MONTE DEI PASCHI DI SIENA
BANCA DAL 1472

Accentramento Moduli di Adesione alla FEA (Firma Elettronica Avanzata) - SAL

Azioni Intraprese - Sintesi

Nel corso delle scorse settimane sono state poste in essere una serie di azioni finalizzate a quantificare con un miglior livello di approssimazione le evidenze rivenienti dal Rapporto di Revisione 085/2018. In particolare:

18/12/2018

1. Avvio **Monitoraggio Moduli di Adesione FEA «prioritari»** relativi a clienti che hanno sottoscritto Contratti e Fondi (KRI su **72.810** Moduli da ricercare)

27/12/2018

2. Avvio **Task Force «interfunzionale»** per verifiche approfondite sul livello di archiviazione dei Moduli di Adesione alla FEA su un campione di **165 Filiali la cui analisi verrà completata entro il 15 gennaio**

31/12/2018

3. **Sospensione operatività con Firma Grafometrica per ca. 1,3** mln di clienti e contestuale rilascio di pop-up informativo alla rete, processi di post-vendita FEA e modulistica specifici per clienti con FEA sospesa, bacheca messaggi e documenti normativi a supporto

04/01/2019

4. **Avvio Monitoraggio Moduli di Adesione FEA «non prioritari»** (1,3 mln di Moduli complessivi da ricercare)

15/01/2019

5. **Consolidamento approfondimenti sulle attività*** (contrattuali e dispositive) **poste in essere dai clienti** con FEA Sospesa e stima potenziali impatti economico patrimoniali

6. Definizione **azioni di Remediation** per quei clienti di cui non è stato ritrovato archiviato in filiale il Modulo di Adesione alla Fea (Attività in corso a cura di Legale e Compliance da definirsi entro il 15 gennaio)

1/02/2019

7. **Pianificazione e avvio azioni di remediation - contatto con i clienti** per la regolarizzazione della sottoscrizione del servizio FEA (firma nuovo Modulo predisposto con legale e Compliance)

* ai sensi del Doc Normativo D 1747 le operazioni che è possibile firmare in modalità grafometrica possono riguardare: contratti di monetica (carte di credito, debito e prepagate), operazioni di sportello (prelievi, versamenti, assegni, bonifici, incassi commerciali, cambio contanti, etc…), Fondi Anima, KYC, Mifid, privacy, variazione recapiti telematici, conti a pacchetto (che possono includere il Dossier Titoli – Il Dossier Titoli stand alone non è ancora sottoscrivibile con FEA), digital banking, etc

Azioni Intraprese

1 Avvio Monitoraggio Moduli di Adesione FEA «prioritari»

Il 18 dicembre è stato attivato il monitoraggio giornaliero a cura della Direzione Rete del KRI relativo a quei clienti «prioritari» , che hanno cioè firmato almeno un Documento Contrattuale o sottoscritto un Fondo Anima. Al 9 gennaio 2019 (dopo 13 giorni lavorativi) rispetto ai **72.810** Moduli di adesione sono stati individuati in filiale e accentrati nelle modalità previste (archiviazione mediante Spunta Documentale e Pacco Pardo): **45.851** moduli pari al **63%**.

Area Territoriale	Monitoraggio Arretrati FEA prioritari				
	18/12/18		08/01/19		
	Da recuperare	Recuperati	Da recuperare	Recuperati	% recuperati
NORD OVEST	10.774	60	2.882	7.952	73%
NORD EST	7.466	125	2.489	5.102	67%
TOSCANA	18.591	253	7.996	10.848	58%
CENTRO E SARDEGNA	11.439	277	4.151	7.565	65%
SUD E SICILIA	23.535	290	9.441	14.384	60%
TOTALE	**71.805**	**1.005**	**26.959**	**45.851**	**63%**

Il 18 dicembre sono state attivate anche Visite Organizzative su un campione ridotto di filiali, finalizzate a verificare le modalità operative seguite per l'archiviazione della documentazione. Da queste prime visite organizzative sono emerse evidenze quantitative in linea con i trend del KRI ed alcune prassi operative di archiviazione non sempre omogenee o in linea con quanto previsto in normativa (ad es.: archiviazione nei documenti di cassa, in pacchi pardo di sfollamento archivi, in pacchi pardo generici etc….)

