etc.).

Successivamente Basilichi procede in autonomia all'esecuzione, coordinandosi con le funzioni aziendali interessate, per lo più con la Funzione Immobiliare ed il Dipartimento Organizzazione Area Territoriale di riferimento, per poi riferire nella successiva sessione del Tavolo su quanto effettuato e su quanto pianificato per le settimane successive.

Al Tavolo vengono portate anche situazioni particolari, non previste né prevedibili all'inizio del processo, che rendono necessarie nuove installazioni o sostituzioni.

Il Team di Audit ha partecipato, in qualità di osservatore, ai Tavoli tenutisi nel mese di aprile, constatando il dettaglio delle analisi effettuate e l'efficace coordinamento delle diverse funzioni coinvolte da parte di ATM Manager.

- e) Analisi del processo decisionale per l'installazione degli ATM remoti e di verifica ex-post dell'efficacia

Il processo decisionale per l'installazione degli ATM remoti è stato definito e condiviso con le AT nella seconda metà del 2017 nell'ambito delle iniziative del programma "Banca Più" e prende l'avvio dalla segnalazione, da parte delle strutture di Rete, dell'opportunità commerciale dell'iniziativa.

La decisione viene presa dalla Funzione Commerciale sulla base di un *business case* a 3 anni, che considera una serie di informazioni (ricavi stimati, costi, possibilità di acquisizione di clientela, etc.), stabilite dalla Funzione Commerciale medesima e fornite dalle strutture di Rete mediante un template.

Dall'analisi della documentazione fornita al Team di Audit è emerso che nel 2017 la Funzione Commerciale ha ricevuto n. 10 richieste di nuove installazioni, di cui n. 8 sono state accolte. Nel 2018 le richieste sono state n. 2, entrambe accolte. Per tutte è stato predisposto e valutato il *business case*.

Per valutare ex post l'efficacia delle decisioni, nel mese di marzo u.s. la Funzione Commerciale, sempre nell'ambito delle iniziative del programma "Banca Più" ha avviato un'attività strutturata di ottimizzazione della rete degli ATM remoti, basata sulla valutazione della redditività degli ATM.

Sulla base di un modello sviluppato internamente, che tiene conto dei ricavi prodotti dall'ATM e dei relativi costi di gestione, sono stati individuati n. 106 ATM, di cui è stata proposta alle rispettive AT la dismissione.



OBIETTIVO

Accertare che i processi decisionali connessi alla sostituzione degli ATM siano oggettivi, documentati e che ne sia verificata ex-post l'efficacia.

PERIMETRO/ METODOLOGIA

- ☐ Interviste, analisi documentale, analisi di dati, osservazione delle prassi
- ☐ Periodo di riferimento: anno 2018

RISCHI IMPATTATI

ID55679: Obsolescenza dell'impianto hardware

Obiettivi SREP: IG 1.2, IG 2.11, IG 6.3

VERIFICHE SVOLTE

- a) Analisi del D00751 – Regolamento n. 1 – Organizzazione della Banca MPS, del Catalogo dei Processi e dei documenti normativi connessi

ESITI

Le responsabilità connesse con l'attività in esame sono chiaramente assegnate.

In particolare, è attribuito alla Funzione Logistica il compito di garantire l'ammodernamento tecnologico e di sicurezza del parco ATM, attraverso la definizione di un piano di aggiornamento (sostituzione) pluriennale.

- b) Analisi delle modalità di definizione del piano di sostituzione ATM e sua esecuzione

Il piano di sostituzione viene predisposto dalla Funzione Logistica tenendo conto della disponibilità di apparati.

I criteri con cui vengono poi individuati i singoli apparati da sostituire sono essenzialmente l'anzianità, la tendenza più o meno ai guasti ed i volumi operativi. Per il 2018, l'obiettivo è stato fissato a 260 sostituzioni (200 cash in e 60 cash out).

Anche in questo caso, come per il piano distributivo, l'elenco dei siti individuati, dopo un confronto con la Funzione Commerciale per evitare eventuali interferenze con il piano da questa predisposto, viene comunicato al c.d. "Tavolo ATM" e, insieme a quelli ricompresi nel piano distributivo, entra nel c.d. "elenco siti".

Riguardo all'esecuzione del piano 2018, alla data del 1/6/2018 erano presenti richieste di sostituzione per n. 193 apparati (170 sostituzioni di cash in e 23 sostituzioni di cash out). Di questi, sono stati installati 147, in anticipo (117%) rispetto alla pianificazione di inizio anno.

5 Attività svolta: attuazione del piano ATM (1 di 2)

GESTIONE FILIERA
DEL CONTANTE

OBIETTIVO	PERIMETRO/ METODOLOGIA	RISCHI IMPATTATI
<p>Valutare l'adeguatezza del processo di installazione ATM nelle sue fasi di predisposizione software e trasporto e rispetto regole di sicurezza.</p> <p>Obiettivi SREP: IG 1.2, IG 2.11, IG 6.3</p>	<p>❑ Interviste, analisi documentale, analisi di dati, osservazione delle prassi</p> <p>❑ Periodo di riferimento: anno 2018</p>	<p>MPS.783282 rischio di mancato conseguimento degli obiettivi aziendali</p> <p>MPS.2108180: Rischio di ritardo/non completezza/errore nel monitoraggio sull'esecuzione dei processi esternalizzati (con esecuzione dei relativi controlli di competenza), con possibile mancata applicazione di penali ai fornitori che non hanno garantito gli SLA concordati.</p>
VERIFICHE SVOLTE	ESITI	
<p>a) Analisi del D00751 – Regolamento n. 1 – Organizzazione della Banca MPS, del Catalogo dei Processi e dei documenti normativi connessi</p>	<p>Le responsabilità connesse con l'attività in esame sono chiaramente assegnate.</p> <p>In particolare, sono attribuiti alla Funzione Logistica i compiti di coordinare le funzioni operative interne (Immobiliare, Monetica IT, Sicurezza), nonché di gestire il budget opex e capex assegnato, con l'obiettivo di massimizzare i livelli di servizio nel rispetto dei vincoli economici e delle risorse disponibili.</p>	
<p>b) Analisi della compliance del contratto con l'outsourcer Bassilichi alle disposizioni della Banca d'Italia</p>	<p>Il "Contratto di Gestione ATM per il Gruppo Montepaschi" è stato stipulato tra il COG e Bassilichi S.p.A. in data 1/1/2009.</p> <p>Trattandosi di un contratto stipulato antecedentemente alla data di entrata in vigore delle disposizioni sull'esternalizzazione di funzioni operative importanti (FOI) di cui all'allora circolare 263 della Banca d'Italia, la Capogruppo lo ha regolarmente segnalato tra i contratti in essere, come richiesto dal Bollettino di Vigilanza del 7/7/2013 della Banca d'Italia.</p> <p>In data 20/7/2015, con decorrenza 1/7/2015, il contratto è stato ceduto a Banca MPS e, trattandosi di una cessione infragruppo, senza modifica del fornitore, non si è dato corso alla comunicazione preventiva necessaria in caso della stipula di un nuovo contratto di esternalizzazione.</p> <p>Anche l'adeguamento del contratto alle nuove disposizioni è avvenuto entro i termini previsti stabiliti dal citato Bollettino di Vigilanza.</p>	



VERIFICHE SVOLTE

- c) *Walkthrough* del processo di installazione presso la filiale 6230 Castelnuovo Berardenga dell'ATM AT103006230500, nelle sue fasi di predisposizione, installazione e attivazione dell'apparato e verifica della sua compliance con la normativa vigente

ESITI

La normativa di riferimento è: per la parte di competenza *outsourcer*, il “Gestione ciclo di vita dei dispositivi ATM e EPP”, vers. 3.5 del 27/12/2010, a suo tempo condiviso dal Consorzio con Bassilichi e non facente parte della nostra normativa aziendale, mentre per quella di competenza Banca, è il “1030D02260 – Gestione operatività ATM”, vers. 1 del 28/11/2017.

In data 22/3/2018, è stata osservata l'operatività di Bassilichi Fabbrica ATM (svolta presso lo stabilimento di Empoli dove avviene la prima configurazione degli apparati) per verificare il *roll out* dell'ATM destinato alla sostituzione di quello presente nella filiale. L'operatività del tecnico di Fabbrica ATM che ha installato il software, configurato e sottoposto a collaudo l'ATM, predisponendolo per la successiva posa in opera, è risultata conforme alla procedura standard, tranne che in alcuni passaggi:

- 1) al momento in cui l'apparato è stato consegnato alla Fabbrica ATM e sballato, l'imballo e la tastiera non erano provvisti dei sigilli *tamper-evident* necessari alla verifica di eventuali manomissioni;
- 2) il tecnico di Bassilichi, difformemente da quanto richiesto, ha sottoscritto il verbale di accettazione e applicato il sigillo *tamper-evident* sulla tastiera;
- 3) al termine della lavorazione, l'ATM è stato ricollocato nel magazzino con lo stesso imballo con cui era pervenuto dal fornitore, ancora privo dei dispositivi antimanomissione previsti nel documento di processo.

Il 3 e il 4/4/2018, presso la filiale, è stata osservata, rispettivamente, l'operatività del vettore Bonocore per la posa dell'ATM e del tecnico di Bassilichi per la configurazione/attivazione del medesimo. In particolare nella prima giornata, sono stati verificati alcuni passaggi difformi dalla normativa:

- 1) il trasportatore ha riferito che, presso il proprio magazzino, l'ATM è stato sballato e nuovamente imballato (con l'imballo precedentemente tolto), in ragione del fatto che risultava privo di sigilli *tamper-evident* e di segnalatori di “cattivo trasporto”. Tale operazione, non prevista nella documentazione, non è stata neppure in alcun modo verbalizzata;
- 2) la filiale, indipendentemente dalla verifica dell'imballaggio, ha comunque autorizzato il posizionamento dell'apparato e sottoscritto il verbale di accettazione;
- 3) riguardo all'ATM sostituito, il trasportatore ha apposto sulla tastiera EPP una semplice etichetta bianca, non *tamper-evident* apponendoci una firma ed effettuato una fotografia dell'etichetta; l'apparecchio è stato poi imballato con l'involucro (adattato) dell'ATM appena installato.

Il tecnico Bassilichi, prima di procedere alla configurazione/attivazione dell'ATM, ha effettuato tutte le verifiche richieste; ha poi formato il personale della filiale sull'utilizzo della macchina e fornito le chiavi della cassaforte. Sono state infine verificate le funzionalità di prelievo e versamento di banconote/assegni. Quindi, è stato sottoscritto il Verbale di Attivazione ed il tecnico ha rimosso l'etichetta *tamper-evident* apposta sulla tastiera EPP in Fabbrica ATM.

Tale criticità è stata fatta presente in fase di revisione e la Funzione Logistica ha provveduto alla sistemazione delle problematiche riscontrate, richiamando il fornitore al rispetto delle procedure e nel contempo è stato rivisto il complessivo processo, migliorando gli strumenti per identificare eventuali manomissioni.

