



UNIMORE
UNIVERSITÀ DEGLI STUDI DI
MODENA E REGGIO EMILIA

Dipartimento di scienze e metodi dell'ingegneria

Corso di laurea magistrale in
Ingegneria Gestionale

AA 2025/2026

**Governance del dato e migrazione cloud nel settore
bancario con l'analisi di un caso di studio sulla
trasformazione del Core Banking**

Relatore:

Francia Franco

Controrelatrice:

Monica Stefania

Laureando:

Fava Riccardo

Sommario

La crescente digitalizzazione del settore bancario sta spingendo gli istituti finanziari verso l'adozione di architetture cloud sempre più evolute, rendendo al contempo necessaria una gestione efficace della governance del dato e delle attività progettuali associate ai processi di trasformazione tecnologica. In questo contesto, la presente tesi analizza il ruolo del cloud computing, del data management e del project management all'interno di un progetto di migrazione verso una piattaforma cloud-native.

Il lavoro è stato sviluppato attraverso una prima analisi teorica dei concetti di cloud computing e data governance, approfondendo successivamente il framework Cloud Data Management Capabilities (CDMC) come modello di riferimento per la gestione dei dati in ambienti cloud. Tali elementi sono stati poi applicati all'analisi di un caso di studio reale relativo alla migrazione dei dati dei conti correnti di un importante gruppo bancario italiano verso una nuova piattaforma Core Banking.

L'analisi ha evidenziato un elevato livello di allineamento tra le pratiche adottate nel progetto e i principi definiti dal framework CDMC, in particolare per quanto riguarda governance, sicurezza, classificazione e protezione del dato. Sono tuttavia emerse alcune opportunità di miglioramento legate all'ottimizzazione di specifici processi operativi. Lo studio ha inoltre evidenziato il ruolo centrale del Project Management Office nel coordinamento delle attività progettuali e ha permesso di valutare il potenziale contributo dell'intelligenza artificiale generativa nel supporto alle attività di pianificazione, monitoraggio e reporting.

Il principale contributo dell'elaborato consiste nell'integrare l'analisi teorica dei modelli di data governance con l'osservazione diretta di un progetto reale di trasformazione cloud, fornendo una valutazione critica delle pratiche adottate e delle possibili evoluzioni future del project management e della gestione del dato nel settore bancario.

Indice

1. Introduzione

- 1.1 Obiettivi e struttura della tesi
- 1.2 Contesto della tesi: digital transformation e centralità del dato
- 1.3 Il ruolo del cloud nel settore bancario
- 1.4 Metodologia della ricerca

2. Cloud Computing e Data Management

- 2.1 Cloud Computing: evoluzione, modelli e caratteristiche
- 2.2 Benefici, rischi e criticità del Cloud Computing
- 2.3 Data Management nel cloud
- 2.4 Cloud Computing e Data Management nel settore bancario
- 2.5 Il quadro normativo per la gestione del dato nel settore bancario

3. Il Framework CDMC

- 3.1 Origini e obiettivi
- 3.2 Struttura del framework
- 3.3 Le sei componenti del Framework

4. Il PMO nei programmi di migrazione cloud e il contributo della Generative AI

- 4.1 Il project management nell'era della trasformazione digitale
- 4.2 Applicazioni della generative AI nelle attività di project management
- 4.3 Benefici, limiti e sfide d'adozione

5. Dal sistema legacy al cloud: migrazione dei dati dei conti correnti

- 5.1 Contesto e obiettivi del progetto

- 5.2 Principali risultati e benefici per la banca
- 5.3 Evoluzione dell'architettura IT: dal sistema legacy al cloud – based
- 5.4 Il piano di migrazione
- 5.5 Governance e coordinamento del progetto
- 5.6 Il ruolo del PMO all'interno del progetto

6. Confronto tra approcci teorici e realtà progettuale

- 6.1 Analisi del progetto rispetto al framework CDMC
- 6.2 Potenziale contributo della generative AI nella gestione del progetto
- 6.3 Sintesi delle evidenze emerse

7. Conclusioni

- 7.1 Considerazioni finali sul caso di studio
- 7.2 Il contributo del framework CDMC alla governance del dato
- 7.3 L'evoluzione del project management nell'era dell'intelligenza artificiale
- 7.4 Sviluppi futuri

Capitolo primo

1. Introduzione

Il presente capitolo introduce il contesto teorico e tecnologico all'interno del quale si sviluppa il lavoro di tesi, con particolare riferimento ai processi di trasformazione digitale che stanno interessando il settore bancario. Dopo aver delineato gli obiettivi dell'elaborato, l'attenzione viene posta sulla crescente centralità del dato come asset strategico e sul ruolo del cloud computing quale principale fattore abilitante dell'innovazione nei servizi finanziari.

Vengono inoltre approfondite le principali opportunità e criticità derivanti dall'adozione di infrastrutture cloud in ambito bancario, evidenziando gli impatti in termini di efficienza operativa, sicurezza, governance e gestione delle informazioni e vengono infine citate le metodologie utilizzate per la stesura del presente elaborato. Questo inquadramento iniziale costituisce la base teorica necessaria per comprendere le tematiche affrontate nei capitoli successivi e per contestualizzare il caso di studio analizzato nel corso della tesi.

1.1 Obiettivi e struttura della tesi

La presente tesi si colloca all'interno dell'ampio processo di trasformazione digitale che sta interessando il settore bancario, con particolare attenzione al ruolo sempre più centrale assunto dal dato e alle modalità con cui esso viene gestito in ambienti tecnologici evoluti. In questo contesto, l'adozione del cloud computing rappresenta una leva strategica fondamentale, in grado di abilitare nuovi modelli operativi e di supportare una gestione più efficiente, flessibile e scalabile delle informazioni. Tuttavia, tale evoluzione introduce al contempo nuove complessità, soprattutto in termini di governance, sicurezza e controllo del dato, aspetti particolarmente rilevanti in un settore altamente regolamentato come quello bancario.

Alla luce di queste considerazioni, il lavoro prende avvio da un'analisi generale dei concetti di cloud computing e data management, con l'obiettivo di delinearne le principali caratteristiche, i benefici e le criticità in un contesto trasversale. Questo inquadramento teorico costituisce la base per approfondire successivamente le specificità del settore bancario, in cui la gestione del dato assume un ruolo ancora più delicato e strategico. In tale ambito, viene analizzato il framework CDMC (*Cloud Data Management Capabilities*), che rappresenta un modello strutturato di riferimento per la gestione e il controllo dei dati in ambienti cloud, fornendo linee guida e best practice volte a garantire sicurezza, qualità e tracciabilità delle informazioni lungo il loro intero ciclo di vita.

Partendo da questo quadro teorico, la tesi si sviluppa ulteriormente attraverso l'analisi di un caso reale relativo a un progetto di migrazione in cloud dei dati dei conti correnti di un istituto bancario. Lo studio del caso consente di osservare concretamente come tali principi vengano applicati nella pratica, mettendo in evidenza le modalità operative adottate, le principali criticità affrontate e il ruolo svolto dal Project Management Office (PMO) nel coordinamento delle attività progettuali.

Per perseguire tali obiettivi, la tesi è stata strutturata in sette capitoli, organizzati secondo un percorso che conduce progressivamente dagli aspetti teorici a quelli applicativi. Nella prima parte dell'elaborato vengono introdotti i concetti fondamentali relativi al cloud computing, al data management e alle peculiarità del settore bancario, fornendo il quadro teorico necessario alla comprensione delle tematiche affrontate. Successivamente, l'attenzione si concentra sul framework Cloud Data Management Capabilities (CDMC), analizzato nelle sue componenti principali e nelle relative best practice per la gestione dei dati in ambienti cloud. Completa il quadro teorico un approfondimento dedicato al project management nei programmi di trasformazione digitale e al ruolo emergente dell'intelligenza artificiale generativa a supporto delle attività di pianificazione, coordinamento, monitoraggio e supporto decisionale. In tale ambito vengono analizzate le principali applicazioni della Generative AI nella gestione dei progetti, nonché i benefici e le sfide associate alla sua adozione nei contesti organizzativi complessi.

La seconda parte della tesi è dedicata all'analisi di un caso di studio reale riguardante un progetto di migrazione in cloud dei dati dei conti correnti di un importante gruppo bancario italiano. In tale contesto vengono approfonditi il ruolo del Project Management

Office (PMO), l'evoluzione dell'architettura tecnologica, il piano di migrazione e le attività di governance adottate per garantire il successo dell'iniziativa. Sulla base delle conoscenze acquisite nella parte teorica, viene infine sviluppata una valutazione critica del progetto, finalizzata a evidenziare possibili aree di miglioramento e ad analizzare come determinati approcci, metodologie o strumenti avrebbero potuto contribuire ad aumentarne ulteriormente l'efficienza e l'efficacia.

Ciascun capitolo è articolato in specifici paragrafi che consentono di approfondire in modo progressivo i diversi temi trattati. Inoltre, l'elaborato è corredato da figure e schemi esplicativi che supportano la comprensione degli argomenti analizzati, con particolare riferimento agli aspetti architetturali, organizzativi e progettuali del caso di studio. Il lavoro si conclude infine con un capitolo dedicato alle conclusioni, nel quale vengono sintetizzati i principali risultati emersi e formulate alcune considerazioni finali sulle prospettive future della gestione dei dati e dei progetti di migrazione cloud nel settore bancario.

In questa prospettiva, viene inoltre proposta una riflessione sull'evoluzione dei modelli di gestione dei progetti e della governance dei dati, anche alla luce delle più recenti innovazioni tecnologiche, tra cui l'introduzione di strumenti basati su intelligenza artificiale.

1.2 Contesto della tesi: digital transformation e centralità del dato

La digitalizzazione rappresenta oggi un fenomeno strutturale e irreversibile che sta trasformando profondamente tutti i settori economici, inclusi quelli tradizionalmente più conservativi come quello bancario e finanziario. Tecnologie emergenti quali l'intelligenza artificiale, i big data, la blockchain e il cloud computing sono passate in breve tempo dall'essere concetti teorici o trend emergenti a elementi concreti e abilitanti del cambiamento, con un impatto significativo sui modelli operativi e strategici delle istituzioni finanziarie.

In questo scenario, il dato assume un ruolo sempre più centrale, configurandosi come uno degli asset più rilevanti per la creazione di valore. Le istituzioni finanziarie si trovano oggi a gestire volumi crescenti di informazioni provenienti da molteplici fonti, interne ed esterne, che devono essere raccolte, integrate, analizzate e valorizzate in

modo efficace. Il dato non rappresenta più soltanto un supporto ai processi operativi, ma diventa un elemento chiave per abilitare decisioni strategiche, sviluppare nuovi prodotti e servizi e migliorare la relazione con il cliente.

L'intensificarsi della competizione, unitamente all'ingresso di nuovi attori come le fintech, ha spinto le banche a ripensare i propri modelli di business, orientandosi verso soluzioni più aperte e collaborative, come il paradigma del *banking-as-a-platform*. In questo contesto, gli istituti finanziari integrano servizi offerti da partner terzi, rendendo ancora più cruciale la capacità di gestire e condividere dati in modo sicuro ed efficiente. La crescente interconnessione tra attori diversi amplifica infatti la necessità di garantire qualità, coerenza e tracciabilità delle informazioni lungo l'intero ciclo di vita del dato.

Parallelamente, anche il quadro normativo si evolve per rispondere ai nuovi rischi introdotti dalla digitalizzazione. Questo evidenzia come la gestione del dato non possa prescindere da un adeguato livello di controllo, sicurezza e governance, soprattutto in un settore caratterizzato da elevata sensibilità delle informazioni trattate.

Le aspettative dei clienti, sempre più orientate verso servizi digitali rapidi, accessibili e personalizzati, rappresentano un ulteriore fattore di spinta al cambiamento. Gli utenti richiedono esperienze fluide e integrate, spesso completamente gestibili tramite dispositivi mobili. In tale contesto, la capacità di analizzare i dati dei clienti in modo tempestivo e accurato diventa fondamentale per offrire servizi su misura, migliorare la customer experience e rafforzare la fidelizzazione.

La trasformazione digitale si configura quindi non solo come adozione di nuove tecnologie, ma come un processo più ampio che coinvolge l'intera organizzazione, richiedendo un'evoluzione dei processi interni, delle competenze e della cultura aziendale. [1]

La valorizzazione del dato richiede infatti strutture organizzative dedicate, modelli di governance chiari e strumenti tecnologici adeguati a garantirne qualità, disponibilità e sicurezza lungo tutto il ciclo di vita.

Nonostante i numerosi benefici, le banche si trovano ad affrontare anche importanti sfide. Tra queste emergono la resistenza al cambiamento, sia a livello organizzativo che da parte della clientela, e le crescenti problematiche legate alla sicurezza informatica.

L'aumento delle transazioni digitali e della quantità di dati trattati espone infatti le istituzioni a un rischio maggiore di attacchi e violazioni, rendendo indispensabile l'adozione di misure di protezione avanzate e di un approccio strutturato alla gestione

dei dati. In questo scenario, il cloud computing emerge come una delle principali tecnologie abilitanti della trasformazione digitale nel settore finanziario.

1.3 Il ruolo del cloud nel settore bancario

In tale contesto, il cloud computing si configura come uno dei principali fattori abilitanti della trasformazione digitale nel settore bancario. Esso consente l'accesso on-demand a risorse IT scalabili e flessibili, secondo modelli di servizio a consumo (*pay-as-you-go*), riducendo la necessità di investimenti in infrastrutture fisiche e semplificando la gestione operativa. Le istituzioni finanziarie stanno progressivamente migrando applicazioni e infrastrutture verso il cloud, sfruttandone le potenzialità per aumentare l'efficienza, migliorare la resilienza dei sistemi e accelerare l'innovazione tecnologica.

Uno dei principali vantaggi risiede nella capacità del cloud di supportare la gestione di grandi volumi di dati, caratteristica fondamentale in un settore in cui la produzione e l'archiviazione di informazioni sono in costante crescita. Le banche sono infatti tenute a conservare dati finanziari dettagliati per lunghi periodi, sia per esigenze operative sia per obblighi normativi. In questo scenario, il passaggio da infrastrutture *on-premise* a soluzioni cloud consente di ottimizzare i costi di storage e di elaborazione, offrendo al contempo maggiore flessibilità e capacità di adattamento alle esigenze di business.

Il cloud rappresenta inoltre un elemento chiave per l'adozione di tecnologie avanzate come l'intelligenza artificiale e il machine learning, che richiedono elevate capacità computazionali. Grazie alla disponibilità di infrastrutture altamente performanti, le banche possono sviluppare modelli predittivi, automatizzare processi operativi e migliorare le attività di analisi dei dati, contribuendo a una gestione più efficiente e proattiva delle informazioni. Questo rafforza ulteriormente la centralità del dato, che diventa il fulcro attorno al quale si sviluppano nuovi servizi e strategie competitive.

Dal punto di vista della sicurezza, il cloud ha raggiunto livelli di maturità tali da rappresentare una soluzione affidabile anche per un settore altamente regolamentato come quello bancario. I principali provider offrono meccanismi avanzati di protezione, tra cui crittografia dei dati, sistemi di monitoraggio continuo e strumenti di rilevamento delle anomalie. A ciò si aggiungono funzionalità integrate di *disaster recovery* e continuità operativa, che consentono alle istituzioni finanziarie di rispondere in modo

tempestivo a eventuali incidenti o interruzioni dei servizi. Parallelamente, le soluzioni cloud supportano il rispetto delle normative vigenti, facilitando l'implementazione di controlli e procedure richiesti dal contesto regolatorio.

Un ulteriore elemento di rilievo è rappresentato dalla possibilità di scalare rapidamente le risorse in funzione della domanda. Questo permette, ad esempio, di gestire picchi di utilizzo legati al lancio di nuovi servizi digitali senza dover sostenere investimenti anticipati in infrastrutture. In tal modo, le banche possono migliorare la propria reattività e offrire servizi più performanti, contribuendo a soddisfare le crescenti aspettative della clientela.

Nonostante i numerosi benefici, l'adozione del cloud comporta anche sfide significative, soprattutto in termini di integrazione con sistemi legacy e gestione della complessità architetturale. Per molti istituti, infatti, i sistemi informativi si sono sviluppati nel tempo in modo stratificato, rendendo il processo di migrazione particolarmente delicato. Tuttavia, proprio queste criticità stanno spingendo le banche a intraprendere percorsi di modernizzazione più ampi, in cui il cloud rappresenta un elemento centrale per il rinnovamento delle infrastrutture e dei modelli operativi.

In definitiva, il cloud computing si afferma come una leva strategica per il settore bancario, non solo per i benefici in termini di efficienza e riduzione dei costi, ma soprattutto per il suo ruolo nel supportare una gestione avanzata del dato. In un contesto in cui l'informazione rappresenta il principale fattore competitivo, la capacità di sfruttare appieno le potenzialità del cloud diventa un elemento chiave per garantire innovazione, sicurezza e sostenibilità nel lungo periodo.

1.4 Metodologia della ricerca

L'elaborato è stato sviluppato adottando una metodologia di ricerca di tipo qualitativo basata sullo studio di caso (case study research), approccio particolarmente indicato per analizzare fenomeni contemporanei all'interno del loro contesto reale, soprattutto quando i confini tra fenomeno e contesto risultano difficilmente distinguibili. Secondo Yin (2018), il caso di studio costituisce infatti una metodologia di ricerca particolarmente appropriata quando l'obiettivo non è quello di isolare le variabili

oggetto di analisi, bensì comprendere in modo approfondito le dinamiche attraverso cui un determinato fenomeno si manifesta in uno specifico contesto organizzativo.

L'adozione di tale approccio risulta coerente con gli obiettivi del presente elaborato, finalizzato ad analizzare un programma di migrazione verso un'infrastruttura cloud-native all'interno di un istituto bancario di grandi dimensioni. La complessità tecnica, organizzativa e gestionale dell'iniziativa, unitamente alla presenza di molteplici attori coinvolti e di numerose interdipendenze tra i diversi stream progettuali, rende infatti il caso di studio la metodologia più idonea per approfondire le modalità attraverso cui il progetto è stato pianificato, governato e realizzato.

La ricerca affiancata dal case study consente di integrare differenti fonti informative al fine di costruire una rappresentazione il più possibile completa del fenomeno analizzato. In coerenza con tale impostazione metodologica, il presente lavoro combina la revisione della letteratura scientifica e della normativa di riferimento con l'analisi diretta del caso di studio, sviluppata attraverso l'osservazione delle attività progettuali, la consultazione della documentazione interna e l'esperienza maturata dall'autore durante il periodo di tirocinio svolto presso il Project Management Office coinvolto nel programma di trasformazione.

L'analisi è stata sviluppata seguendo un approccio progressivo. Dopo aver definito il quadro teorico relativo alla trasformazione digitale, al cloud computing, alla governance del dato e ai principali riferimenti normativi europei, l'elaborato approfondisce il caso di studio, analizzando le caratteristiche del programma di migrazione, il modello di governance adottato, il ruolo del Project Management Office e l'applicazione del framework Cloud Data Management Capabilities (CDMC) quale strumento di valutazione delle pratiche di data governance implementate nel progetto.

L'impiego del case study ha quindi consentito di mettere in relazione i principali contributi teorici con un'esperienza progettuale concreta, evidenziando come i modelli di governance del dato, le metodologie di project management e le tecnologie cloud trovino applicazione operativa all'interno di un programma di trasformazione digitale caratterizzato da elevati livelli di complessità organizzativa e tecnologica. [2]

Capitolo secondo

2. Cloud computing e data management

Il presente capitolo analizza il paradigma del cloud computing e il ruolo del data management all'interno dei moderni processi di trasformazione digitale. In una prima fase verranno approfondite l'evoluzione storica del cloud computing, le sue principali caratteristiche e i modelli di servizio maggiormente diffusi, evidenziandone funzionamento e ambiti applicativi. Successivamente, l'attenzione sarà rivolta ai benefici e alle criticità connesse all'adozione del cloud, con particolare riferimento agli aspetti di sicurezza, governance e gestione operativa delle infrastrutture digitali.

Il capitolo proseguirà poi con un approfondimento sul tema del data management in ambienti cloud, analizzando le principali pratiche di gestione, protezione e valorizzazione del dato, nonché i modelli di governance necessari a garantirne qualità, sicurezza e conformità normativa, tali concetti verranno poi contestualizzati nel settore bancario, evidenziando il ruolo strategico assunto dal cloud computing e dalla gestione dei dati nei processi di innovazione e modernizzazione delle istituzioni finanziarie per concludere infine con un'analisi del quadro normativo di riferimento a livello europeo.

2.1 Cloud Computing: modelli, caratteristiche ed evoluzione

Il cloud computing è un modello che consente un accesso di rete onnipresente, pratico e su richiesta a un insieme condiviso di risorse informatiche configurabili, quali reti, server, capacità di archiviazione, applicazioni e servizi, che possono essere rapidamente rese disponibili e rilasciate con un minimo sforzo di gestione o di interazione con il fornitore del servizio. [3]

Sebbene la diffusione su larga scala del cloud sia un fenomeno relativamente recente, le sue origini teoriche risalgono agli anni Sessanta, periodo in cui iniziò a svilupparsi l'idea di rendere le risorse computazionali condivise e accessibili a più utenti contemporaneamente.

In una fase iniziale, i sistemi informatici erano caratterizzati da elevati costi di acquisizione e gestione, motivo per cui venivano utilizzati prevalentemente da grandi organizzazioni o istituzioni governative. In tale contesto nacquero i primi studi sulla condivisione delle risorse hardware, con l'obiettivo di massimizzarne l'utilizzo e ridurre gli sprechi. Questo approccio trovò una concreta applicazione negli anni Settanta attraverso lo sviluppo delle tecnologie di virtualizzazione, che permisero di eseguire più sistemi operativi e applicazioni su una stessa macchina fisica mediante la creazione di macchine virtuali. La virtualizzazione rappresentò un passaggio fondamentale per l'evoluzione del cloud computing, poiché introdusse il concetto di infrastruttura astratta e dinamicamente allocabile.

Parallelamente, il progresso delle reti di telecomunicazione e la crescente diffusione di Internet contribuirono a trasformare progressivamente il modello tradizionale di elaborazione locale in un sistema distribuito e accessibile da remoto. Negli anni Novanta, con l'affermazione del World Wide Web e dei modelli client-server, le tecnologie necessarie al funzionamento del cloud raggiunsero un livello di maturità sufficiente per consentire la nascita dei primi servizi erogati via rete. Fu in questo periodo che iniziò a diffondersi il concetto di software accessibile online, anticipando i moderni modelli di distribuzione basati sul cloud.

La vera affermazione del cloud computing avvenne tuttavia nei primi anni Duemila, grazie alla crescente necessità di gestire volumi sempre maggiori di dati e alla diffusione di infrastrutture Internet ad alta velocità. Da quel momento il cloud si è evoluto rapidamente, passando da semplice soluzione per l'hosting di applicazioni a ecosistema tecnologico complesso, capace di supportare servizi avanzati legati all'intelligenza artificiale, all'Internet of Things, ai big data e all'analisi predittiva. Oggi il cloud computing costituisce uno degli elementi fondamentali dell'economia digitale e continua a evolversi verso architetture sempre più distribuite, automatizzate e integrate.