Azioni Intraprese

2 Avvio Task Force interfunzionale per verifiche approfondite su 165 filiali

Il 27 dicembre è stata attivata una Task Force interfunzionale, con il coinvolgimento di strutture di Area Territoriale e di DG, coordinata da AO per verificare il reale stato di archiviazione dei Moduli di Adesione al Servizio FEA su un campione più rappresentativo (165 filiali a target).
Ad oggi la situazione della Task Force è la seguente:

Risorse Assegnate per Area Territoriale

AREA TERRITORIALE	Assegnate
NORD OVEST	75
NORD EST	56
TOSCANA	58
CENTRO E SARDEGNA	56
SUD E SICILIA	63
TOTALE	308

Risorse Assegnate per Direzione

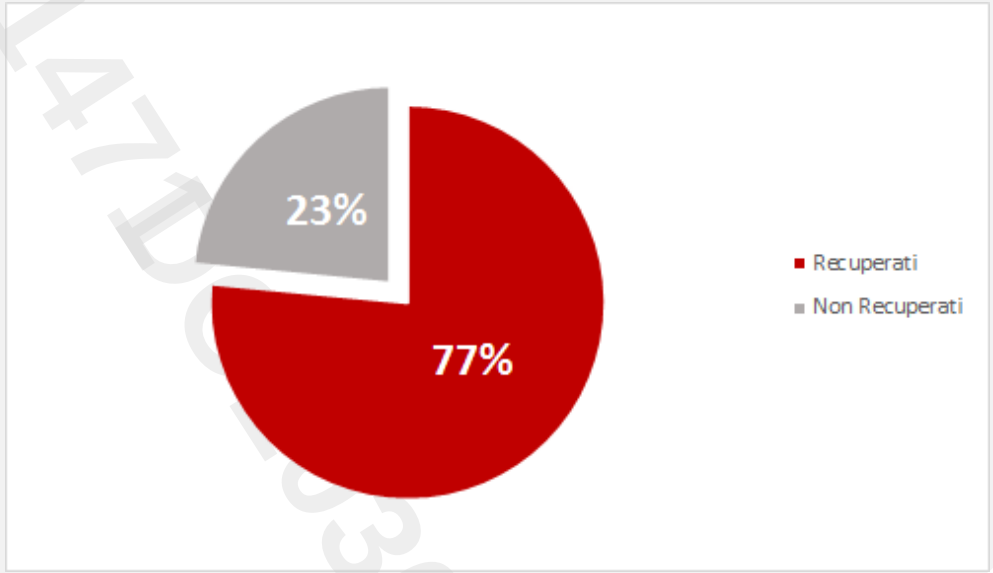
DIREZIONE	Assegnate
CAE	31
CCO	103
CHCO	43
CLO	33
COO	98
TOTALE	308

Azioni Intraprese

2 Al 9 di gennaio la Task Force risulta attivata su tutte le 165 filiali previste. I risultati saranno disponibili il 15 gennaio, sotto le **primissime** evidenze :

Area Territoriale	# Moduli TOTALI	KRI PRIORITARI						KRI SECONDARI						# Filiali Campione	# Filiali Completate
		Baseline Moduli (con contratti)	# Mod Cartaceo Trovati		# Moduli non trovati	Da Lavorare	% Moduli recuperati da TF	Baseline Moduli (senza contratti)	# Mod Cartaceo Trovati		# Moduli non trovati	Da Lavorare	% Moduli recuperati da TF		
			Firmati	Non firmati/Non regolari					Firmati	Non firmati/Non regolari					
NORD OVEST	50.698	3.599	2.479	206	633	281	69%	47.099	26.060	6.512	5.431	9.096	55%	37	14
NORD EST	18.276	848	720	24	104	-	85%	17.428	12.575	834	4.000	19	72%	32	30
TOSCANA	25.611	1.941	1.692	55	181	13	87%	23.670	16.330	2.867	3.081	1.392	69%	32	15
CENTRO E SARDEGNA	16.917	1.331	1.000	21	174	136	75%	15.586	10.484	258	2.104	2.740	67%	30	8
SUD E SICILIA	47.223	3.429	2.233	117	227	852	65%	43.794	20.190	2.351	2.635	18.618	46%	34	-
TOTALE	158.725	11.148	8.124	423	1.319	1.282	73%	147.577	85.639	12.822	17.251	31.865	58%	165	67

La rilevazione da parte della Task Force si è conclusa nel **41%** delle filiali campione (67 filiali) ed ha evidenziato che mediamente sono stati recuperati il **77% dei moduli**



