POLITECNICO DI TORINO

Collegio di Ingegneria Gestionale

Corso di Laurea Magistrale in Engineering and Management

Tesi di Laurea di II livello

IT Governance Maturity Assessment: rilevazione del livello di maturità dei processi IT per una Banca italiana

Relatore:

Prof. Domenico Augusto Maisano

Candidata:

Giulia Falzone
Matricola n. 315181

Novembre 2024

INDICE

LISTA ACRONIMI

- **AD**: Amministratore Delegato
- **AI**: Artificial Intelligence
- **API**: Application Programming Interface
- **AWS**: Amazon Web Services
- **BRM**: Business Relationship Management
- **CIO**: Chief Information Officer
- **CMDB**: Configuration Management Database
- **COBIT**: Control Objectives for Information and Related Technology
- **COO**: Chief Operating Officer
- **CSI**: Continual Service Improvement
- **DDoS**: Distributed Denial of Service
- **DLT**: Distributed Ledger Technology
- **DORA**: Digital Operational Resilience Act
- **EBA**: European Banking Authority
- **FSI**: Financial Services Industry
- **FY**: Fiscal Year
- **GDPR**: General Data Protection Regulation
- **GLBA**: Gramm-Leach Bliley Act
- **IAM**: Identity and Access Management
- **ICT**: Information and Communication Technology
- **IDS**: Intrusion Detection System
- **IEC**: International Electrotechnical Commission
- **IoT**: Internet of Things
- **IPS**: Intrusion Prevention System
- **ISACA**; Information System Audit and Control Association
- **ISO**: International Organization for Standardization
- **IT**: Information Technology
- **ITIL**: Information Technology Infrastructure Library
- **KPI**: Key Performance Indicator
- **MFA**: Multi-Factor Authentication
- **MTA**: Mercato Telematico Azionario
- **NPLs**: Non-Performing Loans
- **OGC**: Office of Government Commerce
- **PSD2**: Payment Services Directive 2
- **RBAC**: Role-Based Access Control
- **S.B**: Società Benefit
- **SCA**: Strong Customer Authentication
- **SDLC**: Software Development Life Cycle
- **SLA**: Service Level Agreement
- **STAR**: Segmento Titoli con Alti Requisiti
- **TPP**: Third Party Provider

INTRODUZIONE

Negli ultimi decenni, il rapido sviluppo dell'Information Technology (IT) ha rivoluzionato in modo significativo il settore dei servizi finanziari, introducendo cambiamenti profondi sia nelle operazioni che nell'offerta di nuovi prodotti, il che ha reso l'IT una componente cruciale per le strategie di sviluppo e le innovazioni delle istituzioni. In un contesto caratterizzato da una crescente digitalizzazione dei processi, oggi è possibile affermare che l'IT non rappresenta più un semplice supporto tecnico per lo svolgimento delle operazioni quotidiane, bensì si sta progressivamente affermando come una vera e propria leva strategica per il miglioramento delle prestazioni aziendali, la gestione del rischio e la creazione di un vantaggio competitivo sostenibile nel lungo termine. L'integrazione di tecnologie emergenti come, ad esempio, cloud computing, intelligenza artificiale e blockchain, ha aperto nuove prospettive per le istituzioni finanziarie, rendendo possibile una maggiore efficienza operativa e una personalizzazione dei servizi senza precedenti. Tuttavia, come spesso accade, questi sviluppi tecnologici hanno introdotto al contempo numerose sfide significative in termini di sicurezza informatica, compliance normativa e gestione del cambiamento; infatti, le istituzioni finanziarie si trovano oggi ad affrontare una complessità regolamentare mai affrontata prima, con normative rigorose quali, ad esempio, GDPR e PSD2, le quali impongono standard sempre più elevati per la protezione dei dati personali e la sicurezza delle transazioni. In questo scenario, la governance IT riveste un ruolo fondamentale, poiché si prefigge di assicurare che l'uso delle tecnologie informatiche sia strettamente allineato agli obiettivi strategici aziendali. In particolare, la sua efficacia dipende dalla capacità di ottimizzare le risorse tecnologiche, gestendole in modo efficiente e in linea con le esigenze del business, oltre a mitigare i rischi associati all'introduzione di nuove tecnologie. Per raggiungere questi risultati, quindi, è essenziale che le istituzioni finanziarie valutino il livello di maturità dei loro processi IT e identifichino le aree di miglioramento sulle quali intervenire.

