

DRAFT



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

Data Quality LGD

Rapporto n. 082/2018

Siena,

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

La presente revisione è stata indirizzata a valutare i presidi messi in atto a garanzia della qualità dei dati nell'ambito del sistema di alimentazione della base dati di calcolo del parametro «Loss Given Default» a partire dai sistemi del Contenzioso. L'attività è stata in prevalenza focalizzata su Banca MPS in quanto preponderante nell'alimentazione della base dati.

In tale contesto sono stati esaminati i seguenti ambiti:

- *l'architettura del sistema di alimentazione con particolare focus sugli aspetti di sicurezza logica e di qualità dei dati dipendenti dal sistema (in termini di riservatezza, disponibilità, ripristinabilità, tracciabilità e integrità);*
- *l'efficacia dei controlli di Data Quality a presidio delle singole fasi del sistema di alimentazione (in termini di accuratezza, completezza, coerenza e tempestività).*

La revisione ha prevalentemente interessato le seguenti Strutture:

- *«Servizio Credit Risk Models», in quanto responsabile della stima del parametro LGD;*
- *«Servizio Applicazioni Bilancio e Rischi» del Consorzio, in quanto responsabile della base dati di calcolo del parametro LGD;*
- *«Servizio Credito» del Consorzio, in quanto Servizio alimentante della base dati di calcolo.*

Nel corso delle attività è stato coinvolto anche il «Servizio Sicurezza Informatica e BCM» del Consorzio, in qualità di gestore delle politiche di sicurezza logica.

La revisione è stata svolta mediante:

- *colloqui con i referenti delle Strutture interessate e osservazione delle prassi agite;*
- *analisi documentale (normativa aziendale, documentazione acquisita);*
- *analisi dell'infrastruttura informatica implementata e controlli di sicurezza logica;*
- *analisi dei principali controlli di data quality implementati;*
- *verifiche di data quality dirette sugli archivi informatici oggetto di esame.*

In ottemperanza alle disposizioni di Vigilanza ed in conformità agli Standard di Audit del Gruppo, i risultati della revisione con l'evidenza delle principali criticità rilevate, dei conseguenti ambiti di miglioramento e dei relativi interventi correttivi sono stati comunicati alle competenti Funzioni.

Overview

ANAGRAFICA INTERVENTO

Intervento: Data Quality LGD

Obbligatorietà: SI

Unità auditate: Servizio Credit Risk Models; COG: Servizio Applicazioni Bilancio e Rischi, Servizio Credito, Servizio Sicurezza Informatica e BCM

Tipologia di intervento: Settoriale – in loco

Data open meeting: 09/10/2018

Data exit meeting: 17/12/2018, 18/12/2018, 21/12/2018

Responsabile Audit Team: Silvia de Mauro

Audit Team:

» Duccio Fabbri

ESITO INTERVENTO

GRADE COMPLESSIVO INTERVENTO

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

Il Grade complessivo dell'intervento, come previsto dagli Standard di audit, è in funzione della numerosità e rilevanza (bassa-media-alta), oltre che dell'impatto in termini di rischio, dei gap aperti a seguito dell'intervento stesso, come riassunto nella tabella seguente:

Grade	n. complessivo Gap	con n. Gap Alti
Rating 1 (verde)	< 5	0
Rating 2 (giallo)	≥ 5	0
Rating 3 (arancione)	qualsiasi	da 1 a 2
Rating 4 (rosso)	qualsiasi	≥ 3

In sede di attribuzione finale del grade vi è sempre la discrezionalità da parte del CAE di rivedere il giudizio finale sia in termini peggiorativi che migliorativi, motivando opportunamente tale scelta

FATTORE CAUSALE	DISTRIBUZIONE DEI GAP PER RILEVANZA		
	ALTA	MEDIA	BASSA
Risorse			
Processi		1	
Sistemi		1	
Totale		2	

ORGANI DESTINATARI DEL PRESENTE AUDIT

LEGAL ENTITY	ORGANO DESTINATARIO
	Consorzio Operativo Gruppo MPS* Presidente CDA
	Consorzio Operativo Gruppo MPS* Amministratore Delegato
	Consorzio Operativo Gruppo MPS* Direttore Generale
	Consorzio Operativo Gruppo MPS* Collegio Sindacale
	Consorzio Operativo Gruppo MPS* Referente Internal Audit

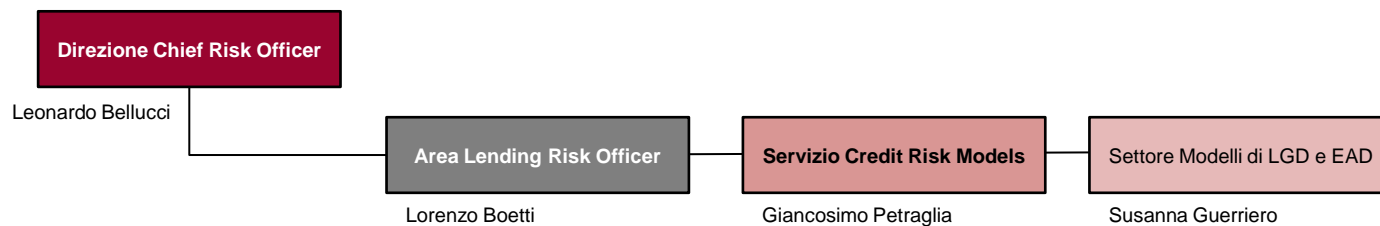
PRECEDENTI INTERVENTI DI REVISIONE (SE ESISTENTI)

AMBITO INTERVENTO	PERIODO DELLA VERIFICA	N. RAPPORTO	GRADE INTERVENTO
-	-	-	-

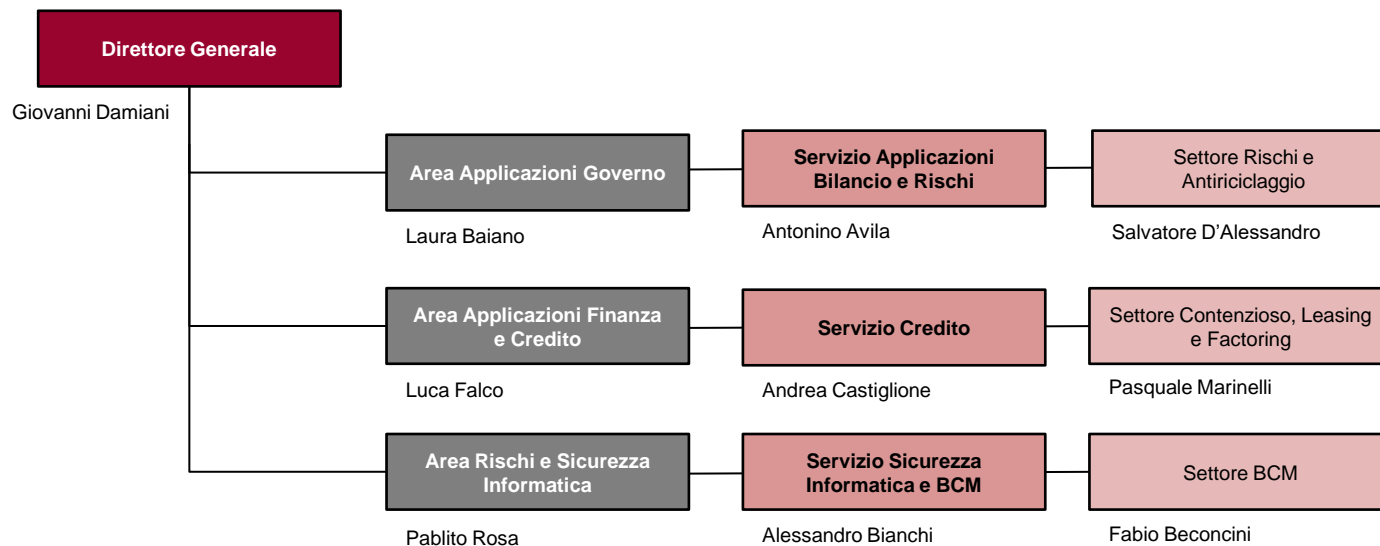


Organigramma Strutture Auditate

BMPS - Capogruppo bancaria



Consorzio Operativo Gruppo Montepaschi



Executive Summary (1/2)

SICUREZZA LOGICA DEL SISTEMA DI ALIMENTAZIONE

Idonee misure di sicurezza logica. Documentazione tecnica non sempre esaustiva

A partire da luglio 2018 il sistema di alimentazione della base dati di calcolo LGD, storicamente alimentata tramite flussi diretti dai sistemi del Contenzioso, è stato ricondotto a uno standard che prevede la centralità del *data warehouse* aziendale.

L'impianto del sistema è stato validato dalla Funzione di Business in stretta collaborazione con le Strutture tecniche del Consorzio.

L'implementazione delle nuove procedure ha permesso di ottimizzare le logiche di alimentazione e ha, altresì, consentito di riorganizzare la documentazione funzionale e tecnica delle stesse. Tale documentazione è risultata completa di tutte le informazioni necessarie a ricostruire il percorso di derivazione e trasformazione dei dati dal *data warehouse* aziendale alla base dati di calcolo LGD.

E' risultata invece non esaustiva la documentazione tecnica delle procedure di alimentazione del *data warehouse* aziendale a partire dai sistemi del Contenzioso (cfr. gap 1).

A presidio del sistema di alimentazione della base dati di calcolo LGD è stata accertata la presenza di un efficace sistema di monitoraggio e di idonee misure di sicurezza logica, finalizzate a garantire la *riservatezza*, l'*integrità* dei flussi informativi nonché la *ripristinabilità* e la *disponibilità* dei dati registrati negli archivi.