Azioni Intraprese

3 Sospensione Operatività con Firma Grafometrica per 1,3 mln di clienti

Il 31 dicembre 2018 è stato attivato il blocco operativo per quei clienti (1.289.434 NGR – alcuni clienti hanno più di un Modulo di Adesione) il cui Modulo di Adesione risulta ancora da verificare e reperire in filiale. Tali clienti possono operare in modalità cartacea ordinaria o tramite Firma Digitale Remota (se posseduta). Comunicazioni inviate alla rete:

- **Attivato pop-up informativo** visibile esclusivamente agli Operatori di Sportello e Gestori (il pop-up riporta il messaggio: Cliente con Servizio FEA sospesa- Cfr D 1747)
- **Inviata Bacheca Messaggi** (ogni giorno per 5 giorni) contenente il seguente messaggio:

> *"Si porta a conoscenza della Rete che, a partire dal 31 dicembre 2018, saranno temporaneamente sospesi i Servizi di "Firma Elettronica Avanzata e Dematerializzazione Documenti" (Servizio FEA) e "Firma su Tablet e Contabili Digitali" per tutti i clienti che vi hanno aderito antecedentemente al 22 dicembre 2015 al fine di consentire la verifica della conformità e completezza della documentazione contrattuale correlata. Nel periodo di sospensione è garantita a questi clienti la possibilità di continuare ad operare con i normali supporti cartacei.*
> *Il Servizio riprenderà per i singoli clienti via via che le verifiche saranno state ultimate, con eventuale integrazione documentale, ove necessario. Per i clienti che hanno aderito a partire dal 22 dicembre 2015 il Servizio sarà erogato regolarmente.*
> *-Documento di riferimento: D1747 "Gestione delle Firme Elettroniche ed operatività digitale nei processi di Rete"*

- **Pubblicato aggiornamento Normativa** D1747 e Manuale Operativo M159: contenenti le istruzioni operative che le filiali devono seguire per la corretta archiviazione dei Moduli di Adesione rivenuti in filiale

Azioni Intraprese

4 Avvio Monitoraggio Moduli di Adesione FEA «non prioritari»

Il 4 di gennaio è stato attivato il monitoraggio giornaliero a cura della Direzione Rete del secondo KRI sulla tematica FEA, relativo a tutti i Moduli da ricercare che sono complessivamente **1.299.806 comprensivi anche dei 72.810 monitorati a parte come KRI «prioritari»** (cfr. slide 2).
Al 9 gennaio 2019 rispetto ai **1.299.806** Moduli di Adesione complessivi sono stati individuati in filiale e accentrati nelle modalità previste (archiviazione mediante Spunta Documentale e Pacco Pardo): **298.542** moduli pari al **23%**.
Nei prossimi giorni sarà attivata la funzione di ripristino dell'utilizzo della FEA per i clienti con Modulo accentrato e validazione avvenuta (il processo prevede un controllo di presenza delle firme con eventuale riciclo sulla Rete).

Area Territoriale	Monitoraggio Arretrati FEA complessivi				
	04/01/19		09/01/19		
	Da recuperare	Recuperati	Da recuperare	Recuperati	% recuperati
NORD OVEST	157.895	38.769	114.269	82.395	42%
NORD EST	193.582	31.860	165.007	60.435	27%
TOSCANA	271.710	28.888	253.824	46.774	16%
CENTRO E SARDEGNA	146.315	26.654	127.878	45.091	26%
SUD E SICILIA	365.914	38.219	340.286	63.847	16%
TOTALE	**1.135.416**	**164.390**	**1.001.264**	**298.542**	**23%**

Azioni Intraprese

5 Consolidamento approfondimenti sulle attività (contrattuali e dispositive) poste in essere dai clienti con FEA Sospesa e stima potenziali impatti economico patrimoniali

In attesa del consolidamento dei risultati delle nuove estrazioni in corso, si riporta uno spaccato del numero di clienti per Tipologia di Operazione ad oggi disponibile:

Tipologia operazione	# NGR
Fondi	83.908
Contratti	72.220
Titoli*	11.265
KYC*	73.585
MiFID*	101.268
Altro*	1.045.979

Precedenti 16.141

Precedenti 58181

* Da Consolidare

Azioni Intraprese

6 Definizione azioni di Remediation per quei clienti di cui non è stato ritrovato archiviato in filiale il Modulo di Adesione alla Fea (Attività in corso a cura di Legale e Compliance da definirsi entro il 15 gennaio)

Nel caso in cui l'esito della ricerca in filiale del Modulo di Adesione firmato abbia dato esito negativo è necessario richiamare il cliente per regolarizzare il rapporto instaurato, tramite una nuova sottoscrizione del Modulo stesso o di altra documentazione . Le funzioni Legale e Compliance stanno definendo il contenuto del nuovo Modulo (di «regolarizzazione»).

