Data: 22.06.2022

Perimetro Bancario[1]

Composto dalle piattaforme relative a soluzioni per clienti operanti in ambito Bancario, in particolare:

- banche autorizzate in Italia, ad eccezione delle succursali di banche extracomunitarie aventi sede nei paesi del Gruppo dei Dieci ovvero in quelli inclusi in un apposito elenco pubblicato e periodicamente aggiornato dalla Banca d'Italia;
- capogruppo di gruppi bancari;
- imprese di riferimento che sono responsabili del calcolo dei requisiti patrimoniali e del rispetto delle disposizioni prudenziali applicabili su base consolidata.

Per i servizi contrattualizzati che prevedono il trattamento di questo Perimetro di Dati sono state definite le seguenti misure ulteriori misure aggiuntive a quelle previste per il perimetro dei Dati Personali Comuni.

ID MISURA	Categoria	Testo requisito
AuL-ICT.008.1 AuL-ICT.008.2	Audit log	La piattaforma tramite cui è effettuato il trattamento di dati, o l'eventuale piattaforma centralizzata di Identity Management ad essa connessa, è configurata in maniera tale da: - produrre la registrazione degli accessi logici (Access Log), compresi i tentativi falliti di accesso, effettuati da parte degli Amministratori di Sistema Addetti IT interni ed esterni - conservare le registrazioni per un periodo di sei mesi.
AuL-ICT.010.1 AuL-ICT.010.2	Audit log	E' garantita la completezza, l'immodificabilità e la possibilità di verificare l'integrità delle registrazioni dei log di accesso degli Addetti IT (ad es. tramite l'invio a sistemi di Log Collecting centralizzati).
AuL-ICT.012.1 AuL-ICT.012.2	Audit log	La piattaforma tramite cui è effettuato il trattamento di dati, o l'eventuale piattaforma centralizzata di Identity Management ad essa connessa, è configurata in maniera tale da prevedere tecnologie di sincronizzazione al fine di mantenere allineata la data e l'ora associata agli accessi registrati nei log.
AuL-ICT.013.1 AuL-ICT.013.2	Audit log	Le registrazioni dei log relativi agli accessi (access log) alla piattaforma degli Addetti IT includono le seguenti informazioni: - il sistema target e l'eventuale applicazione acceduta; - evento che ha generato il log (login, logout, failure login); - utenza, data e ora di inizio / fine connessione.
AuL-ICT.016.1	Audit log	La piattaforma prevede meccanismi di registrazione degli accessi logici (access log), compresi i tentativi falliti di accesso, effettuati degli End User Autorizzati e la conservazione degli stessi per un periodo non inferiore a sei mesi.
AuL-ICT.017.1	Audit log	E' garantita la completezza, l'immodificabilità e la possibilità di verificare l'integrità delle registrazioni dei log di accesso degli End User Autorizzati (ad es. tramite l'invio a sistemi di Log Collecting centralizzati).

[1] Circolare n. 263 del 27 dicembre 2006 – 15° aggiornamento del 2 luglio 2013 – sotto paragrafo Destinatari della Disciplina