L'obiettivo principale del presente elaborato è analizzare il processo di IT Governance Maturity Assessment condotto, nel corso del periodo di tirocinio svolto presso Deloitte Consulting, su un Istituto di Credito italiano. L'analisi effettuata rappresenta un passo fondamentale per garantire una gestione ottimale delle risorse IT, favorendo così la creazione di valore aggiunto per la Banca, un miglioramento continuo delle sue performance operative e una maggiore capacità di adattarsi ai rapidi mutamenti del mercato.

Il corpo centrale della presente tesi è strutturato in tre capitoli principali, di seguito brevemente descritti:

1. Il **primo capitolo** offre una presentazione dettagliata dell'azienda promotrice dell'attività, ovvero Deloitte S.r.l. S.B., evidenziando la sua evoluzione come Società Benefit, illustrando le principali aree professionali in cui opera da diversi anni, tracciandone la storia dal 1845 fino ad oggi e sottolineando al contempo il suo ruolo di leader nel settore dei servizi professionali. Inoltre, il capitolo offre una descrizione dell'Istituto di Credito cliente, con particolare attenzione alla sua storia e alla sua evoluzione nel panorama finanziario italiano, fornendo il contesto necessario per l'analisi successiva;
2. Il **secondo capitolo** fornisce un'analisi approfondita del ruolo strategico dell'Information Technology nel settore dei servizi finanziari, tracciandone l'evoluzione storica e descrivendo le principali innovazioni tecnologiche che stanno trasformando l'industria. Nel dettaglio, vengono esaminati temi come l'automazione, la centralizzazione dei sistemi bancari, la sicurezza informatica, la compliance normativa e la regolamentazione tecnologica. Inoltre, nella seconda metà del capitolo, viene introdotto il concetto di IT Governance, con un focus sulle principali best practice;
3. Il **terzo capitolo** pone tutta l'attenzione sul progetto di IT Governance Maturity Assessment condotto per l'Istituto di Credito italiano. Viene inizialmente fornita una panoramica del progetto, seguita da un'analisi del quadro normativo che ha fortemente influenzato le scelte strategiche della Banca, ovvero DORA e la Circolare n. 285. Il capitolo include un confronto dei benchmark di settore attraverso vari IT Maturity Assessment condotti su altre istituzioni finanziarie italiane e descrive il framework sviluppato da Deloitte, il tutto inteso come attività preliminari alla definizione di un framework dei processi IT ad hoc per la Banca, con conseguente classificazione degli stessi per priorità. A seguire viene illustrato e dettagliato l'approccio metodologico utilizzato dal team Deloitte per effettuare l'assessment e, infine, vengono sintetizzati alcuni degli esiti ottenuti per i processi ritenuti prioritari, classificati a loro volta in esiti di dettaglio ed esiti di sintesi.

Infine, le conclusioni riassumono i principali risultati e ostacoli riscontrati durante lo svolgimento delle attività nel periodo di stage, proponendo riflessioni sulle sfide future legate alla governance IT e all'adozione delle nuove tecnologie nel settore finanziario.

CAPITOLO 1

In data 2 maggio 2024 ha avuto inizio il tirocinio oggetto della presente tesi presso una delle principali società di consulenza appartenenti alle cosiddette “Big Four”, in particolare il tirocinio curriculare in questione è stato svolto presso Deloitte Consulting S.r.l. S.B. Tale percorso formativo si inserisce all'interno dell'area del servizio di consulenza "Core Business Operations", specificamente nella service line "Cloud and Engineering - Application Modernization and Migration". L'obiettivo primario di questa area è migliorare ed incrementare le potenzialità delle aziende clienti attraverso la transizione dalle infrastrutture on-premise al Cloud, con il chiaro intento di conseguire un vantaggio competitivo significativo. Vengono sviluppate e implementate soluzioni personalizzate, rivolte a diverse tipologie di settori industriali quali sanità, bancario, assicurativo e molti altri.