Relativamente all'*integrità* delle informazioni utilizzate per il calcolo del parametro, benché l'analisi degli accessi alla base di calcolo abbia evidenziato la presenza di 3 utenze nominative con privilegi di accesso in modifica, nessuna di queste risulta aver condotto operatività che comportasse l'alterazione dei dati archiviati^(*). La criticità, rappresentata dalla scrivente Funzione in sede di *exit meeting*, è stata sanata prima della pubblicazione del presente rapporto.

Inoltre, le prassi operative in uso, nel caso di valorizzazioni anomale dei dati non rettificabili tramite gli applicativi a supporto, prevedono che la Funzione di Business richieda la correzione diretta nei sistemi del Contenzioso, nuove estrazioni e conseguentemente l'esecuzione di un nuovo caricamento. Le verifiche hanno consentito di appurare che tali interventi sono eseguiti dal Consorzio nel rispetto della normativa interna^(**).

Sul *data warehouse* aziendale non sono, invece, risultate definite utenze nominative con privilegi tali da consentire la modifica delle informazioni registrate. E' stata, tuttavia, rilevata l'impossibilità di monitorare le attività svolte direttamente sui dati, sebbene, a garanzia della *tracciabilità*, il log degli accessi diretti fosse già quotidianamente messo in sicurezza. Su indicazione della scrivente Funzione, il Consorzio, ha provveduto, in corso di revisione, a rendere disponibile un'indagine (su *Sid Navigator*) dedicata al monitoraggio degli accessi diretti al sistema «Teradata», piattaforma che ospita il *data warehouse* aziendale, a prescindere dallo strumento utilizzato.

Le verifiche condotte hanno, infine, rilevato un vuoto normativo in relazione al processo di gestione del ciclo di vita delle utenze per l'accesso al sistema «Teradata». Tale carenza è risultata solo parzialmente compensata dalle prassi operative in uso che sono risultate, peraltro, incomplete e basate su un documento normativo^(***) non più in vigore. L'assenza di un processo formale e/o prassi consolidate circa la gestione delle abilitazioni sul sistema non garantisce, altresì, una corretta e costante attività di *review* delle utenze nel rispetto del principio del *least privilege* (cfr. gap 2).

^(*) periodo osservato: giugno-settembre 2018.

^(**) D00139 – *Processo Change Management*.

^(***) M 00004 - *Manuale: Procedura di gestione abilitazioni particolari* del Consorzio.



Executive Summary (2/2)

EFFICACIA DEI PRESIDI DI CONTROLLO

Adeguati presidi di controllo a garanzia della qualità dei dati.

Il Settore Modelli di LGD e EAD (*Business Data Steward* per l'output rilevante LGD) ha espresso in maniera esaustiva i requisiti di Data Quality da applicare alla base dati di calcolo del parametro, esplicitando i controlli a copertura delle dimensioni della qualità intrinseca dei dati in termini di: *accuratezza, completezza, integrità, tempestività, coerenza e correttezza*.

I controlli sono stati implementati dal Settore Rischi e Antiriciclaggio del Consorzio, *Technical Data Steward* per l'output rilevante LGD, e successivamente validati dalla Funzione di Business.

L'esito dei controlli *IrionDQ*, piattaforma utilizzata per le verifiche sui dati, è nel continuo monitoraggio dalla Funzione di Business che analizza le segnalazioni indirizzandole verso le strutture competenti per la risoluzione, evidenziando così un adeguato presidio sulla materia.

Tra le attività indirizzate a garantire l'integrità e la qualità dei dati rileva anche l'applicativo *Swiffer*, finalizzato a eseguire controlli tecnici massivi su specifiche tipologie di dati presenti nel *data warehouse* aziendale. Al fine di rendere tutti i Settoriali del Consorzio autonomi nella gestione delle segnalazioni di propria competenza, a partire da settembre 2017 è stato reso disponibile uno specifico canale informativo (indagine su *Sid Navigator*). Questo canale, tuttavia, non è stato adeguatamente comunicato a tutte le Funzioni tecniche interessate, limitando, di fatto, il necessario monitoraggio degli esiti prodotti dai controlli. Su richiesta del team di audit, a novembre 2018 l'informativa è stata fornita diffusamente a tutte le Strutture del Consorzio affinché potessero avviare opportune attività di analisi e le eventuali azioni di *remediation*.

I test eseguiti direttamente sulle basi dati analizzate (*data warehouse* aziendale e base dati di calcolo LGD), finalizzati a verificare la qualità dei dati in termini di *accuratezza* e *coerenza*, non hanno evidenziato particolari anomalie. Gli esiti, condivisi con le Funzioni interessate, hanno confermato la coerenza tra quanto archiviato nel *data warehouse* aziendale rispetto ai sistemi di origine del Contenzioso, non ravvisando, pertanto, introduzioni di alterazioni delle informazioni nella procedura di alimentazione. In relazione all'attuale modalità di stima del parametro LGD, non sono, infine, state evidenziate criticità o particolari casistiche da approfondire.



Audit findings

N.	PROCESSO	GAP	RILEVANZA (A/M/B)	RISCHIO	FATTORE CAUSALE	RACCOMANDAZIONE	STRUTTURA OWNER	SCADENZA (GG/MM/AA)	CODICE OB SSM
1	Gestione IT qualità dei dati	<p>Documentazione sulle procedure di alimentazione del data warehouse aziendale a partire dai Sistemi del Contenzioso non esaustiva</p> <p>Al fine di consentire la verifica sulla qualità dei dati e identificare le operazioni svolte sugli stessi, è necessario che le procedure di estrazione, trasformazione, controllo, caricamento e sfruttamento dei dati siano adeguatamente documentate e siano mantenute nel continuo aderenti ai sistemi informativi di produzione.</p> <p>In relazione al sistema di alimentazione del data warehouse aziendale a partire dai sistemi del Contenzioso, la documentazione resa disponibile non è esaustiva di tutte le informazioni necessarie a ricostruire il percorso di derivazione e trasformazione dei dati dal sistema origine al sistema destinazione.</p>	M	Operativo	Sistemi	<p>Integrare la documentazione esistente</p> <p>Aggiornare ed integrare la documentazione inerente il sistema di alimentazione del data warehouse aziendale a partire dai Sistemi del Contenzioso.</p>	<p>COG</p> <p>Servizio Credito</p>	<p>Studio di fattibilità</p> <p>31/01/2019</p>	IG.7.12 BIS
2	Gestione dei processi operativi di sicurezza logica	<p>Processo di gestione delle abilitazioni di accesso al sistema Teradata non definito</p> <p>Il processo di gestione delle utenze per l'accesso al sistema Teradata non risulta normato. Tale carenza è solo parzialmente compensata dalle prassi operative che risultano incomplete (*). Relativamente ai nuovi censimenti ad esempio, le prassi in uso prevedono che la richiesta sia inoltrata dal responsabile della risorsa alla Funzione Gestione Utenti. Non risulta, tuttavia, completamente delineato l'iter approvativo: nel caso di utente Banca l'abilitazione viene concessa previa autorizzazione della Funzione Organizzazione mentre per gli utenti del Consorzio non è ancora stata individuata una Funzione di riferimento.</p> <p>(*) Le prassi in uso si attengono ancora a quanto era stabilito nel «M 00004 - Manuale: Procedura di gestione abilitazioni particolari» non più in vigore.</p>	M	Operativo	Processi	<p>Formalizzare il processo di gestione delle abilitazioni al sistema Teradata</p> <p>Formalizzare il processo di gestione delle abilitazioni al sistema Teradata in modo da coprire l'intero ciclo di vita delle utenze e definire una attività di review periodica delle abilitazioni in essere.</p>	<p>COG</p> <p>Servizio Sicurezza Informatica e BCM</p>	<p>30/04/2019</p>	N.A



Overview obiettivi di controllo SSM

Pillar	Processo	Numero Obiettivi di controllo
Internal Governance & SCI	Gestione IT qualità dei dati	1

A	B	C	D	NA
-	1	-	-	-

Codice	Obiettivi di controllo	Percentuale di completamento	Rating	GAP Associati
IG.7.1 2 BIS	Verificare che la governance e l'infrastruttura supportino un livello adeguato di qualità dei dati Verificare che i dati finanziari e di rischio soddisfino i requisiti relativi all'accuratezza, all'accessibilità, all'integrità, alla completezza e alla tempestività.	75%	B	Gap n. 1 MEDIO