OBIETTIVO	PERIMETRO/ METODOLOGIA	RISCHI IMPATTATI
<p>Valutare l'adeguatezza delle procedure operative per il caricamento valori degli ATM in service.</p> <p>Obiettivi SREP: IG 1.2, IG 2.11, IG 6.3</p>	<p><input type="checkbox"/> Interviste, analisi documentale, analisi di dati, osservazione delle prassi</p> <p><input type="checkbox"/> Periodo di riferimento: anno 2018</p>	<p>MPS.2108180: Rischio di ritardo/non completezza/errore nel monitoraggio sull'esecuzione dei processi esternalizzati (con esecuzione dei relativi controlli di competenza), con possibile mancata applicazione di penali ai fornitori che non hanno garantito gli SLA concordati.</p>
VERIFICHE SVOLTE	ESITI	
<p>a) Analisi del D00751 – Regolamento n. 1 – Organizzazione della Banca MPS, del Catalogo dei Processi e dei documenti normativi connessi</p>	<p>Le responsabilità connesse con l'attività in esame sono chiaramente assegnate.</p> <p>In particolare, sono attribuiti alla Funzione Logistica i compiti di:</p> <p><input type="checkbox"/> gestire e coordinare la filiera fisica del contante, garantendone la disponibilità e presidiando la corretta esecuzione dei servizi per gli ATM in <i>service</i> (c.d. "remoti");</p> <p><input type="checkbox"/> monitorare la corretta contabilizzazione dei movimenti di contante degli ATM in <i>service</i>.</p>	
<p>b) Analisi del contratto con l'<i>outsourcer</i> B.T.V.</p>	<p>Il servizio "caricamento valori nelle apparecchiature ATM" in <i>service</i> è compreso nel più ampio contratto "Convenzione Quadro CW2005328 Servizio Trasporto e Contazione Valori", stipulato dalla Banca con l'<i>outsourcer</i> B.T.V. S.p.A. in data 17/10/2016, con scadenza fissata per il 30/04/2020.</p> <p>Oltre al caricamento è previsto anche che B.T.V. effettui la manutenzione di primo livello e collabori agli interventi di assistenza tecnica effettuati dai manutentori. È previsto anche l'utilizzo di uno strumento informatico predittivo per l'attivazione del servizio di caricamento che ottimizzi lo stock di contante in giacenza ed il numero di viaggi, garantendo al contempo la più ampia disponibilità del canale.</p> <p>Il contratto prevede livelli di servizio e penali in caso di mancato rispetto, con un tetto pari al 10% del valore del contratto stesso.</p>	
<p>c) Analisi della compliance del contratto con l'<i>outsourcer</i> B.T.V. alle disposizioni della Banca d'Italia</p>	<p>La "Convenzione Quadro CW2005328 Servizio Trasporto e Contazione Valori", nel cui ambito ricade il servizio di caricamento valori nelle apparecchiature ATM, è stata stipulata dalla Banca con B.T.V. S.p.A. in data 17/10/2016, in sostituzione del precedente contratto con BA.SE. S.r.l., società appartenente allo stesso gruppo di B.T.V. (Gruppo Battistolli) e da quest'ultima incorporata in data 29/7/2016.</p> <p>L'esternalizzazione, già avviata prima del 2013, era stata segnalata tra quelle in essere, come richiesto dal Bollettino di Vigilanza del 7/7/2013 della Banca d'Italia. L'attuale contratto non è stato oggetto di comunicazione preventiva in quanto non si è configurata la fattispecie della modifica del fornitore. Esso contiene, inoltre, le previsioni richieste dalla Circolare 285 della Banca d'Italia.</p>	

VERIFICHE SVOLTE

- d) Analisi delle procedure operative per il caricamento valori degli ATM in *service*

- e) Analisi delle modalità di monitoraggio delle prestazioni dell'*outsourcer* e delle azioni intraprese a seguito dell'eventuale mancato raggiungimento dei livelli di servizio contrattualmente previsti

ESITI

Il servizio “caricamento valori nelle apparecchiature ATM” in *service* si basa su di una programmazione che viene definita giornalmente da Bassilichi per conto di B.T.V. mediante l'applicativo proprietario B.Ahead, un sistema intelligente di *cash forecasting* e *cash management* in grado, tra le altre cose, di effettuare proiezioni circa le future necessità di sovvenzione denaro.

Elaborando le informazioni relative all'erogato medio ed alla giacenza per ogni singolo apparato registrate nei sistemi della Banca, B.Ahead determina quando l'ATM necessita di un caricamento ed il relativo importo, per poi inviare l'ordine a B.T.V., tramite un flusso informatico generato dalla trx SY00. La possibilità di caricamenti non richiesti è esclusa grazie al controllo automatico che impedisce il caricamento dell'ATM se il relativo ordine non è stato emesso.

B.T.V., direttamente o mediante corrispondenti, provvede alla sostituzione dei cassette presenti nell'ATM con dei cassette nuovi preparati nella Sala Conta in base all'ordine inviato dalla trx SY00.

I cassette rimossi vengono trasportati alla Sala Conta. Le attività di quadratura sono svolte dal Reparto Cash ATM con le stesse modalità di quelle svolte in filiale, sulla base dei dati contabili rivenienti da Paschi Face e dei dati sulla materialità delle banconote forniti dalla Sala Conta (importi residui e caricati).

Le prestazioni dell'*outsourcer* B.T.V. vengono monitorate mediante incontri mensili di Vendor Review in cui sono analizzati tutti gli indicatori del contratto, tra cui quelli del servizio di caricamento valori. I KPI sono calcolati dall'*outsourcer* e la Funzione Logistica effettua delle verifiche a campione, o se emergono situazioni rilevanti.

Dall'analisi della documentazione relativa al periodo tra settembre 2017 e marzo 2018 è risultato che gli SLA, relativi ai minuti di indisponibilità per errore di previsione ed ai minuti di indisponibilità per ritardo nel caricamento, sono stati sempre ampiamente rispettati, tanto che nel 2017 non sono state elevate penali ed il livello complessivo di indisponibilità è risultato inferiore anche a quello delle migliori filiali.

Anche la frequenza dei viaggi è oggetto di verifiche a campione mediante l'analisi dei resi rientrati in Sala Conta dopo il caricamento, e non sono emerse situazioni che possano mettere in dubbio la necessità dei viaggi effettuati dai trasportatori.

5 Attività svolta: esercizio (3 di 9)

OBIETTIVO	PERIMETRO/ METODOLOGIA	RISCHI IMPATTATI
<p>Valutare l'adeguatezza dell'infrastruttura tecnologica e applicativa degli ATM in termini di applicazione software e colloquio con i sistemi centrali.</p> <p>Obiettivi SREP: BM 7.8, IG 7.6</p>	<ul style="list-style-type: none"> ❑ Interviste, analisi documentale, analisi di dati, ❑ Rif. PCI PIN Transaction Security Point of Interaction Security Requirements - Information Supplement: ATM Security Guidelines 	<p>ID55682: Obsolescenza dell'infrastruttura software</p> <p>ID55324: Perdita di dati dovuti a malfunzionamento del software</p>
VERIFICHE SVOLTE	ESITI	
<p>a) Analisi del contratto COG - TAS</p>	<p>TAS è proprietario delle applicazioni deputate al funzionamento del mondo ATM ("Neptune" e "XFS"; queste sono concesse in licenza d'uso al COG), per le quali eroga i servizi di manutenzione, assistenza telefonica ed assistenza in esercizio. I rapporti con il fornitore sono regolati da un contratto più generale che ricomprende tutti i prodotti TAS per cui il COG ha acquisito i diritti d'uso; questo, benché privo di una chiara indicazione circa KPI, SLA ed eventuali penali, disciplina i tempi di assistenza tecnica e risoluzione delle problematiche (cfr. "Allegato 2 al contratto", "Manutenzione ordinaria").</p> <p>Il contratto in argomento risulta scaduto in data 31/12/2017 ed è in fase di rinnovo. A tale proposito si osserva che il fornitore è comunque vincolato ad erogare i servizi contrattualizzati per i sei mesi successivi alla scadenza (cfr. Art. 4). Alla data del 28/05/2018 il Settore Acquisiti ICT riferisce che la Banca è in attesa della formalizzazione dell'offerta da parte di TAS.</p>	
<p>b) Analisi dell'infrastruttura tecnologica del mondo ATM - Software presente sugli ATM</p> <p>(cfr. Allegato 3 – Infrastruttura ATM)</p>	<p>L'apparato ATM è configurato a tutti gli effetti come un qualsiasi computer aziendale (macchina SIP) sul quale sono installati anche gli strati software deputati al suo funzionamento.</p> <p>Su tutti gli ATM è presente l'antivirus standard aziendale.</p> <p>L'applicazione core dell'ATM (Neptune) è installata e funziona con i corretti presidi di sicurezza, in particolare:</p> <ul style="list-style-type: none"> ❑ i diritti di accesso alle diverse risorse del sistema sono assegnati alle utenze applicative in conformità al principio dei "minimi privilegi" (possedere abilitazioni adeguate alle necessità operative della risorsa o dell'applicazione e non eccedenti); ❑ le attività svolte sono tracciate su appositi LOG che prevedono la cifratura delle informazioni archiviate. <p>Il software (XFS) per la gestione delle varie periferiche della macchina (tastierino, roller cash, ecc.) cifra i messaggi scambiati; questo garantisce riservatezza delle informazioni in transito ed autenticazione del mittente riducendo, al contempo, il rischio di attacchi informatici di tipo man in the middle.</p> <p>Si osserva che Microsoft cesserà il supporto per i sistemi operativi attualmente installati sugli ATM (XP Windows Embedded e Windows 7) rispettivamente a gennaio 2019 e gennaio 2020. L'utilizzo di ATM con un sistema operativo non più supportato dal fornitore esporrebbe a rischi operativi elevati, sia in termini di</p>	



VERIFICHE SVOLTE

ESITI

- c) Analisi dell'infrastruttura tecnologica del mondo ATM - Applicazioni centrali deputate al funzionamento degli ATM
(cfr. Allegato 3 – Infrastruttura ATM)

possibili malfunzionamenti e blocchi delle macchine, che per l'aumento delle vulnerabilità di sicurezza logica derivanti dall'assenza di patch rilasciate nel continuo dal produttore. Benché la tematica risulti comunque già indirizzata (cfr. BR 66181), stante gli elevati rischi sottesi, la scrivente Funzione in fase di exit meeting ha sollecitato le competenti strutture affinché venga mantenuta alta l'attenzione sull'argomento.

Sono state analizzate le applicazioni centrali necessarie al funzionamento degli ATM:

- ☐ Gateway, applicazione dipartimentale che collega il software ATM con i servizi bancari quali conti correnti, bonifici, ecc.;
- ☐ GE.BA, applicazione mainframe (Host) per la gestione in accentrato di tutti gli ATM;
- ☐ Anagrafe ATM, applicazione dipartimentale con la quale vengono configurati i parametri necessari al collegamento dell'ATM con l'Host centrale.

L'unico punto d'attenzione emerso riguarda l'applicativo Gateway. Questo è realizzato sulla piattaforma software di IBM denominata WebSphere nella versione 7 che, ad oggi, non risulta più supportata dal produttore (IBM l'ha dichiarata "end of support" a decorrere da Aprile c.a.). Alla data di pubblicazione del presente rapporto era in fase di valutazione l'offerta del fornitore (TAS) per l'aggiornamento di Gateway alla versione più recente di WebSphere (V 9.0).

- d) Analisi dell'infrastruttura tecnologica del mondo ATM - Applicazioni di monitoraggio sul parco ATM
(cfr. Allegato 3 – Infrastruttura ATM)

Le principali applicazioni di monitoraggio sono il "Cruscotto ATM" (applicativo custom ad uso interno) e "B-Ready" (applicativo sviluppato e utilizzato da Basilichi).

Nel caso in cui il contante erogabile presente sul singolo ATM scenda sotto il minimo previsto, la necessità di provvedere al ricarica dei cassetti è segnalata, in tempo reale, sul cruscotto ATM. Viceversa, non è prevista un'analogia indicazione a seguito del superamento del massimale (cfr. verifica "d" della slide 38 dalla quale è emersa una perdita superiore alle attese, causata dai superamenti di massimale). Peraltro, per quanto riguarda gli ATM cash-in con ricircolo, la giacenza totale del contante non è, ad oggi, un'informazione disponibile a sistema (Gap 6). Si osserva che la problematica è nota e solo parzialmente indirizzata (prevista l'implementazione di un "quadro informativo" che consenta la fruibilità di tale informazione); Il BR (54196) di riferimento alla data del 15/06/2018 non era ancora stato approvato.

Lo strumento B-Ready di Basilichi è orientato a presidiare gli aspetti riguardanti i malfunzionamenti e gli interventi di manutenzione. L'applicativo è connesso alla rete della Banca, attinge alle informazioni presenti in GE.BA e raccoglie i codici di malfunzionamento trasmessi dagli ATM. Ad ogni evento critico viene associato un owner di risoluzione (es. Rete, manutentore, vigilanza, COG, Direzione Generale) e, con frequenza oraria, viene inviato al Cruscotto ATM un campo informativo sullo stato degli interventi tecnici in corso.

Tramite B-Ready si possono risolvere da remoto alcune anomalie operando dei comandi quali reset delle periferiche, ripresa di un servizio e riavvio del PC dell'ATM.