1.1 Presentazione dell’azienda promotrice dell’attività

Deloitte Touche Tohmatsu Limited, comunemente nota come Deloitte, è una delle più grandi società di servizi professionali al mondo, avente una lunga storia di eccellenza e innovazione nei servizi di audit, consulenza, consulenza finanziaria, risk management e consulenza fiscale[1]. Deloitte ad oggi opera in oltre 150 paesi attraverso una rete di società affiliate che forniscono servizi a una vasta gamma di clienti, tra cui aziende multinazionali, piccole e medie imprese, enti governativi e organizzazioni non-profit; in Fig. 1.1 è mostrata una fotografia, a novembre 2023, del Network globale. La presenza globale di Deloitte permette alla società di fornire servizi localizzati con una prospettiva globale, adattandosi alle specifiche esigenze di ciascun mercato e cliente. Le società del network sono unite dalla stessa mission e condividono gli stessi valori, offrendo un elevato standard di servizi ai clienti, mediante l’uso di metodologie e linee guida condivise. All'interno del singolo paese o regione, le società del network operano in qualità di entità separate e indipendenti nell'ambito del proprio framework giurisdizionale.

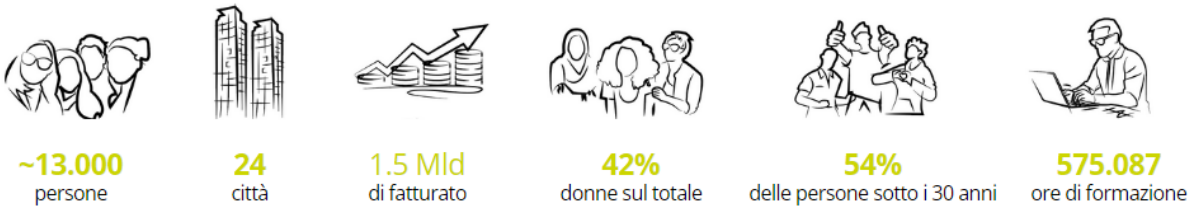
[1] Treccani (2012), *Deloitte Touche*, Enciclopedia Treccani - Lessico del XXI Secolo, URL: Deloitte & touche - Enciclopedia - Treccani

Figura 1.1 – Deloitte, identità internazionale

FONTE*: Deloitte (2024), Insdel - Home, Deloitte,*
URL: About us (deloitte.com) (24/09/2024)

Verso la fine dell'anno solare 2023, Deloitte in Italia ha annoverato più di 10.000 professionisti e professioniste all'interno del suo organico, dimostrando una crescita significativa nel settore. L'azienda ha registrato un fatturato di oltre 1,3 miliardi di euro, evidenziando un incremento del 23% rispetto all'esercizio finanziario dell'anno precedente (FY22). Tale espansione economica evidenzia non solo la solidità della struttura aziendale sulla quale Deloitte ha da sempre fondato le sue basi, ma anche la capacità di adattarsi con successo in un mercato in continua evoluzione. Il FY24 si è concluso con risultati straordinari: +15% rispetto al 2023, con un fatturato che ha superato 1,5 miliardi di euro; cresce anche l'organico: +10%, raggiungendo oltre 13.000 persone. Oggi Deloitte si distingue, inoltre, per la sua presenza capillare sul territorio nazionale, con uffici distribuiti in più di 20 città, vedi Fig. 1.2. Questa diffusione territoriale rappresenta un importante punto di forza per l'azienda in quanto le permette di garantire un servizio di alta qualità e prossimità ai propri clienti, indipendentemente dalla loro ubicazione, confermando così la propria posizione di riferimento nel settore dei servizi professionali in Italia.

Figura 1.2 – Deloitte in Italia



FONTE*: Deloitte (2024), Insdel - Home, Deloitte,*
URL: About us (deloitte.com) (24/09/2024)

1.1.1 Società Benefit

La disciplina delle società benefit è contenuta all'interno della legge n.208 del 28/12/2015 (legge di Stabilità 2016) Art.1, Commi 376-384, entrata in vigore a partire dal 1° gennaio 2016, che le ha configurate come società che operano con il chiaro obiettivo di generare un impatto positivo sociale ed ambientale, insieme ai tradizionali obiettivi di profitto finanziario[2]. Tali società integrano la responsabilità sociale d'impresa nel loro modello di business mediante l'uso di pratiche responsabili, sostenibili e trasparenti nei confronti di persone, comunità, territori, enti ed altri portatori di interessi. Tali società possono essere organizzate sia come enti non profit che come società a responsabilità limitata e, indipendentemente dalla forma giuridica scelta, entrambe le tipologie di organizzazioni sono tenute a dimostrare la loro responsabilità in ambito sociale e ambientale attraverso la redazione e la pubblicazione di un dettagliato rapporto di sostenibilità. Quest'ultimo ha lo scopo di documentare e valutare l'impatto delle attività svolte, al fine di garantire la massima trasparenza nei confronti di tutti gli stakeholder coinvolti. Il modello di Società Benefit si qualifica, quindi, come un valore aggiunto distintivo rispetto alle forme societarie tradizionali già esistenti.