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



Agenda

- 1 Contesto di riferimento
 - 2 Attività svolta
- Allegati*



1 Contesto di riferimento

➤ Ruoli e Responsabilità

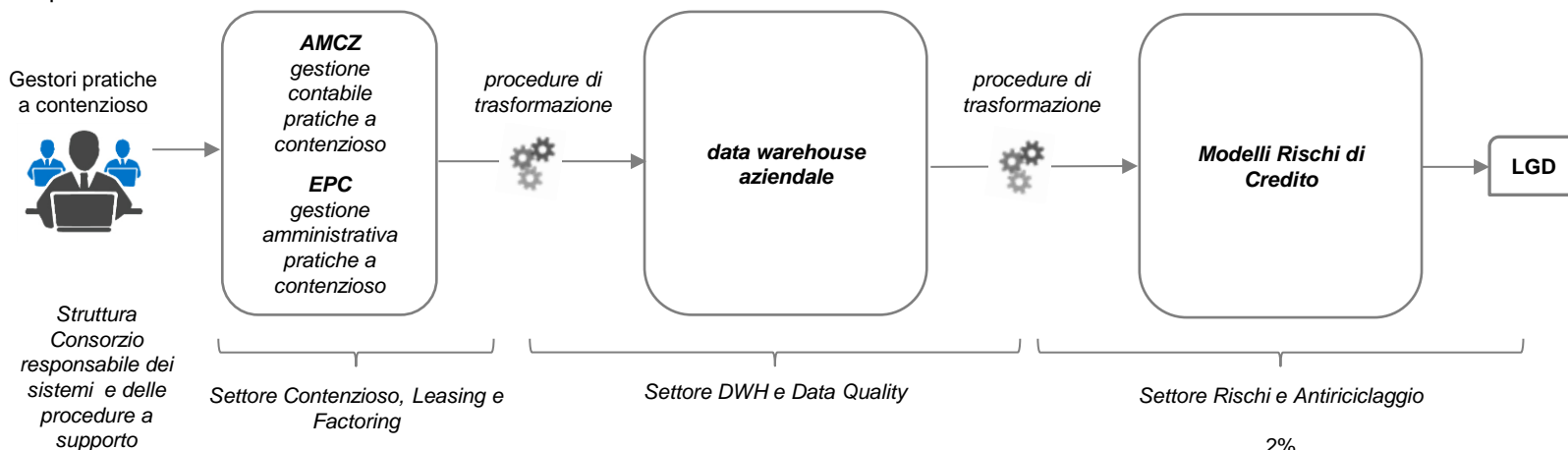
Il parametro *Loss Given Default* (LGD) è uno degli *Output Rilevanti* identificati e gestiti in ambito Data Governance^(*); in tale contesto per il parametro LGD sono identificati i seguenti ruoli:

- *Data Owner*: Area Lending Risk Officer della Capogruppo;
- *Business Data Steward*: Settore Modelli di LGD e EAD della Capogruppo;
- *Technical Data Steward*: Settore Rischi e Antiriciclaggio del Consorzio.

➤ Schema logico del sistema di alimentazione

Il sistema di alimentazione del modello di calcolo del parametro LGD si basa sulle seguenti 2 macro fasi:

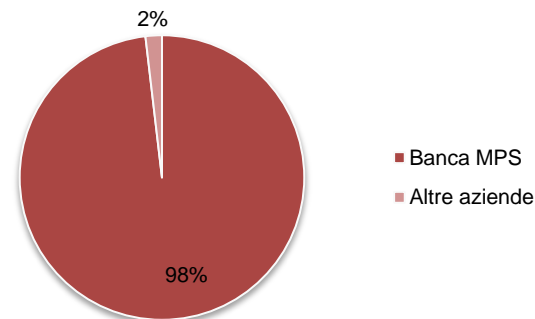
- i dati operativi archiviati nei sistemi del Contenzioso (AMCZ/EPC) sono riversati nel *data warehouse*;
- le informazioni necessarie al calcolo del parametro LGD vengono estratte, secondo la logica dettata dalla Funzione di Business, direttamente dalle repliche presenti nel *data warehouse* aziendale dei dati del Contenzioso.



➤ Aziende coinvolte

La base dati di calcolo del parametro LGD viene alimentata mensilmente a partire dai dati dei Sistemi del Contenzioso delle Banche MPS, WIDIBA, MPS Leasing & Factoring e MPS Capital Services.

Banca MPS fornisce il contributo preponderante, in termini numerici, al sistema di alimentazione.



Ripartizione flussi alimentanti per Azienda
periodo di osservazione : marzo - dicembre 2018

^(*) Processo di governo finalizzato a presidiare il patrimonio informativo rilevante della Banca, identificato nelle informazioni che consentono attività di indirizzo strategico interno e nelle informative verso l'esterno – *Output Rilevante* - e garantire uniformità di informazioni anche tra funzioni differenti.



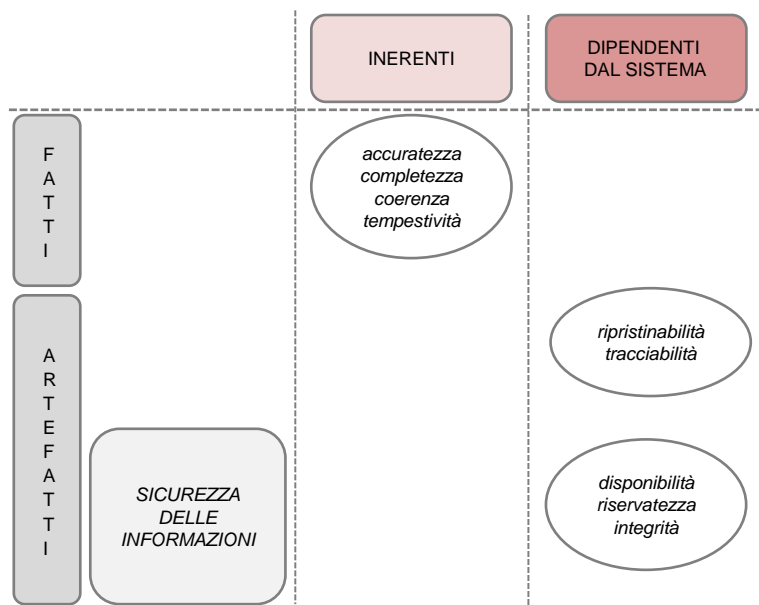
1 Contesto di riferimento – Dimensioni della qualità dei dati

La qualità dei dati si configura come un concetto *multidimensionale*: la sua definizione passa necessariamente dalla determinazione delle *caratteristiche*, o *dimensioni*, di cui essa si compone.

Lo standard *ISO/IEC 25012 «Modello di qualità dei dati»* definisce un modello generale della qualità dei dati che classifica gli attributi di qualità in base a due punti di vista: (i) *inerente* e (ii) *dipendente dal sistema*. Il primo è relativo al valore intrinseco del dato a prescindere dal sistema che lo elabora, mentre il secondo è collegato alle caratteristiche del sistema in cui i dati sono utilizzati indipendentemente dal loro contenuto.

La scala di priorità delle caratteristiche della qualità non è stabilita a livello di standard ma deve essere valutata in base al contesto di riferimento oggetto di indagine.

Caratteristiche della qualità



Il sistema di alimentazione della base dati di calcolo LGD è stato analizzato secondo le seguenti dimensioni della qualità^(*):

Caratteristiche inerenti

- accuratezza: grado in cui i dati hanno attributi che rappresentano correttamente il valore reale degli attributi previsti di un concetto o evento.
- completezza: grado con cui i dati associati con un'entità hanno valore per tutti gli attributi attesi e le istanze di entità correlate.
- coerenza: grado con cui i dati hanno attributi che sono privi di contraddizioni e sono coerenti con altri dati.
- tempestività (o attualità): grado in cui i dati hanno attributi che sono della giusta età.

Caratteristiche dipendenti dal sistema

- ripristinabilità: grado in cui i dati hanno attributi che consentono di preservare un livello specificato di operazioni e qualità, perfino in caso di guasto.
- disponibilità: grado in cui i dati hanno attributi che ne consentono il richiamo da parte di utenti autorizzati e/o applicazioni.
- riservatezza: grado in cui i dati hanno attributi che assicurano la loro accessibilità e interpretabilità solo da parte di utenti autorizzati. La *riservatezza* è un aspetto della sicurezza delle informazioni, insieme a *disponibilità* e *integrità*, come definito nella norma *ISO/IEC 13335*^(**).
- tracciabilità: grado in cui i dati hanno attributi che forniscono una registrazione degli accessi ai dati e a tutte le modifiche effettuate ai dati.
- integrità: l'informazione deve essere trattata in modo da essere protetta da manomissioni e modifiche non autorizzate^(***).

^(*) le definizioni delle caratteristiche sono tratte da *UNI CEI ISO/IEC 25012 «Modello di qualità dei dati»*

^(**) *ISO/IEC 13335 «Information technology – Security techniques – Management of information and communications technology security»*

^(***) *D01815 – «Direttiva di Gruppo in materia di Definizione Strategica, Politiche e Misure di Sicurezza Logica»*

2 Attività svolta: Sicurezza Logica del Sistema di Alimentazione (1 di 8)

GESTIONE IT QUALITÀ DEI DATI

SICUREZZA LOGICA
SISTEMA DI
ALIMENTAZIONE

EFFICACIA DEI
PRESIDI DI
CONTROLLO

OBIETTIVO

Valutare l'architettura del sistema di alimentazione con particolare focus sugli aspetti di sicurezza logica e di qualità dei dati dipendenti dal sistema (in termini di *riservatezza, disponibilità, ripristinabilità e tracciabilità*).

PERIMETRO/ METODOLOGIA

Interviste, raccolta documentale, analisi delle evidenze, analisi dei dati, accesso diretto ai sistemi.

RISCHI IMPATTATI

55272 - Accessi non autorizzati ad applicazioni o dati sensibili
55622 - Indisponibilità dei sistemi
55656 – Perdita dell'integrità dei dati

Obiettivo di controllo: IG.7.12 BIS

VERIFICHE SVOLTE

Analisi dei requisiti funzionali e della documentazione tecnica a supporto del sistema di alimentazione della base dati di calcolo LGD.

ESITI

A partire da luglio 2018 il sistema di alimentazione della base dati di calcolo LGD, storicamente alimentata tramite flussi di scambio prodotti dal *Settore Contenzioso, Leasing e Factoring*, è stato ricondotto ad uno standard aziendale che prevede la centralità del *data warehouse* aziendale. In sintesi:

- i dati operativi archiviati nei sistemi del Contenzioso (AMCZ/EPC) sono riversati nel *data warehouse* aziendale e sono resi, pertanto, disponibili a tutti i possibili utilizzatori;
- le informazioni necessarie al calcolo del parametro LGD vengono estratte, secondo la logica dettata dalla Funzione di Business, direttamente dalle repliche dei dati del Contenzioso presenti nel *data warehouse* aziendale.