Dal punto di vista concettuale, il cloud computing può essere definito come un modello di erogazione di risorse informatiche tramite Internet, accessibili on-demand e secondo logiche di pagamento basate sull'effettivo utilizzo. Tali risorse comprendono capacità di elaborazione, storage, networking, piattaforme software e applicazioni, che possono essere rapidamente allocate e rilasciate senza la necessità di investimenti diretti in infrastrutture fisiche. [4]

L'evoluzione del cloud computing ha portato alla definizione di differenti modelli di servizio, progettati per rispondere a esigenze specifiche in termini di controllo, gestione e utilizzo delle risorse IT. I principali modelli attualmente diffusi sono Infrastructure as a Service (IaaS), Platform as a Service (PaaS) e Software as a Service (SaaS). Tali modelli si differenziano principalmente per il livello di gestione affidato al provider cloud e per il grado di responsabilità mantenuto dall'utente finale.

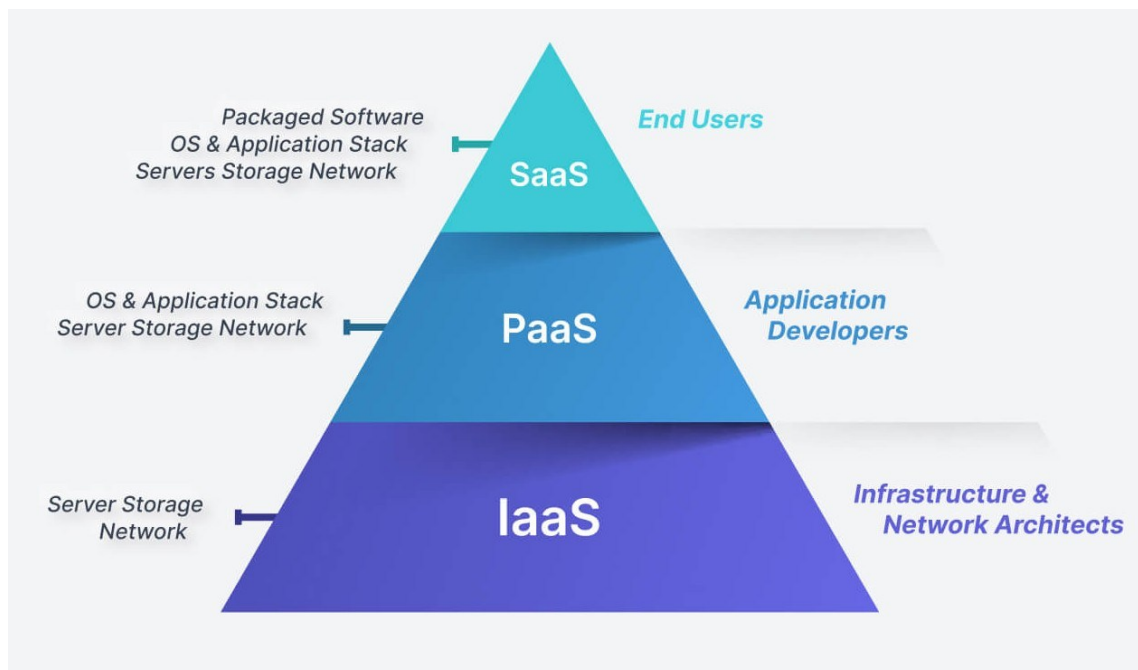


Figura 1. Modelli di cloud computing (estratta da: [IaaS-vs.-PaaS-vs.-SaaS-Comparison-1.jpg](#))

L'Infrastructure as a Service (IaaS) è un modello di servizio che consente all'utente di disporre di risorse fondamentali di elaborazione, archiviazione, rete e altre risorse informatiche di base, sulle quali può distribuire ed eseguire software arbitrario, inclusi sistemi operativi e applicazioni. L'utente non gestisce né controlla l'infrastruttura cloud sottostante, ma mantiene il controllo sui sistemi operativi, sulle applicazioni distribuite, sullo storage e, in alcuni casi, su specifici componenti di rete, come i firewall host. [3]

L'IaaS consente alle organizzazioni di sostituire le tradizionali infrastrutture on-premise con ambienti virtualizzati altamente scalabili e accessibili on-demand. Le risorse possono essere allocate rapidamente e modificate in funzione delle esigenze operative, evitando investimenti elevati in hardware fisici e riducendo i costi legati alla manutenzione delle infrastrutture.

Uno dei principali vantaggi di questo modello è rappresentato dalla flessibilità. Le aziende possono aumentare la capacità elaborativa o lo spazio di archiviazione in tempi molto ridotti, adattandosi rapidamente ai cambiamenti della domanda. Questo approccio risulta particolarmente utile in presenza di carichi di lavoro variabili o temporanei, poiché consente di utilizzare esclusivamente le risorse necessarie.

Dal punto di vista operativo, l'IaaS offre anche benefici legati all'affidabilità e alla continuità del servizio. Le infrastrutture cloud sono generalmente distribuite su più data center e integrate con sistemi di backup e disaster recovery, garantendo elevati livelli di disponibilità e ridondanza dei dati. Inoltre, la virtualizzazione permette di migliorare l'utilizzo delle risorse fisiche e di semplificare le attività di gestione e monitoraggio.

Le principali applicazioni del modello IaaS includono l'hosting di applicazioni web, l'analisi di grandi quantità di dati, gli ambienti di sviluppo e test e le attività di high performance computing. In tutti questi casi, il cloud infrastrutturale permette di accedere rapidamente a elevate capacità computazionali senza dover sostenere costi infrastrutturali permanenti.

Il Platform as a Service (PaaS) è un modello di servizio che permette all'utente di distribuire sull'infrastruttura cloud applicazioni sviluppate o acquisite, utilizzando linguaggi di programmazione, librerie, servizi e strumenti messi a disposizione dal provider. L'utente non gestisce né controlla l'infrastruttura cloud sottostante, comprese reti, server, sistemi operativi e risorse di archiviazione, ma mantiene il controllo sulle applicazioni distribuite e, ove previsto, sulle configurazioni dell'ambiente di hosting delle stesse. [3]

In questo modello, gli utenti non devono gestire direttamente l'infrastruttura hardware o le componenti di base del sistema, potendosi concentrare principalmente sulle attività di sviluppo e implementazione del software. Il provider si occupa della gestione delle risorse infrastrutturali, degli aggiornamenti e della manutenzione della piattaforma, semplificando significativamente le attività operative.

Il principale vantaggio del PaaS risiede nella velocità di sviluppo e nella riduzione della complessità tecnica. Gli sviluppatori possono creare, testare e distribuire applicazioni in ambienti già predisposti, riducendo i tempi di configurazione e migliorando la collaborazione tra i gruppi di lavoro. Inoltre, il modello favorisce l'adozione di metodologie agili e pratiche di sviluppo continuo.

Le piattaforme PaaS risultano particolarmente rilevanti anche nell'ambito dell'intelligenza artificiale e dell'analisi avanzata dei dati, poiché mettono a disposizione strumenti già integrati per l'elaborazione di modelli, l'automazione dei processi e la gestione dei flussi informativi.

Dal punto di vista architetturale, il PaaS si basa su un'infrastruttura cloud integrata con strumenti software e interfacce di gestione accessibili tramite rete. La presenza di middleware e servizi condivisi facilita la comunicazione tra applicazioni e consente a più team di operare contemporaneamente sullo stesso ambiente di sviluppo.

Le principali applicazioni del modello PaaS riguardano lo sviluppo di applicazioni web e mobile, la realizzazione di servizi digitali scalabili e la gestione di ambienti collaborativi per la programmazione e il testing.

Il Software as a Service (SaaS) è un modello di servizio che consente all'utente di utilizzare applicazioni eseguite sull'infrastruttura cloud del provider. Le applicazioni sono accessibili da diversi dispositivi client tramite un'interfaccia leggera, come un browser web, oppure attraverso specifiche interfacce di programmazione. L'utente non gestisce né controlla l'infrastruttura cloud sottostante, incluse reti, server, sistemi operativi, capacità di archiviazione e funzionalità dell'applicazione, fatta eccezione per eventuali limitate impostazioni di configurazione personalizzabili. [3]

Nel modello SaaS, il provider gestisce integralmente l'infrastruttura, la manutenzione del software, gli aggiornamenti, la sicurezza e i backup, mentre l'utente si limita all'utilizzo dell'applicazione. Questo approccio consente di ridurre significativamente la complessità tecnica e i costi di gestione per le organizzazioni.

Uno dei principali vantaggi del SaaS è rappresentato dalla semplicità di accesso. Le applicazioni possono essere utilizzate da qualsiasi dispositivo connesso a Internet, favorendo mobilità, collaborazione e continuità operativa. Inoltre, i modelli di pagamento basati su abbonamento permettono alle aziende di sostenere costi proporzionati all'effettivo utilizzo del servizio.

Dal punto di vista tecnico, molte soluzioni SaaS adottano architetture multi-tenant, in cui una singola istanza del software serve più utenti contemporaneamente. Questo consente di ottimizzare l'utilizzo delle risorse e ridurre i costi operativi, mantenendo al contempo elevati livelli di scalabilità.

Le applicazioni SaaS trovano impiego in numerosi ambiti, tra cui gestione aziendale, customer relationship management, collaborazione documentale, produttività individuale e gestione dei processi organizzativi. La diffusione di questo modello è stata favorita dalla crescente esigenza di accesso remoto alle applicazioni e dalla necessità di garantire continuità operativa anche in contesti di lavoro distribuito.

I modelli IaaS, PaaS e SaaS si differenziano principalmente per il livello di controllo e responsabilità attribuito all'utente finale. Nel modello IaaS, l'organizzazione mantiene un elevato grado di controllo sull'ambiente software e sulle configurazioni di sistema, mentre il provider gestisce esclusivamente l'infrastruttura fisica e virtuale. Nel PaaS, invece, il provider si occupa anche della piattaforma software e degli strumenti di sviluppo, lasciando all'utente la gestione delle applicazioni e dei dati. Infine, nel SaaS, la quasi totalità delle componenti tecnologiche viene gestita dal provider, mentre il cliente utilizza direttamente il software come servizio.

La scelta del modello più adatto dipende dalle esigenze specifiche dell'organizzazione, dal livello di personalizzazione richiesto, dalle competenze tecniche disponibili e dal grado di controllo desiderato sulle infrastrutture e sui dati.

Negli ultimi anni, l'evoluzione del cloud computing ha inoltre portato alla diffusione di modelli sempre più avanzati e integrati, caratterizzati da elevati livelli di automazione, orchestrazione delle risorse e distribuzione geografica dei servizi. Tecnologie emergenti come edge computing (modello in cui la potenza di calcolo viene mantenuta il più vicino possibile alla fonte dei dati per minimizzare la latenza e diminuire i tempi di risposta), intelligenza artificiale e Internet of Things stanno contribuendo a ridefinire ulteriormente il ruolo del cloud, trasformandolo in un'infrastruttura sempre più centrale per il funzionamento delle organizzazioni moderne e per la gestione dei dati su larga scala. [5]

2.2 Benefici, rischi e criticità del cloud computing

L'adozione del cloud computing rappresenta oggi una delle principali direttrici di innovazione per le organizzazioni pubbliche e private. La scelta di migrare servizi e dati verso infrastrutture cloud non costituisce esclusivamente una decisione tecnologica, ma implica una valutazione strategica che richiede di bilanciare benefici economici, flessibilità operativa e rischi connessi alla sicurezza, alla governance e alla continuità dei servizi. [6]

La possibilità di accedere a risorse informatiche in modalità on-demand, secondo modelli flessibili e scalabili, ha modificato profondamente il modo in cui le imprese progettano, gestiscono ed evolvono le proprie infrastrutture IT. Tuttavia, accanto ai numerosi vantaggi introdotti da queste tecnologie, emergono anche rischi e criticità che richiedono un approccio strutturato in termini di governance, sicurezza e gestione operativa.

Tra i principali benefici del cloud computing vi è innanzitutto la scalabilità delle risorse. Le organizzazioni possono aumentare o ridurre capacità computazionale, storage e servizi in funzione delle reali esigenze operative, evitando investimenti iniziali elevati in infrastrutture fisiche. Questo consente una maggiore flessibilità nella gestione dei carichi di lavoro e permette di rispondere rapidamente a variazioni della domanda o all'introduzione di nuovi servizi digitali. Il modello pay-per-use contribuisce inoltre a trasformare i costi IT da investimenti fissi a costi variabili, favorendo una maggiore ottimizzazione economica e una gestione più efficiente delle risorse.

Un ulteriore vantaggio riguarda la velocità di implementazione e l'accesso continuo all'innovazione tecnologica. I provider cloud rendono disponibili piattaforme, servizi e strumenti costantemente aggiornati, consentendo alle aziende di adottare rapidamente nuove tecnologie senza dover gestire direttamente attività di manutenzione o aggiornamento infrastrutturale. In questo modo il cloud favorisce processi di innovazione continua, riducendo il time-to-market di applicazioni e servizi digitali.

Il cloud computing assume inoltre un ruolo centrale nella gestione e valorizzazione dei dati. La disponibilità di infrastrutture altamente performanti permette di archiviare, elaborare e analizzare grandi volumi di informazioni in modo rapido ed efficiente. Questo aspetto risulta particolarmente rilevante in contesti caratterizzati da una forte crescita dei dati prodotti, nei quali l'accesso tempestivo alle informazioni rappresenta

un elemento strategico per il supporto alle decisioni aziendali. Le piattaforme cloud consentono infatti di integrare strumenti avanzati di analytics, machine learning e intelligenza artificiale, ampliando le possibilità di utilizzo del dato e favorendo lo sviluppo di modelli decisionali data-driven.

Dal punto di vista operativo, il cloud migliora anche accessibilità e collaborazione. Le applicazioni e i dati possono essere resi disponibili in modo distribuito, favorendo il lavoro remoto, l'integrazione tra team geograficamente distanti e la condivisione delle informazioni in tempo reale. Tale caratteristica ha acquisito crescente rilevanza negli ultimi anni, contribuendo a rendere le organizzazioni più flessibili e resilienti.

Nonostante questi benefici, l'adozione del cloud comporta anche una serie di rischi e criticità che devono essere attentamente valutati. Uno degli aspetti più rilevanti riguarda la sicurezza delle informazioni. Sebbene i principali provider cloud offrano livelli di protezione elevati, il rischio di violazioni dei dati, accessi non autorizzati o configurazioni errate rimane significativo. In molti casi, infatti, le vulnerabilità non derivano direttamente dall'infrastruttura del provider, bensì da errori di gestione, policy di accesso non adeguate o assenza di controlli strutturati da parte dell'organizzazione cliente.

In questo contesto assume particolare importanza il modello di shared responsibility, secondo cui la sicurezza dell'ambiente cloud è condivisa tra provider e cliente. Il fornitore garantisce la protezione dell'infrastruttura fisica e dei servizi di base, mentre l'organizzazione utilizzatrice mantiene la responsabilità relativa alla configurazione delle risorse, alla gestione delle identità digitali, alla protezione dei dati e al monitoraggio degli accessi. La mancanza di consapevolezza rispetto a questa suddivisione delle responsabilità rappresenta una delle principali cause di incidenti e problematiche operative negli ambienti cloud.

Un ulteriore elemento critico riguarda il rischio di perdita o indisponibilità dei dati. Errori umani, configurazioni non corrette o strategie di backup insufficienti possono compromettere la continuità operativa e la disponibilità delle informazioni. Per questo motivo risultano fondamentali adeguate strategie di disaster recovery e business continuity, supportate da meccanismi automatici di replica, backup periodici e piani di ripristino testati regolarmente.

Tra le criticità maggiormente discusse vi è inoltre il cosiddetto vendor lock-in, ovvero la dipendenza tecnologica da un singolo provider cloud. L'utilizzo di servizi proprietari

può rendere complesso un eventuale trasferimento verso altre piattaforme, limitando la flessibilità dell'organizzazione e aumentando la dipendenza contrattuale e tecnologica dal fornitore scelto. Per ridurre tale rischio, molte aziende adottano strategie ibride o multi-cloud, orientate a distribuire servizi e applicazioni su ambienti differenti, aumentando interoperabilità e resilienza.

Anche la gestione dei costi rappresenta un aspetto particolarmente delicato. Sebbene il cloud permetta una riduzione degli investimenti iniziali, un utilizzo non controllato delle risorse può determinare incrementi significativi della spesa operativa. Ambienti di test non dismessi, risorse sovradimensionate o mancanza di monitoraggio possono infatti compromettere i benefici economici inizialmente previsti. Di conseguenza, la governance finanziaria del cloud assume un ruolo fondamentale per garantire sostenibilità ed efficienza nel lungo periodo.

L'adozione del cloud richiede inoltre una profonda evoluzione culturale e organizzativa. Le organizzazioni devono sviluppare nuove competenze tecniche e ridefinire processi operativi e modelli di governance. Tematiche come automazione, Infrastructure as Code (IaC), gestione centralizzata delle identità e processi CI/CD diventano elementi essenziali per garantire affidabilità, sicurezza e qualità operativa. La carenza di competenze interne rappresenta pertanto una delle principali criticità nei percorsi di migrazione e trasformazione cloud.

Infine, particolare attenzione deve essere posta agli aspetti normativi (vedi capitolo 2.5) e di compliance. In settori regolamentati, come quello bancario, la gestione dei dati in ambienti cloud deve rispettare requisiti stringenti in termini di tracciabilità, protezione delle informazioni, localizzazione dei dati e auditabilità dei processi. Ciò rende necessaria l'adozione di modelli di governance strutturati e di controlli continui volti a garantire conformità alle normative vigenti.

In definitiva, il cloud computing non rappresenta solamente un'evoluzione tecnologica, ma un cambiamento più ampio che coinvolge processi, organizzazione e modelli di gestione del dato. I benefici derivanti da scalabilità, innovazione ed efficienza possono essere pienamente raggiunti soltanto attraverso un approccio consapevole e strutturato, capace di integrare aspetti tecnologici, organizzativi e normativi all'interno di una strategia di trasformazione digitale coerente e sostenibile. [7]

2.3 Data management nel cloud

L'adozione del cloud computing ha trasformato non solo le infrastrutture tecnologiche delle organizzazioni, ma anche le modalità con cui i dati vengono raccolti, archiviati, elaborati e distribuiti. In un contesto caratterizzato da volumi di informazioni sempre più elevati e dalla necessità di garantire accessibilità e rapidità di elaborazione, la gestione dei dati assume un ruolo strategico fondamentale.

La possibilità di accedere a grandi quantità di dati provenienti da fonti eterogenee ha portato le organizzazioni a investire sempre più in sistemi di data management capaci di garantire efficienza operativa, qualità delle informazioni e supporto ai processi decisionali. In ambienti cloud, tali sistemi consentono di automatizzare numerosi processi aziendali, riducendo errori e inefficienze nella gestione delle transazioni e migliorando la scalabilità delle infrastrutture.

Uno degli aspetti centrali della gestione dei dati riguarda l'architettura informativa, ossia l'insieme di componenti, regole e tecnologie utilizzate per organizzare e governare i dati all'interno dell'organizzazione. In ambito cloud, le aziende possono adottare differenti soluzioni di archiviazione e gestione, come database operativi, data warehouse e data lake, scegliendo configurazioni flessibili e virtualizzate in funzione delle esigenze operative e analitiche. Parallelamente, la modellazione dei dati permette di rappresentare logicamente relazioni, flussi informativi e processi, favorendo integrazione e interoperabilità tra sistemi differenti.

La crescente centralità del dato rende inoltre necessaria l'adozione di strutture di governance in grado di garantire qualità, sicurezza e conformità normativa lungo tutto il ciclo di vita delle informazioni. La data governance comprende infatti l'insieme di policy, procedure e responsabilità finalizzate a disciplinare l'accesso, l'utilizzo e la protezione dei dati all'interno dell'organizzazione. In ambienti cloud, tali attività assumono un'importanza ancora maggiore, poiché i dati risultano distribuiti tra piattaforme, applicazioni e servizi differenti, spesso accessibili da più utenti e dispositivi contemporaneamente.

Tra gli elementi fondamentali della governance dei dati rientra il controllo degli accessi, che consente di definire chi può visualizzare, modificare o utilizzare determinate informazioni. L'adozione di sistemi di autenticazione avanzata, criteri di autorizzazione granulari e politiche basate sul principio del least privilege permette di limitare il rischio

di accessi non autorizzati e di proteggere i dati sensibili. A questi strumenti si affiancano meccanismi di cifratura, monitoraggio continuo delle attività e segmentazione delle reti, finalizzati a rafforzare ulteriormente il livello di sicurezza delle infrastrutture cloud.

Un altro aspetto centrale riguarda la qualità del dato. Affinché le informazioni possano supportare correttamente processi operativi e decisionali, è necessario che esse siano accurate, complete, ridondanti, leggibili, accessibili, consistenti, utili e affidabili. [8]

La presenza di dati duplicati, incompleti o inconsistenti può infatti compromettere l'affidabilità delle analisi e generare inefficienze nei processi aziendali. Per questo motivo, le organizzazioni implementano controlli e procedure di validazione finalizzati a verificare la correttezza delle informazioni sia nella fase di acquisizione sia durante il loro utilizzo. La gestione della qualità dei dati assume particolare rilevanza negli ambienti cloud, dove le informazioni vengono continuamente condivise e integrate tra sistemi differenti.

In tale contesto, assumono rilevanza anche strumenti come il data lineage e i cataloghi dati. Il data lineage consente di tracciare l'origine dei dati, le trasformazioni subite e i flussi attraverso cui le informazioni vengono trasferite tra sistemi e applicazioni. Questa attività risulta particolarmente importante nei processi di audit e compliance, poiché permette di ricostruire in modo trasparente il percorso del dato lungo tutto il suo ciclo di vita. I cataloghi dati, invece, rappresentano raccolte centralizzate di metadati e informazioni relative alle risorse informative aziendali, facilitando individuazione, classificazione e utilizzo dei dati all'interno dell'organizzazione.

La gestione del ciclo di vita del dato costituisce un ulteriore elemento fondamentale. Le informazioni devono infatti essere controllate e monitorate fin dalla fase di acquisizione, conservate per periodi coerenti con gli obblighi normativi e successivamente eliminate quando non più necessarie. In questo senso, le organizzazioni definiscono policy specifiche relative alla conservazione, alla replica e alla cancellazione dei dati, garantendo continuità operativa e conformità alle normative vigenti in materia di protezione delle informazioni.

Anche le modalità di elaborazione e distribuzione dei dati possono variare in funzione delle esigenze operative. I sistemi basati su flussi di dati in tempo reale consentono di trasmettere rapidamente gli aggiornamenti man mano che si verificano, risultando particolarmente utili in applicazioni che richiedono tempestività e monitoraggio continuo. Gli aggiornamenti in batch, invece, prevedono l'elaborazione dei dati in

gruppi e vengono utilizzati soprattutto in ambiti analitici e nei processi di data warehousing, dove è necessario consolidare grandi quantità di informazioni prima della loro elaborazione.

In ambienti cloud assume inoltre particolare rilevanza la gestione dei dati master (*Master Data Management*), ovvero l'insieme delle attività finalizzate a garantire coerenza e uniformità dei dati aziendali fondamentali, come quelli relativi a clienti, prodotti o partner commerciali. La sincronizzazione corretta di queste informazioni tra sistemi differenti rappresenta un elemento essenziale per assicurare affidabilità operativa e continuità dei processi aziendali.