Nel 2022 le società operative del network di Deloitte in Italia, prime tra le più grandi società di servizi, hanno intrapreso il lungo percorso di trasformazione in Società Benefit e ad oggi le società del network di Deloitte in Italia che sono diventate Società Benefit sono le seguenti: Deloitte Italy S.p.A., Deloitte Consulting S.r.l., Deloitte Financial Advisory S.r.l., Deloitte Risk Advisory S.r.l.,

[2] Gazzetta Ufficiale della Repubblica Italiana (2015), *Legge di Stabilità 2016 - Legge n.208 del 28 dicembre 2015*, URL: Gazzetta Ufficiale

Officine Innovazione S.r.l., Deloitte Business Solution S.r.l., Studio Tributario e Societario Deloitte S.t.P. S.r.l., Deloitte Legal S.t.Ar.l[3].

1.1.2 Le aree professionali

L'organizzazione di Deloitte offre diverse tipologie di servizi a clienti appartenenti al mondo pubblico e privato e provenienti da molteplici settori[4], di seguito viene riportata la suddivisione dell'azienda nelle proprie aree di servizio principali, mostrata graficamente in Fig. 1.3:

- *Audit & Assurance*: Deloitte offre servizi di revisione contabile e assicurazione per aiutare le organizzazioni a migliorare la qualità delle informazioni fornite agli stakeholders. Non si tratta di una semplice verifica dei numeri, mediante questo servizio Deloitte attesta i successi, annuncia le nuove sfide del mercato e, soprattutto, offre solide basi per progettare e migliorare il futuro di ciascun cliente;
- *Consulting:* i servizi di consulenza di Deloitte aiutano i clienti a trasformare le loro strategie aziendali mediante l'implementazione delle più recenti tecnologie e l'ottimizzazione dei processi aziendali. Classificandosi come la principale società di management consulting a livello globale, Deloitte si distingue per la sua straordinaria capacità di supportare i clienti nella risoluzione delle problematiche più complesse. Queste sfide possono essere di natura strategica, riguardando la definizione delle direzioni future e l'allocazione delle risorse, oppure operativa, implicando l'ottimizzazione dei processi e l'implementazione di soluzioni innovative. Deloitte combina una profonda conoscenza del settore con competenze tecniche avanzate per fornire soluzioni personalizzate e di alto valore, aiutando così le organizzazioni a raggiungere i loro obiettivi in un contesto di crescente competitività e complessità del mercato. Di particolare rilievo è la capacità di mettere in pratica i consigli che vengono forniti, così da sostenere i clienti nei mercati in cui operano attualmente e in quelli in cui vorranno essere presenti in un'ottica futura. Per offrire un simile valore, un requisito di fondamentale importanza è la capacità di integrare una vasta gamma di talenti e skills, a livello di capitale umano, adattandoli

[3] Deloitte Italy (2022), *Deloitte diventa Società Benefit*, Deloitte, URL: Deloitte diventa Società Benefit | Deloitte Italy