Questo cambio di approccio è basato su quanto specificato nel BR55282 - *Fonte Unica Dati (FUD) fase 2* - di cui il *Servizio Credit Risk Models* della Capogruppo è referente di Business. La nuova metodologia di alimentazione ha reso di fatto superflua, per le Banche MPS e WIDIBA, la generazione dei flussi di alimentazione diretta dai sistemi del Contenzioso: tali flussi saranno dismessi a partire da gennaio 2019 (cfr. RFC ordinaria C55579), mentre saranno ancora necessari per le Banche MPS Leasing & Factoring e MPS Capital Services, che continueranno ad alimentare la base dati di calcolo LGD con flussi diretti dai sistemi di origine.

L'implementazione delle nuove procedure, che si è basata su una attività di *reverse engineering* delle originali procedure di creazione dei flussi, ha permesso di ottimizzare le logiche di alimentazione e ha, altresì, consentito di riorganizzare la documentazione funzionale e tecnica delle stesse. Tale documentazione è risultata completa di tutte le informazioni necessarie a ricostruire il percorso di derivazione e trasformazione dei dati dal *data warehouse* aziendale alla base dati di calcolo LGD.

In fase di impianto del nuovo sistema, la Funzione di Business, in stretta collaborazione con il *Settore Contenzioso, Leasing e Factoring* e con il *Settore Rischi e Antiriciclaggio* del Consorzio, ha validato la nuova procedura eseguendo test comparativi tra le due modalità di alimentazione.

I test eseguiti non sono sempre stati registrati nello strumento standard di Consorzio (*ALM – Application Lifecycle Management*), ma sono risultati comunque ben documentati.



2 Attività svolta: Sicurezza Logica del Sistema di Alimentazione (2 di 8)

VERIFICHE SVOLTE

Analisi dei requisiti funzionali e della documentazione tecnica a supporto dell'alimentazione del *data warehouse* aziendale a partire dai Sistemi del Contenzioso.

ESITI

Le procedure di alimentazione del *data warehouse* aziendale a partire dai sistemi del Contenzioso ad oggi in produzione sono il risultato di numerose e stratificate implementazioni avvenute in un ampio arco temporale che si sono perfezionate grazie ad un considerevole numero di BR (a titolo esemplificativo ma non esaustivo: BR34560, BR40788, BR56208, BR55203, BR56641, BR44754, BR61174, BR61567).

Il *porting* dei dati su *data warehouse* aziendale rientra nelle attività ITxIT: non viene, pertanto, eseguita una formale accettazione delle implementazioni, tramite UAT, da parte delle Funzioni Business competenti per materia, ma la convalida avviene in base a test tecnici condotti congiuntamente dai settori *owner* dei sistemi di origine e destinazione dei dati, rispettivamente *Settore Contenzioso*, *Leasing e Factoring* e *Settore DWH e Data Quality*.

Il sistema di alimentazione è implementato tramite procedure informatiche che aggregano e trasformano i dati archiviati nei sistemi del Contenzioso secondo logiche utili a renderli maggiormente fruibili ai servizi utilizzatori. Quotidianamente il *data warehouse* viene alimentato con i dati del Contenzioso aggiornati al giorno lavorativo precedente.

Al fine di consentire la verifica sulla qualità dei dati e identificare le operazioni svolte sugli stessi, è necessario che tali procedure siano adeguatamente documentate e siano mantenute nel continuo aderenti ai sistemi informativi di produzione. Tuttavia, la documentazione tecnica fornita a descrizione delle procedure di estrazione dei dati è risultata non esaustiva, in quanto carente, per esempio, della descrizione di dettaglio delle logiche di trasformazione implementate, di una mappatura dei campi di destinazione con quelli di origine corredata da una descrizione dei tipi dato previsti per ogni campo (cfr. gap 1).

Una documentazione tecnica adeguatamente dettagliata, peraltro richiesta dal processo *Sviluppo e modifiche componenti software*, è indispensabile anche per rafforzare la *governance* dei *Technical Data Steward* sui dati di propria pertinenza.

2 Attività svolta: Sicurezza Logica del Sistema di Alimentazione (3 di 8)

GESTIONE IT QUALITÀ DEI DATI

SICUREZZA LOGICA
SISTEMA DI
ALIMENTAZIONE

EFFICACIA DEI
PRESIDI DI
CONTROLLO

VERIFICHE SVOLTE

Overview dell'architettura a supporto del sistema di alimentazione della base dati di calcolo LGD e individuazione dei principali flussi informativi e dei relativi canali di trasmissione.

Verifica del corretto monitoraggio delle procedure di alimentazione e analisi delle segnalazioni di anomalie.

La verifica è stata condotta tramite:

- interviste con i referenti IT delle singole fasi;
- analisi Ticket Remedy (periodo di osservazione luglio-ottobre 2018).

ESITI

Le interviste con le strutture auditate e l'analisi della documentazione tecnica fornita hanno consentito di ricostruire lo schema architetturale del sistema di alimentazione in essere per le Banche commerciali (cfr. Allegato 1).

Ogni fase che compone il sistema di alimentazione è implementata tramite applicazioni *batch* schedate quotidianamente.

I flussi di scambio tra i sistemi transitano attraverso cartelle di rete condivise, nello specifico:

- [\\AP000000012017\DWHP01_DWA_KZ](#) cartella in cui vengono spostati i flussi informativi generati dai Sistemi del Contenzioso prima di essere caricati nel *data warehouse* aziendale;
- [\\nassi1.local\IP0000CRRn05\IP0000CRR_EXT\fy\ext](#) cartella in cui vengono spostati i flussi informativi generati a partire dal *data warehouse* aziendale prima di essere caricati nella base dati di calcolo LGD.

Le verifiche condotte hanno permesso di constatare la presenza di un efficace sistema di monitoraggio a presidio del sistema di alimentazione della base dati di calcolo LGD.

Le singole fasi che costituiscono il sistema di alimentazione vengono, infatti, quotidianamente monitorate attraverso gli strumenti standard di controllo previsti dal Consorzio per le applicazioni *batch* (es. monitor S.A.R.A., *Sistema Automatico Registrazione Abends*).

Inoltre, in caso di errore, vengono aperti ticket Remedy verso la struttura *owner* competente per l'attività di risoluzione. Dall'analisi delle segnalazioni è emerso che, nel periodo di osservazione:

- la fase di produzione dei flussi informativi dai sistemi del Contenzioso non ha generato anomalie;
- la fase di caricamento nel *data warehouse* aziendale dei flussi informativi dai sistemi del Contenzioso si è conclusa in modo anomalo 8 volte;
- la fase di caricamento dei flussi informativi nella base dati di calcolo LGD si è conclusa in modo anomalo 33 volte.

Tutte le segnalazioni aperte sono state correttamente prese in carico.



2 Attività svolta: Sicurezza Logica del Sistema di Alimentazione (4 di 8)

VERIFICHE SVOLTE

Verifica sulla ripristinabilità dei dati: soluzione di Disaster Recovery e policy di *backup* dei sistemi coinvolti nell'alimentazione della base dati di calcolo LGD.

dimensioni: ripristinabilità, disponibilità

ESITI

Le verifiche condotte hanno confermato che le soluzioni tecnologiche adottate permettono di garantire la *ripristinabilità* e *disponibilità* dei dati, nello specifico:

Base dati di calcolo LGD (DB Oracle PD0000DWA):

- è sottoposta a *backup* giornaliero con *retention* pari a 5 versioni;
- è inclusa nella soluzione standard di Disaster Recovery del Consorzio con replica sincrona dei dati tra polo primario, CED di Firenze, e polo secondario, CED di Siena.

Data warehouse aziendale (sistema Teradata):

- in relazione agli ambiti applicativi coinvolti nel sistema di alimentazione, è previsto un *backup* giornaliero con salvataggio integrale delle tabelle movimentate nel giorno stesso;
- il sistema è incluso nella soluzione di Disaster Recovery con CED primario allocato nel polo di Firenze e CED secondario allocato nel polo di Siena; i 2 poli non sono allineati in sincrono ma il polo secondario, se pur sempre attivo, è alimentato in modo asincrono a partire dall'ultimo *backup* disponibile (cfr. rapporto n. 83_2018 «*Test di funzionalità del piano di Disaster Recovery*»). La soluzione di Disaster Recovery implementata per il sistema Teradata presenta, pertanto, un RPO^(*) compreso tra 0 e 24 ore. Ciò non costituisce un limite per il processo «*Gestione del rischio di credito*» che non è classificato tra i processi critici e/o sistemici^(**).

Cartelle di rete condivise:

- [\\nassi1.local\\P0000CRRn05\\P0000CRR_EXT\\fylext](#): la cartella è inclusa nella soluzione standard di Disaster Recovery del Consorzio (replica su polo secondario) e non è sottoposta a *backup* o archiviazioni. Tale scelta non rappresenta una criticità in quanto i flussi informativi sono sempre ricostruibili rilanciando la fase di estrazione dati dal *data warehouse* aziendale.
- [\\AP000000012017\\DWHFP01_DWA_KZ](#): la cartella non è replicata su polo secondario; è previsto un *backup* giornaliero su nastro con *retention* pari a 2 anni. Tale scelta non rappresenta una criticità in quanto i flussi informativi sono sempre ricostruibili rilanciando la fase di estrazione dati dai sistemi del Contenzioso.