7 Pianificazione e avvio azioni di Remediation - Contatto con i clienti per la regolarizzazione della sottoscrizione del servizio FEA (firma nuovo Modulo predisposto con Legale e Compliance)

0028500IS0147DO103

Sintesi andamento GAP

#	Gap	Rilevanza	Owner	Scadenza
1	Operatività con firma grafometrica a rischio disconoscimento e/o trattamento di dati biometrici non autorizzato	A	Direzione Rete	31/12/2019
2	Ritardato o mancato invio del documento di adesione al servizio FEA al Centro Documentale	A	Servizio Organization Partner COO e Process Management Innovation	30/06/2019
3	Assenza di controlli sul formato del documento digitale	A	COG – Servizio Assisted Banking	30/04/2019
4	Mancato rispetto dei presidi minimi di sicurezza logica nella gestione dell'archivio documentale della Banca, IBM Content Manager (CM)	A	COG – Servizio Sistemi Tecnologici	28/02/2019
5	Accesso diretto ai dati eludendo i presidi di controllo definiti	A	COG – Servizio Credito	31/01/2019
6	Disallineamento tra Log Unico e contenuto degli archivi documentali	M	COG – Servizio Assisted Banking	31/12/2018
7	Sistema di Conservazione Sostitutiva – Accountability non garantita	M	Servizio Cash Management, ATM e Logistica	31/05/2019
8	Assenza controlli su l'integrità dei documenti inoltrati in Conservazione Sostitutiva (CS)	M	COG – Servizio Assisted Banking	30/04/2019
9	Assenza di una relazione tecnica aggiornata di cui al Provvedimento del Garante in tema di biometria	B	Servizio Organization Partner COO e Process Management Innovation	31/01/2019
10	Annullamento operazioni di sportello: inoltro in Conservazione Sostitutiva di documenti non validi	B	COG – Servizio Assisted Banking	31/01/2019
11	Archiviazione dei documenti contenenti i dati biometrici dei clienti all'interno del sistema informativo della Banca	B	COG – Servizio Assisted Banking	31/12/2018
12	Inaffidabilità delle informazioni relative all'ubicazione delle tavolette grafometriche	B	COG – Servizio Sistemi Tecnologici	31/01/2019