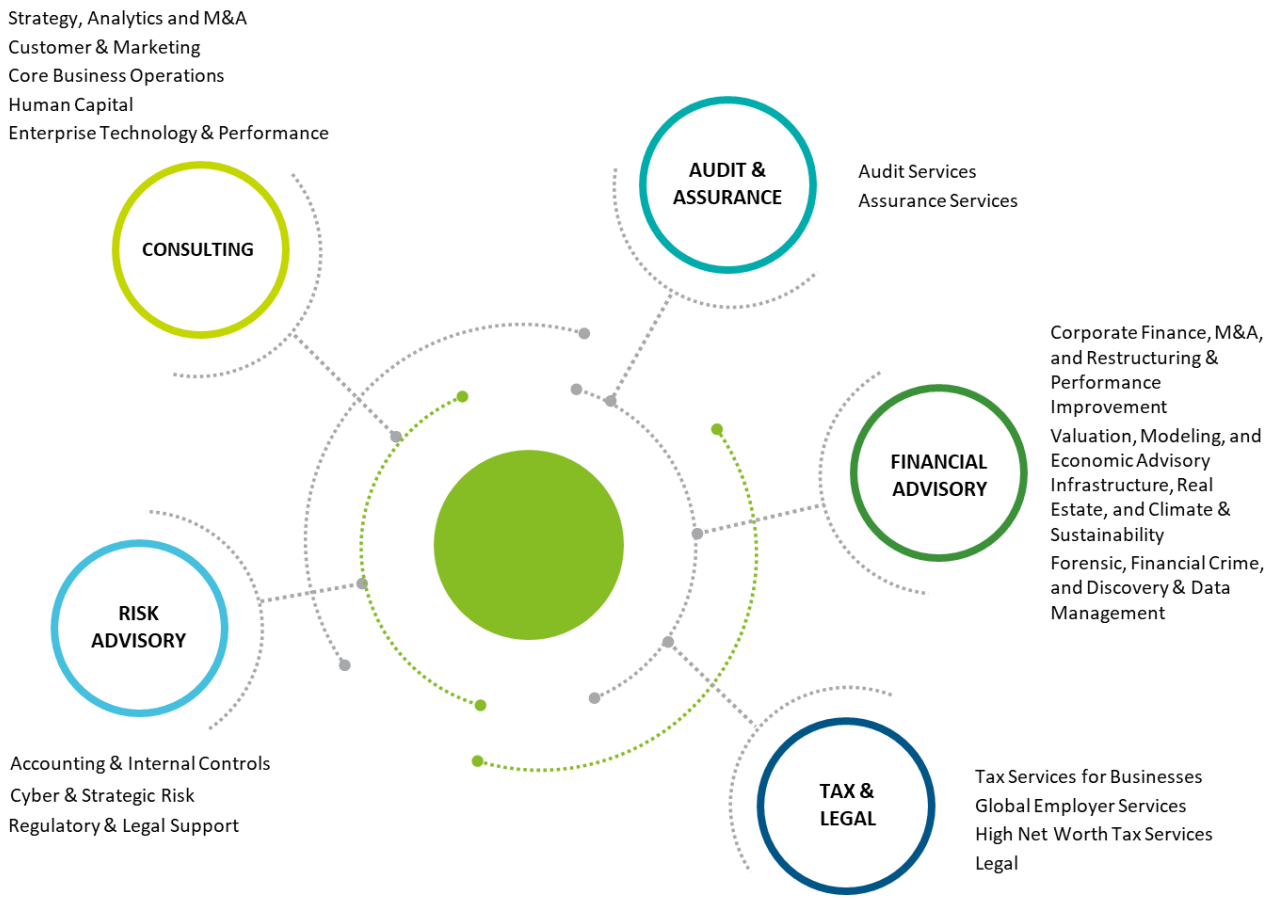
[4] Deloitte Italy (2024), *Deloitte Italia - Servizi professionali alle imprese*, Deloitte, URL: I nostri servizi | Deloitte

alle esigenze specifiche dei settori industriali, delle attività e delle organizzazioni dei diversi clienti;

- *Risk Advisory:* Deloitte si focalizza sulla gestione del rischio inteso come fonte di vantaggio competitivo per le organizzazioni aiutando le aziende a gestire il rischio in modo più efficace, permettendo loro di liberare il proprio massimo potenziale. Quest'area di servizio contribuisce a creare e proteggere valore per tutti gli stakeholder, attraverso strategie avanzate di gestione del rischio, preparando le aziende ad affrontare le incertezze e a sfruttare le opportunità del mercato nel migliore dei modi;
- *Financial Advisory:* nell'odierno mercato in rapida evoluzione, i servizi di consulenza finanziaria di Deloitte aiutano le aziende a prosperare, affrontando le sfide più complesse e cogliendo le opportunità strategiche. In particolare, vengono fornite ai clienti soluzioni innovative per gestire fusioni e acquisizioni, ristrutturazioni, valutazioni e altre operazioni finanziarie complesse;
- *Tax & Legal:* Deloitte offre una vasta gamma di servizi fiscali e legali, rivolte sia ad imprese che a privati, con l'intento di attuare una prevenzione di tipo proattivo dell'erosione della ricchezza, aiutando cioè i clienti a gestire le loro obbligazioni fiscali e conformarsi alle normative legali in continua evoluzione.

I servizi in questione, dato l'elevato livello di complessità e l'ampio numero di paesi nei quali vengono erogati, hanno reso necessario l'acquisto di molte sedi differenti dislocate in varie parti del mondo, mentre il quartier generale si trova a New York, all'interno del Paramount Plaza. Nel nostro Paese, ad esempio, la Deloitte opera come Deloitte Italy S.p.A dal 1923, oggi la Deloitte Italy risulta essere una delle più grandi realtà nei servizi professionali di consulenza alle imprese grazie al suo approccio multidisciplinare e alla presenza capillare sul territorio nazionale.