VERIFICHE SVOLTE

- e) Analisi della sicurezza dei flussi tra le applicazioni

- f) Analisi della procedura di manutenzione e assistenza effettuate da TAS sugli applicativi forniti e della difettosità del software.

Valutazione della procedura con la quale vengono scalati i malfunzionamenti sugli applicativi TAS del mondo ATM.

ESITI

I messaggi scambiati tra l'ATM e i sistemi centrali risultano cifrati dal prodotto Stunnel gestito da TAS.

Unica eccezione è la fase di autenticazione del cliente nell'operatività "cardless".

L'operatività "cardless" consente di accedere agli ATM in assenza della carta, utilizzando per l'autenticazione le credenziali (utente e password) rilasciate al cliente per il servizio di Digital Banking. L'invio di tali credenziali dall'ATM ai sistemi centrali avviene su un canale non cifrato (protocollo "http") esponendo pertanto al rischio di intercettazione e furto in caso di attacchi malevoli (Gap 7). Tutte le comunicazioni successive avvengono su canale protetto (cifratura tramite Stunnel).

Il rischio derivante dal furto delle credenziali è comunque parzialmente mitigato dall'impiego della "strong authentication" (sia nell'accesso al Digital Banking che nell'utilizzo della funzionalità "cardless" sull'ATM). Per poter operare sull'ATM o disporre sul Digital Banking, all'eventuale frodatore mancherebbe ancora il terzo fattore di autenticazione, la cosiddetta OTP - One Time Password, password temporanea inviata al cellulare certificato dell'utente o generata sulla chiavetta OTP posseduta.

Sono state rilevate prassi operative che, di fatto, limitano il monitoraggio degli interventi effettuati da TAS sul software ATM, non consentendo quindi una valutazione qualitativa né dell'assistenza né del software fornito (Gap 8).

Sul sistema di ticketing aziendale (Remedy) sono riportati solo alcuni degli incidenti/anomalie inerenti gli applicativi del mondo ATM. Infatti, nelle prassi osservate, le problematiche vengono segnalate tramite email da Bassilichi (responsabile per il monitoraggio degli ATM) direttamente a TAS.

Questa comunicazione avviene frequentemente in assenza di qualsiasi coinvolgimento del Settore Monetica del COG.

Il fornitore utilizza un sistema di ticketing proprietario su cui ad oggi il Settore Monetica non esegue nessun tipo di monitoraggio, non verificando neppure i tempi di risoluzione delle anomalie.

Dall'analisi dei dati forniti dal Settore Monetica relativamente alle modifiche software (*Request for Change*) effettuate dal primo gennaio 2017 alla fine di aprile 2018, non è stato possibile individuare le modifiche di correzione ai software, necessarie per una valutazione della loro difettosità, in quanto vengono generalmente accorpate ai rilasci progettuali.

5 Attività svolta: esercizio (6 di 9)

CHANGE, RELEASE E
DEPLOYMENT MANAGEMENT

OBIETTIVO	PERIMETRO/ METODOLOGIA	RISCHI IMPATTATI
<p>Accertare che i processi di change, release e deployment management vengano seguiti per i rilasci in produzione relativi ai software del mondo ATM.</p> <p>Obiettivi SREP: IG 6.3</p>	<ul style="list-style-type: none"> ❑ Interviste, analisi documentale, analisi di dati ❑ Rif. PCI PIN Transaction Security Point of Interaction Security Requirements - Information Supplement: ATM Security Guidelines 	<p>ID55460: Modifiche applicative non autorizzate</p> <p>ID55304: Incompleta/errata pianificazione dei test.</p> <p>ID55667: Incompleta/errata pianificazione dell' installazione</p>
VERIFICHE SVOLTE	ESITI	
<p>a) Analisi della procedura di rilascio in produzione delle modifiche software relative agli applicativi utilizzati in ambito ATM</p>	<p>Le prassi attualmente in uso per il rilascio in produzione di modifiche software sugli apparati ATM risultano le seguenti:</p> <ul style="list-style-type: none"> ❑ i referenti applicativi del COG inseriscono le RFC (<i>Request for Change</i>) come da processo standard di "<i>change management</i>"; i pacchetti software vengono generalmente predisposti dai fornitori che effettuano i test tecnici necessari in fase di sviluppo, mentre i test in ambiente di collaudo vengono svolti dai referenti applicativi stessi; ❑ i referenti applicativi comunicano l'esigenza di rilascio software all'ATM Manager, funzione che coordina tutti gli attori che hanno necessità di distribuire software sugli ATM; ❑ infine il <i>deploy</i> sulle macchine viene effettuato da Basilichi, la quale agisce a seguito di autorizzazione ricevuta tramite email da ATM Manager. Si osserva che il contratto in vigore tra Banca e Basilichi ad oggi non ricomprende questa attività (Gap 3). <p>Cautelativamente la prima distribuzione avviene su un ristretto numero di ATM, in caso di esito positivo è poi estesa a tutta la popolazione.</p> <p>La distribuzione sui sistemi centrali (quali GE.BA e Gateway) avviene invece nel rispetto del processi standard di "<i>change, release e deployment management</i>".</p>	
<p>b) Analisi ambienti di coding e collaudo</p>	<p>Esistono due laboratori di prova per gli ATM, uno a Firenze e l'altro a Padova. Le macchine presenti in entrambi i laboratori sono attestate sull'ambiente di collaudo; tale ambiente rispecchia quello di produzione, eccezion fatta per l'eventuale presenza di software più aggiornati rispetto a quelli presenti in produzione. Non risulta presente un ambiente di test: i test del software (Neptune, GE.BA, Gateway) vengono effettuati direttamente da TAS nei propri locali di Bologna dove è presente un apparato che simula il collegamento ai sistemi dipartimentali, host e interbancari; tale ambiente non è collegato con il COG.</p> <p>I laboratori di collaudo vengono utilizzati per l'omologazione/certificazione di nuovi modelli acquistati, per testare le nuove versioni dei vari software installati e per verificare tutte le funzionalità meccaniche, anche quelle di cash in, cash out, bollettini, F24, ecc. Nel caso, ai fini delle prove, sia necessario l'uso di contante, viene ingaggiato un trasporto valori, per poi restituire il contante in Sala Conta una volta ultimati i test.</p>	



OBIETTIVO	PERIMETRO/ METODOLOGIA	RISCHI IMPATTATI
<p>Valutare gli aspetti di sicurezza logica, quali controllo accessi e modalità di tracciatura, dell'infrastruttura tecnologica degli ATM in termini di applicazione software e connessioni di rete.</p> <p>Obiettivi SREP: IG 2.6, IG 6.3</p>	<p>Interviste, analisi documentale, analisi di dati a campione, analisi access list</p> <p>Rif. PCI PIN Transaction Security Point of Interaction Security Requirements - Information Supplement: ATM Security Guidelines</p>	<p>ID55196: Non adeguato governo degli accessi</p> <p>ID55225: Accesso non autorizzato al sistema da reti esterne</p>
VERIFICHE SVOLTE	ESITI	
a) Analisi del controllo accessi per i componenti dell'infrastruttura tecnologica: analisi procedura di richiesta utenze	<p>Per operare sugli ATM sono necessarie due tipologie di abilitazioni, le utenze/profilature dipartimentali per amministrare i pacchetti installati sulle macchine stesse e le utenze/profilature sull'applicazione GE.BA per gestire da accentrato il parco ATM.</p> <p>Entrambe le prassi utilizzate per le richieste di abilitazioni sono risultate conformi alla normativa aziendale (D150 del COG e D389 della Banca). La parte dipartimentale dipende da autorizzazioni rilasciate su Active Directory da Gestione Utenti. Il prodotto GE.BA ha utenze e profilature proprietarie: le richieste provengano dai vari responsabili (frequentemente dall'ATM Manager) alla Funzione Gestione Utenti, la quale veicola la richiesta al <i>Settore Monetica</i> (System Owner) abilitato ad attribuire utenze e profilature.</p>	
b) Analisi del controllo accessi per i componenti dell'infrastruttura tecnologica: analisi degli utenti	<p><u>Utenze dipartimentali.</u> La gestione degli utenti abilitati ad operare sugli ATM avviene tramite una foresta di Active Directory dedicata (dominio ATM.gruppo.mps). Gli utenti presenti in tale dominio, tra cui quelli con privilegi di amministratore, non figurano sul sistema aziendale accentrato di controllo accessi (OIM con interfaccia NIU - Nuova Interfaccia Utente). In assenza di un connettore automatico, la Funzione Gestione Utenti esegue manualmente l'allineamento tra i due sistemi con rischio di errori e disallineamenti (Gap 4).</p> <p><u>GE.BA.</u> Generalmente gli utenti ed i relativi profili assegnati sono privi di scadenza temporale, inoltre non è implementata nessuna procedura per la disabilitazione/rimozione dell'utenze non più necessarie (ad esempio a seguito di una variazione d'incarico, cessazione, ecc.).</p> <p>L'analisi condotta sulle 210 utenze con profili abilitati alle modifiche¹, ne ha evidenziate n. 98 (pari circa al 46%) con anomalie (es. circa la metà risultano inesistenti sulle piattaforma NIU, n. 8 utenti censiti doppi o tripli, in alcuni casi con matricole disabilite, ecc.). Risulta evidente che tali utenze non sono oggetto di verifiche periodiche così come previsto anche da normativa aziendale (cfr D389) (Gap 5).</p>	

¹Analisi eseguita sui dati forniti dal Settore Monetica in data 12/03/2018.

VERIFICHE SVOLTE

ESITI

- c) Analisi della tracciatura effettuata dalle componenti dell'infrastruttura tecnologica.

Sono stati valutati i log dei prodotti GE.BA e Anagrafica ATM.

Il log GE.BA viene tenuto in linea per 3 mesi ed ha uno storico off line di 3 anni.

Il log dell'applicativo Anagrafe ATM traccia le modifiche effettuate ai dati presenti in anagrafe; non traccia invece l'accesso e le interrogazioni effettuate degli operatori.

- d) Analisi componenti di rete: analisi connessioni di rete degli ATM locati in filiale e degli ATM remoti

Gli ATM locati in filiale sono attestati su una rete virtuale dedicata agli ATM, quindi segmentata, ma non segregata, ovvero non protetta da nessun apparato di rete, quale firewall, che permetta la definizione di filtri per limitare la raggiungibilità IP ad altre reti.

Gli ATM remoti sono invece attestati in una rete virtuale separata dalla rete aziendale tramite un firewall. Le regole definite sul firewall sono però risultate insufficienti: dagli ATM è infatti possibile raggiungere via IP, oltre ai CED locati su Siena e Firenze, anche la Direzione Generale presente sulla piazza di Siena (Gap 2).

Questo, oltre a rappresentare un rischio di accessi indebiti alla intranet aziendale, contrasta con il documento delle policy di sicurezza (D1815) che disciplina, tra le altre cose, l'accesso alle reti: "La rete, le sue componenti e i servizi da essa erogati, devono essere protetti da accessi non autorizzati, anche da remoto, attraverso adeguate configurazioni degli apparati. La rete telematica aziendale deve essere segmentata in modo tale da garantire l'accesso ai sistemi, in maniera differenziata, solo da parte del personale autorizzato.

- e) Analisi componenti di rete: analisi connessioni di rete di Fabbrica ATM e della sede Bassilichi dalla quale viene effettuata assistenza tecnica al parco ATM

I siti di Bassilichi Fabbrica ATM (Empoli) e Firenze via Petrocchi sono collegati alla rete della Banca tramite una rete destinata ad accogliere enti esterni, separata dalla rete aziendale da un firewall. Anche in questo caso le regole impostate sul firewall sono risultate insufficienti, da entrambe le sedi è infatti possibile raggiungere via IP tutte le reti della Banca (Gap 2).

In via Petrocchi è inoltre presente una infrastruttura di rete che permette anche a macchine non standard SIP di connettersi alla rete della Banca. Il colloquio è regolato da una access-list non mantenuta e, pertanto, potrebbe risultare non coerente con le effettive esigenze operative (Gap 2).