^(*) Punto di Ripristino o Recovery Point Objective (RPO): ultimo istante di salvataggio dei dati fino al quale è garantita l'integrità degli stessi.

^(**) cfr. allegato «E» pubblicato sul *teamsite* «BCM – Continuità Operativa BMPS», estrazione del 13/11/2018



2 Attività svolta: Sicurezza Logica del Sistema di Alimentazione (5 di 8)

GESTIONE IT QUALITÀ DEI DATI

SICUREZZA LOGICA
SISTEMA DI
ALIMENTAZIONE

EFFICACIA DEI
PRESIDI DI
CONTROLLO

VERIFICHE SVOLTE

Analisi della sicurezza dei canali di trasmissione dei dati: verifica dei permessi di accesso alla cartella di rete condivisa in cui vengono spostati i flussi informativi generati dai Sistemi del Contenzioso prima di essere caricati nel *data warehouse* aziendale.

Utenze e relativi permessi sono stati forniti, in data 31/10/2018, dal *Settore Erogazione Applicativa*.

dimensioni: riservatezza, integrità

Analisi della sicurezza dei canali di trasmissione dei dati: verifica dei permessi di accesso alla cartella di rete condivisa in cui vengono spostati i flussi informativi generati a partire dal *data warehouse* aziendale prima di essere caricati nella base dati di calcolo LGD.

Utenze e relativi permessi sono stati forniti, in data 08/11/2018, dal *Settore Erogazione Applicativa*.

dimensioni: riservatezza, integrità

ESITI

Le verifiche condotte hanno permesso confermare la sicurezza del canale di trasmissione, in termini di *riservatezza* e *integrità*.

L'analisi dei permessi di accesso alla cartella di rete condivisa [\AP000000012017\DWHP01_DWA_KZ](#) ha, infatti, rilevato la presenza di 7 utenze nominative, appartenenti al gruppo di amministrazione *mps.local\lg1030\xdwhKZadm*, con controllo completo sulla stessa.

Le utenze sono associate a dipendenti del Consorzio, nello specifico:

- 6 utenze del *Servizio Credito*, gestore della cartella;
- 1 utenza del *Servizio Sistemi Tecnologici*, detentore del governo delle componenti dell'architettura tecnologica del Consorzio.

Le verifiche condotte hanno permesso confermare la sicurezza del canale di trasmissione, in termini di *riservatezza* e *integrità*.

L'analisi dei permessi di accesso alla cartelle di rete condivisa

[\nassi1.local\IP0000CRRn05\IP0000CRR_EXT\fy\ext](#) ha, infatti, rilevato la presenza di:

- 4 utenze nominative con accesso in sola lettura associate a dipendenti del Consorzio, nello specifico:
 - 2 utenze del *Servizio DWH e Reporting*;
 - 2 utenze del *Servizio Applicazioni Bilancio e Rischi*.
- 2 gruppi di amministrazione, *local\lg0\lxdba* e *local\lg0\lxadm*, con controllo completo sulla stessa. Tutte le utenze incluse nei gruppi sono riferibili a risorse ricomprese nella lista degli amministratori di sistema del Consorzio, come confermato in data 17/12/2018 dal *Settore BCM*.



2 Attività svolta: Sicurezza Logica del Sistema di Alimentazione (6 di 8)

VERIFICHE SVOLTE

Analisi delle utenze nominative per l'accesso diretto ai dati storicizzati nella base dati di calcolo LGD.

Utenze e relativi profili abilitativi sono stati forniti in data 14/11/2018 dal Servizio Sistemi Tecnologici del Consorzio.

dimensioni: riservatezza, integrità

ESITI

Dalle informazioni risultanti dalle interviste con il Settore Rischio e Antiriciclaggio è emerso che le tabelle della base dati di calcolo LGD in cui vengono caricati i dati estratti dal *data warehouse* aziendale (*tabelle target FY20*), una volta terminata la fase di storicizzazione, non possono essere più modificate né tramite interventi manuali né tramite script/programmi di aggiornamento.

Tuttavia l'analisi delle utenze ha rilevato la presenza di 3 utenze nominative con abilitazione in scrittura (2 dipendenti e 1 consulente esterno riferibili al Servizio Applicazioni Bilancio e Rischio) appartenenti al gruppo *Active Directory ora_gap_fy_crr_u@local*.

In lettura è risultato, altresì, abilitato un elevato numero di utenze nominative associate a personale, sia interno che esterno, afferente a strutture Banca e consortili eterogenee, così distribuito tra i seguenti gruppi di *Active Directory*:

- *ora_pu_fy_crrmg_s@local*: n. 286 utenze
- *ora_pu_fy_crrmg_siu_s@local*: n. 256 utenze
- *ora_pu_fy_crrmg_lstage_s@local*: n. 191 utenze
- *ora_pu_fy_crrmg_lstage_siu_s@local*: n. 220 utenze
- *ora_pu_fy_crrmg_staging_s@local*: n. 57 utenze
- *ora_pu_fy_crrmg_staging_siu_s@local*: n. 187 utenze

La criticità, rappresentata dalla scrivente Funzione in sede di *exit meeting*, è stata sanata prima della pubblicazione del presente rapporto. A far data dal 17/01/2019 il Servizio *Credit Risk Models*, utente responsabile della base dati di calcolo LGD, ha provveduto a rimuovere le utenze abilitate in scrittura e ad effettuare una *review* delle utenze abilitate in lettura riservando il privilegio solo quando ritenuto effettivamente necessario a svolgere le mansioni assegnate (rispetto del principio di *least privilege*).

Sulla base dati di calcolo LGD sono risultate, inoltre, definite 21 utenze nominative di amministrazione appartenenti al gruppo *Active Directory oraadmin@local*. Tutti le utenze sono riferibili a risorse ricomprese nella lista degli amministratori di sistema del Consorzio, come confermato in data 17/12/2018 dal Settore BCM.

2 Attività svolta: Sicurezza Logica del Sistema di Alimentazione (7 di 8)

GESTIONE IT QUALITÀ DEI DATI

SICUREZZA LOGICA
SISTEMA DI
ALIMENTAZIONE

EFFICACIA DEI
PRESIDI DI
CONTROLLO

VERIFICHE SVOLTE

Verifica del processo di gestione delle abilitazioni di accesso al *data warehouse* aziendale (sistema Teradata).

Analisi delle utenze nominative per l'accesso diretto ai dati: *data warehouse* aziendale (sistema Teradata).

L'elenco delle utenze è stato fornito in data 20/11/2018 dal *Settore Sistemi Centrali*.

dimensioni: riservatezza, integrità

ESITI

Le verifiche condotte hanno rilevato un vuoto normativo in relazione al processo di gestione del ciclo di vita delle utenze per l'accesso al sistema Teradata. Tale carenza è risultata solo parzialmente compensata dalle prassi operative^(*) in uso che sono, peraltro, incomplete (cfr. gap 2). Relativamente ai nuovi censimenti, ad esempio, le prassi in uso prevedono che la richiesta sia inoltrata dal responsabile della risorsa alla Funzione *Gestione Utenti*. Non è risultato, tuttavia, completamente delineato l'iter approvativo: nel caso di utente Banca l'abilitazione viene concessa previa autorizzazione della Funzione *Organizzazione* mentre per gli utenti del Consorzio non è ancora stata individuata una Funzione di riferimento.

Le utenze sono censite direttamente in Teradata dagli amministratori del sistema: al fine di automatizzare il processo di gestione delle abilitazioni è stato sviluppato, come da standard Consorzio, un connettore OIM (*Oracle Identity Manager*) dedicato che, alla data della verifica, non è risultato operativo.

L'analisi delle evidenze ha rilevato che nel sistema Teradata:

- in scrittura non risultano abilitate utenze nominative;
- in lettura risultano abilitate utenze nominative afferenti a strutture Banca e consortili eterogenee, nello specifico:
 - 130 utenze, di cui 2 risultate cessate, abilitate alla lettura dei dati di cui il *Settore Contenzioso, Leasing e Factoring* risulta *Technical Data Steward* (ambito applicativo KZ);
 - 90 utenze, di cui 4 risultate cessate, abilitate alla lettura dei dati di cui il *Settore Rischi e Antiriciclaggio* risulta *Technical Data Steward* (ambito applicativo FY).

Risultano altresì presenti 109 utenze con abilitazione trasversale, ovvero con accesso all'intero contenuto informativo del *data warehouse* aziendale, nello specifico:

- 73 utenze assegnate al Consorzio, di cui 2 utenze risultate cessate;
- 36 utenze afferenti alla Funzione *Internal Audit* (35 assegnate a Banca MPS, 1 utenza assegnata a Banca MPS Capital Services).

L'assenza di un processo formale e/o prassi consolidate circa la gestione delle abilitazioni sul sistema Teradata non garantisce una corretta e costante attività di *review* delle utenze nel rispetto del principio del *least privilege* (cfr. gap 2).

Sono state, infine, rilevate 11 utenze nominative di amministrazione delle quali 2 sono risultate cessate. Su segnalazione della scrivente Funzione, il *Settore Sistemi Centrali* ha provveduto, in data 22/11/2018, alla rimozione di tali utenze dagli amministratori del sistema Teradata.

Tutti le restanti utenze sono riferibili a risorse ricomprese nella lista degli amministratori di sistema del Consorzio, come confermato in data 17/12/2018 dal *Settore BCM*.

^(*) Dal punto di vista operativo il Consorzio si attiene a quanto era stabilito nel M 00004 - *Manuale: Procedura di gestione abilitazioni particolari*, documento che non risulta in vigore e non è stato sostituito da altri documenti normativi.