La gestione dei dati nel cloud si basa sull'integrazione di tre componenti principali: archiviazione, elaborazione e networking. Le soluzioni di cloud storage consentono di memorizzare dati attraverso infrastrutture virtualizzate altamente scalabili, mentre le istanze di cloud computing permettono di elaborare le informazioni supportando attività operative, analitiche e applicazioni avanzate come intelligenza artificiale e machine learning. Parallelamente, il cloud networking garantisce la connessione sicura tra risorse, sistemi e ambienti differenti, attraverso reti virtuali e meccanismi di isolamento progettati per proteggere i carichi di lavoro e i dati in transito.

In questo scenario assume particolare importanza il modello di responsabilità condivisa, secondo il quale la sicurezza e la gestione del dato vengono ripartite tra provider cloud e organizzazione cliente. Il provider è responsabile della protezione dell'infrastruttura fisica e dei servizi di base, mentre il cliente mantiene il controllo sulla configurazione degli ambienti, sulla gestione degli accessi, sulla protezione delle applicazioni e sulle strategie di backup e disaster recovery. Questo modello richiede quindi elevata consapevolezza organizzativa e competenze specifiche, poiché molte problematiche di sicurezza derivano non tanto dall'infrastruttura cloud stessa, quanto da configurazioni errate o da una gestione inadeguata degli ambienti.

Per questo motivo, tra le principali best practice nella gestione dei dati in ambienti cloud rientrano l'adozione di sistemi di monitoraggio continuo, l'automazione dei processi di controllo, la definizione di strategie di backup strutturate e l'implementazione di policy di accesso rigorose. A queste si aggiungono attività di formazione del personale, aggiornamento continuo delle competenze e sviluppo di modelli di governance capaci di garantire una gestione efficace, sicura e conforme delle informazioni.

Nel complesso, la gestione dei dati rappresenta oggi uno degli elementi centrali dell'ecosistema cloud. La capacità di garantire qualità, sicurezza, disponibilità e tracciabilità delle informazioni costituisce infatti un fattore strategico fondamentale per supportare processi decisionali, innovazione tecnologica e continuità operativa. In settori caratterizzati da elevata sensibilità del dato e forte regolamentazione, come quello bancario, tali aspetti assumono un'importanza ancora maggiore, rendendo indispensabile l'adozione di modelli strutturati e avanzati di data governance. [9]

2.4 Cloud Computing e Data Management nel settore bancario

Negli ultimi anni, il settore bancario ha progressivamente accelerato i propri processi di digitalizzazione, adottando nuove tecnologie per migliorare efficienza operativa, sicurezza e qualità dei servizi offerti alla clientela. In questo contesto, il cloud computing rappresenta uno degli strumenti più rilevanti, poiché consente alle istituzioni finanziarie di modernizzare le proprie infrastrutture tecnologiche e gestire in modo più efficace grandi volumi di dati.

Come visto nei paragrafi precedenti, il cloud computing permette di utilizzare risorse IT scalabili e accessibili on-demand, riducendo la necessità di investimenti elevati in infrastrutture fisiche. Questo aspetto assume particolare importanza nel settore bancario, dove gli istituti sono tenuti a conservare enormi quantità di dati finanziari e operativi per lunghi periodi di tempo, sia per esigenze di business sia per obblighi normativi. L'utilizzo di soluzioni cloud consente quindi di ottimizzare i costi legati allo storage e all'elaborazione delle informazioni, garantendo al tempo stesso maggiore flessibilità e capacità di adattamento.

Il dato rappresenta oggi uno degli asset più strategici per le banche. Le istituzioni finanziarie raccolgono quotidianamente informazioni provenienti da transazioni, strumenti di pagamento, applicazioni digitali e interazioni con i clienti. La capacità di gestire, integrare e analizzare questi dati in modo rapido ed efficiente permette di supportare processi decisionali, migliorare l'esperienza della clientela e sviluppare nuovi servizi digitali.

In questo scenario, il cloud computing diventa un importante abilitatore del data management, offrendo infrastrutture capaci di supportare attività di analisi avanzata,

business intelligence e automazione dei processi. Le banche possono infatti sfruttare tecnologie come intelligenza artificiale e machine learning per identificare anomalie, prevenire frodi, automatizzare attività ripetitive e sviluppare modelli predittivi utili a migliorare l'efficienza operativa e la qualità dei servizi.

Parallelamente, molte istituzioni finanziarie stanno utilizzando il cloud per avviare processi di modernizzazione delle proprie infrastrutture IT. Per anni, infatti, il settore bancario si è basato su sistemi legacy spesso rigidi, costosi da mantenere e difficilmente integrabili con tecnologie moderne. Il cloud consente di trasferire progressivamente dati e applicazioni verso ambienti più flessibili e scalabili, favorendo maggiore agilità operativa e capacità di innovazione.

Un ulteriore elemento di rilievo riguarda la sicurezza. Le banche gestiscono dati altamente sensibili e rappresentano frequentemente obiettivi di attacchi informatici e tentativi di frode. Le moderne piattaforme cloud integrano sistemi avanzati di protezione, tra cui crittografia dei dati, monitoraggio continuo, autenticazione avanzata e strumenti di rilevamento delle anomalie. Inoltre, come già evidenziato, il cloud facilita l'implementazione di strategie di disaster recovery e continuità operativa, aspetti fondamentali in un settore fortemente regolamentato.

Il cloud computing ha inoltre favorito la nascita di nuovi modelli di business digitali, come le banche completamente online e le realtà fintech, che basano gran parte dei propri servizi su infrastrutture cloud. Questo ha aumentato la competitività del settore e spinto anche gli istituti tradizionali ad accelerare i propri percorsi di innovazione.

Nonostante i numerosi vantaggi, l'adozione del cloud nel settore bancario richiede comunque particolare attenzione sotto il profilo della governance e della gestione del dato. La presenza di informazioni sensibili e la forte regolamentazione del settore rendono infatti indispensabile l'adozione di modelli strutturati di data management, capaci di garantire qualità, sicurezza, tracciabilità e conformità lungo tutto il ciclo di vita delle informazioni. [10]

2.5 Il quadro normativo per la gestione del dato nel settore bancario

La crescente digitalizzazione del settore bancario e la progressiva diffusione delle tecnologie cloud hanno determinato una significativa evoluzione del quadro normativo europeo in materia di gestione del dato, sicurezza informatica e resilienza operativa. La migrazione di applicazioni e informazioni verso infrastrutture distribuite, unitamente alla crescente centralità del dato nei processi decisionali e operativi, ha infatti reso necessario definire regole e standard volti a garantire elevati livelli di protezione, tracciabilità e controllo delle informazioni.

In tale contesto, le istituzioni finanziarie sono chiamate a operare all'interno di un sistema regolamentare articolato, caratterizzato dalla presenza di disposizioni che disciplinano aspetti differenti ma strettamente interconnessi della gestione del dato e delle tecnologie digitali. Il corpus normativo europeo applicabile alle organizzazioni bancarie che adottano soluzioni cloud si sviluppa principalmente attorno a tre ambiti fondamentali: la protezione dei dati personali, la gestione del rischio ICT e delle esternalizzazioni tecnologiche, e la sicurezza delle infrastrutture digitali critiche.

Regolamenti e linee guida quali il General Data Protection Regulation (GDPR), le disposizioni emanate dall'European Banking Authority (EBA), il Digital Operational Resilience Act (DORA) e la Direttiva NIS2 non devono essere considerati come strumenti indipendenti, bensì come componenti di un quadro normativo integrato finalizzato a garantire sicurezza, continuità operativa e conformità nell'utilizzo delle tecnologie digitali. La comprensione di tale contesto regolamentare risulta particolarmente rilevante ai fini del presente elaborato, poiché consente di contestualizzare le scelte progettuali adottate nel caso di studio e di interpretare il ruolo dei framework di governance del dato, quali il Cloud Data Management Capabilities (CDMC), nel supportare le organizzazioni nel perseguimento degli obiettivi di conformità e gestione del rischio.

Regolamento generale sulla protezione dei dati GDPR

Il Regolamento (UE) 2016/679, noto come General Data Protection Regulation (GDPR), costituisce il principale riferimento normativo europeo in materia di protezione dei dati personali. Entrato in applicazione il 25 maggio 2018, il regolamento ha introdotto un quadro normativo uniforme a livello europeo finalizzato a garantire un

elevato livello di tutela delle persone fisiche con riferimento al trattamento dei dati personali, rafforzando al contempo gli obblighi in capo alle organizzazioni che raccolgono, elaborano e conservano tali informazioni.

Nel settore bancario, caratterizzato dalla gestione di grandi volumi di dati altamente sensibili, il GDPR assume un ruolo particolarmente rilevante, influenzando direttamente le modalità con cui gli istituti finanziari progettano i propri sistemi informativi e definiscono i processi di gestione del dato. Le banche sono infatti chiamate a garantire che tutte le attività di trattamento siano svolte nel rispetto dei principi generali stabiliti dal regolamento, adottando adeguate misure organizzative e tecnologiche volte ad assicurare sicurezza, trasparenza e accountability.

Tra i principi maggiormente rilevanti nel contesto del presente elaborato figurano il principio di minimizzazione dei dati, previsto dall'articolo 5 comma 1 lettera c, secondo cui devono essere trattati esclusivamente i dati strettamente necessari al perseguimento delle finalità previste; il principio di limitazione della conservazione articolo 5 comma 1, che impone di mantenere i dati personali per un periodo non superiore a quello necessario rispetto agli scopi del trattamento; e il principio di privacy by design e by default, disciplinato dall'articolo 25, che richiede l'integrazione delle misure di protezione dei dati fin dalle prime fasi di progettazione dei sistemi e dei processi aziendali.

L'adozione di infrastrutture cloud e la realizzazione di programmi di migrazione, come quello analizzato nel presente lavoro, comportano ulteriori implicazioni in termini di conformità normativa. Il GDPR prevede infatti specifici requisiti relativi al trasferimento dei dati personali verso Paesi terzi, disciplinando le condizioni alle quali tali trasferimenti possono essere effettuati e introducendo particolari garanzie nel caso in cui i dati vengano trattati al di fuori dello Spazio Economico Europeo (art. 44-49). Inoltre, i rapporti tra l'istituto finanziario, in qualità di titolare del trattamento, e il provider cloud, che generalmente assume il ruolo di responsabile del trattamento (art. 30), devono essere formalizzati attraverso specifici accordi contrattuali che definiscano in modo chiaro ruoli, responsabilità e misure di sicurezza adottate.

Un ulteriore elemento di particolare rilevanza riguarda gli obblighi di documentazione e tracciabilità introdotti dal regolamento. Le organizzazioni sono infatti tenute a mantenere costantemente aggiornato il registro delle attività di trattamento, documentando i flussi informativi, le finalità perseguite e le misure di protezione

adottate. In un contesto caratterizzato dalla migrazione verso architetture cloud distribuite, tale attività assume un'importanza strategica, poiché consente di garantire piena visibilità sui dati trattati e di assicurare la conformità ai requisiti normativi lungo l'intero ciclo di vita dell'informazione. [11]

Linee guida EBA su outsourcing e cloud

Il quadro normativo europeo in materia di outsourcing nel settore bancario è stato progressivamente rafforzato dall'European Banking Authority (EBA) attraverso l'emanazione di specifiche linee guida finalizzate a disciplinare i rischi derivanti dall'esternalizzazione di funzioni aziendali a fornitori terzi, inclusi i provider di servizi cloud. In particolare, le Raccomandazioni EBA sul Cloud Outsourcing (EBA/REC/2017/03) e le successive Linee Guida sugli accordi di outsourcing (EBA/GL/2019/02) definiscono un insieme di requisiti volti a garantire un adeguato presidio dei rischi connessi all'utilizzo di servizi esternalizzati.

Le Linee Guida EBA sugli accordi di outsourcing introducono specifici obblighi per gli istituti finanziari, tra cui il mantenimento di un registro aggiornato degli accordi di outsourcing, la distinzione tra funzioni critiche o importanti e funzioni non critiche, l'esecuzione di attività di due diligence nei confronti dei fornitori prima della stipula del contratto e la definizione di adeguati meccanismi di controllo sulle eventuali sub-esternalizzazioni effettuate dal provider.

Nel contesto bancario, particolare rilevanza assume la classificazione delle funzioni esternalizzate come critiche o importanti, in quanto tali attività sono soggette a requisiti di governance e controllo più stringenti. Nel caso di progetti di migrazione del core banking verso infrastrutture cloud di tipo Infrastructure as a Service (IaaS), l'esternalizzazione riguarda infatti sistemi essenziali per l'erogazione dei servizi bancari e richiede pertanto l'adozione di specifiche misure di presidio. Tra queste rientrano la predisposizione di adeguate strategie di uscita (*exit strategy*), la definizione di diritti di audit nei confronti del provider e l'implementazione di processi di monitoraggio continuo finalizzati a garantire la continuità operativa e la resilienza dei servizi erogati. [12][13]

DORA – Digital Operational Resilience Act

Il Regolamento (UE) 2022/2554 sulla resilienza operativa digitale del settore finanziario, noto come Digital Operational Resilience Act (DORA), rappresenta uno dei più recenti e rilevanti interventi normativi europei in materia di gestione del rischio ICT nel settore finanziario. Entrato in vigore il 16 gennaio 2023 e applicabile a partire dal 17 gennaio 2025, il regolamento introduce per la prima volta un quadro normativo armonizzato e vincolante volto a rafforzare la resilienza operativa digitale delle istituzioni finanziarie dell'Unione Europea.

DORA si fonda su un insieme di requisiti finalizzati a garantire che gli intermediari finanziari siano in grado di prevenire, gestire e rispondere efficacemente a incidenti e minacce di natura informatica. Tra gli elementi centrali del regolamento figurano l'obbligo di implementare un framework strutturato di gestione del rischio ICT (art. 5-15), l'adozione di processi per la classificazione e la segnalazione degli incidenti informatici significativi alle autorità competenti (art. 17-23), l'esecuzione periodica di test di resilienza operativa digitale sui sistemi ICT (art. 24-27) e la definizione di specifici presidi per la gestione del rischio derivante da fornitori terzi di servizi ICT, inclusi i provider cloud (art. 28-44). Il regolamento promuove inoltre la condivisione volontaria delle informazioni relative alle minacce informatiche tra gli operatori del settore finanziario, al fine di rafforzare la capacità complessiva di prevenzione e risposta agli attacchi (art. 45).

Nel contesto di programmi di trasformazione come quello analizzato nel presente elaborato, DORA assume una rilevanza particolarmente significativa. La migrazione di sistemi core verso infrastrutture cloud comporta infatti la necessità di garantire elevati livelli di resilienza operativa, continuità del servizio e controllo sui fornitori tecnologici coinvolti. Le attività di test, le procedure di disaster recovery, il monitoraggio continuo dei sistemi e la definizione di adeguati meccanismi di governance rappresentano pertanto elementi essenziali per assicurare la conformità ai requisiti introdotti dal regolamento e garantire la continuità operativa dei servizi bancari anche in presenza di eventi avversi. [14]

Direttiva NIS2

Un ulteriore riferimento normativo rilevante è rappresentato dalla Direttiva (UE) 2022/2555, nota come NIS2 (*Network and Information Security Directive 2*), entrata in

vigore nel gennaio 2023 con l'obiettivo di rafforzare il livello comune di cybersicurezza all'interno dell'Unione Europea. La direttiva introduce requisiti più stringenti in materia di gestione del rischio cyber, sicurezza delle reti e dei sistemi informativi, continuità operativa e segnalazione degli incidenti, risultando complementare al regolamento DORA per quanto riguarda il rafforzamento della resilienza digitale delle infrastrutture critiche, estendendo l'applicabilità di queste normative e la disciplina cyber anche alle entità del settore finanziario classificate come infrastrutture critiche. [15]

Capitolo terzo

3. Il Framework CDMC

L'obiettivo del capitolo è quello di approfondire il funzionamento del Cloud Data Management Capabilities (CDMC) framework, evidenziandone struttura, finalità e principali aree operative. In particolare, verranno analizzate le motivazioni che hanno portato alla nascita del CDMC e il contesto in cui il framework è stato sviluppato, caratterizzato dalla crescente diffusione di ambienti single-cloud, multi-cloud e hybrid-cloud e dalla necessità di garantire maggiore controllo, sicurezza e conformità nella gestione dei dati.

Successivamente, l'attenzione sarà rivolta alla struttura del framework e alla suddivisione delle sue capabilities, con particolare riferimento alle sei componenti fondamentali che costituiscono il nucleo del modello: Governance & Accountability, Cataloging & Classification, Accessibility & Usage, Protection & Privacy, Data Lifecycle e Data & Technical Architecture. Per ciascuna di esse verranno evidenziati obiettivi, controlli, ambiti applicativi e quadro normativo, mostrando come il framework definisca un insieme organico di pratiche e requisiti finalizzati a garantire affidabilità, tracciabilità e protezione dei dati negli ambienti cloud.

3.1 Origini e obiettivi

La crescente adozione di ambienti cloud ha evidenziato la necessità di definire modelli strutturati per la gestione, il controllo e la governance dei dati. Sebbene il cloud computing offra elevati livelli di flessibilità e scalabilità, la gestione delle informazioni in ambienti distribuiti, multi-cloud e ibridi introduce problematiche legate a sicurezza, conformità normativa, tracciabilità e controllo operativo. Tali criticità risultano particolarmente rilevanti nei contesti in cui vengono trattati dati sensibili o sottoposti a requisiti regolamentari stringenti.

In questo scenario nasce il framework Cloud Data Management Capabilities (CDMC), sviluppato con l'obiettivo di definire un insieme di best practice per la gestione e il controllo dei dati negli ambienti cloud. Il framework fornisce linee guida, controlli e

capacità operative finalizzate a supportare le organizzazioni nei processi di migrazione, integrazione e gestione dei dati in ambienti single-cloud, multi-cloud e hybrid-cloud.

L'obiettivo principale del CDMC è quello di costruire maggiore fiducia, affidabilità e trasparenza nell'utilizzo delle tecnologie cloud, promuovendo un approccio standardizzato alla gestione del dato. Il framework si rivolge a tutti gli attori dell'ecosistema cloud: organizzazioni utilizzatrici, cloud service provider, fornitori tecnologici, consulenti e autorità di regolamentazione.

Per le organizzazioni che adottano servizi cloud, il CDMC rappresenta un modello strutturato di processi, controlli e pratiche verificabili, particolarmente rilevante nella gestione dei dati sensibili. Per i cloud service provider, invece, il framework definisce requisiti e controlli che possono essere integrati e automatizzati all'interno delle piattaforme cloud, favorendo maggiore standardizzazione e aumentando la fiducia del mercato. Anche i fornitori di tecnologie e servizi possono utilizzare il framework per sviluppare soluzioni più affidabili e coerenti con gli standard di governance richiesti dalle organizzazioni. Infine, il CDMC fornisce supporto anche a consulenti, system integrator e organismi di controllo, offrendo un riferimento condiviso per attività di assessment, audit, formazione e verifica della conformità.

Il framework CDMC si configura quindi come un modello di valutazione e certificazione delle capacità organizzative necessarie a garantire una gestione controllata dei dati negli ambienti cloud. A differenza di altri framework focalizzati esclusivamente sugli aspetti infrastrutturali o tecnologici, il CDMC pone particolare attenzione al controllo dei dati sensibili, alla governance delle informazioni e all'automazione dei processi di gestione e monitoraggio.

Pur essendo un framework autonomo, il CDMC presuppone che l'organizzazione disponga già di solide basi di data management. In questo senso, esso si integra con altri modelli sviluppati dall'EDM Council, in particolare con il DCAM (Data Management Capability Assessment Model), che rappresenta un framework più ampio dedicato alle capacità generali di gestione dei dati. Il CDMC estende tali principi al contesto cloud, concentrandosi sulle problematiche specifiche introdotte dagli ambienti distribuiti e virtualizzati.

Il framework è stato sviluppato dall'EDM Council attraverso il CDMC Work Group, istituito nel maggio 2020 e composto da oltre 300 professionisti tra dirigenti aziendali, ingegneri, esperti tecnologici e specialisti di data management provenienti da più di 100

organizzazioni a livello globale. Tra i partecipanti figurano importanti cloud service provider, società di consulenza, aziende tecnologiche e organizzazioni specializzate nella protezione dei dati e nella compliance normativa.

Gli obiettivi principali dell'iniziativa erano molteplici. In primo luogo, sviluppare un framework capace di fornire linee guida condivise sulle principali capacità di gestione dei dati in ambienti cloud, allineandole alle best practice di settore. Un ulteriore obiettivo consisteva nella creazione di un modello di valutazione standardizzato, utile per misurare il livello di maturità e preparazione delle organizzazioni rispetto alla gestione dei dati nel cloud. Parallelamente, il framework è stato progettato per favorire la collaborazione tra provider cloud, aziende e fornitori tecnologici, accelerando lo sviluppo di funzionalità e controlli necessari a supportare le migrazioni cloud e la gestione sicura dei dati. Infine, il progetto mira a garantire un miglioramento continuo del framework stesso attraverso attività di aggiornamento, formazione e diffusione delle best practice.

La struttura del CDMC riprende l'approccio metodologico già adottato nel framework DCAM, mantenuto dall'EDM Council a partire dal 2014. Il framework identifica infatti un insieme articolato di capacità di controllo e governance necessarie per garantire una gestione responsabile del dato negli ambienti cloud.

In particolare, il CDMC evidenzia alcune esigenze fondamentali per il controllo dei dati in ambienti distribuiti. Le organizzazioni devono innanzitutto definire responsabilità chiare, processi di governance e controlli specifici per i dati migrati o creati nel cloud. Risulta inoltre essenziale conoscere in ogni momento quali dati siano presenti negli ambienti cloud e quale sia il loro livello di sensibilità, così da poter automatizzare controlli di accesso, monitoraggio e protezione. Il framework sottolinea anche l'importanza di applicare controlli lungo l'intero ciclo di vita del dato, garantendo corrette politiche di conservazione, archiviazione e cancellazione delle informazioni. A ciò si aggiunge la necessità di progettare architetture dati e configurazioni tecnologiche coerenti con gli obiettivi di business e con i requisiti normativi. [17]

3.2 Struttura del Framework

Per organizzare in modo strutturato le attività di gestione e controllo dei dati negli ambienti cloud, il framework CDMC suddivide le capacità di data management in sei componenti principali, articolate complessivamente in quattordici capabilities e trentasette sub-capabilities. Queste aree rappresentano il nucleo centrale del framework e definiscono controlli, pratiche operative e funzionalità necessarie per garantire una gestione sicura, affidabile e conforme dei dati negli ambienti cloud.