VERIFICHE SVOLTE

- f) Analisi delle misure di sicurezza logica applicate al pc dell'ATM

ESITI

La verifica dei presidi di sicurezza logica ha evidenziato alcune carenze nella configurazione dell'hardware e del software di base presente sui pc dell'ATM; nello specifico è risultato che:

- ☐ il BIOS degli ATM viene installato senza password;
- ☐ non è previsto l'utilizzo del Boot UEFI;
- ☐ il Boot da usb è lasciato attivo;
- ☐ sui dispositivi ATM è possibile l'avvio in modalità provvisoria;
- ☐ sono assenti strumenti per il blocco/gestione delle periferiche USB.

Gli accertamenti effettuati presso le funzioni del COG, quella incaricata della gestione del software di base (*Settore Sistemi Dipartimentali*), nonché quella responsabile dei presidi di Sicurezza Logica (*Settore Sicurezza Informatica*), hanno evidenziato come nessuna delle strutture coinvolte abbia, al momento, il pieno presidio delle tematiche evidenziate, delle quali, peraltro, non risulta essere stata effettuata nel tempo alcuna analisi di rischio (Gap 1).

5 Attività svolta: monitoraggio/manutenzione (1 di 11)

GESTIONE DEI PROCESSI OPERATIVI
DI SICUREZZA FISICA

OBIETTIVO	PERIMETRO/ METODOLOGIA	RISCHI IMPATTATI
<p>Esaminare elementi di sicurezza fisica, quali sistemi antieffrazione, monitoraggio allarmi e presidi antifrode applicati al parco ATM.</p> <p>Obiettivi SREP: IG 2.3, IG 2.11, IG 6.3</p>	<ul style="list-style-type: none"> Interviste, analisi documentale, analisi di dati Rif. PCI PIN Transaction Security Point of Interaction Security Requirements - Information Supplement: ATM Security Guidelines 	<p>MPS.2843460: Rischio di errata/incompleta definizione della strategia di Sicurezza Fisica con conseguenti perdite economiche</p>
VERIFICHE SVOLTE	ESITI	
<p>a) Analisi policy di sicurezza fisica</p>	<p>La Funzione Sicurezza Fisica Banca ha stabilito uno standard contenente specifiche e dettagliate indicazioni circa i presidi di sicurezza fisica da adottare sugli ATM, dipendentemente dal livello di rischio rilevato sull'ATM stesso; l'analisi di rischio è stata effettuata e viene mantenuta dalla stessa Funzione. Tale standard non è pubblicato in normativa ma risulta comunque diffuso a tutte le strutture che si occupano dell'installazione dell'ATM (ATM Manager e Area Immobiliare), le quali agiscono in conformità allo stesso. La funzione Sicurezza Fisica Banca partecipa, quando direttamente ingaggiata dalla Funzione Logistica, agli incontri settimanali del Tavolo ATM o alla discussione dei casi di ATM oggetto di attacco.</p>	
<p>b) Analisi sistemi di allarmistica/antieffrazione installati</p>	<p>Ad oggi la competenza dell'installazione delle misure di sicurezza predisposte per gli ATM è distribuita tra le seguenti funzioni:</p> <ul style="list-style-type: none"> La Funzione Logistica e la Funzione Commerciale si occupano di acquistare le macchine con le dotazioni minime di sicurezza (<i>Antiskimmer</i>, con la quale si impedisce la clonazione della carta, <i>Shutter rinforzato</i>, ovvero fessura di fuoriuscita del contante più robusta per evitare manomissioni e Blindatura cassaforte CEN 3, categoria appartenente agli standard previsti dalle normative europee). l'Area Immobiliare si occupa di far installare la sensoristica come da standard, ovvero il contatto magnetico sullo sportello dell'ATM, il sensore sismico sulla cassaforte ed il sensore volumetrico del locale in cui è posizionata la macchina. Tali sensori sono collegati con le centrale allarmi locate a Firenze. Il Settore Sicurezza Fisica, si occupa infine delle misure aggiuntive di sicurezza (es Gabbia, DID¹, Uscite di emergenza, TVCC-sistemi di videosorveglianza) necessarie a ridurre il rischio rilevato sull'ATM ad un valore ritenuto accettabile. <p>La funzione Owner dell'individuazione delle misure/apprestamenti di sicurezza fisica da adottare è comunque sempre la Funzione Sicurezza Fisica Banca.</p> <p>Dagli approfondimenti svolti risulta che nel 2016 l'ATM Manager, tramite specifico progetto, ha provveduto ad installare su tutti gli ATM le dotazioni minime di sicurezza.</p>	

¹ Il DID è un dispositivo integrato di deterrenza che ha l'obiettivo di intercettare per tempo il tentativo di furto sull'ATM e di prevenirne la realizzazione. Composto da:

- un sensore di rilevamento presenza persona
- faro LED, microfono con indirizzo IP accessibile da Control Room
- Sirena di allarme
- nebbiogeno

Il DID Light: Versione che prevede solo la videosorveglianza dalle ore 22,00 alle 06,00.



VERIFICHE SVOLTE

ESITI

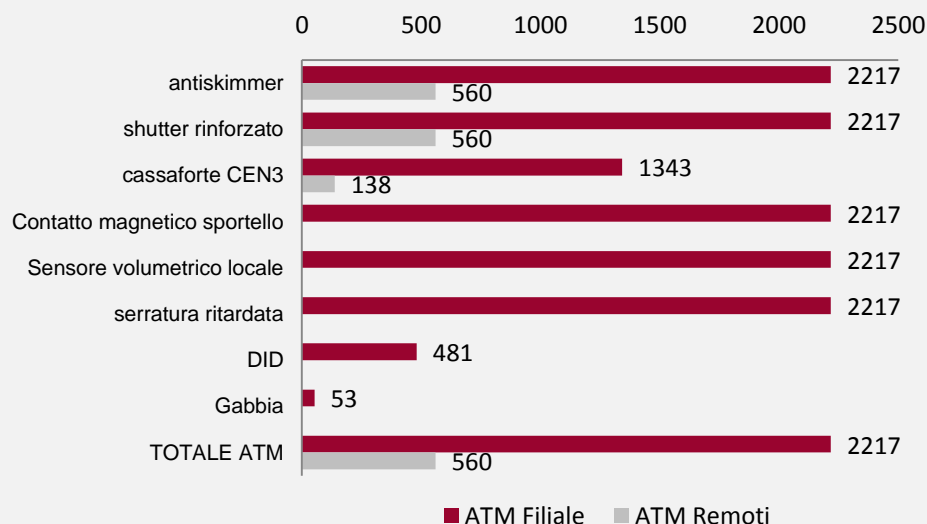
Nel 2017 la Funzione Sicurezza Fisica Banca ha montato 350 DID riportando così ad un livello di rischio più basso tutti gli ATM classificati ad alto rischio.

La stessa Funzione ha pianificato per il 2018 una serie di interventi da completare entro il 30 Ottobre con l'obiettivo di portare tutti gli ATM di filiale al livello di rischio basso/medio-basso. Tali attività sono condotte in parallelo al progetto AIRONE (in carico alla Funzione Immobiliare, che riguarda l'ammodernamento delle infrastrutture di filiale) e all'attività di sostituzione/nuova installazione ATM in carico alle funzioni Logistica e Commerciale.

Nell'ambito di tali attività sono già state installate sugli ATM circa 50 gabbie; queste sono necessarie per impedire l'asportazione dei cassetti dei contanti e per evitare che l'esplosione dell'ATM innescata tramite esplosivi solidi e liquidi arrechi ulteriori danni anche alla filiale.

Il progetto di messa in sicurezza degli ATM non comprende quelli remoti, per i quali la sicurezza fisica è demandata all'ente ospitante ed è compresa nel canone di affitto degli spazi. Gli allarmi presenti sugli ATM remoti non sono generalmente collegati con la centrale allarmi ma in caso di manomissione producono un allarme acustico.

L'analisi effettuata (dati forniti dal *Settore Sicurezza Fisica* in data 20/04) sulle misure fisiche attualmente installate sugli ATM ha rilevato la copertura riportata nel grafico sotto.



VERIFICHE SVOLTE

- c) Analisi del sistema di monitoraggio degli allarmi di sicurezza fisica sugli ATM

Gli allarmi delle filiali e degli ATM sono monitorati dal *Settore Control Room* e da Bassilichi (sale allarmi situate entrambe a Firenze); ogni struttura monitora con le stesse modalità (h 24x365) la metà delle filiali di Gruppo. Nel caso in cui l'allarme scatti durante l'orario di lavoro viene contattata la filiale, altrimenti viene allertata la vigilanza tramite i numeri telefonici di riferimento.

Sono oggetto di monitoraggio gli ATM di tutte le filiali e circa 200 ATM fra esternalizzati c/o locali Banca e remoti.

Gli allarmi monitorati in accentrato per gli ATM sono quelli relativi al:

- ☐ Contatto magnetico sullo sportello,
- ☐ Sensore sismico sulla cassaforte,
- ☐ Sensore volumetrico del locale in cui è posizionata la macchina.

Nel caso in cui sia installato il dispositivo DID sono accentrati sul sistema di monitoraggio anche i seguenti ulteriori allarmi:

- ☐ Segnalazioni provenienti dall'agente software a bordo dell'ATM (anti skimmer, shutter rinforzato)
- ☐ il sensore sismico posizionato frontalmente
- ☐ il rilevatore di presenza nei pressi ATM

È in corso di attivazione un nuovo sistema di monitoraggio allarmi (MyCentrax CWM) che, tramite un sistema di correlazione, permette di assegnare una priorità agli allarmi evidenziando quelli a maggiore rischio. Attualmente è in fase di test l'integrazione tra gli allarmi dei sensori e le telecamere della videosorveglianza; lo step successivo prevede l'attivazione del sistema di correlazione sopra citato.

- d) Analisi della numerosità eventi criminosi e confronto con massimali definiti sugli ATM

Dall'analisi degli eventi criminosi avvenuti nel 2017 e primo trimestre 2018 su ATM locati in filiale con giacenza superiore ai 40.000 euro, è emerso che 7 dei 21 ATM "bombati" avevano una giacenza che superava il massimale previsto e che ha portato ad una perdita di circa 95.000 euro oltre le attese della banca, pari circa al 7% dell'asportato totale sugli ATM analizzati.

A tal proposito è stata recentemente attivata una copertura assicurativa sulle macchine ATM compresa nella polizza "BBB" che copre i danni relativi ai "valori asportati" per rapine o furti. La franchigia per evento è di 100K€ quindi non copre in genere l'importo asportato ma sono assicurati anche i danni subiti dalle macchine in caso di attacco criminoso; la clausola prevede che per gli ATM installati da meno di 7 anni venga rimborsato il valore totale della macchina mentre per quelli che, alla data del sinistro, abbiano già superato il settimo anno di installazione, l'importo del danno sarà pari al 50%.

5 Attività svolta: monitoraggio/manutenzione (4 di 11)

GESTIONE DEI PROCESSI OPERATIVI
DI SICUREZZA FISICA

VERIFICHE SVOLTE

e) Analisi presidi antifrode

ESITI

Il Settore Sicurezza Informatica del COG ha la responsabilità, come normato nel D2260, di raccogliere le segnalazioni su eventi sospetti di frode sugli ATM. Gli accertamenti evidenziano che il Settore segue le corrette prassi, raccogliendo informazioni circa le anomalie da tutte le possibili fonti (filiale, control room e funzione di monitoraggio ATM di Bassilichi), ripristinando in autonomia l'ATM o dando indicazioni alla filiale su come procedere per il ripristino o per la denuncia in caso di accertata manomissione per frode. Tutte le segnalazioni vengono registrate manualmente in un database e messe a disposizione per le funzioni deputate alla gestione degli ATM.



OBIETTIVO

Valutare l'adeguatezza delle procedure operative per il monitoraggio del funzionamento e per la manutenzione del parco ATM

Obiettivi SREP: IG 1.2, IG 2.11, IG 6.3

PERIMETRO/ METODOLOGIA

- ☐ Interviste, analisi documentale, analisi di dati, osservazione delle prassi
- ☐ Periodo di riferimento: anno 2018

RISCHI IMPATTATI

ID55622 Rischio derivante dalla indisponibilità di servizi offerti dall'ATM dovuta a malfunzionamenti tecnici dell'apparecchiatura, della stampante oppure alla fine/mancanza del rotolo per la stampa scontrini.