Allegati

0058500011S50147DO1036

GAP 1

Owner: Direzione Rete – Contributor: Ser. OP COO e Process Mng Innovation

Ril	Problema	Descrizione Gap	Fatti	Soluzione	Rilascio	Scadenza
A	Operatività con firma grafometrica a rischio disconoscimento e/o trattamento di dati biometrici non autorizzato	Prima dell'accentramento obbligatorio (dicembre 2015) le istruzioni operative prevedevano la conservazione in filiale dell' adesione al servizio di FEA (circa 1,3 mln di documenti). Questa condizione espone ad una minore certezza di recupero della documentazione e non ne garantisce la correttezza formale (es. presenza delle firma). Quanto detto è stato confermato da una ricognizione compiuta presso un campione di filiali, i cui esiti hanno rilevato un'elevata percentuale (99% in un caso e 65% nell'altro) di documentazione non firmata e/o archiviata in maniera non appropriata. Quanto sopra non tutela efficacemente dal rischio di disconoscimento di operazioni sottoscritte grafometricamente da un cliente senza preventiva adesione al Servizio di FEA, né dal rischio di non conformità per il trattamento non autorizzato di dati biometrici con possibili sanzioni amministrative.	I documenti di adesione ante 21/12/2015* (circa 1,3 mln di contratti) risultano non accentrati per scelta organizzativa; per tali documenti gli esiti delle verifiche campionarie (**su due filiali**) hanno registrato percentuali che oscillano tra il 65% ed il 99% di documentazione non firmata; è già stato avviato un tentativo di raccolta massiva alla fine del 2017 che si è concluso a metà del 2018 senza risultati significativi (solo 12.102 recuperi).	▫ Estrazione modulistica dei clienti aderenti alla FEA ante 21/12/2015 con ripulitura dei moduli accentrati nella prima campagna di spunta 2017 ▫ Creazione spunte con invio tranche da 100k a 200k a settore portali interni COG (mail inviate da Bencini a Salotti) – dal 22/11/2018 ▫ Caricamento massivo firmatari su DWH da CM – BR 79634. Dati consolidati al 31/10/2018 (BR 79634) ▫ Pubblicazione M159 e D1748 in occasione della conclusione della fase di creazione delle spunte documentali in Rete ▫ Inoltro a funzione CRM (Lauro) file pratiche riconducibili a firmatari di fondi e/o contratti ▫ Introduzione blocco applicativo che non permetta agli NGR privi del Modulo di Adesione accentrato di operare in Grafometrica ▫ Pubblicazione M159 e D1748 per gestione «sospensione» FEA ▫ Creazione batch di alimentazione target periodica dei firmatari su DWH da CM per aggiornamento periodico dati post 31/10/2018 (BR 79634) e caricamento dati fino al 27/12/2018 ▫ Rimozione vincolo all'utilizzo delle firme elettroniche per le AT/DT interessate (minore efficacia Firma Digitale per operazioni sportello) Per i clienti per i quali non è stato rintracciato il documento originario ▫ Predisposizione modulo da sottoporre alla firma ▫ Produzione massiva moduli (BR 79950 da pianificare e approvare) ▫ Predisposizione campagne o nuove spunte documentali	20/11/2018 3/12/2018 31/10/2018 3/12/2018 18/12/2018 31/12/2018 31/12/2018 31/12/2018 gg.mm.2019 *Tbd*	31/12/2019

GAP 2

Owner: Ser. OP COO e Process Mng Innovation – Contributor: Ser. Controlli, Conf. e Operations

Ril	Problema	Descrizione Gap	Fatti	Soluzione	Rilascio	Scadenza
A	Ritardato o mancato invio del documento di adesione al servizio FEA al Centro Documentale	Gli accertamenti hanno riguardato quei clienti per i quali le Filiali/Centri Specialistici non hanno trasmesso al Centro Documentale il documento di adesione al Servizio di FEA tramite procedura PARDO: • documenti "sospesi" (n. 9.671 al 30/04/18, su un totale di 1.360.697 prodotti). L'analisi sui suddetti documenti ha rilevato sospesi datati (il 60% originato ante 2018) e giustificativi per la sospensione in gran parte vaghi, assenti o che confermano la mancata firma del cliente; • documenti "annullati" (n. 16.839 al 30/04/18). Per questi è stato verificato su un campione di 30 unità che fosse stata inibita l'operatività con firma grafometrica o in caso contrario non vi fossero altri documenti Pardo collegati. Il test è fallito per tutti i casi analizzati. Sospendere o annullare la pratica PARDO non esclude l'operatività con firma grafometrica del cliente e, al contempo, non consente l'effettuazione dei controlli da parte del Centro Documentale (presenza firma e completezza della documentazione di adesione). Come rappresentato nel gap precedente anche questa condizione espone al rischio di disconoscimento di operazioni sottoscritte grafometricamente da un cliente e al rischio di non conformità per il trattamento non autorizzato di dati biometrici.	I documenti di adesione post 20/12/2015 vengono accentrati presso il centro documentale; per tali documenti è stata riscontrata la casistica di pratiche il cui conferimento risulta sospeso o annullato (complessivamente circa 29,5K a luglio 2018) a fronte di motivazioni in gran parte vaghe, assenti o che confermano la mancanza di firma; tali condizioni tuttavia non inibiscono l'operatività con firma grafometrica da parte del cliente.	Soluzione TARGET: ▫ Creare una nuova Working Situation di Annullamento Servizio FEA in modo da rendere automatici i controlli e gli adempimenti previsti a carico del titolare nella soluzione TATTICA ▫ Inibire la possibilità di annullare i record PARDO generato a fronte dell'Adesione al Servizio se non tramite WS di Annullamento Servizio FEA. BR di riferimento n. 81078 da pianificare e approvare Soluzione TATTICA: ▫ Consentire l'annullamento del PARDO solo al titolare di filiale che prima di annullare il documento in PARDO deve verifica che: ▫ non siano state fatte operazioni con FEA dalla data di Adesione; ▫ sia stato estinto il Servizio FEA Costi sostenuti con BR 79180 già completato. ▫ Pubblicato documento normativo di riferimento 1030D1748	30/06/2019 10/12/2018	30/06/2019