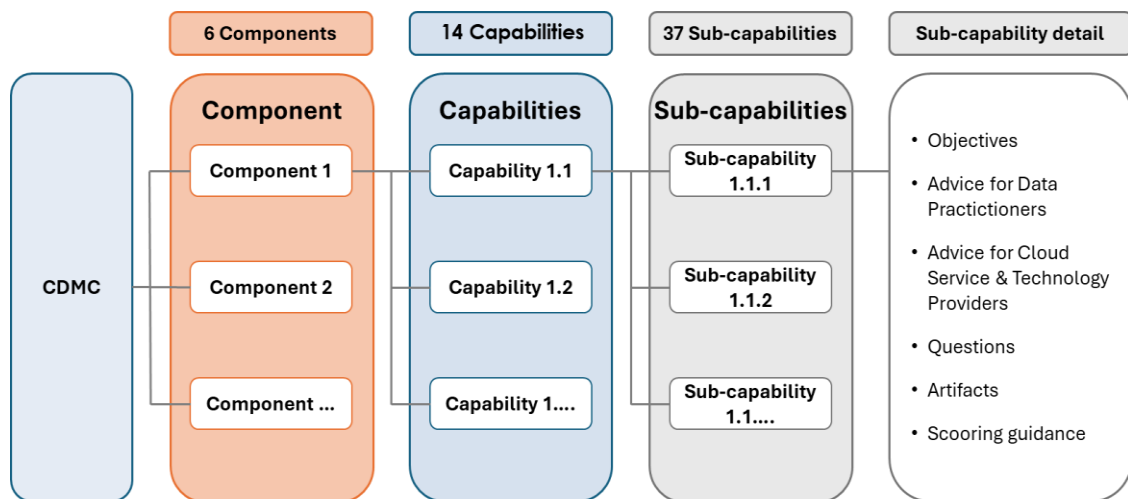


Figura 2. Struttura del framework (elaborazione personale da CDMC_Framework_V1.1.1)

La struttura del CDMC è stata progettata per offrire un approccio organico e standardizzato alla governance del dato, permettendo alle organizzazioni di identificare in modo chiaro responsabilità, controlli e requisiti necessari lungo tutto il ciclo di vita delle informazioni. Ogni componente affronta infatti uno specifico ambito della gestione del dato nel cloud e raccoglie al proprio interno un insieme di capabilities, cioè capacità operative e organizzative considerate fondamentali per garantire sicurezza, qualità, tracciabilità e conformità normativa.

Le capabilities vengono ulteriormente suddivise in sub-capabilities, che rappresentano requisiti più specifici, controlli dettagliati e pratiche implementative necessarie per raggiungere gli obiettivi definiti dal framework. Questa struttura gerarchica consente

alle organizzazioni di analizzare il proprio livello di maturità nella gestione dei dati cloud e di individuare eventuali gap nei processi di governance, sicurezza e controllo.

L'approccio adottato dal CDMC risulta particolarmente rilevante negli ambienti cloud moderni, caratterizzati da elevata distribuzione delle risorse, forte automazione e continua movimentazione dei dati tra piattaforme differenti. In questi contesti, la semplice presenza di strumenti tecnologici non è sufficiente a garantire una corretta gestione delle informazioni: è necessario definire processi standardizzati, controlli verificabili e responsabilità chiaramente attribuite.

Le sei componenti del framework coprono quindi l'intero ecosistema della gestione del dato nel cloud, includendo aspetti legati alla governance, alla classificazione dei dati, alla protezione delle informazioni sensibili, alla qualità del dato, alla gestione del ciclo di vita e al monitoraggio continuo dei controlli. L'obiettivo è creare un modello integrato che permetta alle organizzazioni di mantenere elevati livelli di affidabilità e trasparenza anche in ambienti tecnologici complessi e distribuiti.

Dal punto di vista metodologico, il framework adotta una struttura gerarchica articolata su più livelli. Le componenti rappresentano le macroaree di controllo e governance, le capabilities identificano le capacità organizzative richieste, mentre le sub-capabilities descrivono nel dettaglio i controlli e le pratiche operative necessarie per l'implementazione del framework. Questo approccio consente alle organizzazioni di valutare il proprio livello di maturità nella gestione dei dati in ambienti cloud e di individuare eventuali aree di miglioramento.

L'organizzazione gerarchica del CDMC permette quindi di collegare obiettivi strategici, requisiti di governance e controlli operativi all'interno di un unico modello integrato. Tale impostazione favorisce sia le attività di assessment sia i processi di implementazione e monitoraggio continuo delle pratiche di gestione del dato negli ambienti cloud. [18]

3.3 Le sei componenti del framework

Il framework CDMC organizza le attività di gestione e controllo del dato in sei principali aree funzionali, progettate per coprire in modo integrato tutti gli aspetti della governance dei dati negli ambienti cloud. Le componenti del framework affrontano tematiche che spaziano dalla definizione delle responsabilità organizzative fino alla progettazione dell'architettura tecnica, includendo aspetti legati alla sicurezza, alla classificazione dei dati, alla gestione degli accessi e al controllo dell'intero ciclo di vita delle informazioni.

Le sei component sono:

1. Governance & Accountability
2. Cataloging & Classification
3. Accessibility & Usage
4. Protection & Privacy
5. Data Lifecycle
6. Data & Technical Architecture

Ciascuna area affronta aspetti specifici della gestione dei dati negli ambienti cloud e definisce controlli, pratiche e requisiti finalizzati a garantire sicurezza, tracciabilità, qualità e conformità lungo l'intero ciclo di vita delle informazioni.

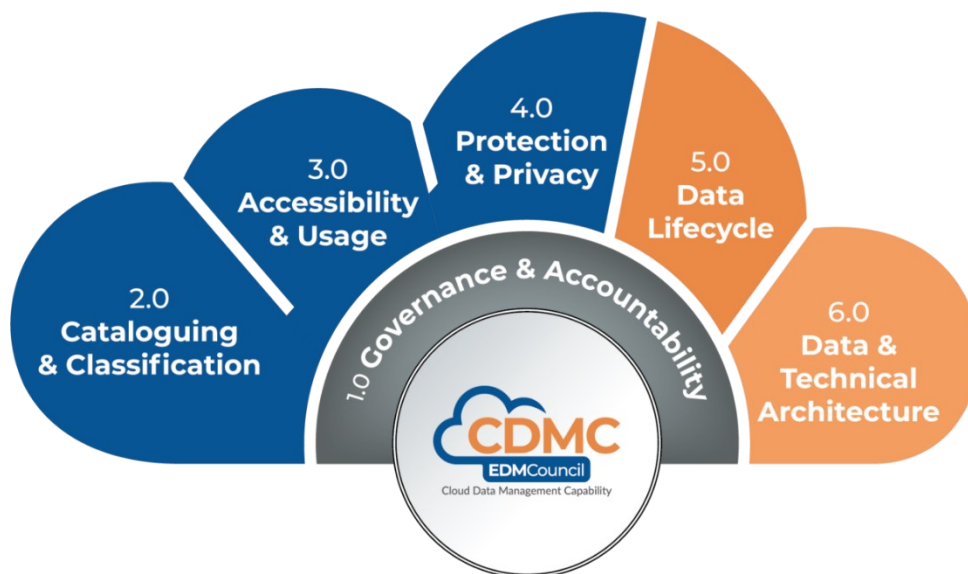


Figura 3. Le sei componenti del framework (estratta da CDMC_Framework_V1.1.1)

1. Governance & Accountability

La componente *Governance & Accountability* rappresenta il fondamento dell'intero framework CDMC, poiché definisce l'insieme di processi, responsabilità e meccanismi di controllo necessari per garantire una gestione efficace e sostenibile dei dati negli ambienti cloud. L'obiettivo principale di quest'area è assicurare che le organizzazioni adottino modelli di governance chiari, strutturati e coerenti con gli obiettivi di business, con i requisiti normativi e con il livello di rischio accettabile.

Il framework sottolinea in particolare l'importanza della definizione di business case formalizzati relativi alla gestione dei dati nel cloud, che devono essere approvati, condivisi e monitorati da tutti gli stakeholder coinvolti. La gestione dei dati in ambienti cloud richiede infatti il coordinamento tra differenti figure organizzative, tra cui responsabili della governance dei dati, team IT, funzioni di cybersecurity, compliance, risk management e management aziendale.

Un ulteriore elemento centrale riguarda la definizione delle responsabilità e dei processi decisionali. Il framework evidenzia come ogni organizzazione debba stabilire ruoli chiari per la supervisione, il controllo e il monitoraggio dei dati, garantendo trasparenza

nelle attività e tracciabilità delle decisioni adottate. In questo contesto assumono particolare rilevanza i processi di audit, revisione periodica e verifica della conformità, necessari per assicurare che le politiche di gestione dei dati rimangano coerenti con l'evoluzione delle esigenze operative e normative.

L'approccio proposto dal CDMC mira quindi a creare un equilibrio tra innovazione tecnologica, gestione del rischio e sostenibilità operativa, favorendo l'adozione del cloud attraverso processi governati, misurabili e continuamente monitorati. [19]

In tale ambito risulta rilevante la normativa DORA (art. 5 – 15 ICT Risk Framework) [14] che impone un ICT Risk Management framework formalizzato con responsabilità chiaramente attribuite al management, mentre le Guidelines EBA (GL/2019/02 art 12 – 14) [13] richiedono una governance strutturata dei contratti di outsourcing cloud.

2.Cataloging & Classification

La componente *Cataloging & Classification* si concentra sull'identificazione, catalogazione e classificazione dei dati presenti negli ambienti cloud. Secondo il framework, una gestione efficace del dato richiede innanzitutto la capacità di sapere quali informazioni siano presenti nei sistemi, dove siano archiviate, chi possa accedervi e quale livello di sensibilità esse possiedano.

Per raggiungere tali obiettivi, il CDMC promuove l'adozione di cataloghi dati centralizzati e sistemi di metadata management capaci di descrivere in modo strutturato le informazioni aziendali. I cataloghi consentono infatti di migliorare la visibilità sui dati, facilitarne la ricerca e supportare attività di governance, compliance e controllo.

Parallelamente, il framework attribuisce grande importanza alla classificazione dei dati, processo attraverso cui le informazioni vengono suddivise in categorie sulla base della loro criticità, sensibilità o valore aziendale. Tale classificazione rappresenta un elemento essenziale per l'applicazione automatizzata delle policy di sicurezza e dei controlli di accesso, soprattutto nei contesti cloud caratterizzati da elevata distribuzione e dinamicità delle risorse.

Il framework evidenzia inoltre come la classificazione debba essere mantenuta aggiornata nel tempo attraverso processi continui di monitoraggio e revisione, poiché il valore e la sensibilità dei dati possono cambiare in funzione dell'evoluzione del contesto operativo e normativo. [21]

Anche in questo ambito risultano di notevole importanza la normativa DORA (art. 8 ICT Asset Management) [14], in quanto richiede il mantenimento di un registro aggiornato degli asset ICT (inclusi i dati) e il GDPR (art. 30 registro dei trattamenti) [11] il quale, invece, impone la registrazione di tutti i trattamenti di dati personali.

3.Accessibility & Usage

La componente *Accessibility & Usage* riguarda il controllo degli accessi e l'utilizzo corretto dei dati negli ambienti cloud. Il framework sottolinea come la protezione delle informazioni non dipenda esclusivamente dalla sicurezza infrastrutturale, ma anche dalla capacità di garantire che l'accesso ai dati avvenga in modo controllato, tracciabile e coerente con le autorizzazioni definite dall'organizzazione.

In particolare, il CDMC promuove l'adozione di modelli di access control basati sul principio del *least privilege*, secondo cui utenti e applicazioni devono poter accedere esclusivamente ai dati strettamente necessari allo svolgimento delle proprie attività.

Questo approccio consente di ridurre significativamente il rischio di accessi impropri o utilizzi non autorizzati delle informazioni. Tale principio risulta esplicitamente richiesto anche dalle linee guida EBA (GL/2019/02 art. 76 controllo degli accessi).[13]

Il framework pone inoltre particolare attenzione alla gestione delle identità digitali e all'automazione dei controlli di autorizzazione, favorendo l'implementazione di sistemi di autenticazione avanzata, monitoraggio continuo e logging delle attività. La tracciabilità degli accessi rappresenta infatti un elemento fondamentale sia per la sicurezza sia per la conformità normativa, poiché permette di ricostruire le operazioni effettuate sui dati e identificare eventuali anomalie o violazioni.

L'area *Accessibility & Usage* include anche controlli relativi all'utilizzo dei dati da parte di applicazioni, servizi cloud e processi automatizzati, con l'obiettivo di garantire che le informazioni vengano trattate in modo coerente con le policy aziendali e con i requisiti normativi applicabili. [22]

Tali best practice sono anche trattate e confermate dal GDPR, che impone la limitazione dell'accesso ai dati personali al solo personale autorizzato. [11]

4. Protection & Privacy

La componente *Protection & Privacy* è dedicata alla protezione dei dati e alla tutela della privacy all'interno degli ambienti cloud. Questa area assume particolare rilevanza nei contesti caratterizzati dalla presenza di dati sensibili, informazioni personali o asset critici per il business.

Il framework definisce un insieme di controlli finalizzati a garantire confidenzialità, integrità e disponibilità delle informazioni durante tutte le fasi del loro utilizzo. Tra gli elementi principali rientrano la cifratura dei dati, la segmentazione delle reti, il monitoraggio continuo delle attività, la gestione delle vulnerabilità e l'implementazione di sistemi di protezione contro minacce informatiche e accessi non autorizzati.

Il CDMC attribuisce inoltre grande importanza alla protezione dei dati personali e alla conformità rispetto alle normative sulla privacy, come il GDPR. Le organizzazioni devono quindi essere in grado di identificare le informazioni sensibili, applicare adeguati livelli di protezione e dimostrare il rispetto delle normative attraverso controlli verificabili e processi di audit.

Un ulteriore aspetto centrale riguarda la gestione dei rischi associati alla distribuzione dei dati tra ambienti cloud differenti. In contesti multi-cloud o hybrid-cloud, infatti, la protezione delle informazioni richiede controlli uniformi e coordinati, capaci di garantire sicurezza e coerenza indipendentemente dalla piattaforma utilizzata. [23]

Questa componente del framework è quella di maggiore convergenza di normative; infatti, essa viene trattata dal GDPR (art. 32 sicurezza del trattamento) [11], da NIS2 (art. 21 misure di gestione del rischio) [15] e da DORA (art. 9 protezione ICT) relativamente alla protezione delle informazioni.[14]

5. Data Lifecycle

La componente *Data Lifecycle* si focalizza sulla gestione del dato lungo tutto il suo ciclo di vita, dalla creazione fino alla conservazione e alla successiva eliminazione. Il framework evidenzia come una gestione efficace dei dati richieda processi strutturati capaci di garantire qualità, disponibilità, tracciabilità e conformità normativa in ogni fase.

In particolare, il CDMC promuove l'adozione di policy relative alla conservazione, alla replica, all'archiviazione e alla cancellazione dei dati, assicurando che le informazioni

vengano gestite per periodi coerenti sia con gli obblighi normativi sia con le esigenze operative dell'organizzazione. In questo ambito, il rispetto delle disposizioni di legge assume particolare rilevanza, poiché possono emergere esigenze solo apparentemente contrastanti: il GDPR richiede infatti la cancellazione dei dati personali quando non sono più necessari rispetto alle finalità del trattamento (art. 5.1, principio di limitazione della conservazione) [11], mentre la Banca d'Italia impone la conservazione minima delle informazioni per un periodo di 10 anni anche successivamente alla cessazione del rapporto con il cliente [15].

Parallelamente, vengono definiti controlli relativi alla qualità del dato, alla gestione delle modifiche e alla tracciabilità delle trasformazioni effettuate nel tempo.

Il framework sottolinea inoltre l'importanza di implementare strategie di backup e disaster recovery adeguate, in grado di garantire continuità operativa e recuperabilità delle informazioni in caso di incidenti o interruzioni dei servizi cloud. In questo contesto, assumono particolare rilevanza i meccanismi di replica dei dati e le strategie di distribuzione geografica delle informazioni.

L'approccio lifecycle-oriented proposto dal CDMC permette quindi di considerare il dato come una risorsa dinamica, soggetta a continui processi di aggiornamento, utilizzo, conservazione e protezione. [23]

6.Data & Technical Architecture

La componente *Data & Technical Architecture* riguarda infine la progettazione delle architetture tecnologiche e dei modelli infrastrutturali necessari per supportare la gestione dei dati negli ambienti cloud. Il framework evidenzia come la struttura tecnica dell'ambiente cloud rappresenti un elemento essenziale per garantire scalabilità, interoperabilità, sicurezza e sostenibilità operativa.

Questa area comprende la definizione delle architetture dati, delle configurazioni infrastrutturali e delle tecnologie utilizzate per supportare archiviazione, elaborazione, integrazione e distribuzione delle informazioni. Il framework promuove architetture flessibili e standardizzate, capaci di supportare ambienti multi-cloud e hybrid-cloud e di adattarsi all'evoluzione delle esigenze organizzative.

Particolare attenzione viene posta anche all'automazione dei processi di gestione e controllo, attraverso strumenti di orchestration, Infrastructure as Code (IaC) e

monitoraggio continuo delle configurazioni. Tali soluzioni consentono di migliorare affidabilità, coerenza e velocità operativa, riducendo il rischio di errori manuali e configurazioni non conformi.

Il CDMC sottolinea inoltre l'importanza dell'interoperabilità tra piattaforme differenti e della capacità di integrare servizi cloud eterogenei mantenendo livelli adeguati di governance e controllo del dato. Questo aspetto risulta particolarmente rilevante nei moderni ecosistemi digitali, caratterizzati dalla crescente diffusione di architetture distribuite e dall'integrazione continua tra servizi, applicazioni e provider cloud differenti. [25]

A livello normativo l'architettura tecnica viene regolamentata sia da DORA che da EBA, in particolare DORA (art. 11 Business Continuity) [14] impone test di resilienza obbligatori, mentre EBA (GL/2019/02 art. 89-96 exit strategy, audit, sub-outsourcing) [13] richiede exit strategy definite e diritti di audit sui provider cloud.

Capitolo quarto

4. Il PMO nei programmi di migrazione cloud e il contributo della Generative AI

L'obiettivo del capitolo è quello di analizzare il ruolo che l'intelligenza artificiale generativa può assumere all'interno delle attività di project management, evidenziandone le principali applicazioni e il potenziale contributo nella gestione di progetti caratterizzati da elevati livelli di complessità. In particolare, verrà inizialmente approfondito il contesto in cui operano oggi i project manager, evidenziando come la crescente complessità dei programmi di trasformazione digitale abbia aumentato la necessità di strumenti in grado di supportare in modo più efficace le attività di pianificazione, coordinamento e controllo e abbia portato alla nascita di diverse tipologie di project manager.

Successivamente, l'attenzione sarà rivolta alle principali applicazioni della Generative AI nei processi di project management, analizzando il supporto che tali tecnologie possono fornire nelle attività di gestione documentale, monitoraggio progettuale, comunicazione con gli stakeholder, produzione di reportistica e supporto ai processi decisionali. Infine, verranno esaminati i principali benefici derivanti dall'adozione di tali strumenti, nonché le limitazioni e le sfide che le organizzazioni devono affrontare per garantirne un utilizzo efficace e consapevole all'interno dei contesti progettuali.

4.1 Il project management nell'era della trasformazione digitale



Figura 4. Project management nella trasformazione digitale (disponibile su: [*Il Digital Transformation Manager: governare la trasformazione digitale – OMURA*](#))

Negli ultimi anni la trasformazione digitale ha modificato profondamente il modo in cui le organizzazioni progettano, sviluppano ed erogano prodotti e servizi. L'adozione di tecnologie quali cloud computing, intelligenza artificiale, big data e architetture distribuite ha reso possibile l'introduzione di nuovi modelli operativi e nuove opportunità di business, ma ha anche determinato un significativo incremento della complessità dei progetti. Le iniziative di trasformazione digitale non si limitano infatti all'implementazione di nuove soluzioni tecnologiche, bensì coinvolgono contemporaneamente processi, persone, strutture organizzative e modelli di governance, generando un elevato numero di interdipendenze che devono essere gestite in modo coordinato.

In questo contesto, i progetti risultano sempre più caratterizzati da elevata incertezza, requisiti in continua evoluzione e forte integrazione tra molteplici sistemi e applicazioni. La crescente diffusione di ecosistemi digitali complessi richiede infatti la collaborazione di numerosi stakeholder appartenenti a differenti aree aziendali, ciascuno

portatore di esigenze, priorità e obiettivi specifici. Parallelamente, l'accelerazione dei processi di innovazione impone alle organizzazioni la necessità di ridurre i tempi di realizzazione delle iniziative, mantenendo al contempo elevati standard di qualità, sicurezza e conformità normativa.

Tra i principali fattori che contribuiscono alla complessità dei progetti di trasformazione digitale vi sono le numerose dipendenze esistenti tra applicazioni, infrastrutture e processi di business. Una modifica apportata a una componente del sistema può infatti produrre effetti su molte altre aree dell'organizzazione, rendendo necessario un continuo coordinamento tra i diversi team coinvolti. A ciò si aggiunge la complessità tecnica derivante dall'adozione di nuove tecnologie, che spesso richiedono competenze specialistiche e processi di integrazione articolati. Anche la presenza di un elevato numero di stakeholder rappresenta un elemento critico, poiché rende necessario bilanciare aspettative differenti e garantire un costante allineamento tra obiettivi strategici ed esigenze operative.

Particolarmente rilevante risulta inoltre la cosiddetta complessità dinamica, tipica dei progetti innovativi. Durante il ciclo di vita progettuale possono infatti emergere nuove esigenze di business, variazioni normative, cambiamenti organizzativi o evoluzioni tecnologiche che richiedono continui adattamenti della pianificazione iniziale. In tali contesti, la capacità di reagire rapidamente ai cambiamenti diventa un fattore determinante per il successo dell'iniziativa. [25]

L'aumento della complessità progettuale ha inevitabilmente modificato anche il ruolo del Project Manager. Se in passato tale figura era prevalentemente associata ad attività di pianificazione, monitoraggio delle tempistiche e controllo dei costi, oggi è chiamata a svolgere un ruolo molto più ampio e strategico. Il Project Manager deve infatti garantire il coordinamento tra team multidisciplinari, gestire le dipendenze tra iniziative differenti, supportare i processi decisionali e favorire la comunicazione tra le diverse componenti organizzative coinvolte nel progetto.

Parallelamente all'evoluzione del ruolo del Project Manager, anche il Project Management Office (PMO) ha assunto una funzione sempre più rilevante nel governo dei programmi di trasformazione. Secondo il *Project Management Institute* (PMI, 2017), il PMO può assumere differenti configurazioni in funzione del livello di autorità esercitato e dei servizi forniti all'organizzazione. Una prima tipologia è rappresentata dal PMO di supporto, che svolge prevalentemente attività di consulenza metodologica,

predisposizione di standard, formazione e condivisione delle best practice, lasciando ai Project Manager la piena autonomia nella gestione operativa dei progetti. Il PMO di controllo, invece, esercita un ruolo di supervisione e governance, monitorando la conformità ai processi organizzativi, verificando il rispetto degli standard di project management e supportando il management attraverso attività di reporting e controllo delle performance. Infine, il PMO direttivo assume la responsabilità diretta della gestione dei progetti o dei programmi, coordinando le iniziative e assegnando le risorse necessarie al raggiungimento degli obiettivi strategici dell'organizzazione. La scelta della configurazione più appropriata dipende dal livello di maturità organizzativa e dalla complessità delle iniziative da governare.

Parallelamente all'evoluzione del ruolo del Project Manager, nelle organizzazioni hanno assunto crescente rilevanza anche le strutture di Project Management Office (PMO), chiamate a supportare la governance dei progetti e dei programmi. Il PMO può assumere differenti configurazioni in funzione del livello di autorità esercitato: da strutture con funzione prevalentemente di supporto metodologico e documentale, fino a modelli con responsabilità di controllo e coordinamento o, nei contesti più maturi, con un ruolo direttivo nella gestione dei progetti. La configurazione adottata dipende dal livello di complessità organizzativa e dagli obiettivi strategici perseguiti dall'organizzazione. [26]

Accanto alle tradizionali competenze di project management assumono quindi crescente importanza capacità legate alla gestione del cambiamento, al problem solving, alla negoziazione e alla governance degli stakeholder. Il successo di un progetto non dipende più esclusivamente dalla corretta esecuzione delle attività pianificate, ma anche dalla capacità di interpretare scenari in continua evoluzione e di prendere decisioni rapide sulla base di informazioni spesso numerose, eterogenee e distribuite tra differenti fonti.