2 Attività svolta: Sicurezza Logica del Sistema di Alimentazione (8 di 8)

VERIFICHE SVOLTE

ESITI

Verifica delle operazioni di accesso *data warehouse* aziendale (sistema Teradata) .

dimensione: tracciabilità

Le attività svolte dagli utenti che abbiano ricevuto abilitazioni per l'accesso diretto ai dati devono essere oggetto di periodica verifica. A tale scopo, nello strumento *SID Navigator*, sono state rese disponibili indagini dedicate, nello specifico:

- per basi dati DB2: «*Audit DML DB2\Log interventi Db2 Gadis*»;
- per basi dati dipartimentali: «*Audit DML DB2\Log interventi Oracle\Teradata*».

Tuttavia è emerso che, per quanto attiene le basi dati dipartimentali, lo strumento in argomento non consente di monitorare gli accessi diretti al sistema Teradata, sebbene, a garanzia della tracciabilità delle operazioni condotte sui dati, il log degli accessi diretti sia salvato quotidianamente, dal *Settore Sistemi Centrali*, in una tabella dedicata (tabella *Oracle TDAUDIT.TD5114E_AUDIT_DETAILS*) .

Su richiesta del team di audit, il *Settore Reporting*, in collaborazione con il *Settore Sistemi Centrali*, ha provveduto in data 18/12/2018 a rendere disponibile una indagine dedicata al monitoraggio degli accessi diretti al sistema Teradata a prescindere dallo strumento utilizzato («*Audit DML DB2\Log interventi Oracle\Teradata LGINT003 – Interventi TERADATA - Estrazione per Matricola e Periodo*»).

Verifica delle operazioni di accesso alla base dati di calcolo LGD: analisi del log degli accessi diretti ai dati.

L'attività è stata condotta analizzando i dati estratti tramite esecuzione della indagine di monitoraggio degli accessi diretti ai dati «*Audit DML DB2\Log interventi Oracle\Teradata*» disponibile su *SID Navigator* (periodo di osservazione giugno-settembre 2018).

dimensione: tracciabilità

L'analisi del log degli accessi diretti alle *tabelle target FY20* della base dati di calcolo LGD non ha rilevato accessi in modifica. Tutte le istruzioni archiviate sono di sola lettura (eseguite sia da dipendenti che collaboratori esterni appartenenti a strutture Banca e consortili eterogenee).

2 Attività svolta: Efficacia dei presidi di controllo (1 di 5)

GESTIONE IT QUALITÀ DEI DATI

SICUREZZA LOGICA
SISTEMA DI
ALIMENTAZIONE

EFFICACIA DEI
PRESIDI DI
CONTROLLO

OBIETTIVO

Accertare l'efficacia dei controlli di Data Quality a presidio delle singole fasi del sistema di alimentazione (in termini di *accuratezza*, *completezza*, *coerenza* e *tempestività*) tramite verifiche puntuali dei controlli in essere e verifiche dirette sui dati.

Obiettivo di controllo: IG.7.12 BIS

PERIMETRO/ METODOLOGIA

Interviste, raccolta documentale, analisi delle evidenze, analisi dei dati, accesso diretto ai sistemi.

RISCHI IMPATTATI

MPS.900060 - La mancata/incompleta definizione dei requisiti di business per la gestione dei dati e delle procedure (per verificarne completezza, accuratezza, tempestività di elaborazione), generata da un processo di gestione dei dati inadeguato, può portare a una mancata ottimizzazione dell'uso delle informazioni e a informazioni non disponibili come previsto. Ciò può comportare perdite economiche e impatti reputazionali.

VERIFICHE SVOLTE

Verifica della presenza di requisiti di Business formalizzati in materia di Data Quality per il controllo della base dati di calcolo LGD.

dimensioni: *accuratezza*, *completezza*, *integrità*, *coerenza* e *tempestività*

ESITI

La Funzione di Business, responsabile per l'Output rilevante LGD - *Settore Modelli di LGD e EAD*, ha espresso in maniera esaustiva i requisiti in materia di controllo della qualità dei dati storicizzati nella base dati di calcolo del parametro. Le specifiche sono state formalizzate nei BR60265 e BR72440 che descrivono in maniera approfondita le finalità dei controlli, la modalità di integrazione nella piattaforma di Data Quality *IrionDQ*^(*) e le azioni da intraprendere a fronte di una segnalazione di anomalia. Nel dettaglio:

- BR60265, *LGD Implementazione controlli in Piattaforma Data Quality*: ha definito un primo set di controlli da implementare in *IrionDQ* a copertura delle dimensioni *accuratezza* e *completezza*. Tra i controlli di *completezza* è previsto un controllo tecnico di tipo andamentale per verificare che la numerosità dei dati elaborati non si discosti, oltre una soglia prestabilita, dalla numerosità del mese precedente. Il BR risulta chiuso dall'utente di Business e i controlli in produzione da aprile 2018;
- BR72440, *LGD Sviluppo controlli a seguito ispezione TRIM*: ha definito i controlli inerenti la qualità dei dati richiesti nell'ambito dell'*on site inspection TRIM* del 2017-2018 per l'Output rilevante LGD. Dal BR si evince che i controlli, alla data della verifica in corso di implementazione, andranno a coprire le dimensioni della qualità *integrità*, *tempestività*, *coerenza* e *correttezza*, oltre ad incrementare il numero di controlli di *accuratezza* e *completezza*.

^(*) cfr. rapporto n. 90_2018 «Data Governance, Struttura Organizzativa, Framework e Strumenti a Supporto»



2 Attività svolta: Efficacia dei presidi di controllo (2 di 5)

GESTIONE IT QUALITÀ DEI DATI

SICUREZZA LOGICA
SISTEMA DI
ALIMENTAZIONE

EFFICACIA DEI
PRESIDI DI
CONTROLLO

VERIFICHE SVOLTE

Verifica della corretta traduzione dei requisiti di Business in controlli di Data Quality definiti in *IrionDQ*.

La verifica è stata condotta analizzando la reportistica di riepilogo estratta, in data 22/11/2018, dallo strumento *IrionDQ* relativamente al censimento dei controlli.

dimensioni: accuratezza e completezza

ESITI

Su *IrionDQ*, alla data della verifica, sono risultati censiti e attivi 17 controlli che agiscono sulla base dati di calcolo LGD, 5 dei quali operano sui dati memorizzati nelle *tabelle target FY20* (cfr. Allegato 2). I controlli, che costituiscono l'implementazione del BR60265, sono operativi sui dati di tutti gli Istituti alimentanti e coprono due dimensioni della qualità, *accuratezza* con 10 controlli e *completezza* con 7 controlli.

I controlli sono stati implementati dal *Settore Rischi e Antiriciclaggio, Technical Data Steward* per la materia in esame, e sono stati validati dalla Funzione di Business tramite opportuni test di accettazione utente. La Funzione di Business ha, altresì, fornito dettagliate indicazioni su come efficientare i controlli implementati, evidenziando così un adeguato presidio sulla materia e una forte sinergia con le strutture tecniche in ottemperanza al modello organizzativo di *Data Governance* adottato dalla Banca.

Dalle interviste con il referenti delle strutture auditate è, inoltre, emerso che l'esperienza maturata all'interno del *Settore Rischi e Antiriciclaggio* e del *Settore DWH e Data Quality* sta consentendo di implementare in autonomia i controlli all'interno della piattaforma *IrionDQ* senza ricorrere sistematicamente alla consulenza di fornitori esterni, conseguendo così vantaggi per l'Azienda in termini di costi e tempi.



2 Attività svolta: Efficacia dei presidi di controllo (3 di 5)

GESTIONE IT QUALITÀ DEI DATI

SICUREZZA LOGICA
SISTEMA DI
ALIMENTAZIONE

EFFICACIA DEI
PRESIDI DI
CONTROLLO

VERIFICHE SVOLTE

Verifica del corretto monitoraggio dell'esito dei controlli *IrionDQ* e del corrispondente processo di gestione delle attività di *remediation*.

La verifica è stata condotta analizzando la reportistica di riepilogo estratta, in data 22/11/2018, dallo strumento *IrionDQ* relativamente alla fase di esecuzione dei controlli (periodo di osservazione: giugno-ottobre 2018).

ESITI

L'esito delle esecuzioni dei controlli viene archiviato nella piattaforma *IrionDQ*. A fronte di un controllo che termina con esito negativo, viene aperto in automatico un ticket nello strumento di Incident Management del Consorzio, *Remedy*. Poiché lo strumento non è ancora fruibile dalle risorse della Banca, il ticket viene per *default* collegato all'applicazione *APP0000808*, di cui il *Settore Rischi e Antiriciclaggio* è referente IT e il *Servizio Credit Risk Models* è referente di Business.

La prassi attualmente in uso prevede che il referente IT chiuda direttamente il ticket^(*) senza inviare notifica alla Funzione di Business che, pertanto, ha inclusa nello scadenziario delle proprie attività la verifica sistematica degli esiti dei controlli *IrionDQ*.

Dopo aver analizzato l'esito del controllo, la Funzione di Business indirizza le attività di *remediation* in base allo stato delle singole posizioni che hanno generato l'anomalia, nel dettaglio:

- per le posizioni aperte richiede l'intervento del Gestore indicando le opportune correzioni da apportare tramite gli applicativi del Contenzioso;
- per le posizioni cessate, non direttamente rettificabili tramite gli applicativi del Contenzioso, richiede l'intervento del Consorzio indicando le modifiche da apportare tramite accesso diretto ai dati.

Poiché gli interventi diretti sui dati sono azioni di *change* assimilabili a RFC di Urgenza, il Consorzio, attenendosi alla normativa interna^(**), richiede esplicita autorizzazione del *Chief* della Direzione richiedente.