MPS.2843740 Rischio derivante da un non adeguato monitoraggio con possibile insoddisfazione della clientela per quanto concerne i servizi offerti dall'ATM.

MPS.2108180 Rischio di ritardo/non completezza/errore nel monitoraggio sull'esecuzione dei processi esternalizzati (con esecuzione dei relativi controlli di competenza), con possibile mancata applicazione di penali ai fornitori che non hanno garantito gli SLA concordati.

VERIFICHE SVOLTE

- a) Analisi del D00751 – Regolamento n. 1 – Organizzazione della Banca MPS, del Catalogo dei Processi e dei documenti normativi connessi
- b) Analisi del contratto con l'*outsourcer* Basilichi

ESITI

Le responsabilità connesse con l'attività in esame sono chiaramente assegnate.

In particolare, nell'ambito del governo e della gestione operativa degli ATM, è attribuito alla Funzione Logistica il compito di garantire il mantenimento in esercizio delle macchine ATM ai più elevati livelli di disponibilità e di monitorare i livelli qualitativi dei servizi di "Manutenzione, Monitoraggio ed Help Desk", assegnati all'*outsourcer* Basilichi.

Il "Contratto di Gestione ATM per il Gruppo Montepaschi" è stato stipulato tra il COG (allora responsabile del parco ATM) e Basilichi S.p.A. in data 1/1/2009.

Il contratto prevedeva l'esternalizzazione della complessiva gestione operativa del parco ATM della Banca, (p.es. noleggio, predisposizione, installazione ed attivazione degli apparati, servizio di help desk telefonico e di monitoraggio dello stato di funzionamento, manutenzione). La decorrenza del contratto era fissata al 1/1/2009, con scadenza 31/12/2012, con rinnovo automatico di anno in anno e disdetta con preavviso di 3 anni.

VERIFICHE SVOLTE

ESITI

Al momento attuale, parte firmataria per il Gruppo Montepaschi è la Banca MPS e la scadenza è fissata al 3/7/2025.

Nel corso degli anni, il contratto è stato anche oggetto di aggiustamenti ed adeguamenti al mutato quadro delle Disposizioni di Vigilanza con 7 diversi *addenda*, che hanno parzialmente modificato, tra le altre cose, i livelli di servizio originariamente concordati. Dall'analisi è emerso che:

- ☐ il contratto non è più attuale nei contenuti;
- ☐ alcuni SLA più rilevanti sono tarati su volumi non più attuali ed altri sono da reingegnerizzare;
- ☐ il tetto imposto alle penali che l'*outsourcer* deve pagare per il mancato rispetto degli SLA è molto basso e costituisce un disincentivo per Basilichi a migliorare la propria *performance*. A tal proposito è risultato che alcuni importanti SLA relativi al servizio di manutenzione sono costantemente disattesi;

c) Analisi delle modalità di funzionamento del c.d. "Tavolo Bombati e Critici"

Il "Tavolo Bombati e Critici" è la sede in cui vengono valutate le singole situazioni relative agli ATM c.d. "bombati, critici e lungodegenti"(*), oltre alle casistiche di recidività (ATM che hanno richiesto due o più interventi manutentivi ravvicinati - 15 gg - sullo stesso componente o su componenti diversi).

Come per il "Tavolo ATM", si tratta di un gruppo di lavoro informale, che si riunisce settimanalmente, efficacemente coordinato dalla Funzione Logistica, cui partecipano le funzioni Commerciale, Immobiliare, Basilichi e, a seconda dei casi, Sicurezza,

(*) bombato: ATM oggetto di attacco fisico; critico: ATM non operativo da più di 3.000 minuti (50 ore solari); lungodegente: ATM non operativo da più di 5 giorni lavorativi.

Il Team di Audit ha partecipato, in qualità di osservatore, ai Tavoli tenutisi nel mese di aprile, constatando l'efficace coordinamento da parte di ATM Manager. I partecipanti, analizzano puntualmente, dai vari punti di vista, le situazioni problematiche, richiamano eventualmente il fornitore alle responsabilità contrattuali e decidono sul da farsi (p.e. mettere a piano la sostituzione della macchina recidiva).

VERIFICHE SVOLTE

- d) Analisi delle modalità di monitoraggio del funzionamento del parco ATM, svolte dalle funzioni aziendali e dall'*outsourcer* Basilichi

ESITI

Il monitoraggio dello stato di funzionamento del parco ATM viene svolto da Basilichi mediante l'applicativo B.Ready precedentemente citato.

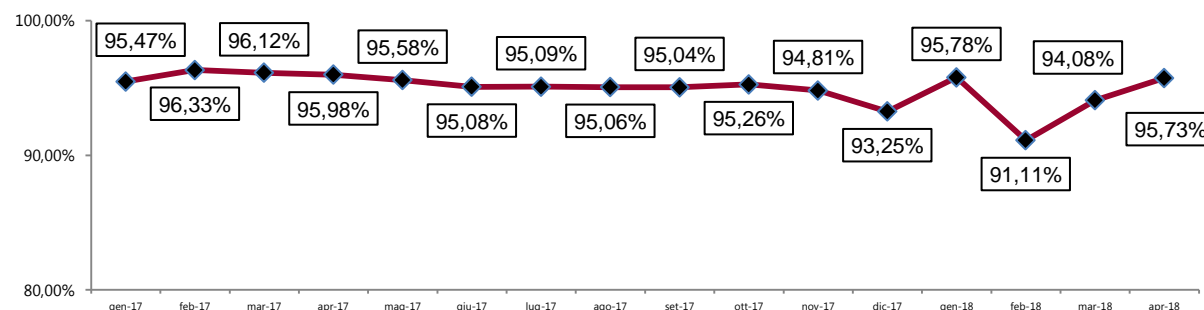
B.Ready segnala in tempo reale lo stato di ciascun apparato e, in caso di anomalia:

- 1) il guasto viene prima analizzato e "trattato" da una sequenza di automatismi correttivi;
- 2) se l'intervento automatico non è risolutivo, l'anomalia viene presa in carico dall'operatore Basilichi che tenta la risoluzione on center (da remoto), anche con eventuale richiesta di intervento da parte del personale della filiale;
- 3) se neppure l'intervento da remoto ha successo, la segnalazione viene passata alla struttura di Basilichi che si occupa della manutenzione (c.d. "Tavolo Operativo") che attiva – attraverso un sistema di *trouble ticketing* – l'intervento on site del tecnico e ne monitora l'andamento e l'esito.

B.Ready dispone, inoltre, di una funzionalità che disabilita l'intervento da remoto qualora si ripeta con eccessiva frequenza il solito guasto facendo ritenere necessario un intervento on site, nonché di una funzionalità di preavviso quando anomalie nel "comportamento" dell'apparato possano far prevedere l'insorgere di un problema.

Le funzioni della Banca tengono sotto controllo la situazione delle anomalie mediante le note che gli operatori di Basilichi inseriscono in B.Ready e che passano sul Cruscotto ATM.

Sin da inizio 2016, Basilichi ha rilasciato un modulo di gestione statistica della disponibilità del Canale ATM; a fine 2016 l'*outsourcer* ha effettuato un nuovo rilascio al fine di allineare la logica di calcolo della disponibilità alle logiche condivise con la Banca. Di seguito si presenta l'andamento dell'indice di disponibilità del canale di prelievo nel periodo gen-17/apr-18(*):



(*) Fonte dati: Basilichi



VERIFICHE SVOLTE

e) Analisi del processo di manutenzione

ESITI

Il servizio di manutenzione degli ATM viene svolto da Basilichi, che si avvale di tecnici propri e delle reti di assistenza dei produttori degli apparati e di B.T.V. per gli apparati in *service*.

Gli interventi si suddividono in 3 categorie:

- 1) manutenzione preventiva;
- 2) manutenzione ordinaria, per la risoluzione dei guasti imputabili all'operatività dell'ATM;
- 3) manutenzione straordinaria, per la risoluzione dei guasti imputabili, in senso più ampio, alla Banca.

Gli interventi di manutenzione ordinaria e straordinaria vengono “disposti” dal Tavolo Operativo, struttura di Basilichi che riceve le segnalazioni dei guasti dal servizio di Help Desk telefonico o dagli addetti del servizio di monitoraggio qualora gli interventi automatici dell'applicativo B.Ready o quelli manuali non abbiano avuto successo.

Le segnalazioni d'intervento on site passate al Tavolo Operativo sono gestite e monitorate con un applicativo dedicato di Basilichi (cd. Remedy). Il guasto viene registrato nella piattaforma, che, via web, gira il ticket (con indicata la scadenza entro cui eseguire l'intervento) al centro di assistenza censito per l'ATM che necessita l'intervento.

Il centro di assistenza/manutentore comunica sempre sull'applicativo Remedy la pianificazione dell'intervento, che viene trasferita al Cruscotto ATM.

La chiusura dell'intervento viene comunicata dal manutentore per lo più tramite flussi informatici. Quando l'intervento viene svolto da B.T.V., il Tavolo Operativo chiede a quest'ultima l'esito dell'attività ed aggiorna Remedy.

Il Tavolo Operativo verifica l'effettiva risoluzione del guasto solo sporadicamente. Le verifiche si concentrano per lo più sui casi di interventi ripetuti sulla stessa macchina. La situazione degli interventi aperti è monitorata giornalmente tramite report prodotti 3 volte al giorno.

Le richieste di intervento sono oggetto di solleciti da parte del Tavolo Operativo, in particolare per i casi di data obiettivo non rispettata. In questo contesto, particolare attenzione è dedicata agli interventi sugli ATM remoti che richiedono la partecipazione congiunta del tecnico e del personale di B.T.V..

La Banca non riceve specifici report sul servizio, ma le problematiche più rilevanti vengono discusse durante gli incontri del “Tavolo Bombati e Critici”.

VERIFICHE SVOLTE

- f) Analisi delle modalità di monitoraggio delle prestazioni dell'*outsourcer* e delle azioni intraprese a seguito dell'eventuale mancato raggiungimento dei livelli di servizio contrattualmente previsti

ESITI

Il contratto prevede numerosi indicatori, alcuni dei quali, relativi ai tempi di installazione, non vengono rilevati, in quanto definiti quando gli ATM venivano noleggiati e non acquistati dalla Banca.

Gli indicatori che vengono effettivamente rilevati si riferiscono alle performance sui servizi di help desk (2) e di manutenzione (14).

Per il servizio di help desk si osserva che il parametro per il calcolo del KPI (numero delle chiamate ricevute) è molto basso rispetto al numero di chiamate effettivamente ricevute (30% circa), per cui lo SLA risulta sempre rispettato, anche se, in media, il 21% delle chiamate rimane inevaso. Per il servizio di manutenzione i risultati mensili mostrano un quasi costante mancato rispetto dei livelli di servizio concordati per tutto il 2017 e per i primi 4 mesi del 2018 (cfr. allegato 4).

Le prestazioni dell'*outsourcer* sono monitorate mediante incontri mensili di Vendor Review (il Team di Audit ha partecipato in qualità di osservatore all'incontro relativo al mese di febbraio 2018, tenutosi il 21/3/2018). In cui Funzione Logistica, la Funzione Acquisti e Funzione Commerciale analizzano e discutono con Basilichi i principali indicatori previsti nel contratto (assistenza tecnica, help desk/monitoraggio e piano di roll-out). I KPI vengono calcolati dall'*outsourcer* e la Funzione Logistica effettua delle verifiche a campione, o se emergono situazioni rilevanti.

A seguito del mancato rispetto sopra descritto per il 2017, Funzione Logistica ha richiesto al Servizio Bilancio e Contabilità l'emissione di fatture a ciclo attivo per € 43.375,51. Tale importo rappresenta la penale massima che può essere richiesta all'*outsourcer*, in conseguenza del tetto contrattuale che ne limita l'importo.