Nei programmi di trasformazione di elevata complessità, caratterizzati dalla presenza di numerosi progetti interdipendenti, il PMO assume inoltre una funzione di coordinamento trasversale finalizzata ad assicurare l'allineamento tra le diverse iniziative e il perseguimento dei benefici strategici del programma. Come evidenziato dal PMI (2017), il Program Management si distingue infatti dalla semplice gestione di singoli progetti poiché richiede una governance integrata delle dipendenze, delle risorse, dei rischi e della comunicazione tra gli stakeholder, al fine di garantire una visione

unitaria dell'intero programma e supportare il raggiungimento degli obiettivi organizzativi. [26]

In questo scenario, caratterizzato da una crescente mole di dati e da livelli di complessità sempre più elevati, emerge l'esigenza di strumenti in grado di supportare il Project Manager nelle attività di coordinamento, analisi e controllo. Le più recenti innovazioni nel campo dell'intelligenza artificiale generativa si inseriscono proprio in questa prospettiva, offrendo nuove opportunità per aumentare l'efficienza delle attività di project management e supportare il governo dei progetti di trasformazione digitale. [25] [27]

4.2 Applicazioni della generative AI nelle attività di project management

L'intelligenza artificiale generativa sta progressivamente trovando applicazione in numerose attività tipiche del project management, supportando i professionisti nella gestione delle informazioni, nella produzione di documentazione e nelle attività di coordinamento e monitoraggio dei progetti. Secondo il Project Management Institute (PMI), l'adozione di tali strumenti sta modificando il modo in cui molte attività operative vengono svolte, consentendo di ridurre il tempo dedicato a compiti ripetitivi e di concentrare maggiormente l'attenzione sugli aspetti strategici e decisionali del progetto.

Uno degli ambiti di applicazione più diffusi riguarda la produzione e la gestione della documentazione progettuale. I modelli di Generative AI possono infatti supportare la redazione di documenti quali project charter, piani di progetto, report di avanzamento, verbali di riunione, documentazione tecnica e presentazioni destinate agli stakeholder. Attraverso l'elaborazione di informazioni fornite dall'utente, tali strumenti sono in grado di generare contenuti strutturati, sintetizzare grandi quantità di dati e produrre documentazione coerente con il contesto progettuale, contribuendo a semplificare attività tradizionalmente caratterizzate da un elevato carico amministrativo.

Un secondo ambito particolarmente rilevante riguarda il supporto alle attività di pianificazione. L'intelligenza artificiale può assistere il Project Manager nella definizione delle attività progettuali, nella scomposizione del lavoro in task elementari, nella costruzione di Work Breakdown Structure (WBS) e nell'identificazione delle

principali dipendenze tra le attività. Attraverso l'analisi delle informazioni disponibili, gli strumenti di Generative AI possono inoltre suggerire possibili approcci di pianificazione, evidenziare attività mancanti o proporre scenari alternativi utili alla definizione del piano di progetto.

La tecnologia trova applicazione anche nelle attività di monitoraggio e controllo. I sistemi basati su Generative AI possono infatti elaborare dati provenienti da differenti fonti, sintetizzare informazioni relative allo stato di avanzamento delle iniziative e supportare la predisposizione di report destinati al management. In questo modo il Project Manager può disporre più rapidamente di una visione consolidata dell'andamento del progetto, facilitando il processo di analisi e di comunicazione verso gli stakeholder.

Un ulteriore ambito di utilizzo riguarda la gestione dei rischi. Secondo il PMI, l'intelligenza artificiale può supportare l'identificazione preliminare dei rischi progettuali attraverso l'analisi della documentazione disponibile e delle caratteristiche dell'iniziativa. I modelli generativi possono contribuire alla definizione dei registri dei rischi, suggerire possibili eventi critici e proporre azioni di mitigazione basate sulle informazioni fornite, offrendo un supporto alle attività di valutazione condotte dal Project Manager.

La Generative AI viene inoltre utilizzata per migliorare i processi di comunicazione e collaborazione tra i diversi stakeholder coinvolti nel progetto. Le funzionalità di sintesi automatica consentono, ad esempio, di produrre riepiloghi di riunioni, evidenziare decisioni prese, identificare azioni da intraprendere e predisporre comunicazioni mirate per differenti categorie di destinatari. Questo tipo di applicazioni risulta particolarmente utile nei progetti caratterizzati da elevata complessità organizzativa e da un numero significativo di soggetti coinvolti.

Infine, il report evidenzia come gli utilizzatori più maturi tendano a impiegare la Generative AI anche come strumento di supporto all'analisi e al processo decisionale. In questi casi l'intelligenza artificiale non viene utilizzata esclusivamente per generare contenuti, ma per elaborare informazioni, confrontare scenari alternativi, formulare ipotesi e supportare le valutazioni del Project Manager. Sebbene la responsabilità finale delle decisioni rimanga sempre in capo al professionista, tali strumenti possono contribuire ad ampliare la capacità di analisi e a velocizzare l'accesso alle informazioni rilevanti.

L'insieme di queste applicazioni evidenzia come la Generative AI stia progressivamente assumendo il ruolo di assistente digitale a supporto delle attività di project management. La sua diffusione interessa ormai l'intero ciclo di vita del progetto, dalla pianificazione iniziale fino alle attività di monitoraggio, comunicazione e reporting, aprendo nuove opportunità per l'evoluzione delle pratiche di gestione dei progetti. [28]

4.3 Benefici, limiti e sfide d'adozione

L'interesse verso l'impiego dell'intelligenza artificiale generativa nel project management è cresciuto rapidamente negli ultimi anni, grazie alla capacità di tali strumenti di supportare numerose attività operative e decisionali. Tuttavia, i benefici derivanti dalla loro adozione non dipendono esclusivamente dalla disponibilità della tecnologia, ma sono strettamente legati al modo in cui essa viene integrata nei processi organizzativi e nelle pratiche di gestione dei progetti.

Uno dei principali vantaggi riguarda l'incremento della produttività individuale. La possibilità di automatizzare attività ripetitive, predisporre rapidamente documentazione progettuale, sintetizzare grandi quantità di informazioni e supportare la produzione di report consente di ridurre significativamente il tempo dedicato a compiti a basso valore aggiunto. Questo permette ai professionisti di concentrare maggiormente le proprie energie sulle attività di coordinamento, pianificazione strategica e gestione degli stakeholder, migliorando l'efficacia complessiva del processo di project management.

Accanto ai benefici in termini di efficienza operativa, l'intelligenza artificiale generativa può contribuire a migliorare la qualità delle analisi e dei processi decisionali.

L'elaborazione rapida di informazioni provenienti da fonti differenti, la possibilità di confrontare scenari alternativi e il supporto all'identificazione preventiva dei rischi consentono infatti di ampliare la capacità di analisi dei team di progetto e di disporre di elementi aggiuntivi a supporto delle decisioni. In questo contesto, la tecnologia assume un ruolo di supporto alle attività manageriali, favorendo una maggiore disponibilità di informazioni e una migliore comprensione delle dinamiche progettuali.

I benefici non si limitano tuttavia alla sola dimensione individuale. L'utilizzo della Generative AI può favorire una più efficace gestione della conoscenza, una maggiore rapidità nella circolazione delle informazioni e un miglior coordinamento tra i diversi attori coinvolti nel progetto. La capacità di sintetizzare contenuti, generare

comunicazioni mirate e rendere più accessibili informazioni distribuite tra documenti e sistemi differenti contribuisce infatti a semplificare i processi collaborativi e a migliorare la condivisione delle informazioni all'interno dell'organizzazione.

Nonostante le opportunità offerte dalla tecnologia, permangono tuttavia alcuni limiti che richiedono particolare attenzione. Uno degli aspetti più rilevanti riguarda l'affidabilità degli output generati dai modelli di intelligenza artificiale. Sebbene i risultati prodotti siano spesso coerenti e ben strutturati, possono verificarsi casi in cui vengano generate informazioni inesatte, incomplete o prive del corretto contesto. Per questo motivo il giudizio umano continua a rappresentare un elemento fondamentale e ogni contenuto prodotto dall'intelligenza artificiale deve essere sottoposto a un processo di verifica e validazione prima di essere utilizzato all'interno delle attività progettuali.

Ulteriori criticità riguardano la gestione dei dati e delle informazioni aziendali. In particolare, le organizzazioni devono affrontare temi legati alla sicurezza, alla riservatezza delle informazioni e alla conformità normativa, aspetti particolarmente rilevanti nei contesti caratterizzati da elevati requisiti regolamentari. L'introduzione di strumenti basati su intelligenza artificiale richiede quindi la definizione di adeguati modelli di governance, finalizzati a disciplinarne l'utilizzo e a garantire un corretto trattamento dei dati.

Accanto alle sfide tecnologiche emergono anche importanti aspetti di natura organizzativa e culturale. In molte realtà l'adozione della Generative AI si trova ancora in una fase iniziale e avviene spesso attraverso iniziative isolate o utilizzi individuali non pienamente integrati nei processi aziendali. In assenza di una strategia condivisa, di linee guida operative e di adeguati percorsi formativi, il rischio è quello di limitarsi a un utilizzo sporadico della tecnologia, senza riuscire a coglierne pienamente il potenziale. In questo scenario assume particolare rilevanza il tema delle competenze. L'efficacia degli strumenti di Generative AI dipende infatti dalla capacità degli utenti di formulare richieste appropriate, interpretare correttamente i risultati ottenuti e valutarne criticamente l'affidabilità. La creazione di valore non deriva quindi soltanto dalle caratteristiche tecnologiche delle soluzioni adottate, ma anche dalla capacità delle persone di integrarle efficacemente nei processi decisionali e operativi.

L'intelligenza artificiale generativa rappresenta dunque una tecnologia con un elevato potenziale trasformativo per il project management, in grado di migliorare produttività, capacità di analisi e gestione delle informazioni. Allo stesso tempo, il raggiungimento di

tali benefici richiede un approccio consapevole, supportato da adeguati modelli di governance, da investimenti nelle competenze e da una costante supervisione umana. Più che una sostituzione del Project Manager, emerge quindi una logica di collaborazione tra capacità umane e strumenti intelligenti, nella quale la tecnologia diventa un fattore abilitante per una gestione dei progetti più efficiente, informata e orientata al valore. [28]

Capitolo quinto

5. Dal sistema legacy al cloud: migrazione dei dati dei conti correnti

Il presente capitolo presenta un caso di studio relativo a un progetto di migrazione dei dati dei conti correnti verso una nuova architettura cloud-native realizzato nell'ambito del percorso di trasformazione digitale di uno dei principali gruppi bancari italiani. L'analisi prenderà avvio dalla descrizione del contesto progettuale e degli obiettivi strategici dell'iniziativa, evidenziando le motivazioni che hanno guidato la modernizzazione del sistema di core banking e i principali benefici attesi per l'organizzazione.

Successivamente verrà approfondita l'evoluzione dell'architettura IT, illustrando il passaggio dal sistema legacy basato su mainframe alla nuova piattaforma cloud-native e analizzando le diverse fasi che caratterizzano il percorso di transizione. Sarà inoltre descritto il piano di migrazione definito per garantire il trasferimento dei dati e delle funzionalità in condizioni di sicurezza e continuità operativa, con particolare attenzione ai meccanismi di allineamento, validazione e disaster recovery adottati durante il processo.

Infine, il capitolo si concentrerà sugli aspetti di governance e coordinamento del progetto, evidenziando le attività di monitoraggio, gestione degli stakeholder, reporting direzionale e supporto operativo necessarie per garantire il corretto avanzamento dell'iniziativa. Attraverso questo caso di studio sarà possibile osservare l'applicazione concreta dei concetti di cloud computing, data management e governance analizzati nei capitoli precedenti all'interno di un contesto bancario caratterizzato da elevata complessità e criticità operativa.

5.1 Contesto e obiettivi del progetto

Il presente progetto si inserisce all'interno di un più ampio percorso di trasformazione digitale intrapreso da uno dei principali gruppi bancari italiani, finalizzato alla modernizzazione del sistema di Core Banking e all'evoluzione dell'infrastruttura tecnologica verso paradigmi cloud-native. In particolare, l'iniziativa riguarda la migrazione massiva dei conti correnti relativi a tutte le legal entity italiane dal sistema mainframe legacy verso una nuova architettura tecnologica di ultima generazione, progettata per garantire maggiore scalabilità, resilienza e disponibilità continua dei servizi. Tale migrazione rappresenta un passaggio strategico cruciale, in quanto coinvolge uno dei domini applicativi più critici dell'intero ecosistema bancario, ovvero quello che contiene le informazioni relative ai conti correnti di tutti i clienti del gruppo, con impatti diretti sulla gestione operativa e sull'erogazione dei servizi verso clientela retail e corporate.

Uno dei principali macro-obiettivi del progetto consiste nella progressiva dismissione delle componenti legacy attualmente ospitate su infrastrutture mainframe, le quali, pur garantendo nel tempo elevati livelli di affidabilità e velocità computazionale, risultano oggi caratterizzate da rigidità architetturale, elevati costi di mantenimento e limitata capacità di adattamento ai nuovi requisiti di business e tecnologici. La strategia adottata prevede quindi una riallocazione graduale dei servizi verso una piattaforma moderna, basata su un'architettura cloud-native, in grado di assicurare un funzionamento continuo 24/7, elevati standard di performance e una significativa ottimizzazione dei costi infrastrutturali. Questo processo di transizione non si limita a una mera migrazione tecnica, ma implica una profonda revisione del modello di erogazione dei servizi, con l'obiettivo di ridurre la dipendenza dalle infrastrutture monolitiche e favorire una maggiore agilità operativa.

Un ulteriore elemento cardine del progetto è l'introduzione di un'architettura basata su microservizi e su un modello API-driven, che consente la decomposizione delle funzionalità core in servizi indipendenti, interoperabili e scalabili orizzontalmente. Questo approccio permette di incrementare la modularità dell'intero sistema informativo, facilitando l'evoluzione incrementale delle singole componenti e migliorando la capacità di integrazione con sistemi esterni e canali digitali. L'adozione di logiche API-first rappresenta inoltre un fattore abilitante per la standardizzazione

delle interfacce applicative, favorendo una maggiore coerenza architetturale e semplificando i processi di orchestrazione e integrazione tra domini funzionali eterogenei.

Infine, il progetto si pone l'obiettivo di supportare in maniera strutturale la trasformazione digitale dell'intero gruppo bancario verso un modello cloud-native, caratterizzato da elevati livelli di sicurezza, scalabilità e resilienza. In tale contesto, particolare attenzione viene dedicata all'implementazione di meccanismi avanzati di sicurezza by design, alla gestione della continuità operativa e alla capacità del sistema di adattarsi dinamicamente a variazioni di carico e a scenari di fault tolerance. La migrazione rappresenta quindi non solo un'evoluzione tecnologica, ma anche un cambio di paradigma organizzativo e architetturale, volto a rendere l'infrastruttura IT più flessibile, efficiente e allineata alle esigenze di un mercato bancario sempre più digitale e competitivo.

5.2 Principali risultati e benefici per la banca



Figura 5. Principali vantaggi attesi dal progetto di migrazione (estratta da piano industriale 2022- 2025)

Il processo di migrazione del core banking verso la nuova architettura cloud-native è stato progettato non solo come un intervento tecnologico di modernizzazione, ma anche come un'iniziativa strategica orientata alla generazione di benefici concreti e misurabili per l'intero gruppo bancario. Uno dei principali obiettivi del programma riguarda la

capacità di gestire la migrazione su volumi estremamente rilevanti, considerando l'elevato numero di conti correnti e la complessità del perimetro applicativo coinvolto. La strategia adottata consente di affrontare tale complessità attraverso un approccio strutturato, progressivo e controllato, in grado di garantire la corretta transizione dei dati e delle funzionalità senza compromettere la stabilità complessiva del sistema.

Un ulteriore elemento fondamentale è rappresentato dalla garanzia di continuità operativa dei servizi core durante tutte le fasi del processo di migrazione. L'intero disegno architetturale e organizzativo è stato infatti definito con l'obiettivo di minimizzare l'impatto sulle operazioni quotidiane della clientela, assicurando che i servizi bancari essenziali rimangano sempre disponibili e pienamente fruibili. Questo approccio consente di ridurre al minimo le interruzioni e i disservizi, preservando al contempo la qualità dell'esperienza utente e la fiducia nei confronti dell'istituto.

Un altro vantaggio significativo deriva dalla riduzione del rischio complessivo associato all'iniziativa, ottenuta grazie all'introduzione di un modello di governance centralizzato e a un presidio continuo delle dipendenze critiche. Tale struttura di controllo consente di monitorare in maniera costante l'avanzamento delle attività, identificare tempestivamente eventuali criticità e garantire un coordinamento efficace tra i diversi team coinvolti. La presenza di una governance solida rappresenta un elemento chiave per la gestione di un progetto di tale complessità e per la mitigazione dei rischi operativi e tecnologici.

Parallelamente, l'adozione di architetture cloud-based contribuisce in maniera sostanziale al rafforzamento della resilienza e della sicurezza del core banking. La nuova infrastruttura è progettata per garantire elevati livelli di affidabilità, tolleranza ai guasti e capacità di ripristino rapido dei servizi, elementi essenziali in un contesto bancario caratterizzato da requisiti stringenti in termini di continuità e protezione dei dati. Questo si traduce in una maggiore robustezza del sistema complessivo e in una capacità migliorata di rispondere a scenari di stress operativo o eventi imprevisti.

Un ulteriore obiettivo strategico è rappresentato dall'introduzione di un core banking scalabile, pienamente allineato al percorso di trasformazione digitale del gruppo. La nuova architettura è stata progettata con una capacità di crescita significativa, tale da poter supportare un incremento della base clienti fino a tre volte quella attuale, garantendo al contempo prestazioni stabili e prevedibili. Questa caratteristica

rappresenta un elemento abilitante fondamentale per sostenere lo sviluppo futuro del business e l'espansione dei servizi offerti.

Dal punto di vista operativo, il progetto consente inoltre un significativo miglioramento dell'efficienza e della velocità di rilascio delle nuove funzionalità, abilitando una riduzione del time-to-market e una maggiore flessibilità nella gestione delle evoluzioni applicative. L'adozione di paradigmi moderni e di un'architettura modulare permette infatti di semplificare i processi di sviluppo, test e deployment, favorendo un modello di delivery più rapido e reattivo rispetto alle esigenze del mercato.

Infine, la migrazione consente di eliminare progressivamente le inefficienze strutturali e gli sprechi accumulati nel tempo all'interno dell'architettura legacy, frutto di anni di evoluzioni stratificate e rilavorazioni successive. La nuova piattaforma consente quindi di superare le limitazioni del passato, riducendo la complessità tecnica e operativa e introducendo un modello più pulito, standardizzato ed efficiente, in grado di supportare in modo più efficace le esigenze attuali e future del gruppo bancario.

5.3 Evoluzione dell'architettura IT: dal sistema legacy al cloud-based

Il percorso di modernizzazione del core banking analizzato nel presente caso di studio ha comportato una profonda evoluzione dell'architettura IT della banca, attraverso una trasformazione graduale che ha permesso di migrare progressivamente da un'infrastruttura legacy basata su mainframe a una nuova architettura cloud-native. In particolare, il modello cloud che si è scelto di implementare è l'IaaS, al fine di garantire il massimo livello di personalizzazione e adeguatezza del sistema, consentendo inoltre una gestione dello sviluppo delle funzionalità il più efficiente e flessibile possibile. Tale evoluzione non ha riguardato esclusivamente gli aspetti tecnologici, ma ha interessato anche le modalità operative, i modelli di integrazione e le strategie di gestione del dato, con l'obiettivo di garantire continuità operativa, affidabilità e coerenza delle informazioni durante tutte le fasi della transizione, assicurando al contempo la conformità ai principali riferimenti normativi del settore, in particolare alle *EBA Guidelines on Outsourcing*. [13]

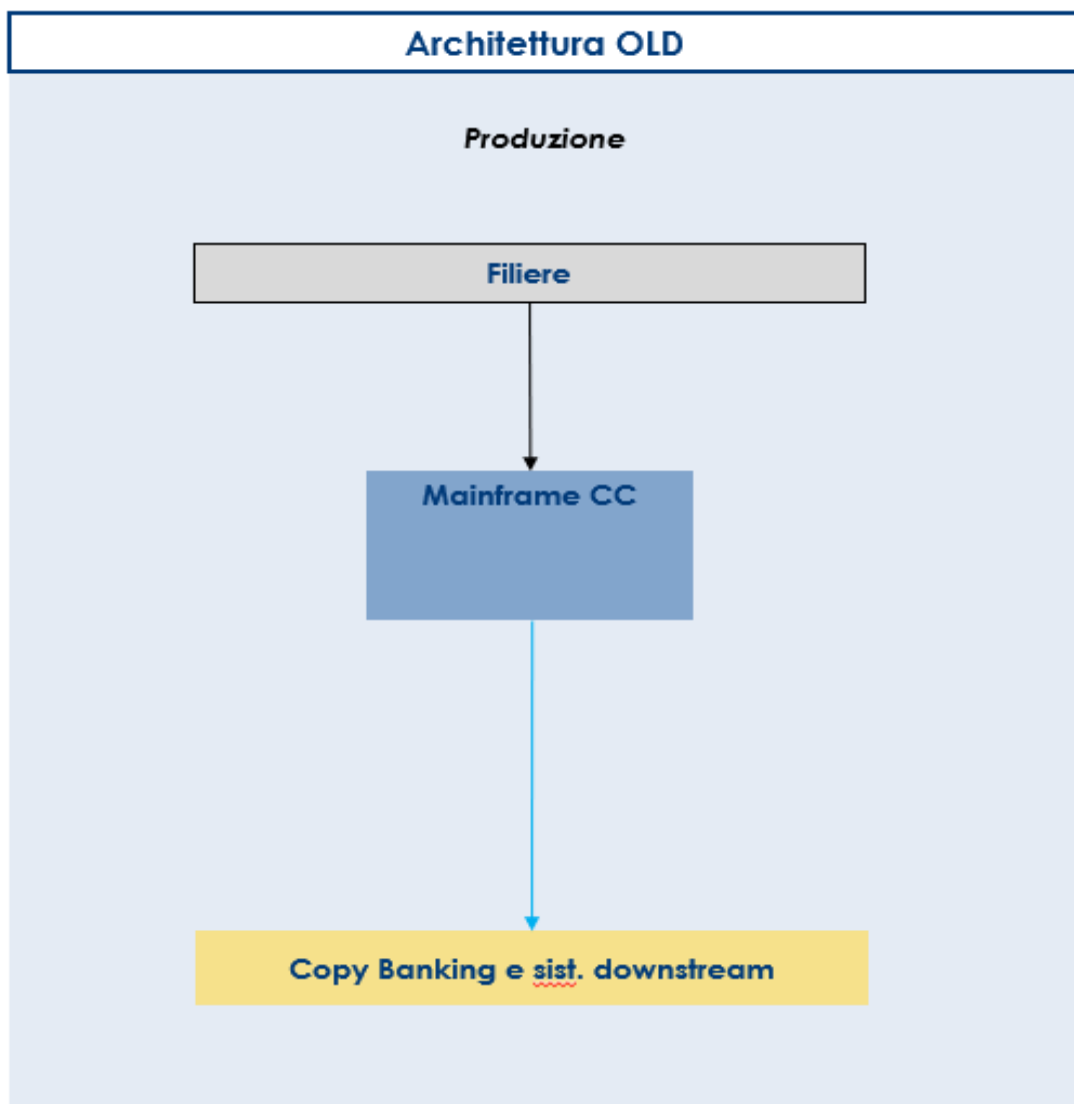


Figura 6. Rappresentazione architettura IT OLD

Nella configurazione iniziale, l'architettura risultava fortemente centralizzata attorno al sistema Core Banking Conti Correnti Mainframe (CC MF), che rappresentava il cuore operativo dell'intero ecosistema bancario. Le diverse filiere applicative della banca inviavano i flussi informativi direttamente al core banking legacy, il quale riceveva le informazioni in input, le elaborava e successivamente distribuiva gli output verso il Copy Banking e verso gli altri sistemi downstream presenti nell'architettura.