GAP 3

Owner: COG Ser. Assisted Banking– Contributor: -

Ril	Problema	Descrizione Gap	Fatti	Soluzione	Rilascio	Scadenza
A	Assenza di controlli sul formato del documento digitale	Allo scopo di garantire *«l'assenza di qualunque elemento nell'oggetto della sottoscrizione atto a modificarne gli atti, fatti o dati nello* stesso *rappresentati»,* la soluzione implementata dalla Banca prevede l'adozione di un formato standard internazionale (ISO 19005-1:2005, PDF/A) per i documenti a Firma Grafometrica. Tuttavia, l'assenza di controlli sul formato dei documenti, in ingresso al sistema di acquisizione delle firma cliente, nonché in uscita dallo stesso, non consente di garantire il rispetto dello standard previsto e quindi dei requisiti di legge. Nel corso delle verifiche è stato infatti rilevato come tale carenza abbia consentito la sottoscrizione di documenti, ab origine non conformi al formato PDF/A, che a oggi risultano illeggibili e pertanto privi di qualsiasi validità.	Con riferimento alla sottoscrizione di operazioni su Fondi Anima: - in data 12/06 sono stati rilasciati in produzione 5 modelli non conformi che hanno determinato l'archiviazione di 165 documenti illeggibili su un totale di 429 sottoscritti. - in data 28/06 sono stati rilasciati in produzione 2 modelli non conformi che hanno determinato l'archiviazione di 18 documenti illeggibili su un totale di 41 sottoscritti.	Soluzione TARGET: ▫ Blocco della pubblicazione template ▫ Verifica Istruzioni, Processo per la pubblicazione informatica dei template ▫ POC tool per la verifica correttezza di template e doc prodotti PDF/A su 350K ▫ Introdurre controlli automatici preventivi sui template ▫ Eseguire un test di correttezza dei template esistenti ▫ Introdurre un controllo app. pre invio di un documento prodotto PDF/A alla firma Soluzione TATTICA: ▫ Pubblicato documento normativo D791 Banca	31/12/2018 31/12/2018 31/01/2019 31/01/2019 31/01/2019 31/01/2019	30/04/2019

GAP 4

Owner: COG Ser. Sistemi Tecnologici - Contributor: Ser. Assisted Banking

Ril	Problema	Descrizione Gap	Fatti	Soluzione	Rilascio	Scadenza
A	Mancato rispetto dei presidi minimi di sicurezza logica nella gestione dell'archivio documentale della Banca, IBM Content Manager (CM)	Nella gestione dell'archivio documentale della Banca (IBM Content Manager) non sono rispettati i presidi minimi di sicurezza logica, sia in termini di gestione delle utenze che di tracciatura delle relative attività svolte. Non è pertanto possibile garantire la riservatezza e l'integrità dei documenti archiviati. Gli strumenti di amministrazione e accesso ai contenuti del Content Manager non sono integrati con le componenti infrastrutturali del controllo accessi, inoltre le prassi agite per la gestione delle utenze (personali e applicative) sono risultate difformi alle policy aziendali in materia. Si evidenziano a tal proposito casi di accesso con utenze applicative e l'utilizzo condiviso tra più persone di un unico utente con privilegi di amministratore. Infine, l'assenza di un log rende impossibile ricostruire a posteriori le attività svolte dai singoli utenti.	-	▫ Riconduzione utenze tecniche a LDAP ▫ Riconduzione utenze applicative a LDAP ▫ Ricondurre l'unica utenza Amministrativa esistente a LDAP ▫ Bloccare l'accesso diretto ai contenuti via applicazione web ▫ Attivazione della tracciatura degli accessi e delle attività di amministrazione ▫ Riattivare utenze per il Presidio Outsourcing ▫ Ri-abilitare utenze Presidio Outsourcing:	31/01/2019 28/02/2019 31/01/2019 31/12/2018 31/12/2018 28/02/2019 Dal 14/01/2018	28/02/2019