Si osserva che il *Settore Modelli di LGD e EAD* ha già richiesto il supporto del *Settore Applicazione Data Governance* per efficientare l'attuale processo con l'obiettivo di definire, per ogni controllo, il corretto gruppo di assistenza a cui assegnare i ticket.

La frequenza dei controlli di norma è mensile e, ad ogni esecuzione, viene elaborato il nuovo set di dati relativo al mese corrente. Tuttavia, nel caso di anomalie rilevate nei dati caricati, la Funzione di Business può richiedere correzioni, nuove estrazioni e conseguentemente l'esecuzione un nuovo caricamento, a seguito del quale i controlli previsti devono essere svolti *ex novo*. Tali situazioni risultano più frequenti nella fase di stima del parametro, attività che necessita della massima attenzione circa la correttezza delle informazioni lavorate.

Nel periodo di osservazione, giugno-ottobre 2018, a fronte di una complessiva esecuzione di 537 controlli *IrionDQ*, sono stati aperti 31 ticket *Remedy* (pari al 6% del totale), prontamente analizzati dalla Funzione di Business e indirizzati verso le strutture competenti per la risoluzione.

^(*) Fanno eccezione le segnalazioni derivanti dai controlli di natura prettamente tecnica che vengono analizzate direttamente dal *Settore Rischi e Antiriciclaggio* del Consorzio.

^(**) D00139 – Processo *Change Management*



2 Attività svolta: Efficacia dei presidi di controllo (4 di 5)

GESTIONE IT QUALITÀ DEI DATI

SICUREZZA LOGICA
SISTEMA DI
ALIMENTAZIONE

EFFICACIA DEI
PRESIDI DI
CONTROLLO

VERIFICHE SVOLTE

Verifica della presenza di controlli di Data Quality sui dati storicizzati nel *data warehouse* aziendale.

La verifica è stata condotta tramite analisi della documentazione fornita, in data 26/10/2018, dal Settore DWH e Data Quality.

dimensioni: accuratezza e coerenza

Verifica del corretto monitoraggio dell'esito dei controlli *Swiffer* e del corrispondente processo di gestione delle attività di *remediation*.

La verifica è stata condotta tramite:

- interviste con i referenti delle strutture;
- esame delle presentazioni del comitato Servizi Resi e Rischi (periodo di osservazione marzo-settembre 2018);
- analisi degli esiti dei controlli *Swiffer* attivi sull'ambito applicativo Contenzioso, fornita in data 26/10/2018 dal Settore DWH e Data Quality.

ESITI

Il Settore DWH e Data Quality ha sviluppato un motore, denominato *Swiffer*^(*), per il controllo della qualità dei dati archiviati nel *data warehouse* aziendale. L'iniziativa si inquadra tra le attività di Data Governance finalizzate a garantire l'integrità e la qualità dei dati nelle basi dati gestite dal Consorzio: il Servizio Data Governance e Reporting Management riporta periodicamente gli esiti dei controlli al Comitato Rischi della Capogruppo. I risultati sono, altresì, presentati nell'ambito del Comitato Servizi Resi e Rischi del Consorzio.

I controlli tecnici *Swiffer* sono eseguiti, con cadenza mensile, massivamente sulle tabelle del *data warehouse* e sono mirati ad evidenziare valorizzazioni anomale di alcune tipologie di campi (es: presenza di caratteri di controllo nei campi testuali, campi non valorizzati, valori non appartenenti al dominio di riferimento, codici sintatticamente errati). Alla data della verifica sono risultati attivi 11 controlli riconducibili alle dimensioni *accuratezza* e *coerenza* (cfr. Allegato 3).

Gli esiti dei controlli *Swiffer* non sono integrati all'interno della piattaforma *IrionDQ*, sebbene tale possibilità sia in fase di valutazione da parte del Consorzio (studio di fattibilità ITxIT BR67488, *Analisi invio esiti controlli Swiffer in Irion*).

Le attività di verifica condotte hanno evidenziato che, nel periodo di osservazione marzo – settembre 2018, il numero di *warning Swiffer* ascrivibili al Settore Contenzioso, Leasing e Factoring si è mantenuto circa costante attorno al valore 2,3 Mln, pur evidenziando un leggero *trend* in crescita^(**). Il Settore Contenzioso, Leasing e Factoring non ha, infatti, avviato opportune attività di analisi per valutare le possibili azioni di *remediation* da mettere in atto.

Da approfondimenti successivi è emerso che il mancato monitoraggio degli *warning* era da imputarsi ad una carenza di comunicazione che ha precluso al Settore di ricevere, da settembre 2017 a novembre 2018, notifica degli esiti dei controlli.

A decorrere da settembre 2017, infatti, l'elenco delle risultanze dei controlli, in precedenza pubblicato nel *teamsite* «<http://web1ework.gruppo.mps.local/sites/SPE003/0010/prjdatgov201/Data Quality IT>», è reso disponibile nello strumento *SID Navigator* tramite una indagine dedicata, «Data Quality\Swiffer\Elenco Warning per Servizio». Tuttavia la nuova modalità di recupero degli esiti dei controlli è stata segnalata ai soli settoriali con maggior numero di *warning (top performer)*, senza un coinvolgimento complessivo delle strutture interessate dal fenomeno. Si osserva, inoltre, che il Settore Contenzioso, Leasing e Factoring non è mai risultato *top performer*.

Su richiesta del team di audit, a novembre 2018, l'informativa è stata fornita diffusamente a tutte le strutture del Consorzio affinché potessero avviare le opportune attività di analisi e le eventuali azioni di *remediation*.

^(*) cfr. rapporto n. 90_2018 «Data Governance, Struttura Organizzativa, Framework e Strumenti a Supporto»

^(**) numero di *warning* : 2.290.851 (marzo 2018) - 2.297.434 (settembre 2018), da presentazioni comitato Servizi Resi e Rischi



2 Attività svolta: Efficacia dei presidi di controllo (5 di 5)

GESTIONE IT QUALITÀ DEI DATI

SICUREZZA LOGICA
SISTEMA DI
ALIMENTAZIONE

EFFICACIA DEI
PRESIDI DI
CONTROLLO

VERIFICHE SVOLTE

Verifica del rispetto dei tempi di *cut off* stabiliti per la disponibilità delle informazioni relative all'Output Rilevante LGD.

dimensione: tempestività

Verifica della qualità dei dati tramite esecuzione diretta di *query* di controllo predisposte dal team di audit.

dimensioni: accuratezza e coerenza

ESITI

Il calcolo del parametro LGD è soggetto al *Fast Closing*, ovvero a vincoli di *cut off*. Per rispettare questi vincoli anche la produzione delle basi dati necessarie deve rispettare scadenze ben precise. Il calendario delle scadenze viene fornito dallo *Staff Area Amministrazione e Bilancio e Presidio Qualità Informazione*. Il *Settore Rischi e Antiriciclaggio* ha riferito che i limiti temporali imposti per le attività di produzione dei dati, allo stato attuale, non sono risultati critici.

Il team di audit ha predisposto un *set* di *query*, per il controllo della qualità dei dati, riconducibili alle dimensioni di *accuratezza* e *coerenza*, come di seguito dettagliato:

- sul *data warehouse* aziendale sono state eseguite, su alcune tabelle coinvolte nel calcolo del parametro LGD, 8 *query* di controllo *Swiffer* rilevando un comportamento conforme con quanto atteso. Sono, inoltre, state eseguite ulteriori 20 *query* di controllo costruite dal team di audit. I risultati ottenuti sono stati condivisi con il *Settore Contenzioso, Leasing e Factoring* che ha confermato la coerenza di quanto archiviato nel *data warehouse* aziendale rispetto ai sistemi di origine del Contenzioso, non ravvisando, pertanto, introduzioni di alterazioni delle informazioni nella procedura di alimentazione.
- Nella base dati di calcolo LGD sono state eseguite, sulle *tabelle target FY20*, 56 *query* di controllo. I risultati sono stati condivisi con il *Settore Modelli di LGD e EAD* che, in relazione alla attuale modalità di stima del parametro LGD, non ha evidenziato criticità o particolari casistiche da approfondire.