Questi sistemi downstream svolgevano e continuano a svolgere un ruolo fondamentale all'interno dell'ecosistema informativo della banca. Oltre a ricevere e memorizzare i dati elaborati dal Core Banking, essi rappresentano infatti un importante meccanismo di salvaguardia e continuità operativa, garantendo la disponibilità delle informazioni anche

in presenza di eventuali anomalie o malfunzionamenti dei sistemi principali. In questo modello architetturale, il mainframe costituiva quindi il punto centrale di elaborazione e controllo dell'intero ciclo operativo dei conti correnti.

Per superare le criticità già citate in precedenza del modello legacy è stato avviato il processo di evoluzione architetturale verso il nuovo ambiente cloud-native. Tuttavia, considerata la criticità dei sistemi coinvolti e la necessità di garantire continuità ai servizi bancari, la migrazione non poteva avvenire in modalità “big bang”, ovvero tramite una sostituzione immediata del vecchio sistema. È stato quindi adottato un approccio graduale e controllato, articolato in differenti fasi evolutive.

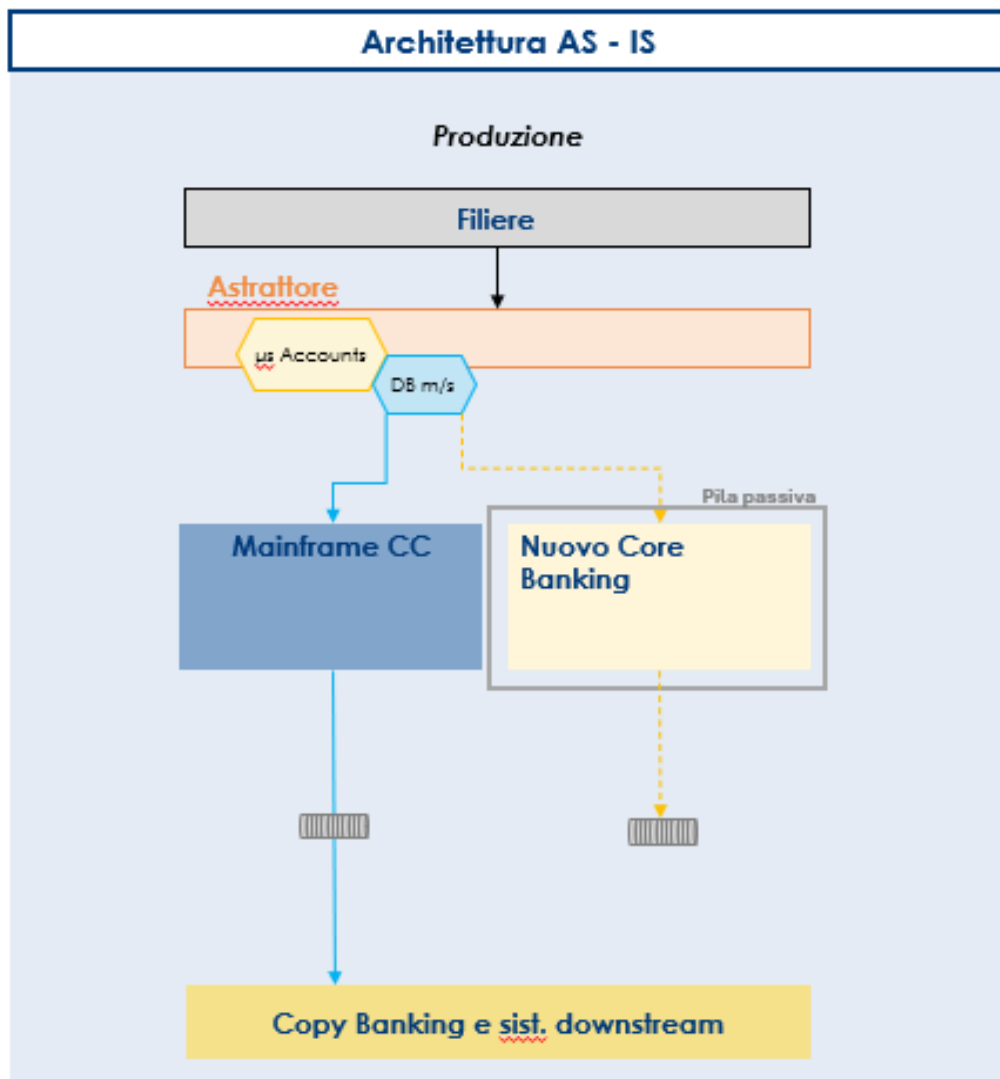


Figura 7. Rappresentazione architettura IT attuale

Nell'attuale configurazione architetturale, infatti, il sistema CC MF è ancora presente e continua a rappresentare il sistema master operativo della banca, ma al suo fianco è stato introdotto il nuovo Core Banking cloud-native. Questa fase intermedia rappresenta uno dei momenti più delicati e strategici dell'intero programma di trasformazione.

L'elemento centrale della nuova architettura è rappresentato da un componente denominato "astrattore", introdotto con l'obiettivo di gestire la coesistenza tra il sistema legacy e il nuovo Core Banking. Le filiere applicative non comunicano più direttamente con il CC MF, ma inviano i propri flussi all'astrattore, che agisce come layer di integrazione e smistamento delle informazioni.

L'astrattore ha il compito di duplicare i flussi ricevuti in input e inoltrarli contemporaneamente sia al sistema legacy CC MF sia al nuovo Core Banking cloud-native. In questo modo, entrambi i sistemi ricevono esattamente le stesse informazioni operative e possono elaborarle parallelamente. Questa configurazione prende il nome di Dual Run e rappresenta una delle pratiche più utilizzate nei programmi di migrazione di sistemi mission critical, specialmente in contesti ad alta criticità come quello bancario, dove si devono rispettare linee guida sulle procedure di disaster recovery, come definito anche all'interno della normativa DORA.[14]

In uscita dai due core le informazioni vengono scritte sui topic, quelle del master su un topic pay che poi procederà ad inviarle verso i sistemi downstream, mentre quelle del sistema slave su un topic pap di scarto. L'obiettivo del Dual Run non è ancora quello di utilizzare il nuovo core banking per l'operatività reale della banca, bensì quello di verificare che il nuovo sistema produca esattamente gli stessi risultati del sistema legacy in ogni scenario operativo.

Attualmente, quindi, il nuovo Core Banking riceve ed elabora tutti i flussi informativi provenienti dalle filiere, ma gli output generati non vengono ancora utilizzati ai fini operativi. Il sistema cloud-native opera, infatti, in parallelo rispetto al mainframe esclusivamente a scopo di verifica, monitoraggio e validazione funzionale.

L'intero processo di Dual Run è basato sul principio della quadratura costante tra i due sistemi. Per garantire che il comportamento del nuovo core banking sia perfettamente allineato a quello del sistema legacy, vengono effettuate verifiche periodiche, mediante l'utilizzo di uno strumento detto quadratore Google, che a intervalli regolari durante l'arco della giornata verifica i disallineamenti. Tali controlli consistono nella

misurazione della quadratura tra i dati elaborati dai due sistemi e vengono eseguiti sei volte al giorno, attraverso rilevazioni denominate da SK1 a SK6.

Le attività di quadratura consentono di confrontare in modo puntuale gli esiti delle elaborazioni effettuate dal CC MF e dal nuovo Core Banking, verificando che ogni operazione produca risultati identici in entrambi gli ambienti. L'obiettivo finale di questa fase è raggiungere una quadratura costante pari al 100%, condizione necessaria per garantire che il nuovo sistema possa sostituire completamente il mainframe senza introdurre anomalie operative o inconsistenze nei dati.

Il raggiungimento di tale obiettivo richiede tuttavia il completamento dello sviluppo di alcuni componenti ancora mancanti all'interno del nuovo Core Banking. Durante questa fase, infatti, vengono progressivamente corrette eventuali differenze comportamentali, ottimizzati i processi di elaborazione e completate le funzionalità necessarie per garantire piena equivalenza operativa tra i due ambienti.

Una volta terminati gli sviluppi e raggiunti livelli di quadratura stabili e affidabili, il progetto potrà entrare nella fase finale della migrazione. In questa configurazione target, il nuovo Core Banking cloud-native diventerà il sistema master operativo della banca, sostituendo definitivamente il CC MF.

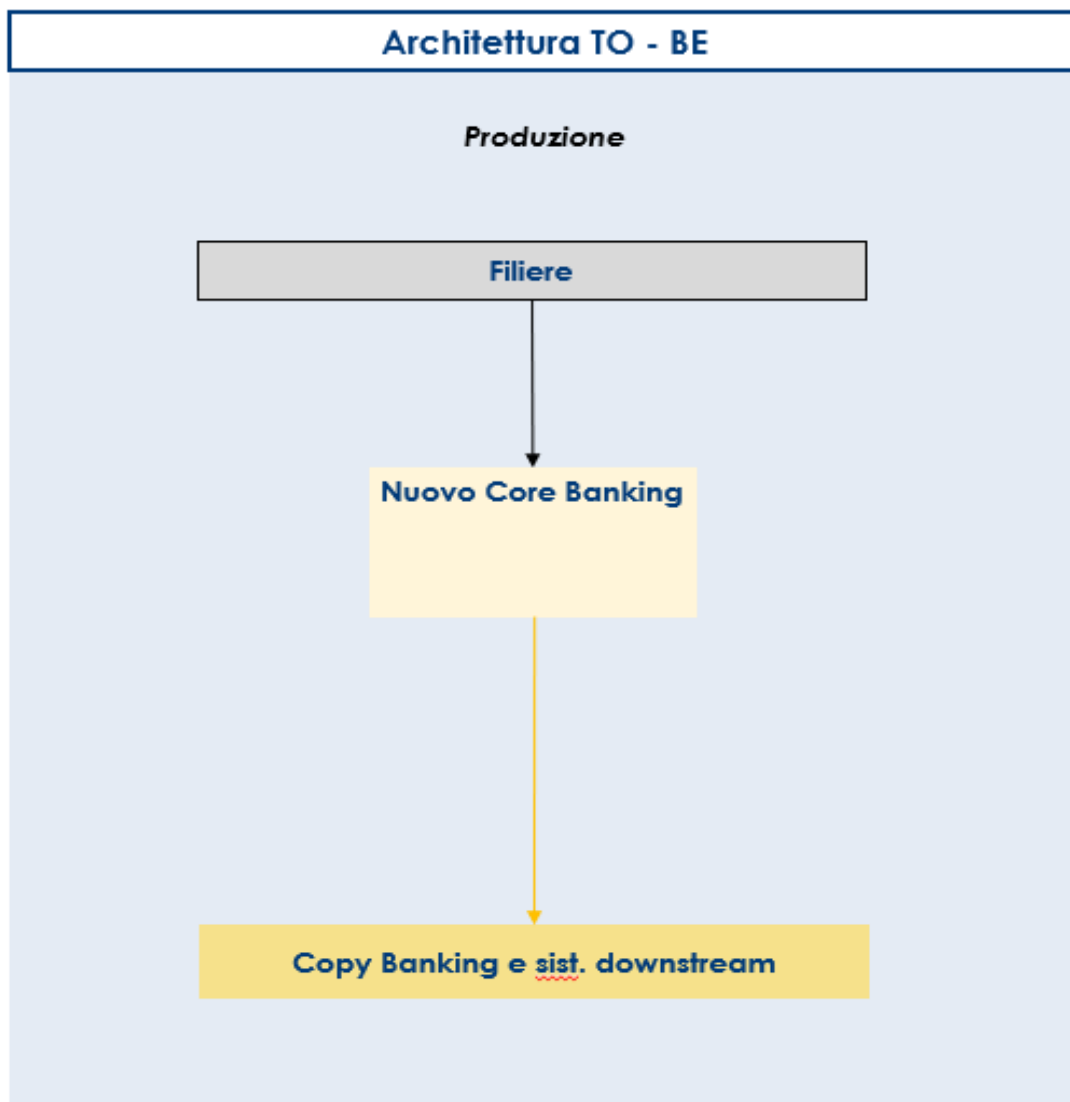


Figura 8. Rappresentazione nuova architettura IT target

L'architettura finale tornerà quindi a una configurazione più lineare e semplificata, ma completamente rinnovata dal punto di vista tecnologico. Le filiere applicative invieranno direttamente i propri flussi al nuovo Core Banking, che provvederà all'elaborazione delle informazioni e alla successiva distribuzione dei dati verso il Copy Banking e gli altri sistemi downstream.

Anche nella nuova architettura, tali sistemi continueranno a svolgere funzioni fondamentali di replica, conservazione e protezione delle informazioni, garantendo resilienza, continuità operativa e disponibilità dei dati. Tuttavia, a differenza del modello precedente, il nuovo ecosistema sarà costruito su paradigmi architetturali moderni, caratterizzati da maggiore scalabilità, modularità e capacità evolutiva.

Il passaggio a un'architettura cloud-native consentirà infatti di introdurre modelli basati su microservizi, integrazioni API-driven e componenti distribuiti, migliorando significativamente flessibilità operativa, rapidità di rilascio e capacità di adattamento alle evoluzioni del business. Inoltre, la nuova infrastruttura permetterà di sfruttare meccanismi avanzati di automazione, orchestrazione e monitoraggio continuo, aumentando resilienza e disponibilità dei servizi core.

L'evoluzione architetturale descritta rappresenta quindi un elemento centrale dell'intero programma di trasformazione digitale della banca. Il progetto non consiste semplicemente nella sostituzione di una piattaforma tecnologica, ma nella costruzione di un nuovo modello operativo orientato al cloud computing, alla centralità del dato e alla modernizzazione del core banking secondo paradigmi maggiormente flessibili, scalabili e resilienti.

5.4 Il piano di migrazione

Il raggiungimento di una quadratura stabile e costante pari al 100% tra il sistema legacy CC MF e il nuovo Core Banking rappresenta il prerequisito fondamentale per poter avviare l'effettivo processo di migrazione dei conti correnti verso la nuova piattaforma cloud-native. Tuttavia, la sola validazione funzionale del nuovo sistema non è sufficiente a garantire il successo dell'iniziativa. Affinché la migrazione possa essere eseguita in sicurezza, è infatti necessario che anche il processo operativo di impianto e trasferimento dei dati sia stato preventivamente testato, verificato e consolidato.

Per questo motivo, parallelamente alle attività di sviluppo e validazione del nuovo Core Banking, vengono eseguite periodicamente simulazioni complete dell'evento di migrazione. Tali esercitazioni hanno l'obiettivo di verificare la correttezza delle procedure operative, misurare le tempistiche di esecuzione, individuare eventuali criticità e garantire che tutte le componenti coinvolte siano in grado di operare correttamente durante il passaggio effettivo in ambiente di produzione.

Con il termine impianto si intende il processo attraverso il quale i conti correnti e tutte le relative informazioni vengono caricati all'interno del nuovo Core Banking. Dal punto di vista tecnico, l'impianto consiste nel popolamento delle tabelle del database della nuova piattaforma mediante i dati provenienti dal sistema legacy. Si tratta quindi del

momento in cui il patrimonio informativo gestito dal CC MF viene trasferito e reso disponibile sul nuovo ambiente.

Le simulazioni attualmente eseguite non avvengono tuttavia sull'ambiente produttivo della banca, ossia quello utilizzato quotidianamente per la gestione delle operazioni reali dei clienti. Esse vengono effettuate in ambienti dedicati e separati dalla produzione, così da evitare qualsiasi impatto sull'operatività ordinaria dell'istituto e consentire l'esecuzione di test approfonditi in condizioni controllate.

Per garantire un processo di migrazione affidabile e ripetibile, è stato definito un modello operativo articolato in cinque fasi consecutive, ciascuna delle quali contribuisce alla corretta esecuzione dell'evento finale.

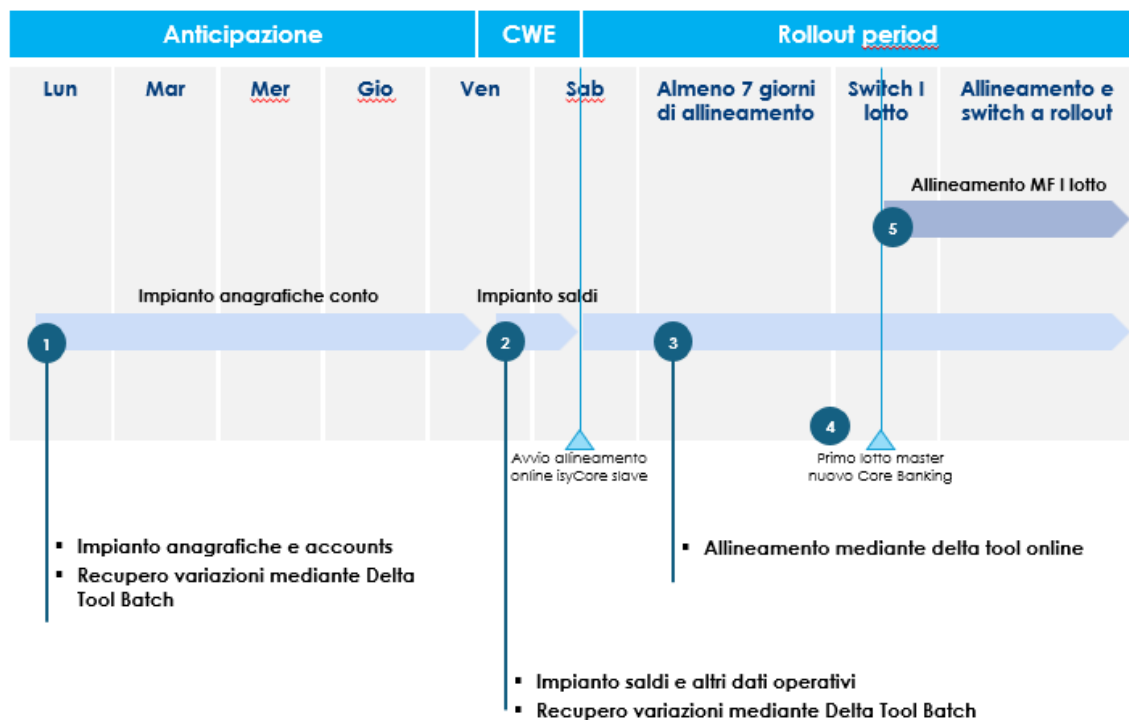


Figura 9. Timeline operativa del processo di migrazione

Il processo prevede come primo step l'impianto delle anagrafiche e degli account, seguito dal caricamento delle restanti informazioni operative, tra cui saldi, movimenti e dati correlati. Successivamente viene avviato un periodo di allineamento controllato tra i due sistemi, finalizzato a verificare il corretto funzionamento della nuova piattaforma in condizioni operative reali. Solo al termine di tale fase sarà possibile procedere con il passaggio effettivo dei conti correnti al nuovo Core Banking.

L'avvio del processo è previsto all'inizio della settimana operativa, generalmente nella giornata di lunedì, con il caricamento delle anagrafiche e degli account sul nuovo sistema. Poiché durante questa fase il sistema legacy continua a essere l'unico ambiente operativo della banca, i dati presenti nei due sistemi tendono inevitabilmente a divergere a causa delle normali attività svolte dai clienti e dagli operatori.

Per mantenere allineate le basi dati viene quindi attivato uno specifico componente applicativo denominato Delta Tool. Tale strumento ha il compito di intercettare le variazioni che avvengono sul sistema legacy e replicarle sul nuovo Core Banking, garantendo che quest'ultimo disponga sempre di informazioni aggiornate rispetto all'ambiente operativo principale.

Nella notte tra venerdì e sabato viene eseguita la seconda fase dell'impianto, durante la quale vengono trasferite tutte le restanti entità necessarie al funzionamento del sistema, comprese le informazioni relative ai saldi e agli altri dati operativi. La scelta di questa finestra temporale non è casuale: il fine settimana rappresenta infatti il periodo caratterizzato dal minor volume di operazioni bancarie, riducendo così il rischio operativo e semplificando la gestione dell'intero processo.

Anche durante questa fase il Delta Tool continua a svolgere un ruolo fondamentale, mantenendo sincronizzati i due ambienti ed evitando che eventuali modifiche intervenute durante l'impianto possano generare disallineamenti tra il sistema legacy e il nuovo Core Banking.

Nelle prime due fasi della migrazione il Delta Tool opera in modalità batch. In questa configurazione, le variazioni rilevate sul sistema legacy vengono temporaneamente accumulate e successivamente trasferite al nuovo Core Banking attraverso elaborazioni pianificate. Questo approccio consente di gestire grandi volumi di dati in modo efficiente durante le attività di caricamento iniziale.

Una volta completato l'impianto, il Delta Tool passa invece a una modalità di funzionamento online. Da questo momento ha inizio la terza fase dove il nuovo Core Banking viene aggiornato in modalità near real time, ricevendo quasi istantaneamente tutte le variazioni generate sul sistema legacy. L'avvio di questa modalità segna l'inizio della fase di rollout.

Il periodo di rollout è la parte più delicata dell'intero processo. Durante questo intervallo temporale il nuovo Core Banking viene sottoposto a un monitoraggio continuo al fine di verificarne il corretto comportamento in condizioni operative reali. In

particolare, vengono effettuati controlli finalizzati a garantire l'idempotenza delle operazioni, ossia la capacità del sistema di evitare duplicazioni indesiderate e di assicurare che una stessa transazione non venga elaborata più volte.

Solo al termine di questo periodo di osservazione e dopo aver verificato la piena stabilità della piattaforma sarà possibile avviare la quarta fase della migrazione, ovvero il passaggio dei conti correnti al nuovo Core Banking. Anche questa attività non verrà eseguita in un'unica soluzione, ma seguirà un approccio progressivo e controllato. La clientela verrà infatti suddivisa in differenti lotti di migrazione, che saranno trasferiti gradualmente dal sistema legacy al nuovo ambiente cloud-native. Questa strategia consente di limitare i rischi operativi e di intervenire tempestivamente qualora emergessero anomalie durante il processo.