COPIA DI LAVORO

GAP 5

Owner: COG Ser. Credito – Contributor: -

Ril	Problema	Descrizione Gap	Fatti	Soluzione	Rilascio	Scadenza
A	Accesso diretto ai dati eludendo i presidi di controllo definiti	È stato accertato l'utilizzo dell'applicativo "Gestione Tabellare" per condurre attività di accesso diretto in modifica ai dati operativi, eludendo tutti i presidi di controllo ad oggi implementati per garantire il rispetto delle policy di sicurezza logica di Gruppo. Lo strumento in argomento ha peraltro evidenziato evidenti limiti negli aspetti di sicurezza logica tra i quali: l'assenza di meccanismi automatici di attribuzione e/o revoca delle abilitazioni che tengano conto, ad esempio, dell'effettiva assegnazione delle risorse alle strutture aziendali; l'assenza di un log auditabile; l'impossibilità di intercettare gli accessi ai dati attraverso gli strumenti preposti al monitoraggio. Tenuto conto dell'ampia diffusione nell'utilizzo dello strumento all'interno del Consorzio, nonché della rilevanza dell'informazione relativa agli accessi in modifica anche ai fini della corretta valutazione del rischio informatico, è stata da subito avviata una specifica attività finalizzata a ricondurre l'accesso diretto ai dati nell'ambito delle corrette Policy di Gruppo.	-	▫ Disabilitare accesso a Gestione Tabellare e ricondurre la gestione a GADIS ▫ Oscurare Gestione Tabellare dall'anagrafica delle applicazioni COG	31/12/2018 31/12/2018	31/01/2019

COPIA NON CONTROLLATA DOC-036

GAP 6

Owner: COG Ser. Assisted Banking– Contributor: -

Ril	Problema	Descrizione Gap	Fatti	Soluzione	Rilascio	Scadenza
M	Disallineamento tra Log Unico e contenuto degli archivi documentali	Le verifiche a campione condotte sul perimetro delle operazioni di sportello hanno evidenziato casi di operazioni sottoscritte grafometricamente a fronte delle quali non risultano prodotte e quindi archiviate le relative distinte elettroniche	-	▫ Spostare al termine dell'operazione la scrittura del log e registrare le eccezioni ▫ Risolvere il bug che ha generato 184 disallineamenti tra Log Unico e contenuto degli archivi documentali per operazioni di cambio a/b grafometriche allo sportello: le operazioni sono andate in cartaceo	31/01/2019 26/11/2018	31/01/2019*

COPIA NON VALIDA

* Concordata con Audit post formalizzazione

GAP 7

Owner: Ser. Cash Mng, ATM e Logistica – Contributor: -

Ril	Problema	Descrizione Gap	Fatti	Soluzione	Rilascio	Scadenza
M	Sistema di Conservazione Sostitutiva – Accountability non garantita	Non risultano garantite l'accountability e la ricostruibilità delle operazioni effettuate tramite Portale Documenti*. Il sistema di loggatura, benché in grado di rilevare l'utenza che ha effettuato l'accesso, non tiene traccia dei documenti acceduti né delle operazioni effettuate (visualizzazione e/o download). (*) Portale Documenti: applicazione web di In.Te.S.A. s.p.a messa a disposizione di BMPS per la consultazione on line dei documenti in Conservazione Sostitutiva - https://mps.tdocgold.intesa.it/	Il sistema di tracciatura dello strumento per l'accesso ai documenti, «Portale Documenti», non è in grado di rilevare né cosa è stato acceduto né le operazioni effettuate (interrogazione/download).	Concordare con il fornitore una gestione degli accessi con loggatura coerente con le richieste emerse in sede di Audit	31/05/2019	31/05/2019

GAP 8

Owner: COG Ser. Assisted Banking– Contributor: -

Ril	Problema	Descrizione Gap	Fatti	Soluzione	Rilascio	Scadenza
M	Assenza controlli su l'integrità dei documenti inoltrati in Conservazione Sostitutiva (CS)	E' stata rilevata l'assenza di un controllo atto a garantire che il documento elettronico sottoscritto grafometricamente del cliente non abbia subito modifiche prima dell'apposizione della firma digitale della Banca e che quindi non vengano archiviati in Conservazione Sostitutiva documenti alterati e pertanto non opponibili in giudizio	-	▫ Sviluppo di una funzione che controlli: Il documento ha un formato PDF/A; la firma è valida	31/03/2019	30/04/2019

COPIA CONTROLLATA DOC-036

GAP 9

Owner: Ser. OP COO e Process Mng Innovation – Contributor: Ser. Assisted Banking (COG)