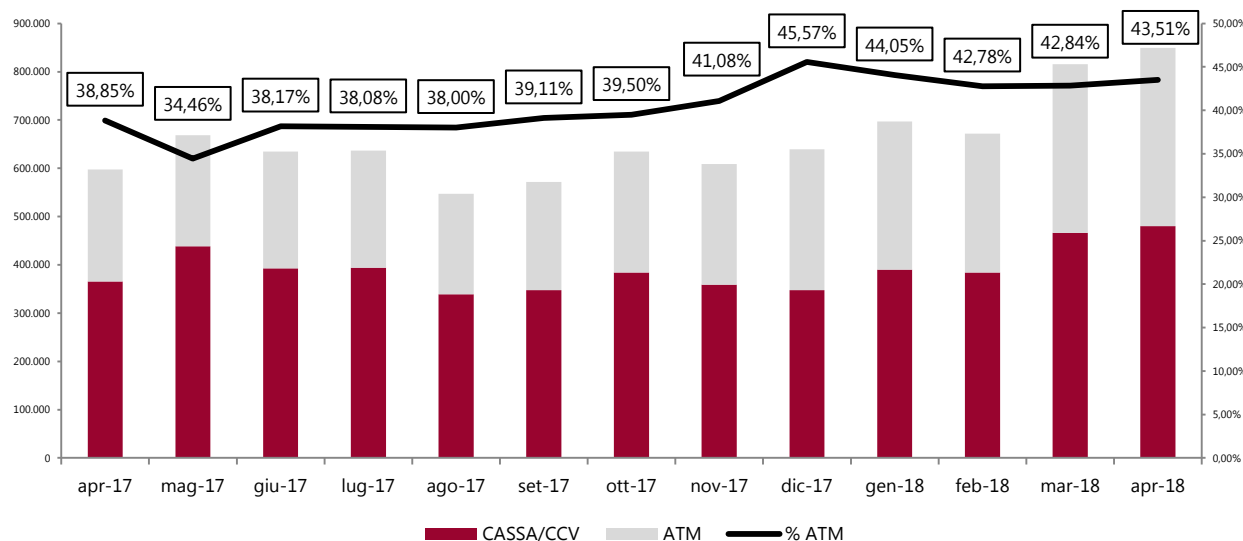
OBIETTIVO	PERIMETRO/ METODOLOGIA	RISCHI IMPATTATI
<p>Valutare l'adeguatezza delle modalità di monitoraggio commerciale del parco ATM</p> <p>Obiettivi SREP: IG 1.2, IG 2.11</p>	<p>❑ Interviste, analisi documentale, analisi di dati, osservazione delle prassi</p> <p>❑ Periodo di riferimento: anno 2018</p>	<p>ID50613 Non adeguata valutazione della profittabilità dei nuovi prodotti</p> <p>ID51559 Mancata o non tempestiva azione di monitoraggio sull'effettivo raggiungimento degli obiettivi definiti</p>
VERIFICHE SVOLTE	ESITI	
<p>a) Analisi del D00751 – Regolamento n. 1 – Organizzazione della Banca MPS, del Catalogo dei Processi e dei documenti normativi connessi</p>	<p>Le responsabilità connesse con l'attività in esame sono chiaramente assegnate.</p> <p>In particolare, sono attribuiti alla Funzione Commerciale i compiti di monitorare le performance operative (funzionalità) e le anomalie (disponibilità) degli ATM e di presidiare e monitorare le iniziative di migrazione dell'operatività dai canali fisici tradizionali al canale ATM.</p>	
<p>b) Analisi delle modalità di monitoraggio della disponibilità del parco ATM</p>	<p>La Funzione Commerciale ha reso disponibile su COGNOS un report mensile sui disservizi ATM per le funzioni di prelievo e di versamento che elenca, per ogni singolo ATM oggetto di disservizio, il minutaggio del disservizio suddiviso per owner (rete/altri), assieme alle relative percentuali, dando evidenza di quelle maggiormente significative.</p> <p>Le situazioni in cui il livello di indisponibilità risulta particolarmente elevato vengono, poi, discusse con le funzioni interessate, per comprendere le cause dei disservizi ed adottare le necessarie iniziative correttive.</p>	
<p>c) Analisi delle modalità di determinazione ed assegnazione alla Rete degli obiettivi relativi all'indice di migrazione dei versamenti e di verifica sul suo andamento</p>	<p>Il potenziamento del parco ATM è funzionale al raggiungimento dell'obiettivo del programma "BANCA Più" di un indice di migrazione dei versamenti su ATM al 60% al 31/12/2018 (50% al 30/6/2018), a sua volta collegato all'obiettivo del Piano di Ristrutturazione 2017-2021 del 70%.</p> <p>Per il raggiungimento di tale livello, Funzione Commerciale ha individuato e assegnato a ciascuna filiale dotata di cash-in obiettivi differenziati, calcolati tenendo conto di diversi fattori (p.e. livello già raggiunto, attitudine all'uso del contante in quella zona geografica, tipologia della clientela, periodo trascorso dall'installazione del cash-in, etc.).</p> <p>La Funzione Commerciale ha reso disponibile su COGNOS una serie di report con coni di visibilità a livello di AT, DTR e Filiale che su base settimanale o mensile, evidenziano l'andamento dell'indice di migrazione dei versamenti rispetto agli obiettivi assegnati. Funzione Commerciale, inoltre, pubblica su di un Team Site ulteriori affinamenti di tali calcoli.</p>	

VERIFICHE SVOLTE

ESITI

I risultati conseguiti dalla Rete sono oggetto di confronto nei periodici SAL che l'Area Digital & Physycal Banking tiene con le strutture di territoriali.

Di seguito un grafico che rappresenta l'andamento dell'indice nel periodo da aprile 2017 a aprile 2018.



Dati forniti da Funzione Commerciale - per il periodo da aprile a novembre 2017 non sono comprese le operazioni effettuate con Carta Debit Mastercard e con modalità *cardless*, per cui i dati non sono del tutto comparabili

6 Audit findings: *gap alti*

GAP	Alti	Medi	Bassi
	1	7	0

La tabella riepiloga i gap a rilevanza alta emersi nel corso della revisione e le relative raccomandazioni.

GAP ALTI

Carenze nei presidi di sicurezza logica sugli apparati ATM

Si rileva l'assenza di criteri e stringenti meccanismi di controllo per la corretta assegnazione alle utenze dei diritti di accesso sulle diverse risorse di sistema che rispettino il principio del "least privilege".

A tale proposito si osserva che, in relazione all'incidente avvenuto in data 19/02/2018, la cancellazione dei file di sistema che ha determinato il blocco degli ATM non sarebbe stata possibile se alle componenti software installate sulle macchine fossero stati assegnati profili abilitativi circoscritti alle effettive necessità applicative, piuttosto che privilegi di amministratore che, di fatto, rendevano possibile il pieno controllo della macchina.

Si rileva inoltre che non risultano attivi i seguenti presidi per la messa in sicurezza del software di base degli ATM:

- assenza di password per l'accesso al BIOS,
- assenza del boot UEFI e della relativa funzionalità di secure boot,
- abilitazione della modalità provvisoria di avvio,
- boot da USB attivo,
- assenza di strumenti per il blocco/gestione di periferiche USB non autorizzate.

RACCOMANDAZIONI

FATTORE
CAUSALE

Implementare adeguati presidi di sicurezza logica sugli ATM

Sulla base di una valutazione dei rischi, definire delle linee guida per la messa in sicurezza degli ATM e implementare i relativi presidi in conformità a quanto definito.

In particolare:

- (1) definire stringenti criteri per l'assegnazione dei diritti di accesso alle diverse tipologie di utenze nel rispetto del principio del "least privilege". Istituire un presidio di controllo sulla corretta attuazione di suddetti criteri vincolante al rilascio in produzione di nuovi sviluppi;
- (2) attivare i presidi sul software di base ritenuti necessari a garantire il livello di sicurezza definito.



6 Audit findings: *gap medi*

GAP	Alti	Medi	Bassi
	1	7	0

La tabella riepiloga i gap a rilevanza media emersi nel corso della revisione e le relative raccomandazioni.

GAP MEDI

RACCOMANDAZIONI

FATTORE
CAUSALE

Carenze nella segregazione delle reti

Le reti utilizzate per la connessione degli ATM remoti, della Fabbrica ATM (Bassilichi) e della sede Bassilichi in via Petrocchi a Firenze sono segregate dalla intranet aziendale tramite firewall sul quale sono settate però regole poco restrittive che potrebbero risultare inefficaci.

Inoltre, il personale di Bassilichi può utilizzare macchine non SIP per connettersi dalla sede di Firenze in via Petrocchi ad una sottorete interna della Banca. Infine la rete sulla quale sono attestati gli ATM di filiale non risulta segregata dalla restante rete aziendale.

Segregare opportunamente la rete interna della Banca

Implementare la miglior soluzione per segregare la intranet aziendale dalla rete degli ATM remoti, della Fabbrica ATM e delle sedi di Bassilichi tramite applicazione di regole più restrittive applicate sui firewall.

Fare in modo che Bassilichi si connetta alle risorse aziendali esclusivamente mediante postazioni SIP. Nel caso in cui questa opzione non fosse applicabile, provvedere ad modificare l'access list definita sul firewall per l'accesso dei PC non SIP di Bassilichi applicando regole restrittive e limitazioni anche in termini di "porte di accesso" e non solo di IP.

Identificare e implementare infine la soluzione ottimale in termini di costi/benefici per segregare la rete degli ATM di filiale.

Attività di deployment svolta da Bassilichi in assenza di contratto

Il deploy (rilascio in produzione) dei pacchetti software sugli apparati ATM viene effettuato da Bassilichi per conto della Banca e non del COG, funzione owner del processo, in assenza di copertura contrattuale.

Ricondurre il deploy all'interno del COG

Ricondurre all'interno delle strutture consortili l'attività di rilascio in produzione dei pacchetti software sugli apparati ATM.

Procedere alla bonifica delle abilitazioni sull'applicativo DAS.



6 Audit findings: *gap medi*

GAP	Alti	Medi	Bassi
	1	7	0

La tabella riepiloga i gap a rilevanza media emersi nel corso della revisione e le relative raccomandazioni.

GAP MEDI

Utenze abilitate alla gestione degli apparati ATM non integrate nello strumento accentrato di controllo accessi

3 Le utenze abilitate nel dominio Active Directory dedicato agli ATM (DO000001000001) non sono presenti sul sistema aziendale accentrato di gestione delle utenze (OIM) in quanto non è implementato il connettore di allineamento tra i due sistemi. Tali utenze vengono quindi gestite manualmente dalla funzione Gestione Utenti con corrispondenti rischi di disallineamento tra la struttura di assegnazione della risorsa e i privilegi operativi attribuiti.

Utenze dell'applicativo GE.BA non gestite nel rispetto della normativa aziendale

4 L'applicativo Gestione Bancomat (GE.BA) ha una profilatura proprietaria gestita dal Settore Monetica il quale, su richiesta della gestione utenti, provvede a censire direttamente sul prodotto le utenze e associarle ai profili. Dall'analisi effettuata¹, è emerso che sulle 210 utenze esaminate, con profili abilitati alle modifiche, numero 98 (pari circa al 46%) risultano presentare anomalie (es. circa la metà risultano inesistenti sulle piattaforma Nuova Interfaccia Utente, 8 utenti risultano censiti doppi o tripli, in alcuni casi con matricole disabilitate, ecc). Risulta quindi che tali utenze non sono oggetto delle verifiche periodiche previste nel documento normativo 389.

¹Analisi eseguita sui dati forniti dal Settore Monetica in data 12/03/2018

RACCOMANDAZIONI

Automatizzare la gestione delle utenze del dominio ATM

Implementare un sistema di allineamento automatico tra il Dominio ATM dell'Active Directory ed il sistema accentrato di controllo accessi.



Condurre una bonifica delle utenze GE.BA

Effettuare un'attività di bonifica delle utenze censite in GE.BA, con particolare attenzione a quelle assegnate agli operatori esterni. Eseguire, in conformità alle regole aziendali in materia (cfr. D. 389 "Sistema Informativo Unitario (S.I.U.) - Accesso e Abilitazioni"), una *review* semestrale delle utenze.