Considerata la criticità del servizio bancario, è stata inoltre prevista una specifica strategia di disaster recovery finalizzata a garantire la possibilità di ripristinare rapidamente il sistema legacy in caso di problematiche gravi sul nuovo Core Banking. Tale ulteriore livello di sicurezza, oltre a rispondere a specifiche esigenze operative del business, è richiesto anche dal regolamento DORA [14], che impone alle istituzioni finanziarie l'adozione di misure volte a rafforzare la resilienza operativa e la sicurezza delle infrastrutture ICT. Durante la fase successiva allo switch, ovvero la quinta e ultima fase, il Delta Tool continuerà infatti a essere utilizzato per mantenere aggiornato anche il CC MF, invertendo il flusso di sincronizzazione precedentemente adottato. In questo modo il sistema legacy conserverà una copia costantemente allineata delle informazioni presenti sul nuovo Core Banking e potrà essere nuovamente designato come sistema master qualora si rendesse necessario effettuare un rollback dell'intera migrazione.

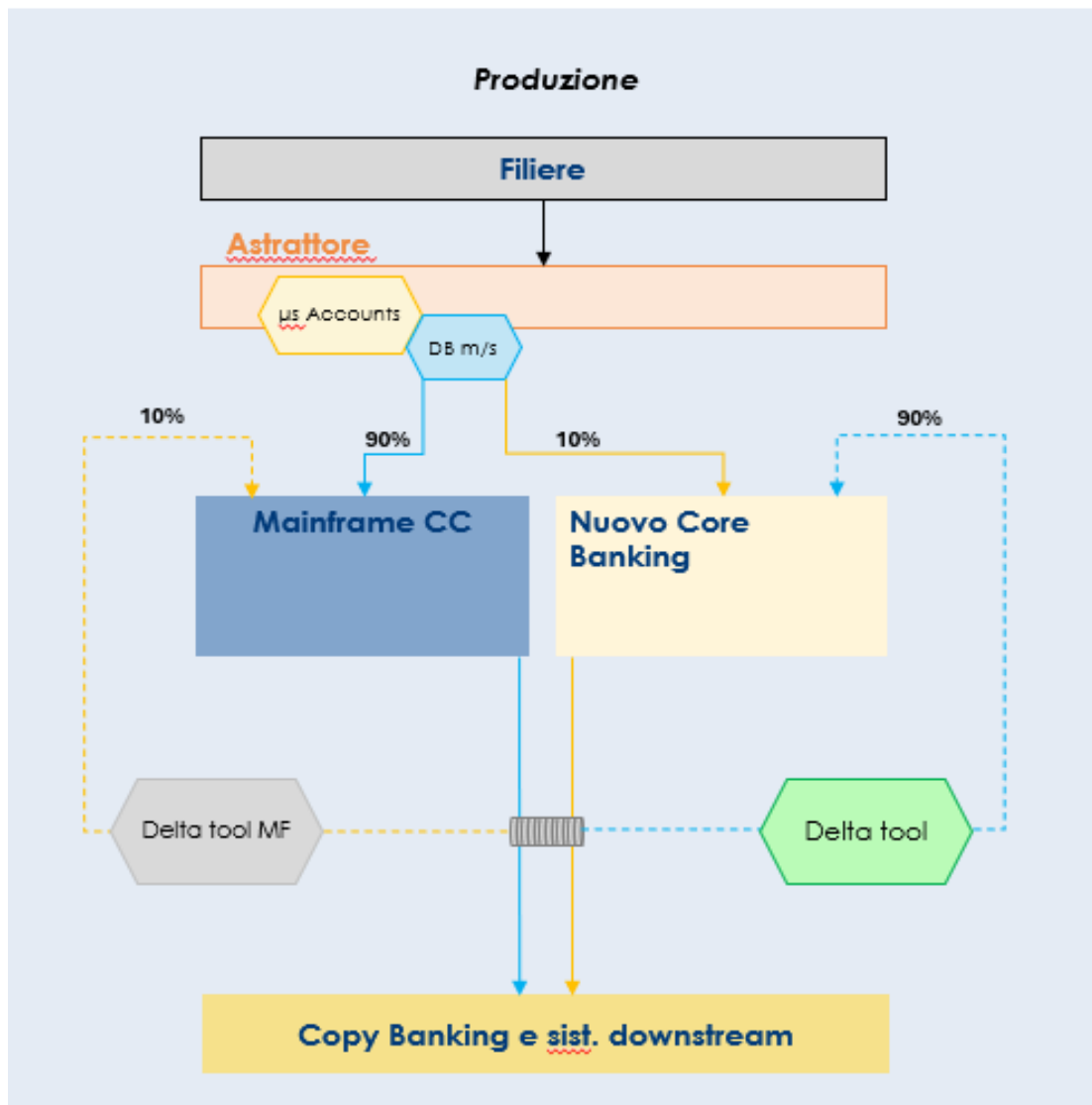


Figura 10. Architettura completa comprendente i Delta Tool necessari per l'allineamento dei due Core Banking in fase di migrazione e per un eventuale rollback

L'approccio descritto evidenzia come, in un contesto altamente regolamentato e critico quale quello bancario, il successo di una migrazione cloud non dipenda esclusivamente dalla qualità della nuova piattaforma tecnologica, ma anche dalla definizione di procedure operative rigorose, dalla capacità di controllare costantemente la coerenza dei dati e dall'adozione di adeguate strategie di continuità operativa e gestione del rischio.

5.5 Governance e coordinamento del progetto

La complessità e la criticità del programma di migrazione hanno reso necessario l'adozione di un modello di governance strutturato, finalizzato a garantire il coordinamento tra le numerose iniziative coinvolte e a supportare il processo decisionale durante tutte le fasi del progetto. La presenza di molteplici stakeholder, appartenenti sia alle strutture IT sia alle funzioni di business, ha richiesto un presidio costante delle attività e un monitoraggio continuo dell'avanzamento complessivo del programma.

In questo contesto, una delle attività principali ha riguardato il coordinamento trasversale tra i diversi team coinvolti nella trasformazione del core banking. Lo stream di migrazione risultava infatti fortemente dipendente dall'avanzamento di numerose iniziative parallele, tra cui lo sviluppo delle nuove componenti applicative, la realizzazione delle integrazioni, le attività di test e la preparazione degli ambienti necessari all'esecuzione degli impianti. È stato quindi fondamentale garantire un costante allineamento tra le diverse strutture coinvolte, monitorando dipendenze, criticità e possibili impatti sul piano complessivo di migrazione.

Particolare rilevanza ha assunto il monitoraggio quotidiano dello stato di avanzamento del programma attraverso incontri ricorrenti con il management e con i responsabili dei principali stream progettuali. Tali momenti di confronto rappresentavano uno strumento essenziale per verificare il raggiungimento degli obiettivi intermedi, condividere eventuali criticità e supportare le decisioni necessarie alla prosecuzione delle attività. Durante questi incontri venivano analizzati i principali indicatori di avanzamento del progetto, con particolare attenzione ai risultati delle attività di Dual Run e agli esiti delle simulazioni di migrazione.

Tra gli elementi maggiormente monitorati vi erano le verifiche di quadratura tra il sistema legacy CC MF e il nuovo Core Banking, effettuate attraverso le sei rilevazioni giornaliere denominate SK1, SK2, SK3, SK4, SK5 e SK6. L'analisi costante di tali indicatori consentiva di valutare il livello di allineamento tra i due sistemi e di identificare tempestivamente eventuali anomalie o differenze comportamentali che avrebbero potuto compromettere il raggiungimento della quadratura completa. Sebbene i valori potessero presentare fisiologiche oscillazioni nel corso della giornata in

funzione delle elaborazioni in esecuzione, nel periodo più recente del programma i livelli di quadratura si sono mantenuti stabilmente superiori al 99%, con picchi di quadratura fino al 99.9% evidenziando un elevato grado di affidabilità del processo di migrazione e confermando la progressiva maturazione del nuovo ecosistema applicativo. Tali livelli seppur molto alti però non sono ancora considerati soddisfacenti, in quanto sono una quadratura costante del 100% può garantire alla banca di non esporsi a rischi.

Parallelamente, venivano esaminati gli esiti delle simulazioni di impianto, con l'obiettivo di verificare la stabilità delle procedure di migrazione, il rispetto delle tempistiche previste e la corretta esecuzione dei meccanismi di sincronizzazione tra i due ambienti. Le simulazioni hanno rappresentato uno degli strumenti principali per validare il modello operativo adottato e preparare l'organizzazione agli eventi di migrazione effettivi. Avviate nel mese di aprile, esse risultano tuttora in corso e, al momento della stesura del presente elaborato, sono state eseguite complessivamente più di venti simulazioni, con una frequenza media prossima a due esercizi settimanali. La reiterazione continua di tali attività ha consentito di testare in modo approfondito le procedure operative, consolidare il coordinamento tra i diversi team coinvolti e individuare preventivamente eventuali criticità suscettibili di compromettere il corretto svolgimento degli impianti.

A supporto di queste attività, è stato inoltre predisposto un sistema di reporting direzionale volto a consolidare le informazioni provenienti dai diversi cantieri progettuali e a fornire una visione integrata dello stato del programma. Tale reporting ha consentito al management di disporre di un quadro aggiornato sull'evoluzione della migrazione, sui principali rischi identificati e sulle azioni correttive eventualmente necessarie.

L'insieme di queste attività ha contribuito a garantire un governo efficace del progetto, favorendo il coordinamento tra le diverse funzioni coinvolte e assicurando un controllo continuo sull'avanzamento di un'iniziativa caratterizzata da elevata complessità tecnologica e da requisiti particolarmente stringenti in termini di affidabilità, continuità operativa e qualità del dato.

5.6 Il ruolo del PMO all'interno del progetto

All'interno di questo contesto progettuale, il ruolo svolto nell'ambito del Project Management Office è stato principalmente orientato al supporto delle attività di governance e coordinamento dello stream di migrazione, contribuendo a garantire il presidio operativo delle iniziative necessarie al raggiungimento degli obiettivi di programma.

Una parte significativa delle attività ha riguardato il monitoraggio strutturato delle milestone progettuali, delle dipendenze tra i diversi cantieri di lavoro e dei principali rischi associati alle varie fasi della migrazione. In un programma caratterizzato da una forte interconnessione tra sviluppo applicativo, test, attività infrastrutturali e preparazione degli eventi di impianto, è risultato fondamentale assicurare una visione integrata dell'avanzamento complessivo, individuando tempestivamente eventuali elementi di criticità in grado di influenzare le tempistiche o la qualità delle attività pianificate.

Parallelamente, è stato svolto un costante lavoro di raccordo tra le diverse strutture coinvolte nel progetto, favorendo l'allineamento tra le esigenze funzionali espresse dal business, i vincoli tecnici delle architetture applicative e le necessità operative dei team responsabili della delivery. Tale attività ha contribuito a facilitare la condivisione delle informazioni, la gestione delle dipendenze e la definizione delle priorità operative, elementi particolarmente rilevanti in un contesto caratterizzato dalla presenza di numerosi stakeholder e da un elevato livello di complessità organizzativa.

Un ulteriore ambito di coinvolgimento ha riguardato la predisposizione e l'aggiornamento della reportistica direzionale a supporto del management. Attraverso l'analisi e il consolidamento delle informazioni provenienti dai diversi stream progettuali è stato possibile fornire una rappresentazione puntuale dello stato di avanzamento delle attività, evidenziando i principali elementi di attenzione, l'evoluzione dei rischi e le eventuali azioni correttive necessarie a garantire il rispetto degli obiettivi pianificati.

Particolare rilevanza hanno assunto inoltre le attività di definizione e monitoraggio dei modelli operativi adottati per la migrazione. In questo ambito è stato fornito supporto alla pianificazione e al coordinamento delle diverse fasi del processo, verificando la

corretta esecuzione delle attività previste e il rispetto dei prerequisiti necessari per l'avvio delle successive fasi progettuali.

Il coinvolgimento operativo è risultato particolarmente significativo durante gli eventi di impianto e le successive attività di stabilizzazione. In tali occasioni è stato garantito un presidio continuo delle operazioni, supportando il coordinamento tra i diversi team coinvolti e monitorando l'avanzamento delle attività durante le finestre di migrazione, al fine di assicurare una gestione controllata dell'intero processo e una rapida risoluzione di eventuali anomalie.

Infine, una componente rilevante del ruolo ha riguardato il supporto alle attività di test management e defect management. La progressiva validazione del nuovo Core Banking ha richiesto infatti un monitoraggio costante dell'avanzamento delle campagne di test, della copertura degli scenari previsti e dello stato di risoluzione delle anomalie individuate. Tale attività ha contribuito a garantire la qualità complessiva della soluzione e a supportare il raggiungimento delle condizioni necessarie per l'avanzamento delle diverse fasi della migrazione.

Capitolo sesto

6. Confronto tra approcci teorici e realtà progettuale

L'obiettivo del capitolo è quello di confrontare il quadro teorico delineato nei capitoli precedenti con le evidenze emerse dall'analisi del caso di studio, al fine di valutare il livello di allineamento tra i modelli di riferimento esaminati e le pratiche effettivamente adottate nel progetto di migrazione cloud analizzato. In particolare, verranno esaminate le modalità con cui i principi del framework Cloud Data Management Capabilities (CDMC) sono stati applicati all'interno del programma, evidenziando gli elementi di maggiore coerenza con il modello teorico e le principali aree di miglioramento emerse nel corso delle attività progettuali.

Successivamente, l'attenzione sarà rivolta al potenziale contributo che gli strumenti di Generative AI potrebbero offrire in un contesto progettuale caratterizzato da elevata complessità organizzativa e tecnologica. Attraverso il confronto tra le attività effettivamente svolte dal Project Management Office e le applicazioni dell'intelligenza artificiale generativa analizzate nel capitolo precedente, verranno individuati i principali ambiti nei quali tali tecnologie potrebbero contribuire ad aumentare l'efficienza operativa, migliorare i processi di coordinamento e supportare le attività di monitoraggio e reporting.

Infine, sulla base delle evidenze raccolte, verrà proposta una sintesi complessiva dei risultati emersi dall'analisi, evidenziando come il successo di programmi di trasformazione digitale di elevata complessità dipenda dall'integrazione tra solide pratiche di governance del dato, efficaci modelli di project management e capacità di adottare strumenti innovativi a supporto dei processi decisionali e operativi.

6.1 Analisi del progetto rispetto al framework CDMC

L'analisi del progetto di migrazione consente di confrontare le pratiche effettivamente adottate con i principi definiti dal framework Cloud Data Management Capabilities (CDMC), evidenziando un livello complessivamente elevato di allineamento tra il modello teorico e le modalità operative osservate nel contesto reale.

Per quanto riguarda la componente Governance & Accountability, il progetto presentava una struttura di governo particolarmente articolata e coerente con quanto previsto dal framework. L'avanzamento delle attività veniva infatti monitorato attraverso incontri periodici con il management e con i responsabili dei diversi stream progettuali, supportati da sistemi di reporting e da indicatori di performance utilizzati per valutare costantemente lo stato della migrazione. Inoltre, con cadenza periodica venivano organizzati momenti di allineamento estesi finalizzati a condividere l'avanzamento complessivo del programma e le principali criticità emerse. Tali pratiche risultano pienamente coerenti con i principi di responsabilizzazione, monitoraggio continuo e supporto ai processi decisionali promossi dal framework.

Anche la componente Cataloging & Classification appariva sostanzialmente allineata alle best practice descritte dal CDMC. La natura particolarmente sensibile delle informazioni gestite imponeva infatti processi rigorosi di classificazione, catalogazione e certificazione del dato, necessari per garantire tracciabilità, qualità e conformità normativa. Durante il progetto è stato possibile osservare come le informazioni fossero costantemente gestite secondo criteri di classificazione ben definiti, elemento fondamentale per supportare le successive attività di controllo, migrazione e protezione.

Per quanto concerne Accessibility & Usage, il progetto adottava meccanismi di controllo degli accessi conformi ai principi di sicurezza previsti dal framework, in particolare attraverso l'applicazione del principio del *least privilege*, secondo cui ogni utente dispone esclusivamente delle autorizzazioni strettamente necessarie allo svolgimento delle proprie attività. Sebbene tale approccio contribuisse a ridurre significativamente il rischio di accessi non autorizzati, sono emerse occasionalmente alcune criticità operative. In alcuni casi, infatti, una valutazione non completamente accurata delle autorizzazioni necessarie comportava l'assenza di utenti abilitati a eseguire specifiche attività, rendendo necessario richiedere nuovi accessi durante le fasi operative e generando conseguenti rallentamenti. Pur non rappresentando una

problematica strutturale, questo aspetto evidenzia come la corretta gestione degli accessi richieda un equilibrio tra sicurezza e operatività.

La componente Protection & Privacy rappresentava uno degli ambiti maggiormente presidiati dell'intero programma. Considerata la natura altamente sensibile dei dati trattati, venivano adottate misure rigorose volte a garantire la protezione delle informazioni e la conformità ai requisiti normativi. Anche durante le attività di test e simulazione, che richiedevano l'utilizzo di dati provenienti dagli ambienti produttivi, venivano applicati specifici meccanismi di mascheramento e limitazione della visibilità delle informazioni, in linea con quanto richiesto dal regolamento GDPR. [11]

In molti casi i dataset utilizzati non risultavano aggiornati o venivano rese disponibili esclusivamente le informazioni strettamente necessarie alle attività da svolgere, riducendo così il rischio di esposizione di dati personali.

Anche la gestione del Data Lifecycle risultava generalmente coerente con i principi definiti dal framework. Il settore bancario è infatti caratterizzato da stringenti obblighi normativi relativi alla conservazione delle informazioni, che impongono il mantenimento dei dati per periodi temporali ben definiti anche successivamente alla chiusura dei rapporti contrattuali, in particolare anche in seguito alla chiusura di un conto, i dati relativi a quest'ultimo vanno mantenuti per un minimo di 10 anni. [16]

Nel caso osservato, le politiche di retention risultavano correttamente implementate nella maggior parte dei casi. Sono tuttavia emerse alcune anomalie legate all'attribuzione errata delle date di conservazione, che in determinate circostanze portavano alcuni dati ad avere scadenze estremamente lontane nel tempo, talvolta dell'ordine di decine o centinaia di anni. Sebbene tali situazioni non compromettessero direttamente la sicurezza o la disponibilità delle informazioni, esse generavano un incremento non necessario dei costi di storage e contribuivano ad aumentare la complessità complessiva della base dati, oltre che comportare una non conformità con regolamenti in materia di privacy dei dati, come il GDPR [11], che impone la cancellazione delle informazioni degli utenti quando non più necessarie. Questo aspetto evidenzia l'importanza di affiancare alle policy di retention anche controlli automatici di qualità e validazione delle informazioni associate al ciclo di vita del dato.

Infine, la componente Data & Technical Architecture rappresentava uno degli elementi centrali dell'intero progetto di trasformazione. L'evoluzione verso un'architettura cloud-native costituiva infatti l'obiettivo principale dell'iniziativa e richiedeva una

progettazione particolarmente accurata delle componenti applicative, delle integrazioni e dei meccanismi di sincronizzazione tra vecchio e nuovo sistema. Durante il progetto è stato possibile osservare un forte presidio architetturale, caratterizzato da processi di progettazione dettagliati, verifiche continue e soluzioni orientate alla resilienza e alla ridondanza. Tale approccio risulta pienamente coerente con le indicazioni del framework, che identifica nell'architettura tecnologica uno degli elementi fondamentali per garantire scalabilità, affidabilità e sostenibilità operativa degli ambienti cloud.

Nel complesso, il confronto tra il framework CDMC e il caso di studio evidenzia un elevato livello di maturità nella gestione dei dati e nella governance della migrazione. Le principali aree di miglioramento individuate non riguardano l'assenza di processi o controlli, quanto piuttosto l'ottimizzazione di alcuni meccanismi operativi, in particolare relativamente alla gestione delle autorizzazioni e al controllo delle politiche di conservazione dei dati. Tali aspetti confermano come, anche in contesti caratterizzati da una governance solida e da elevati standard di controllo, esistano margini di miglioramento finalizzati ad aumentare ulteriormente efficienza operativa e qualità complessiva della gestione del dato.

6.2 Potenziale contributo della generative AI nel progetto

L'analisi delle attività svolte all'interno del programma di migrazione evidenzia come l'introduzione di strumenti di Generative AI avrebbe potuto offrire interessanti opportunità di miglioramento in numerosi ambiti del project management, contribuendo a ridurre il carico operativo associato alle attività amministrative e di coordinamento e consentendo una maggiore focalizzazione sulle decisioni strategiche e sulla gestione delle criticità progettuali.

Uno degli ambiti in cui il contributo dell'intelligenza artificiale sarebbe risultato maggiormente significativo riguarda la produzione della reportistica direzionale. Come descritto nel capitolo precedente, una parte rilevante delle attività del PMO consisteva nella raccolta e nel consolidamento delle informazioni provenienti dai diversi stream progettuali al fine di predisporre report periodici destinati al management. Tali documenti richiedevano un'attività continua di analisi, sintesi e rielaborazione delle informazioni relative allo stato di avanzamento della migrazione, all'andamento delle simulazioni di impianto, ai livelli di quadratura tra i due core banking e all'evoluzione

dei principali rischi progettuali. In questo contesto, strumenti di Generative AI avrebbero potuto automatizzare parte del processo di produzione dei report, trasformando dati strutturati e aggiornamenti operativi in documenti sintetici e coerenti, riducendo sensibilmente il tempo necessario alla loro predisposizione e garantendo una maggiore standardizzazione dei contenuti.

Un secondo ambito di applicazione particolarmente rilevante riguarda il supporto alle attività di pianificazione. Durante il progetto, la definizione delle timeline operative e delle sequenze di attività necessarie all'esecuzione delle simulazioni di migrazione e degli eventi di impianto richiedeva infatti un intenso lavoro manuale di coordinamento e valutazione delle dipendenze tra i diversi stream coinvolti. L'impiego di strumenti di Generative AI avrebbe potuto supportare la costruzione dei piani operativi, suggerendo attività mancanti, evidenziando dipendenze non immediatamente visibili e contribuendo alla definizione di scenari alternativi in presenza di ritardi o criticità. Inoltre, l'analisi di dati storici relativi alle precedenti simulazioni avrebbe potuto consentire stime più accurate delle tempistiche di esecuzione, migliorando l'affidabilità complessiva della pianificazione.

Un ulteriore contributo significativo avrebbe potuto riguardare le attività di comunicazione e coordinamento tra stakeholder. Il programma di migrazione coinvolgeva infatti numerosi soggetti appartenenti a strutture differenti, tra cui team di sviluppo, architetture applicative, infrastrutture, operation, business e management. Tale complessità organizzativa comportava la necessità di svolgere frequenti riunioni di avanzamento e coordinamento, al termine delle quali venivano predisposti verbali e report riepilogativi contenenti decisioni, attività assegnate e punti di attenzione emersi durante gli incontri. In questo ambito, la Generative AI avrebbe potuto automatizzare la produzione dei verbali di riunione e dei relativi action item, generando sintesi strutturate delle discussioni e contribuendo a migliorare la rapidità e la qualità della comunicazione tra i diversi stakeholder coinvolti.

Le potenzialità dell'intelligenza artificiale risultano particolarmente interessanti anche con riferimento alle attività di monitoraggio del programma. Durante il progetto venivano costantemente analizzati indicatori relativi allo stato della migrazione, tra cui gli esiti delle verifiche di quadratura SK1-SK6, l'avanzamento delle campagne di test, lo stato dei defect aperti e i risultati delle simulazioni di impianto. Sistemi basati su Generative AI avrebbero potuto supportare l'interpretazione di tali informazioni,

individuando automaticamente trend, anomalie ricorrenti o situazioni potenzialmente critiche da sottoporre all'attenzione del management. Questo avrebbe consentito una maggiore capacità di analisi preventiva e una più rapida individuazione di possibili fattori di rischio.