Firme e destinatari del rapporto

Ruolo	Cognome e Nome	Firma
Responsabili Audit Team	de Mauro Silvia	
Auditors	Fabbri Duccio	
V° Responsabile del Settore ICT Audit	Salvini Riccardo	
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 di BMPS (invio tramite IAudit)	Selezione
Presidente del CdA	
Amministratore Delegato	
Collegio Sindacale	
Comitato Rischi	
OdV 231	

Altri organi destinatari	
Legal Entity	Organo destinatario
Consorzio Operativo Gruppo MPS	Presidente CDA
Consorzio Operativo Gruppo MPS	Amministratore Delegato
Consorzio Operativo Gruppo MPS	Direttore Generale
Consorzio Operativo Gruppo MPS	Collegio Sindacale
Consorzio Operativo Gruppo MPS	Referente Internal Audit



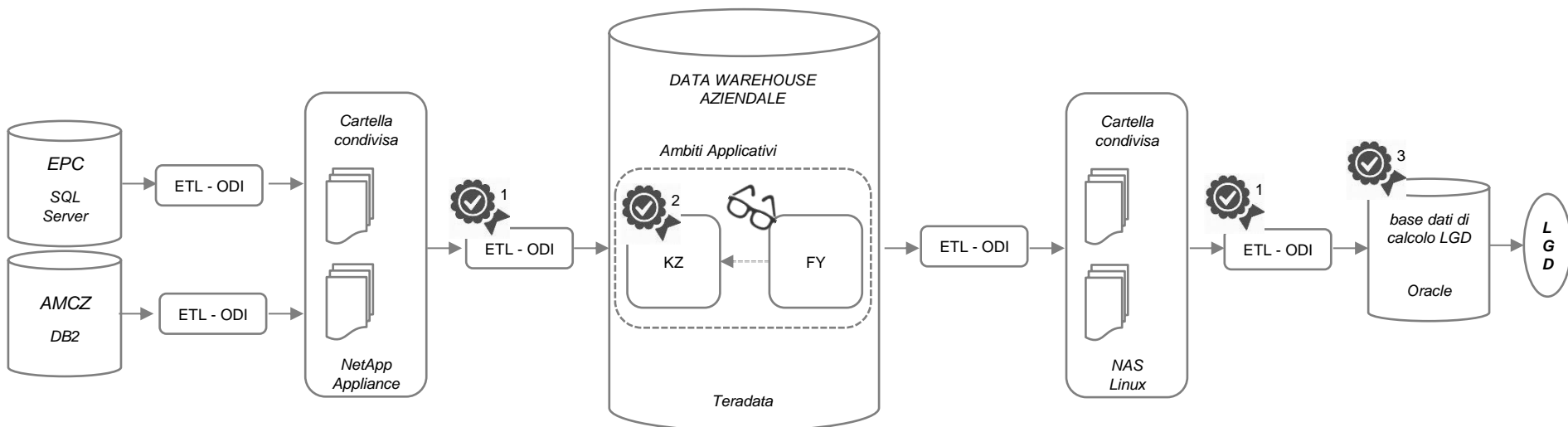
Elenco allegati

- » Allegato 1: Infrastruttura informatica
- » Allegato 2: Elenco controlli *IrionDQ* per output rilevante LGD
- » Allegato 3: Elenco controlli tecnici *Swiffer*



Allegato 1: Infrastruttura informatica

Di seguito il disegno architetturale complessivo del processo di alimentazione della base dati di calcolo LGD con evidenza dei punti di controllo inerenti la qualità dei dati.



➤ Principali componenti del sistema:




- Basi dati**
- **EPC:** gestione amministrativa delle pratiche a contenzioso, *DBMS Microsoft SQL Server*
 - **AMCZ:** gestione contabile delle pratiche a contenzioso, *DBMS IBM DB2*
 - **data warehouse aziendale,** sistema Teradata:
 - il **Settore Contenzioso, Leasing e Factoring** è *Technical Data Steward* per l'ambito applicativo KZ. Contiene Tabelle KZ* replicate dai sistemi origine del Contenzioso
 - il **Settore Rischi e Antiriciclaggio** è *Technical Data Steward* per l'ambito applicativo FY. Contiene Viste FY* costruite a partire dalle Tabelle KZ*
 - **base dati calcolo di LGD:** *DB Modelli rischi di credito - PD0000DWA, DBMS Oracle*

Cartelle di rete condivise

- [\\AP000000012017\DW\HFP01_DWA_KZ](#), definita su *NetApp Appliance*
- [\\nassi1.local\p0000CRRn05\p0000CRR_EXT\fy\ext](#), definita su *NAS Linux*

➤ Per implementare le procedure di estrazione, trasformazione e caricamento viene utilizzato il software di ETL (*Extract, Transform, Load*) *Oracle Data Integrator (ODI)*

➤ Punti di controllo:

-  1 *controlli formato dati*
 2 *controlli tecnici Swiffer*
 3 *controlli IrionDQ*



Allegato 2: Elenco controlli *IrionDQ* per output rilevante LGD

N.	ID CONTROLLO	DESCRIZIONE CONTROLLO	DIMENSIONE QUALITA'	NOTE
1	RU_02	Il Controllo è volto ad evidenziare i codici NGR delle tabelle delle quattro banche che hanno i campi relativi alla provincia (TX_PRV_CLI) e alla sede legale (CD_SEDE_LEGALE) non valorizzati.	Completezza	FY3007E_KZ_ANAGRAFE Controllo tecnico
2	RU_08	Controllo movimenti senza esposizione.	Completezza	FY3009E_KZ_MOVIMENTI FY3008E_KZ_CAPITALE
3	RU_09	Controllo pratiche chiuse con dubbi esiti o altre esposizioni valorizzate.	Completezza	FY3007E_KZ_ANAGRAFE
4	RU_10	Controllo pratiche chiuse con fondi valorizzati e positivi.	Completezza	FY3007E_KZ_ANAGRAFE FY3006E_KZ_DUBBI_ESITI_BIL
5	RU_11	Controllo pratiche chiuse con data di chiusura mancante.	Completezza	FY3007E_KZ_ANAGRAFE FY3008E_KZ_CAPITALE
6	RU_12	Controllo sui dati relativi a GBV, NBV, rettifiche, dubbi esiti forniti dal gestore con quelli che vengono ricalcolati nel nostro DHW NOLEAS.	Accuratezza	FY3037E_VL_RICALCOLO
7	RU_13	Controllo andamentale sulle tabelle contenzioso della numerosità dei record a valle dei flussi in Input al DWH.	Completezza	Il controllo si applica a tutte le <i>tabelle target</i> FY20. Controllo tecnico
8	RU_14	Verifica congruenza data accensione partita a Contenzioso.	Accuratezza	FY2007E_KZ_RAPCONTR
9	RU_15	Verifica presenza rapporti contrattuali con movimento di spesa anomalo.	Accuratezza	FY2007E_KZ_RAPCONTR
10	RU_16	Verifica presenza movimenti di esposizione (fatta eccezione per gli interessi) senza rapporto contrattuale.	Accuratezza	FY2010E_KZ_ESPOSIZIONI
11	RU_19	Verifica esistenza movimenti con segno discorde o storno eccedente.	Accuratezza	FY3009E_KZ_MOVIMENTI
12	RU_21	Verifica esistenza partite con GBV con capitale negativo.	Accuratezza	FY3008E_KZ_CAPITALE
13	RU_22	Verifica esistenza movimenti di perdita negativi.	Accuratezza	FY3009E_KZ_MOVIMENTI
14	RU_24	Controllo quadrature esposizioni Leasing.	Accuratezza	FY3046E_VL_RICALCOLO_LEAS
15	RU_25	Verifica esistenza partite con GBV positivo.	Accuratezza	FY2010E_KZ_ESPOSIZIONI FY2009E_KZ_COSTI FY2008E_KZ_RECUPERI
16	RU_26	Verifica esistenza partite con servizio associato «NON CLASSIFICATO».	Accuratezza	FY3007E_KZ_ANAGRAFE FY3008E_KZ_CAPITALE
17	RU_27	Il Controllo è volto ad evidenziare i codici NGR delle tabelle delle quattro banche che hanno il campo relativo al segmento (CD_PTF_BIS2_DETT_SOGG) non valorizzato.	Completezza	FY3007E_KZ_ANAGRAFE Controllo tecnico

Allegato 3: Elenco controlli tecnici Swiffer

N.	ID CONTROLLO	DESCRIZIONE CONTROLLO	DIMENSIONE QUALITA'
1	SW_CTR_CD_AZIENDA_CLONE	Il controllo conta il numero di occorrenze in cui il campo <i>CD_AZIENDA</i> è diverso dal codice ABI previsto per il DB di riferimento o vale NULL.	Accuratezza
2	SW_CTR_CD_AZIENDA_SUM	Il controllo conta il numero di occorrenze in cui il campo <i>CD_AZIENDA</i> non contiene valori relativi a istituti che appartengono o sono appartenuti al Gruppo MPS.	Accuratezza
3	SW_CTR_CD_BELFIORE	Il controllo cerca tutte le occorrenze di codici catastali comunali che non rispettano il formato previsto (Lettera maiuscola + 4 cifre).	Accuratezza
4	SW_CTR_CD_BELFIORE_OBSOLETO	Il controllo cerca tutte le occorrenze di codici catastali comunali che non abbiano un corrispettivo nella tabella di dominio dedicata, <i>I4_WORK_SHARED.SW_D105_CDBELFIORE BELF</i> .	Coerenza
5	SW_CTR_CD_FISCALE	Il controllo verifica la validità formale del codice fiscale.	Accuratezza
6	SW_CTR_CD_NDC	Il controllo cerca tutti i codici NDC non validi (codice <1) o privi di un corrispettivo nella tabella di dominio dedicata, <i>HA3030E_CLI_AZ_BASE_DB0000</i> .	Accuratezza
7	SW_CTR_CD_NGR	Il controllo cerca i codici NGR non validi (codice <1) o privi di un corrispettivo nella tabella di dominio dedicata, <i>HA3030E_CLI_AZ_BASE_DB0000</i> .	Accuratezza / Coerenza
8	SW_CTR_DT_INIZIO_FINE	Il controllo conta il numero delle occorrenze in cui il campo <i>DT_INI_VAL</i> è maggiore di <i>DT_FINE_VAL</i> , dove <i>DT_FINE_VAL</i> assume il valore '9999-12-31' quando non valorizzato.	Accuratezza
9	SW_CTR_UnreadableChar	Il controllo cerca eventuali caratteri di controllo non stampabili (codici ASCII < CHR(32) e > CHR(126)) nei campi testuali.	Accuratezza
10	SW_CTR_UnreadableChar0	Il controllo cerca tutte le occorrenze di CHR(0) nei campi testuali.	Accuratezza
11	SW_CTR_UnreadableChar26	Il controllo cerca tutte le occorrenze di CHR(26) nei campi testuali.	Accuratezza

Fonte: Settore DWH e Data Quality, data estrazione 26/10/2018