Misure Dati Bancari

Data: 22.06.2022

ID MISURA	Categoria	Testo requisito
AuL-ICT.018.1	Audit log	Le registrazioni dei log relativi agli accessi (access log) degli End User Autorizzati includono le seguenti informazioni: - il sistema target e l'eventuale applicazione acceduta; - evento che ha generato il log (login, logout, failure login); - utenza, data e ora di inizio / fine connessione.
Doc-ICT.008.1	Documentazione	In linea con quanto stabilito a livello contrattuale, risultano formalizzate procedure di comunicazione e coordinamento con il Cliente (o con TIM, nel caso di un fornitore esterno) da attuare nel caso di incidenti di sicurezza informatica e, se previsto, di continuità operativa.
Ris-ICT.008.1 Ris-ICT.008.2	Riservatezza	E' prevista la stesura e la corretta implementazione di procedure atte a regolare il processo di cancellazione dei dati del cliente a seguito della cessazione del contratto (ad es. cessazione di qualsiasi obbligazione derivate da accordi contrattuali oppure in applicazione di specifiche normative) assicurando che tali dati vengano cancellati in maniera definitiva e irreversibile al fine di impedire trattamenti non autorizzati degli stessi da parte di Addetti IT o di eventuali altri Clienti. Le tempistiche di cancellazione sono in linea con quanto previsto a livello contrattule.
Ris-ICT.009.1	Riservatezza	E' garantito l'isolamento logico dei dati relativi a clienti differenti su una medesima piattaforma. In particolare non deve essere possibile accedere/visualizzare i dati di un Cliente diverso da quello che ha acceduto alla piattaforma.
Ris-ICT.009.2	Riservatezza	Per l'erogazione del servizio tramite servizi in community o Cloud Pubblico, è garantito l'isolamento logico dei dati relativi a clienti differenti su una medesima piattaforma. In particolare non deve essere possibile accedere/visualizzare i dati di un Cliente diverso da quello che ha acceduto alla piattaforma. Se il servizio non è erogato tramite community o Cloud Pubblico non sussiste tale vincolo: in tal caso rispondere "SI".
Ris-ICT.013.1	Riservatezza	Risulta garantita l'applicazione delle misure di sicurezza derivanti dalle analisi del rischio (Piano di Sicurezza) relative alla piattaforma a supporto del servizio erogato.

Di seguito i requisiti aggiuntivi da valutare col cliente per adeguarsi alla normativa:

ID MISURA Circolare 263	Categoria	Testo requisito
	Riservatezza	L'applicativo è costruito in maniera tale da prevedere che nella prima schermata di accesso al sistema siano visualizzate le informazioni temporali relative all'ultima sessione effettuata con le stesse credenziali.
1	Documentazione	E' prevista l'eventuale partecipazione della società (TIM) alle attività di redazione o aggiornamento del Piano di Sicurezza (PdS) della piattaforma a supporto (nel caso TIM si configuri come Gestore IT di un sistema della banca);

Misure Dati Bancari

Data: 22.06.2022

ID MISURA Circolare 263	Categoria	Testo requisito
5	Documentazione	E' prevista l'acquisizione della policy di sicurezza informatica aziendale della banca al fine di applicarla, per quanto fattibile e secondo quanto disciplinato a livello contrattuale, nell'ambito della soluzione ICT. E' prevista la possibilità di eseguire delle Gap Analysis di quanto richiesto dalla policy di sicurezza informatica aziendale della banca rispetto a quanto previsto dal Piano di Sicurezza. A seguito di Gap significativi e a seconda di quanto richiesto dalla banca, TIM si impegna a formalizzare contrattualmente tali risultanze (per quanto applicabili) al fine di provvedere all'integrazione delle misure non implementate.
10	Documentazione	Nel caso di richieste specifiche ed esplicite della Banca in merito ai livelli di servizio e alla metodologia di analisi del rischio, con particolare riferimento alla riservatezza, sono previsti SLA specifici da concordare preliminarmente con la Banca in base alle esigenze delle applicazioni e dei processi aziendali della Banca stessa che si avvale del servizio offerto da TIM.
4	Documentazione	Nel caso di richieste specifiche ed esplicite della Banca in merito ai livelli di servizio e alla metodologia di analisi del rischio, con particolare riferimento alla riservatezza, è previsto l'utilizzo, ove possibile, dei livelli di classificazione forniti dalla Banca e formalizzare contrattualmente il trattamento dei dati in base a tali livelli.
2, 13, 16	Documentazione	Nel caso di ulteriori richieste esplicite della Banca, è prevista la possibilità di: - regolamentare all'interno della contrattualistica il raccordo con i ruoli e le procedure definite nel processo di analisi dei rischi del Cliente; - concordare con il Cliente l'esecuzione di specifiche attività di audit; - comunicare periodicamente al Cliente l'ubicazione geografica del/dei data center ed una indicazione del numero di addetti con accesso ai dati riservati od alle componenti critiche definite dallo stesso.
7	Supporti di memorizzazione / Backup	E' prevista la possibilità di concedere al Cliente definiti diritti di accesso alle copie di backup.
11	Log	Nel caso di richieste esplicite della banca, con riferimento almeno alle operazioni critiche ed agli accessi a dati riservati definiti dalla stessa, è prevista la possibilità di implementare meccanismi di audit log (tracciamento attività) in linea con quanto previsto contrattualmente. Tali ulteriori registrazioni, in accordo con le richieste del Cliente, sono definite contrattualmente e conservate per un periodo non inferiore a 24 mesi (salvo diversa indicazione della Banca, a seguito di assunzione del rischio) in archivi non modificabili o le cui modifiche sono puntualmente registrate;
12	Log	Nel caso di richeste esplicite della banca, con riferimento a servizi erogati in community o Cloud Pubblico, è prevista la possibilità di implementare ulteriori meccanismi di audit log (tracciamento attività) e di estrapolarne le risultanze al fine di darne visione al Cliente.
17	Riservatezza	Nel caso in cui il Cliente Banca richieda da Telecom Italia un servizio di full outsourcing di funzioni aziendali ICT, Telecom Italia deve prevedere nel contratto personalizzato come service element aggiuntivo, in relazione ai processi critici individuati dalla Banca, la redazione di un Piano di Continuità Operativa che preveda le misure, sottoforma di procedure, da attuare in caso di crisi con impatto rilevante sul Cliente. A tale proposito Telecom Italia deve