Infine, un ulteriore ambito di possibile applicazione riguarda il supporto alle attività di test management e defect management. Durante la validazione del nuovo Core Banking venivano gestiti numerosi difetti e anomalie che richiedevano analisi, classificazione e monitoraggio costante fino alla loro risoluzione. L'intelligenza artificiale avrebbe potuto contribuire alla categorizzazione automatica dei defect, all'identificazione di problematiche simili già affrontate in passato e alla produzione di sintesi utili per facilitare il lavoro dei team responsabili della risoluzione.

Nel complesso, l'analisi del caso di studio evidenzia come molte delle attività svolte dal PMO siano caratterizzate da un'elevata componente informativa e documentale, rendendole particolarmente adatte all'introduzione di strumenti di Generative AI. Pur non sostituendo il ruolo decisionale, relazionale e strategico del Project Manager, tali tecnologie potrebbero contribuire a ridurre il tempo dedicato alle attività ripetitive e a basso valore aggiunto, migliorando l'efficienza operativa e consentendo una maggiore focalizzazione sugli aspetti di governance, coordinamento e gestione delle criticità che caratterizzano programmi di trasformazione complessi come quello analizzato.

6.3 Sintesi delle evidenze emerse

L'analisi condotta nel presente capitolo ha consentito di confrontare i principi teorici introdotti nei capitoli precedenti con le modalità operative osservate all'interno del progetto di migrazione del core banking, evidenziando sia gli elementi di allineamento sia le principali opportunità di miglioramento.

Per quanto riguarda la gestione del dato, il confronto con il framework CDMC ha mostrato un elevato livello di maturità complessiva del programma. Le pratiche adottate nel progetto risultano infatti ampiamente coerenti con le principali capability previste dal modello, in particolare relativamente agli aspetti di governance, classificazione del dato, controllo degli accessi, protezione delle informazioni e progettazione architetturale. La natura altamente regolamentata del settore bancario e la criticità delle informazioni trattate hanno contribuito all'adozione di processi strutturati e di

meccanismi di controllo rigorosi, consentendo di garantire elevati livelli di sicurezza, tracciabilità e affidabilità durante tutte le fasi della migrazione.

Le principali aree di miglioramento individuate non riguardano l'assenza di processi di governance o di controlli formali, quanto piuttosto l'ottimizzazione di alcuni aspetti operativi. Tra questi emergono, ad esempio, la gestione delle autorizzazioni secondo il principio del least privilege e il monitoraggio delle politiche di retention dei dati, ambiti nei quali sono state riscontrate alcune inefficienze pur in presenza di procedure complessivamente adeguate. Tali evidenze confermano come il raggiungimento di elevati livelli di maturità nella gestione del dato non elimini la necessità di un miglioramento continuo dei processi e dei controlli adottati.

Parallelamente, il confronto con le più recenti evoluzioni del project management ha evidenziato il potenziale contributo che gli strumenti di Generative AI potrebbero apportare in programmi di trasformazione complessi come quello analizzato. Le attività svolte dal PMO risultano infatti fortemente caratterizzate dalla gestione di grandi quantità di informazioni, dalla produzione di documentazione progettuale, dal coordinamento tra stakeholder e dal monitoraggio continuo dell'avanzamento delle iniziative. In questo contesto, l'intelligenza artificiale potrebbe rappresentare un importante fattore abilitante per l'automazione di attività ripetitive e a basso valore aggiunto, contribuendo a migliorare efficienza operativa, rapidità di elaborazione delle informazioni e qualità del supporto decisionale.

L'analisi svolta suggerisce tuttavia che il valore della Generative AI non debba essere interpretato in un'ottica sostitutiva rispetto al ruolo del Project Manager o del PMO. Le attività di coordinamento, gestione delle relazioni, valutazione delle criticità e assunzione delle decisioni continuano infatti a richiedere competenze umane, capacità di giudizio e conoscenza del contesto organizzativo che non possono essere delegate integralmente a strumenti automatizzati. L'intelligenza artificiale appare piuttosto come un elemento complementare, in grado di supportare i professionisti nella gestione delle informazioni e di liberare tempo da dedicare alle attività a maggior valore strategico.

Nel complesso, il caso di studio analizzato evidenzia come il successo di programmi di trasformazione digitale di elevata complessità dipenda dalla combinazione di diversi fattori: una solida governance del dato, processi strutturati di gestione del progetto, un efficace coordinamento tra gli stakeholder coinvolti e la capacità di adottare strumenti innovativi in grado di incrementare l'efficienza operativa. In questa prospettiva,

l'integrazione tra framework di data governance consolidati e tecnologie basate su intelligenza artificiale rappresenta una possibile direzione evolutiva per i futuri programmi di migrazione cloud nel settore bancario, consentendo di coniugare controllo, affidabilità e innovazione all'interno di contesti caratterizzati da crescente complessità tecnologica e organizzativa.

Capitolo settimo

7. Conclusioni

L'obiettivo del presente capitolo è quello di sintetizzare le principali evidenze emerse nel corso dell'elaborato, mettendo in relazione gli aspetti teorici analizzati con i risultati derivanti dallo studio del caso di migrazione cloud esaminato. In particolare, verranno ripresi i principali elementi che caratterizzano il processo di trasformazione digitale del settore bancario e le sfide associate alla modernizzazione delle infrastrutture legacy, evidenziando il ruolo assunto dalla governance progettuale e dalla gestione dei dati nel successo delle iniziative di migrazione verso il cloud.

Successivamente, l'attenzione sarà rivolta al contributo offerto dal framework Cloud Data Management Capabilities (CDMC), analizzandone il valore come modello di riferimento per la governance del dato negli ambienti cloud e valutandone l'applicabilità rispetto alle evidenze emerse dal caso di studio. Verrà inoltre approfondito il tema dell'evoluzione del project management alla luce delle più recenti innovazioni tecnologiche, con particolare riferimento alle opportunità offerte dall'intelligenza artificiale generativa a supporto delle attività di pianificazione, monitoraggio e coordinamento progettuale.

Infine, saranno presentate alcune considerazioni sulle possibili evoluzioni future della gestione dei dati e dei programmi di trasformazione digitale nel settore bancario, evidenziando come l'integrazione tra cloud computing, data governance e strumenti basati su intelligenza artificiale possa rappresentare un importante fattore abilitante per affrontare le sfide poste da contesti organizzativi e tecnologici sempre più complessi.

7.1 Considerazioni finali sul caso di studio

L'analisi sviluppata nel corso dell'elaborato ha evidenziato come il settore bancario stia attraversando una profonda fase di trasformazione digitale, caratterizzata dalla crescente centralità del dato e dalla necessità di adottare infrastrutture tecnologiche più moderne, flessibili e scalabili. In questo contesto, il cloud computing rappresenta uno dei principali fattori abilitanti dell'innovazione, consentendo agli istituti finanziari di superare progressivamente i limiti delle architetture legacy e di supportare modelli operativi maggiormente orientati all'efficienza, alla resilienza e alla valorizzazione delle informazioni.

Il caso di studio analizzato si inserisce pienamente all'interno di questo scenario evolutivo. Il progetto di migrazione dei dati dei conti correnti verso una nuova piattaforma cloud-native ha rappresentato un'iniziativa di particolare rilevanza strategica, non soltanto per la complessità tecnologica delle soluzioni implementate, ma anche per le implicazioni organizzative, operative e di governance che hanno accompagnato l'intero percorso di trasformazione. La necessità di garantire la continuità dei servizi bancari, preservare l'integrità delle informazioni e coordinare numerose iniziative tra loro interdipendenti ha reso il programma particolarmente articolato e caratterizzato da elevati livelli di complessità.

In tale contesto, è emersa con chiarezza l'importanza di una governance strutturata e di un efficace coordinamento tra tutti gli stakeholder coinvolti. La presenza di team appartenenti a differenti ambiti organizzativi, tra cui sviluppo applicativo, architetture, infrastrutture, operation, business e management, ha richiesto un costante allineamento delle attività e un monitoraggio continuo dell'avanzamento progettuale. Gli strumenti di reporting, le riunioni periodiche di avanzamento, le attività di monitoraggio delle milestone e il presidio dei principali rischi hanno rappresentato elementi fondamentali per supportare il processo decisionale e garantire il controllo dell'intero programma.

All'interno di questo scenario, il Project Management Office ha svolto un ruolo particolarmente significativo, contribuendo a garantire la governance operativa dello stream di migrazione e favorendo il coordinamento tra le diverse strutture coinvolte. Le attività di monitoraggio, reporting, gestione delle dipendenze progettuali, supporto agli eventi di impianto e presidio delle campagne di test hanno permesso di mantenere una visione integrata dell'iniziativa, supportando il raggiungimento degli obiettivi prefissati

e contribuendo alla gestione delle criticità emerse durante le diverse fasi del programma.

Nel complesso, l'esperienza analizzata evidenzia come il successo di programmi di trasformazione di tale portata non dipenda esclusivamente dagli aspetti tecnologici, ma richieda la presenza di processi di governance efficaci, di una chiara definizione delle responsabilità e di un costante coordinamento tra le diverse componenti organizzative coinvolte. Il completamento della migrazione e la progressiva adozione del nuovo ecosistema cloud rappresentano la dimostrazione della capacità dell'organizzazione di affrontare con successo un percorso di cambiamento particolarmente complesso, ponendo le basi per future iniziative di innovazione e modernizzazione del patrimonio applicativo e informativo aziendale.

7.2 Il contributo del framework CDMC alla governance del dato

L'analisi condotta nel corso dell'elaborato ha evidenziato come il framework Cloud Data Management Capabilities (CDMC) rappresenti uno strumento particolarmente efficace per interpretare e governare le sfide legate alla gestione dei dati negli ambienti cloud. La crescente diffusione di architetture distribuite, unitamente all'aumento del volume e della criticità delle informazioni trattate dalle organizzazioni, rende infatti necessario adottare modelli di governance capaci di garantire controllo, sicurezza, tracciabilità e conformità normativa lungo l'intero ciclo di vita del dato.

In questo contesto, il CDMC si distingue per la capacità di fornire una visione strutturata e integrata della gestione del dato, superando una concezione esclusivamente tecnologica della trasformazione cloud. Il framework evidenzia infatti come il successo delle iniziative di modernizzazione non dipenda soltanto dall'adozione di nuove infrastrutture o piattaforme digitali, ma richieda la definizione di processi organizzativi, responsabilità, controlli e meccanismi di monitoraggio in grado di garantire una gestione efficace delle informazioni nel tempo.

L'applicazione del framework al caso di studio ha consentito di valutare il progetto secondo una prospettiva sistemica, mettendo in relazione gli aspetti tecnologici della migrazione con le pratiche di governance adottate dall'organizzazione. Il confronto ha mostrato un elevato livello di coerenza tra le modalità operative osservate e i principi

promossi dal CDMC, evidenziando come temi quali la governance del dato, la protezione delle informazioni, la gestione degli accessi e la progettazione delle architetture rappresentino elementi imprescindibili per il successo di programmi di trasformazione di elevata complessità.

L'analisi ha inoltre confermato come la governance del dato assuma un ruolo particolarmente strategico nel settore bancario, dove la sensibilità delle informazioni trattate e la presenza di stringenti requisiti normativi richiedono livelli di controllo particolarmente elevati. In tali contesti, framework come il CDMC non costituiscono solamente un insieme di best practice, ma rappresentano veri e propri strumenti di riferimento per orientare le decisioni progettuali e supportare le organizzazioni nell'adozione di modelli di gestione coerenti con le esigenze di sicurezza, affidabilità e conformità.

Le evidenze emerse suggeriscono infine che il valore del framework non risieda esclusivamente nella sua funzione di assessment o di verifica della conformità, ma soprattutto nella capacità di fornire una guida strutturata per l'evoluzione delle pratiche di data governance. In un contesto caratterizzato da una crescente digitalizzazione dei processi e da un utilizzo sempre più esteso delle tecnologie cloud, l'adozione di modelli come il CDMC può contribuire a favorire una gestione più consapevole e sostenibile del patrimonio informativo aziendale, trasformando il dato da semplice risorsa operativa a vero e proprio asset strategico per l'organizzazione.

7.3 L'evoluzione del project management nell'era dell'intelligenza artificiale

Le trasformazioni tecnologiche che stanno interessando le organizzazioni non riguardano esclusivamente le infrastrutture informatiche o i modelli di gestione del dato, ma coinvolgono in misura crescente anche le modalità attraverso cui i progetti vengono pianificati, monitorati e governati. In questo scenario, l'intelligenza artificiale generativa si sta progressivamente affermando come uno degli strumenti più promettenti per supportare le attività di project management, offrendo nuove opportunità per migliorare l'efficienza operativa e la capacità di gestione di iniziative caratterizzate da elevati livelli di complessità.

Come evidenziato nel corso dell'elaborato, le applicazioni della Generative AI si estendono ormai a numerosi ambiti del ciclo di vita progettuale, dalla produzione della documentazione alla pianificazione delle attività, dal monitoraggio dell'avanzamento alla gestione della comunicazione tra stakeholder. Tali strumenti consentono di elaborare rapidamente grandi quantità di informazioni, automatizzare attività ripetitive e supportare la predisposizione di contenuti e analisi che tradizionalmente richiederebbero un significativo impiego di tempo e risorse.

L'evoluzione attualmente in corso suggerisce tuttavia che il contributo dell'intelligenza artificiale non debba essere interpretato esclusivamente come una forma di automazione delle attività operative. La crescente disponibilità di strumenti capaci di sintetizzare informazioni, individuare correlazioni e supportare processi di analisi apre infatti nuove prospettive anche sul piano decisionale, consentendo ai professionisti di disporre di un supporto sempre più avanzato nella valutazione di scenari complessi e nell'identificazione di possibili criticità progettuali.

Allo stesso tempo, l'adozione di tali tecnologie richiede un approccio consapevole e una chiara comprensione dei relativi limiti. Le capacità generative dei modelli di intelligenza artificiale dipendono infatti dalla qualità delle informazioni utilizzate e possono essere soggette a errori, imprecisioni o interpretazioni non coerenti con il contesto organizzativo. Per questo motivo, il loro impiego deve essere accompagnato da adeguati meccanismi di supervisione e validazione, mantenendo sempre in capo al Project Manager la responsabilità finale delle decisioni e delle valutazioni progettuali.

Alla luce di queste considerazioni, il ruolo del Project Manager appare destinato a evolvere piuttosto che a essere sostituito. Se da un lato l'intelligenza artificiale potrà assumere un ruolo sempre più rilevante nella gestione delle attività amministrative e nell'elaborazione delle informazioni, dall'altro continueranno a essere fondamentali competenze tipicamente umane quali la leadership, la capacità di negoziazione, la gestione delle relazioni, il coordinamento degli stakeholder e il giudizio critico nelle situazioni caratterizzate da elevata incertezza. In questa prospettiva, il valore del professionista non risiederà tanto nella capacità di svolgere attività operative ripetitive, quanto nella capacità di interpretare le informazioni disponibili, guidare il cambiamento e orientare le decisioni strategiche del progetto.

L'intelligenza artificiale generativa può quindi essere considerata non come un elemento sostitutivo, ma come un fattore abilitante dell'evoluzione del project management. La

sua progressiva integrazione nei processi organizzativi potrà contribuire a rendere più efficienti le attività di pianificazione, coordinamento e controllo, consentendo ai professionisti di dedicare una quota crescente del proprio tempo agli aspetti a maggiore valore aggiunto. In un contesto caratterizzato da programmi di trasformazione sempre più complessi, la capacità di integrare competenze manageriali e strumenti basati su intelligenza artificiale rappresenterà verosimilmente uno dei principali fattori distintivi del project management del futuro.

7.4 Sviluppi futuri

Le evidenze emerse nel corso dell'analisi consentono di delineare alcune possibili direttrici di sviluppo sia con riferimento al programma di migrazione analizzato sia, più in generale, all'evoluzione delle pratiche di data governance e project management nel settore bancario.

Per quanto concerne il caso di studio, il programma di trasformazione risulta tuttora in corso e prevede ulteriori attività finalizzate al consolidamento del nuovo ecosistema tecnologico. I prossimi step progettuali riguarderanno infatti il proseguimento delle campagne di test, delle attività di validazione del nuovo Core Banking e il continuo perfezionamento dei processi di impianto e delle procedure operative associate alla migrazione. Tali attività saranno fondamentali per garantire il raggiungimento dei livelli di affidabilità, stabilità e qualità richiesti prima dell'avvio delle migrazioni in ambiente produttivo.

Secondo la pianificazione attuale, le prime entità giuridiche interessate dalla migrazione saranno le legal entity italiane del Gruppo, il cui passaggio al nuovo sistema è previsto a partire da dicembre 2026. Successivamente, il programma proseguirà con la migrazione delle legal entity estere, completando progressivamente il percorso di trasformazione dell'intero ecosistema applicativo. Tale evoluzione comporterà un ulteriore incremento della complessità progettuale, determinato dalla necessità di coordinare iniziative distribuite su differenti contesti organizzativi e normativi, rendendo ancora più rilevante il ruolo della governance progettuale e del coordinamento tra gli stakeholder coinvolti. In questo scenario, l'intelligenza artificiale generativa rappresenta una delle principali opportunità di evoluzione delle attività di Project Management Office. Sebbene il ricorso a strumenti basati su AI sia attualmente in crescita, il potenziale di sviluppo

risulta ancora ampiamente inesplorato. Ad oggi, infatti, l'utilizzo di funzionalità di intelligenza artificiale risulta prevalentemente limitato agli strumenti integrati nel pacchetto Microsoft Office, impiegati principalmente a supporto delle attività documentali e di reporting. L'introduzione di soluzioni più avanzate, quali agenti AI specializzati e sistemi di automazione intelligente, potrebbe consentire di incrementare significativamente il livello di automazione delle attività ripetitive svolte dal PMO, supportando la predisposizione della reportistica, la produzione automatica dei verbali di riunione, il monitoraggio delle milestone, l'analisi dei principali indicatori progettuali e la gestione delle comunicazioni tra i diversi stakeholder.

Parallelamente, un ulteriore ambito di sviluppo particolarmente rilevante riguarda l'evoluzione delle pratiche di governance del dato. L'analisi svolta ha evidenziato la forte coerenza tra il framework Cloud Data Management Capabilities (CDMC) e le esigenze tipiche dei programmi di trasformazione cloud nel settore bancario. In questa prospettiva, una possibile evoluzione futura potrebbe consistere nell'adozione più sistematica e standardizzata del framework all'interno delle organizzazioni finanziarie, utilizzandolo come modello di riferimento per la definizione di best practice, standard operativi e meccanismi di controllo comuni. La capacità del CDMC di coprire in modo integrato aspetti di governance, sicurezza, classificazione, protezione e gestione del ciclo di vita del dato lo rende infatti particolarmente adatto a supportare iniziative di migrazione complesse come quella analizzata.

Nel complesso, le future evoluzioni del settore sembrano orientate verso una sempre maggiore integrazione tra architetture cloud, modelli strutturati di data governance e strumenti basati sull'intelligenza artificiale. La capacità delle organizzazioni di combinare efficacemente tali elementi rappresenterà un fattore determinante per garantire il successo dei futuri programmi di trasformazione digitale, coniugando innovazione tecnologica, controllo operativo e sostenibilità nel lungo periodo.

Bibliografia

- [1] Vial, G. (2019) | Understanding digital transformation: A review and a research agenda. *Journal of Strategic Information Systems* | 28(2), 118–144
- [2] Yin, R. K. (2018) | *Case Study Research and Applications: Design and Methods* | 6th ed. SAGE Publications
- [3] Mell, P., & Grance, T. (2011) | The NIST Definition of Cloud Computing (NIST SP 800-145) | National Institute of Standards and Technology
- [4] IBM | What is cloud computing? | Disponibile su: <https://www.ibm.com/think/topics/cloud-computing?>
- [5] Microsoft Azure | What are IaaS, PaaS, SaaS? | Disponibile su: [What are IaaS, PaaS, and SaaS? | Microsoft Azure](#)
- [6] Martens, B., & Teuteberg, F. (2012) | Decision-making in cloud computing environments: A cost and risk-based approach | *Information Systems Frontiers*, 14(4), 871–893
- [7] Google Cloud | Vantaggi e svantaggi del cloud computing | Disponibile su: [Vantaggi del cloud computing | Google Cloud](#)
- [8] Batini, C., & Scannapieco, M. (2016) | *Data and Information Quality: Dimensions, Principles and Techniques* | Springer
- [9] Amazon Web Service | Cos'è la gestione dei dati? | Disponibile su: <https://aws.amazon.com/it/what-is/data-management/>
- [10] IBM | Che cos'è il cloud banking? | Disponibile su: <https://www.ibm.com/it-it/think/topics/cloud-banking>
- [11] European Union (2016) | Regulation (EU) 2016/679 – General Data Protection Regulation (GDPR) | Official Journal of the EU
- [12] European Banking Authority (2017) | EBA Recommendations on Cloud Outsourcing (EBA/REC/2017/03) | EBA
- [13] European Banking Authority (2019) | EBA Guidelines on outsourcing arrangements (EBA/GL/2019/02) | EBA
- [14] European Union (2022) | Regulation (EU) 2022/2554 on digital operational resilience for the financial sector (DORA) | Official Journal of the EU
- [15] Direttiva (UE) 2022/2555 | Parlamento europeo e del Consiglio del 14 dicembre 2022 (NIS2) | Official Journal of the EU

- [16] Banca d'Italia | Disposizioni per la conservazione e la messa a disposizione dei documenti, dei dati e delle informazioni per il contrasto del riciclaggio e del finanziamento del terrorismo | Articolo 6 comma 4
- [17] EDM Council | Cloud data management capabilities framework (CDMC) | Version 1.1.1 September 2021 | p. 7, 8
- [18] EDM Council | Cloud data management capabilities framework (CDMC) | Version 1.1.1 September 2021 | p. 11, 12
- [19] EDM Council | Cloud data management capabilities framework (CDMC) | Version 1.1.1 September 2021 | '1.0 Governance & Accountability'
- [20] EDM Council | Cloud data management capabilities framework (CDMC) | Version 1.1.1 September 2021 | '2.0 Cataloging & Classification'
- [21] EDM Council | Cloud data management capabilities framework (CDMC) | Version 1.1.1 September 2021 | '3.0 Accessibility & Usage'
- [22] EDM Council | Cloud data management capabilities framework (CDMC) | Version 1.1.1 September 2021 | '4.0 Protection & Privacy'
- [23] EDM Council | Cloud data management capabilities framework (CDMC) | Version 1.1.1 September 2021 | '5.0 Data Lifecycle'
- [24] EDM Council | Cloud data management capabilities framework (CDMC) | Version 1.1.1 September 2021 | '6.0 Data & Technical Architecture'
- [25] Project management Institute | A guide to the project management body of knowledge (PMBOK Guide) | 7th Edition PMI 2021
- [26] PMI (2017) | The Standard for Program Management | 4th ed. Project Management Institute
- [27] Project Management Institute | Pulse of the Profession: Why Complex Project Fail and What Leaders Can Do About It | PMI 2024
- [28] Project Management Institute | First Movers' Advantage: The immediate Benefits of Adopting Generative AI for Project Management | PMI 2024

Ringraziamenti