Per consentire il corretto esercizio delle responsabilità, valutare la coerenza dell'attuale collocazione dell'Utente Responsabile per l'applicazione GE.BA, ingaggiando eventualmente le Funzioni Organizzazione e Rischi Operativi (Settore Rischi Informatici) per ricondurlo nell'ambito di una diversa unità organizzativa di business.



6 Audit findings: *gap medi*

GAP	Alti	Medi	Bassi
	1	7	0

La tabella riepiloga i gap a rilevanza media emersi nel corso della revisione e le relative raccomandazioni.

GAP MEDI

Mancanza di informazioni necessarie al monitoraggio delle giacenze

Le filiali non dispongono dell'informazione relativa alla giacenza di contante negli apparati cash-in.

Inoltre nei sistemi di monitoraggio manca uno strumento che segnali in tempo reale il superamento della giacenza massima totale stabilita per gli ATM (sia cash-in che cash-out).

Ciò comporta inefficienze nella gestione del contante e nell'operatività della filiale, oltre a possibili perdite economiche derivanti da rapina di importo superiore ai massimali stabiliti dalla Banca.

A tal proposito, si osserva che circa il 33% degli ATM di filiale attaccati nel 2017 aveva una giacenza superiore al massimale, per una perdita di circa 95.000 € superiore rispetto a quanto previsto dai massimali (7% dell'asportato totale).

Problematica di sicurezza nella funzionalità "cardless" dell'ATM

Quando viene utilizzata la funzionalità "cardless", ovvero quella che effettua l'identificazione dell'utente tramite le credenziali rilasciate nell'ambito del servizio di internet banking, l'ATM invia ai sistemi centrali utente e password del cliente tramite un protocollo non sicuro (http invece di https).

RACCOMANDAZIONI

Implementare le adeguate soluzioni informatiche per il monitoraggio delle giacenze e del superamento del massimale

Implementare le soluzioni già individuate nel BR 54196 relativamente al monitoraggio delle giacenze.

Introdurre inoltre nei sistemi di monitoraggio uno strumento che segnali il superamento del massimale previsto per gli ATM.

Rendere sicuro il canale di trasmissione delle credenziali dell'utente

Mettere in sicurezza la trasmissione delle credenziali (utente e password dell'Internet Banking) utilizzate sull'ATM nella funzionalità "cardless".

FATTORE
CAUSALE



6 Audit findings: *gap medi*

GAP	Alti	Medi	Bassi
	1	7	0

La tabella riepiloga i gap a rilevanza media emersi nel corso della revisione e le relative raccomandazioni.

GAP MEDI

Assenza di monitoraggio sugli interventi di assistenza di secondo livello svolti da TAS

7 Le richieste di assistenza tecnica di secondo livello sui software del mondo ATM, attivate da Bassilichi verso il fornitore TAS, sono registrate in un sistema di ticketing proprietario a cui il settore Monetica non ha attualmente accesso.

Il Settore pertanto non può svolgere attività di monitoraggio sugli interventi di assistenza di secondo livello effettuati, con particolare riferimento al rispetto dei tempi riportati nel contratto di servizio.*

*Allegato 2 – Manutenzione Ordinaria.

RACCOMANDAZIONI

Istituire un'attività di monitoraggio degli interventi tecnici di secondo livello

Richiedere accesso al sistema di ticketing del fornitore TAS (o alternativamente chiedergli di utilizzare il sistema consortile) al fine di monitorare gli interventi e il rispetto dei tempi di assistenza contrattualizzati.

FATTORE
CAUSALE



Firme e destinatari del rapporto

Ruolo	Cognome e Nome	Firma
Responsabile Audit Team	Monti Andrea	
	Scaccia Michela	
Auditors	Fei Luca	
	Giannetti Claudio	
	Parrini Isabella	
	Volpi Antonio	
V° Responsabile del Settore ICT Audit	Salvini Riccardo	
V° Responsabile del Settore Operational Audit	Scarantino Elena	
V° Responsabile del Servizio ICT & Operational Audit	Lombrano Antonio	
V° Responsabile dell'Area Revisione Specialistica	Furlani Andrea	
V° Responsabile della Direzione Chief Audit Executive	Cocco Pierfrancesco	

Organi destinatari BMPS	Selezione
Presidente del CdA	X
Amministratore Delegato	X
Collegio Sindacale	X
Comitato Rischi	X

Altri organi destinatari	
Legal Entity	Organo destinatario
Consorzio Operativo Gruppo Montepaschi	Presidente del CdA
Consorzio Operativo Gruppo Montepaschi	Amministratore Delegato
Consorzio Operativo Gruppo Montepaschi	Collegio Sindacale



Elenco allegati

- » Allegato 1: Tabella dei gap
- » Allegato 2: Valutazione Obiettivi di controllo SREP
- » Allegato 3: Infrastruttura ATM
- » Allegato 4: Livelli di servizio - Basilichi



Allegato 1: tabella dei gap (1 di 4)

N.	PROCESSO	GAP	RILEVANZA (A/M/B)	RISCHIO	FATTORE CAUSALE	RACCOMANDAZIONE	STRUTTURA OWNER	SCADENZA (GG/MM/AA)	CODICE OB SREP
1	Gestione dei processi operativi di sicurezza logica	<p>Carenze nei presidi di sicurezza logica sugli apparati ATM</p> <p>Si rileva l'assenza di criteri e stringenti meccanismi di controllo per la corretta assegnazione alle utenze dei diritti di accesso sulle diverse risorse di sistema che rispettino il principio del "least privilege".</p> <p>A tale proposito si osserva che, in relazione all'incidente avvenuto in data 19/02/2018, la cancellazione dei file di sistema che ha determinato il blocco degli ATM non sarebbe stata possibile se alle componenti software installate sulle macchine fossero stati assegnati profili abilitativi circoscritti alle effettive necessità applicative, piuttosto che privilegi di amministratore che, di fatto, rendevano possibile il pieno controllo della macchina.</p> <p>Si rileva inoltre che non risultano attivi i seguenti presidi per la messa in sicurezza del software di base degli ATM:</p> <ul style="list-style-type: none"> a) assenza di password per l'accesso al BIOS, b) assenza del boot UEFI e della relativa funzionalità di secure boot, c) abilitazione della modalità provvisoria di avvio, d) boot da USB attivo, e) assenza di strumenti per il blocco/gestione di periferiche USB non autorizzate. 	A	Operativo	Sistemi	<p>Implementare adeguati presidi di sicurezza logica sugli ATM</p> <p>Sulla base di una valutazione dei rischi, definire delle linee guida per la messa in sicurezza degli ATM e implementare i relativi presidi in conformità a quanto definito.</p> <p>In particolare:</p> <ul style="list-style-type: none"> (1) definire stringenti criteri per l'assegnazione dei diritti di accesso alle diverse tipologie di utenze nel rispetto del principio del "least privilege". Istituire un presidio di controllo sulla corretta attuazione di suddetti criteri vincolante al rilascio in produzione di nuovi sviluppi; (2) attivare i presidi sul software di base ritenuti necessari a garantire il livello di sicurezza definito. 	Area Rischi e Sicurezza Informatica (COG)	31/10/2018	IG 6.3

Allegato 1: tabella dei gap (2 di 4)

N.	PROCESSO	GAP	RILEVANZA (A/M/B)	RISCHIO	FATTORE CAUSALE	RACCOMANDAZIONE	STRUTTURA OWNER	SCADENZA (GG/MM/AA)	CODICE OB SREP
2	Gestione dei processi operativi di sicurezza logica	Carenze nella segregazione delle reti	M	Operativo	Sistemi	Segregare opportunamente la rete interna della Banca	Servizio Sistemi Tecnologici (COG) con il supporto Servizio Sicurezza Informatica e BCM (COG)	31/01/2019	IG 6.3
		Le reti utilizzate per la connessione degli ATM remoti, della Fabbrica ATM (Bassilichi) e della sede Bassilichi in via Petrocchi a Firenze sono segregate dalla intranet aziendale tramite firewall sul quale sono settate però regole poco restrittive che potrebbero risultare inefficaci.				Implementare la miglior soluzione per segregare la intranet aziendale dalla rete degli ATM remoti, della Fabbrica ATM e delle sedi di Bassilichi tramite applicazione di regole più restrittive applicate sui firewall.			
		Inoltre il personale di Bassilichi può utilizzare macchine non SIP per connettersi dalla sede di Firenze in via Petrocchi ad una sottorete interna della Banca.				Fare in modo che Bassilichi si connetta alle risorse aziendali esclusivamente mediante postazioni SIP. Nel caso in cui questa opzione non fosse applicabile, provvedere ad modificare l'access list definita sul firewall per l'accesso dei PC non SIP di Bassilichi applicando regole restrittive e limitazioni anche in termini di "porte di accesso" e non solo di IP.			
		Infine la rete sulla quale sono attestati gli ATM di filiale non risulta segregata dalla restante rete aziendale.				Identificare e implementare infine la soluzione ottimale in termini di costi/benefici per segregare la rete degli ATM di filiale.			
3	Change, release e deployment management	Attività di deployment svolta da Bassilichi in assenza di contratto	M	Operativo	Sistemi	Ricondurre il deploy all'interno del COG	Servizio Erogazione (COG)	31/12/2018	IG 6.3
		Il deploy (rilascio in produzione) dei pacchetti software sugli apparati ATM viene effettuato da Bassilichi per conto della Banca e non del COG, funzione owner del processo, in assenza di copertura contrattuale.				Ricondurre all'interno delle strutture consortili l'attività di rilascio in produzione dei pacchetti software sugli apparati ATM. Procedere alla bonifica delle abilitazioni sull'applicativo DAS.			



Allegato 1: tabella dei gap (3 di 4)

N.	PROCESSO	GAP	RILEVANZA (A/M/B)	RISCHIO	FATTORE CAUSALE	RACCOMANDAZIONE	STRUTTURA OWNER	SCADENZA (GG/MM/AA)	CODICE OB SREP
4	Gestione dei processi operativi di sicurezza logica	<p>Utenze abilitate alla gestione degli apparati ATM non integrate nello strumento accentrato di controllo accessi</p> <p>Le utenze abilitate nel dominio Active Directory dedicato agli ATM (DO000001000001) non sono presenti sul sistema aziendale accentrato di gestione delle utenze (OIM) in quanto non è implementato il connettore di allineamento tra i due sistemi. Tali utenze vengono quindi gestite manualmente dalla funzione Gestione Utenti con corrispondenti rischi di disallineamento tra la struttura di assegnazione della risorsa e i privilegi operativi attribuiti.</p>	M	Operativo	Sistemi	<p>Automatizzare la gestione delle utenze del dominio ATM</p> <p>Implementare un sistema di allineamento automatico tra il Dominio ATM dell'Active Directory ed il sistema accentrato di controllo accessi.</p>	Servizio Sicurezza Informatica e BCM (COG)	30/10/2018	IG 2.6
5	Gestione dei processi operativi di sicurezza logica	<p>Utenze dell'applicativo GE.BA non gestite nel rispetto della normativa aziendale</p> <p>L'applicativo Gestione Bancomat (GE.BA) ha una profilatura proprietaria gestita dal Settore Monetica il quale, su richiesta della gestione utenti, provvede a censire direttamente sul prodotto le utenze e associarle ai profili. Dall'analisi effettuata¹, è emerso che sulle 210 utenze esaminate, con profili abilitati alle modifiche, numero 98 (pari circa al 46%) risultano presentare anomalie (es. circa la metà risultano inesistenti sulle piattaforma Nuova Interfaccia Utente, 8 utenti risultano censiti doppi o tripli, in alcuni casi con matricole disabilitate, ecc). Risulta quindi che tali utenze non sono oggetto delle verifiche periodiche previste nel documento normativo 389.</p> <p>¹Analisi eseguita sui dati forniti dal Settore Monetica in data 12/03/2018</p>	M	Operativo	Sistemi	<p>Condurre una bonifica delle utenze GE.BA</p> <p>Effettuare un'attività di bonifica delle utenze censite in GE.BA, con particolare attenzione a quelle assegnate agli operatori esterni. Eseguire, in conformità alle regole aziendali in materia (cfr. D. 389 "Sistema Informativo Unitario (S.I.U.) - Accesso e Abilitazioni"), una review semestrale delle utenze.</p> <p>Per consentire il corretto esercizio delle responsabilità, valutare la coerenza dell'attuale collocazione dell'Utente Responsabile per l'applicazione GE.BA, ingaggiando eventualmente le Funzioni Organizzazione e Rischi Operativi (Settore Rischi Informatici) per ricondurlo nell'ambito di una diversa unità organizzativa di business.</p>	Servizio Digital Banking e ATM (BANCA) con il supporto Servizio Bancassurance e Monetica (COG)	30/9/2018	IG 2.6