Ril	Problema	Descrizione Gap	Fatti	Soluzione	Rilascio	Scadenza
B	Assenza di una relazione tecnica aggiornata di cui al Provvedimento del Garante in tema di biometria	Il «Provvedimento generale prescrittivo in tema di biometria» n. 513 del 12/11/2014 in relazione alla sottoscrizione di documenti informatici, punto 4.4. lettera k), richiede la predisposizione e l'aggiornamento nel continuo di «...una relazione che descriva gli aspetti tecnici e organizzativi delle misure messe in atto dal titolare, fornendo altresì la valutazione della necessità e della proporzionalità del trattamento biometrico rispetto alle finalità...». Tale relazione non è necessaria qualora la Banca sia dotata della certificazione SGSI secondo la norma tecnica ISO/IEC 27001 «...potendo utilizzare la documentazione prodotta nell'ambito della certificazione, integrandola con la valutazione della necessità e della proporzionalità del trattamento biometrico». Le verifiche condotte rilevano, tuttavia, l'assenza di una relazione tecnica aggiornata sul sistema attualmente in esercizio pur non essendo la Banca in possesso della certificazione SGSI secondo la norma ISO/IEC 27001.	Assenza di una relazione tecnica aggiornata	▫ Revisionare la relazione tecnica con il supporto del legale di Euronovate e delle funzioni Compliance e Legale Banca. La relazione deve essere disponibile a richiesta del Garante Privacy.	31/01/2019	31/01/2019

COPIA DI LAVORO

GAP 10

Owner: COG Ser. Assisted Banking– Contributor: -

Ril	Problema	Descrizione Gap	Fatti	Soluzione	Rilascio	Scadenza
B	Annullamento operazioni di sportello: inoltro in Conservazione Sostitutiva di documenti non validi	La procedura informatica di annullamento delle operazioni di versamento in conto corrente prevede che vengano clonati tutti i documenti prodotti in corrispondenza dell'operazione originaria, compreso quello contenente i dati biometrici criptati (blocco grafometrico) e che sui cloni venga quindi apposta una marcatura di annullamento. Il documento clonato, contenente i dati biometrici, viene poi inoltrato in Conservazione Sostitutiva		▫ Eliminare il trasferimento del documento con Watermark «Annullato» in CS – analisi in corso (end 4/01)	31/01/2019	31/01/2019

COPIA NON VALIDA

GAP 11

Owner: COG Ser. Assisted Banking– Contributor: -

Ril	Problema	Descrizione Gap	Fatti	Soluzione	Rilascio	Scadenza
B	Archiviazione dei documenti contenenti i dati biometrici dei clienti all'interno del sistema informativo della Banca	Le verifiche condotte sulle cartelle di rete in cui transitano i documenti elettronici hanno evidenziato la presenza di utenze personali con privilegi di accesso in modifica, rimosse nel corso della revisione su segnalazione della team di audit. Si rileva tuttavia l'impropria archiviazione nelle suddette cartelle dei documenti contenenti i dati biometrici criptati dei clienti; tale circostanza introduce un rischio di accesso non autorizzato ai documenti archiviati al di fuori della Conservazione a Norma	-	▫ Limitare l'accesso alle Cartelle NAS : l'accesso è oggi disponibile per solo a 3 persone, in sola lettura ▫ Ricondurre l'accesso alla gestione CyberArk e gestire la profilazione come Amministratore di sistema ▫ Eliminare dal Backup NAS tutti i documenti che contengono un blocchetto di firma grafometrica	05/10/2018 31/12/2018 15/12/2018	31/12/2018

COPIA CONFORME ALL'ORIGINALE

GAP 12

Owner: COG Ser. Sistemi Tecnologici – Contributor: -

Ril	Problema	Descrizione Gap	Fatti	Soluzione	Rilascio	Scadenza
B	Inaffidabilità delle informazioni relative all'ubicazione delle tavolette grafometriche	Il dato sull'ubicazione delle 13.725 tavolette grafometriche in esercizio al 26/06/2018 contenuto nello strumento di enterprise asset management «Maximo», non è risultato attendibile. Dalle verifiche effettuate su un campione di n. 30 filiali, è infatti emersa la presenza di tavolette ancora in carico a filiali chiuse/oggetto di spin-off (76% del campione), o tavolette collegate da filiali in numero superiore a quello effettivamente assegnato (13% del campione).		▫ Aggiornare la collocazione su «Maximo» delle tavolette grafometriche sulla base delle evidenze rilevabili in automatico	3/01/2019	31/01/2019

COPIA NON CONTROLLATA