ID MISURA Circolare 263	Categoria	Testo requisito
		prevedere l'inserimento all'interno della contrattualistica della definizione e della classificazione degli impatti rilevanti.
18	Riservatezza	Nel caso in cui il Cliente Banca richieda da Telecom Italia un servizio di full outsourcing di funzioni aziendali ICT, Telecom Italia deve prevedere nel contratto personalizzato come service element aggiuntivo, in relazione ai processi critici individuati dalla Banca, la formalizzazione all'interno del contratto dei livelli di servizio assicurati in caso di crisi e delle soluzioni di continuità operativa poste in atto. Qualora i livelli di servizio non siano previsti da Telecom Italia sarà condotta una valutazione specifica di fattibilità. A tale proposito Telecom Italia deve prevedere l'inserimento all'interno della contrattualistica della definizione di “crisi” in termini di disservizio, piattaforme e/o utenze impattate.
19	Riservatezza	Nel caso in cui il Cliente Banca richieda da Telecom Italia un servizio di full outsourcing di funzioni aziendali ICT, Telecom Italia deve prevedere nel contratto personalizzato come service element aggiuntivo, in relazione ai processi critici individuati dalla Banca, la possibilità di: - eseguire attività periodiche di verifica del piano di continuità operativa; - garantire, formalizzandolo a livello contrattuale, la possibilità da parte del Cliente di partecipare a tali verifiche, definendone le modalità ed il perimetro di partecipazione. A tale proposito Telecom Italia deve individuare le procedure da seguire nel caso di partecipazione di esterni alle verifica dei piani di continuità.
20	Riservatezza	Nel caso in cui il Cliente Banca richieda da Telecom Italia un servizio di full outsourcing di funzioni aziendali ICT, Telecom Italia deve prevedere nel contratto personalizzato come service element aggiuntivo, in relazione ai processi critici individuati dalla Banca, l'implementazione di un processo con l'obiettivo di inviare al Cliente, su richiesta dello stesso e previa integrazione contrattuale di clausole di no-disclosure, i propri piani di continuità operativa o informazioni adeguate, al fine di: - permettere la valutazione della qualità delle misure previste; - permettere l'integrazione degli stessi con le soluzioni di continuità operativa realizzate dal Cliente.
21	Riservatezza	Nel caso in cui il Cliente Banca richieda da Telecom Italia un servizio di full outsourcing di funzioni aziendali ICT, Telecom Italia deve prevedere nel contratto personalizzato come service element aggiuntivo, in relazione ai processi critici individuati dalla Banca, l'implementazione di un processo di comunicazione verso il Cliente degli incidenti IT che hanno impatti sulla continuità operativa del servizio. Tali processi, esplicitati attraverso opportune procedure, devono indicare gli attori coinvolti, le tempistiche ed i canali di comunicazione utilizzati.