Allegato 1: *tabella dei gap (4 di 4)*

N.	PROCESSO	GAP	RILEVANZA (A/M/B)	RISCHIO	FATTORE CAUSALE	RACCOMANDAZIONE	STRUTTURA OWNER	SCADENZA (GG/MM/AA)	CODICE OB SREP
6	Enterprise Architecture Management	<p>Mancanza di informazioni necessarie al monitoraggio delle giacenze</p> <p>Le filiali non dispongono dell'informazione relativa alla giacenza di contante negli apparati cash-in. Inoltre nei sistemi di monitoraggio manca uno strumento che segnali in tempo reale il superamento della giacenza massima totale stabilita per gli ATM (sia cash-in che cash-out). Ciò comporta inefficienze nella gestione del contante e nell'operatività della filiale, oltre a possibili perdite economiche derivanti da rapina di importo superiore ai massimali stabiliti dalla Banca.</p> <p>A tal proposito, si osserva che circa il 33% degli ATM di filiale attaccati nel 2017 aveva una giacenza superiore al massimale, per una perdita di circa 95.000 € superiore rispetto a quanto previsto dai massimali (7% dell'asportato totale).</p>	M	Operativo	Sistemi	<p>Implementare le adeguate soluzioni informatiche per il monitoraggio delle giacenze e del superamento del massimale</p> <p>Implementare le soluzioni già individuate nel BR 54196 relativamente al monitoraggio delle giacenze.</p> <p>Introdurre inoltre nei sistemi di monitoraggio uno strumento che segnali il superamento del massimale previsto per gli ATM.</p>	Servizio Cash Management, ATM e Logistica (BANCA)	28/2/2019	IG 7.6
7	Enterprise Architecture Management	<p>Problematica di sicurezza nella funzionalità "cardless" dell'ATM</p> <p>Quando viene utilizzata la funzionalità "cardless", ovvero quella che effettua l'identificazione dell'utente tramite le credenziali rilasciate nell'ambito del servizio di internet banking, l'ATM invia ai sistemi centrali utente e password del cliente tramite un protocollo non sicuro (http invece di https).</p>	M	Operativo	Sistemi	<p>Rendere sicuro il canale di trasmissione delle credenziali dell'utente</p> <p>Mettere in sicurezza la trasmissione delle credenziali (utente e password dell'Internet Banking) utilizzate sull'ATM nella funzionalità "cardless".</p>	Servizio Bancassurance e Monetica (COG)	31/10/2018	BM 7.8
8	Enterprise Architecture Management	<p>Assenza di monitoraggio sugli interventi di assistenza di secondo livello svolti da TAS</p> <p>Le richieste di assistenza tecnica di secondo livello sui software del mondo ATM, attivate da Bassilichi verso il fornitore TAS, sono registrate in un sistema di ticketing proprietario a cui il settore Monetica non ha attualmente accesso.</p> <p>Il Settore pertanto non può svolgere attività di monitoraggio sugli interventi di assistenza di secondo livello effettuati, con particolare riferimento al rispetto dei tempi riportati nel contratto di servizio.*</p>	M	Operativo	Processo	<p>Istituire un'attività di monitoraggio degli interventi tecnici di secondo livello</p> <p>Richiedere accesso al sistema di ticketing del fornitore TAS (o alternativamente chiedergli di utilizzare il sistema consortile) al fine di monitorare gli interventi e il rispetto dei tempi di assistenza contrattualizzati.</p>	Servizio Bancassurance e Monetica (COG)	31/10/2018	IG 7.6

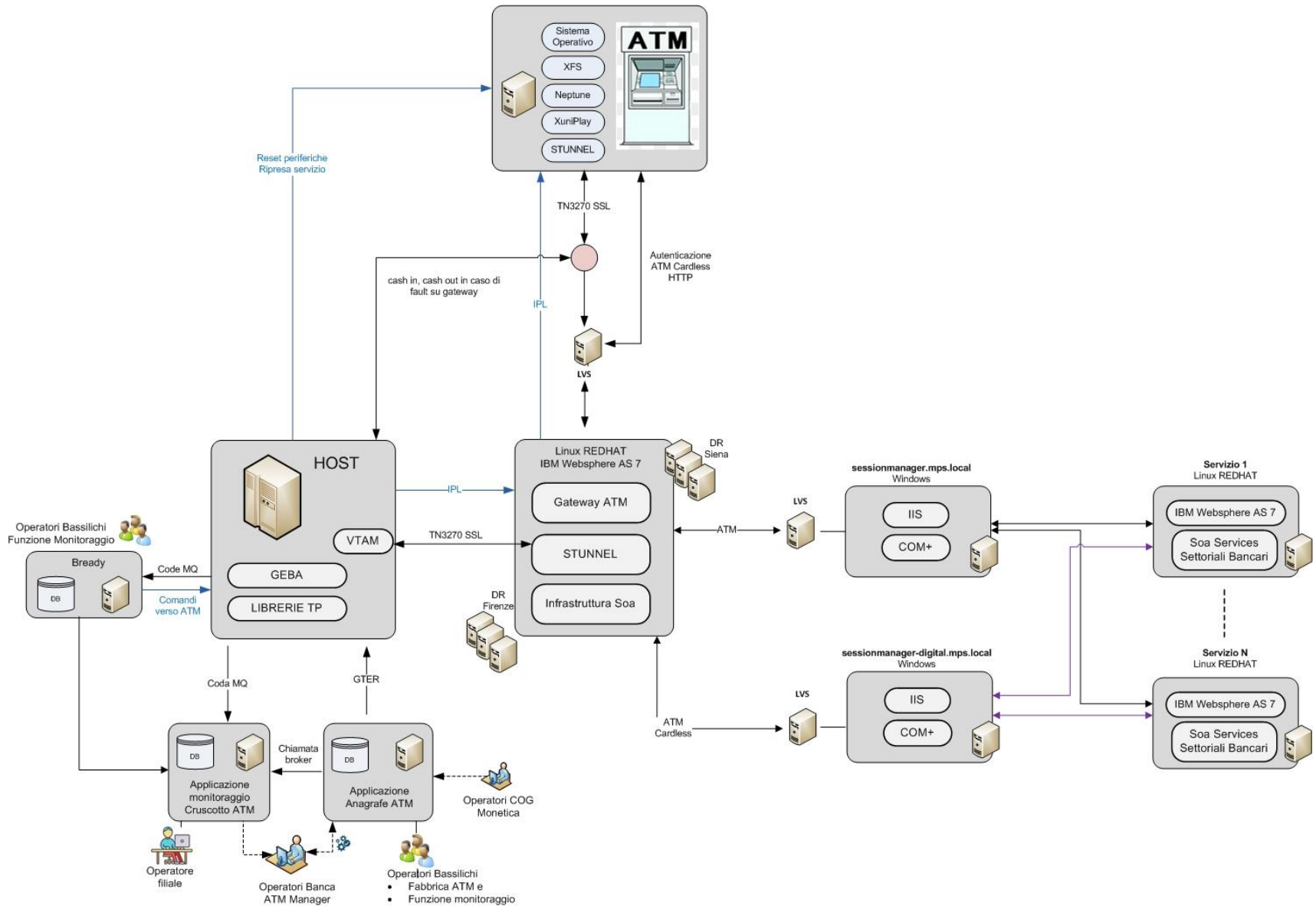
*Allegato 2 – Manutenzione Ordinaria.



Allegato 2: valutazione obiettivi di controllo SREP

Codice	Obiettivi di controllo	Processo	Percentuale di completamento	Rating	Note/ GAP
BM 7.8	Verificare che gli interventi IT vengano effettuati in ottica prospettica (sviluppi strategici in tema di IT), sottoponendo i sistemi a un processo di "continuous innovation" e minimizzando gli ostacoli creati dai "legacy systems"	Enterprise Architecture Management	5%	B	Gap 7
IG 2.6	Verificare che i Responsabili delle diverse linee di business pongano in essere dei controlli efficaci ad identificare, monitorare e segnalare il superamento dei limiti di rischio loro assegnati, agendo in maniera tempestiva nei casi di sfioramento dei limiti di rischio assegnati	Gestione dei processi operativi di sicurezza logica	10%	C	Gap 4 e 5
IG.2.11	Verificare l'esistenza di adeguati e strutturati flussi informativi sia verticali che orizzontali e che gli stessi siano opportunamente codificati	Gestione filiera del contante	40%	B	
IG.6.3	Verificare l'adozione di un set di controlli di linea e la regolare esecuzione da parte delle unità organizzative coinvolte nei processi aziendali	Presidio ATM e canale Self Banking	90%	B	
		Change Release e Deployment Management	5%	B	Gap 3
		Gestione dei processi operativi di sicurezza fisica	20%	B	
		Gestione dei processi operativi di sicurezza logica	10%	C	Gap 1 e 2
IG 7.6	Verificare che il Gruppo/la Banca possieda appropriati sistemi IT, infrastrutture e processi in modo da fornire adeguate, tempestive e complete informazioni all'Organo con Funzione di Supervisione Strategica e all'Organo con Funzione di Gestione per l'identificazione dei rischi e per la sorveglianza	Enterprise Architecture Management	10%	B	Gap 6 e 8

Allegato 3: infrastruttura ATM

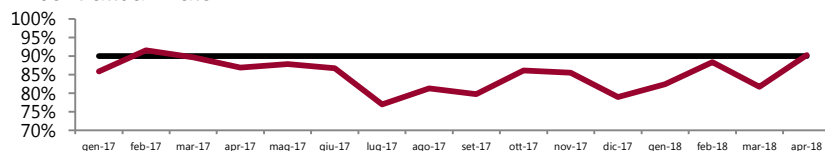


Allegato 4: livelli di servizio - Bassilichi

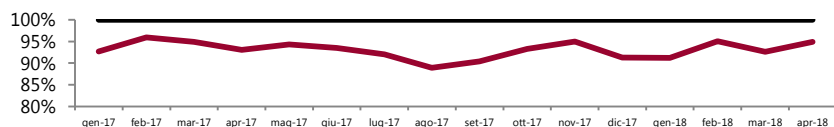
PERFORMANCE SUGLI INTERVENTI BLOCCANTI

ITC1 – Interventi su ATM presidiati e non presidiati

85% degli interventi risolti entro il 1° SLA, rispetto al 90% contrattualizzato

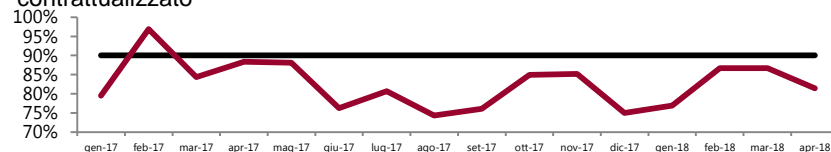


93% degli interventi risolti entro il 2° SLA, rispetto al 100% contrattualizzato

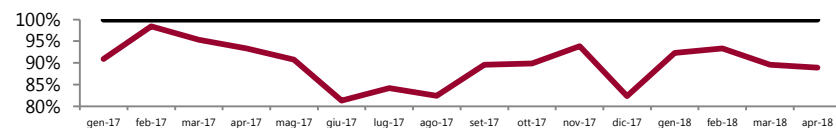


ITC3 – Interventi su ATM VIP

83% degli interventi risolti entro il 1° SLA, rispetto al 90% contrattualizzato



90% degli interventi risolti entro il 2° SLA, rispetto al 100% contrattualizzato



PERFORMANCE HELP DESK

ICM3 – Percentuale dei contatti evasi rispetto alle chiamate attese

- ❑ Lo SLA è quasi sempre rispettato.
- ❑ La media delle chiamate ricevute è mediamente il 30% in più rispetto a quelle attese utilizzato per il calcolo dello SLA.