Misure Dati Bancari

Data: 22.06.2022

ID MISURA Circolare 263	Categoria	Testo requisito
22	Riservatezza	Nel caso in cui il servizio richiesto dal Cliente Banca preveda la presenza di processi a rilevanza sistemica, Telecom Italia deve prevedere nel contratto personalizzato come service element aggiuntivo siti alternativi che permettano la continuità operativa del servizio in coerenza con le analisi del rischio fornite dal Cliente a Telecom Italia. Sulla base dei requisiti e dell'analisi di rischio forniti dal Cliente, tali siti alternativi devono essere situati ad una distanza adeguata dai siti primari, al fine di assicurare un elevato grado di indipendenza tra i due insediamenti.
25	Riservatezza	Nel caso in cui il servizio richiesto dal Cliente Banca preveda la presenza di processi a rilevanza sistemica, Telecom Italia deve prevedere nel contratto personalizzato come service element aggiuntivo, che i siti alternativi siano configurati in modo tale da gestire volumi di attività attestati sui picchi massimi riscontrati nel corso dell'operatività ordinaria.
23	Riservatezza	Nel caso in cui il servizio richiesto dal Cliente Banca preveda la presenza di processi a rilevanza sistemica, Telecom Italia deve prevedere nel contratto personalizzato come service element aggiuntivo che i siti alternativi che garantiscono la continuità operativa del servizio ubicati all'esterno dell'area metropolitana nella quale sono presenti i siti primari utilizzino servizi di supporto (energia, reti di comunicazione, ecc.) distinti da quelli impiegati all'interno dal sito in produzione.
24	Riservatezza	Nel caso in cui il servizio richiesto dal Cliente Banca preveda la presenza di processi a rilevanza sistemica e qualora i siti alternativi fossero ubicati all'interno dell'area metropolitana in cui sono presenti i siti primari, Telecom Italia deve prevedere nel contratto personalizzato come service element aggiuntivo l'esecuzione di analisi del rischio volte ad attestare come trascurabile il rischio di una eventuale contemporanea indisponibilità dei siti primari e alternativi. Tale attività di analisi del rischio deve essere documentata e supportata da pareri di terze parti qualificate (ad es. Protezione Civile, accademici, professionisti).
26 + 27	Riservatezza	Nel caso in cui il servizio richiesto dal Cliente Banca preveda la presenza di processi a rilevanza sistemica, Telecom Italia deve prevedere nel contratto personalizzato come service element aggiuntivo l'implementazione di meccanismi e la definizione di procedure in grado di garantire che il tempo di ripristino di tali processi non superi le quattro ore e che il tempo di ripartenza di tali processi non superi le due ore per le componenti di servizio di propria pertinenza.
28	Riservatezza	Nel caso in cui il servizio richiesto dal Cliente Banca preveda la presenza di processi a rilevanza sistemica, Telecom Italia deve prevedere nel contratto personalizzato come service element aggiuntivo (alternativamente ai meccanismi di ripristino e di ripartenza) l'implementazione di meccanismi di duplicazione dei dati in linea, con l'obiettivo di eliminare o ridurre al minimo la perdita di informazioni. L'intervallo di tempo che intercorre tra il tempo di ripristino e il momento dell'incidente deve essere nullo o prossimo allo zero, in linea con le richieste del Cliente.

Misure Dati Bancari

Data: 22.06.2022

ID MISURA Circolare 263	Categoria	Testo requisito
29	Riservatezza	Nel caso in cui il servizio richiesto dal Cliente Banca preveda la presenza di processi a rilevanza sistemica, Telecom Italia deve prevedere nel contratto personalizzato come service element aggiuntivo l'esecuzione di attività di assessment annuali volte a verificare l'affidabilità dei presidi di continuità operativa (in relazione ai processi a rilevanza sistemica). Solo se esplicitamente richiesto dalla Banca, tali attività devono prevedere la partecipazione attiva ai test da parte di eventuali enti terzi indicati dalla stessa.