Figura 1.3 – Le aree professionali



FONTE*: Deloitte (2024), Insdel - Home, Deloitte,*
URL: About us (deloitte.com) (24/09/2024)

1.1.3 Deloitte dal 1845 ad oggi

La storia di Deloitte inizia nel 1845, quando William Welch Deloitte aprì il suo ufficio a Londra. W.W. Deloitte fu il primo a essere nominato revisore ufficiale di una società pubblica, la Great Western Railway, in cui egli svolse per più di 50 anni l'attività professionale di revisore contabile, il che lo portò ad essere considerato uno dei principali esponenti del settore, nonché creatore dei sistemi contabili e gestionali tutt'ora in uso. Questo segnò quindi l'inizio di una lunga tradizione di eccellenza nell'ambito della revisione contabile. Nel corso degli anni, W.W. Deloitte continuò a crescere e ad espandersi a livello internazionale, fino ad arrivare, nel 1898, all'unione con l'analista aziendale scozzese George Touche, creando così Deloitte & Touche. Questa fusione permise alla società di rafforzare la sua posizione come leader globale nei servizi professionali

grazie all'idea di Touche di creare una società di rating maggiormente concentrata sul mondo finanziario. Infine, l'espansione di Deloitte verso il mercato giapponese e asiatico nel 1968 è da attribuire all'esperto contabile Nobuzo Tohmatsu; riconosciuto oggi come il terzo padre fondatore della Deloitte, Tohmatsu giocò un ruolo cruciale nell'estendere la presenza e l'influenza della società in queste regioni[5].

Oggi Deloitte Touche Tohmatsu Limited è una delle "Big Four", le quattro maggiori società di servizi professionali che si spartiscono il mercato mondiale, insieme a PricewaterhouseCoopers, Ernst & Youg e KPMG. La società continua ogni giorno a crescere e adattarsi alle nuove sfide del mercato globale, mantenendo un impegno costante verso l'eccellenza, l'integrità e l'innovazione tecnologica che stanno alla base del suo successo e sostenendo con forza i propri valori, quali, ad esempio: essere pionieri, prendersi cura degli altri, promuovere l'inclusione e collaborare. Questo ampio concetto viene racchiuso mediante il motto cui Deloitte ispira la propria azione[6]: "Make an impact that matters!", vedi Fig. 1.4.

Figura 1.4 – Slogan Deloitte

FONTE*: Deloitte (2024), Insdel - Home, Deloitte,*
URL: About us (deloitte.com) (24/09/2024)

[5] Daniele Fontana (2017), *La Deloitte Touche Tohmatsu*, Starting Finance, URL: La Deloitte Touche Tohmatsu | Starting Finance

[6] Brand Finance (2024), *Deloitte - Making an impact that matters*, Brand Finance, URL: Deloitte: Making an Impact that Matters | Brand Finance

1.2 Presentazione dell'Istituto di Credito

Il soggetto posto al centro dell'analisi condotta nella presente tesi è il cliente per cui Deloitte Consulting S.r.l. S.B. effettua il servizio di IT Governance Maturity Assessment. L'Istituto di Credito in questione, con una storia consolidata e una reputazione di eccellenza nel panorama finanziario italiano, si distingue per la sua capacità di adattamento e innovazione continua. La valutazione del livello di maturità dell'IT Governance, realizzata da Deloitte, è parte integrante del processo di evoluzione strategica dell'Istituto, il cui obiettivo è ottimizzare la gestione delle risorse IT e garantire un allineamento efficace con gli obiettivi di business.

L'Istituto di Credito fu fondato nel 1983 a Genova con l'intento di operare in veste di intermediario finanziario. Infatti, fin dalla sua istituzione, l'ente si specializzò principalmente nell'attività di acquisto di crediti di impresa e nell'erogazione di finanziamenti, adottando quindi la formula del Factoring. Quest'ultimo è un contratto di natura finanziaria attraverso il quale un'azienda trasferisce i propri crediti commerciali, sia presenti che futuri, a una società specializzata, denominata "Factor". Questo trasferimento viene effettuato con l'obiettivo di ottenere immediatamente liquidità, migliorando in questo modo la gestione del capitale circolante dell'azienda cedente.

Gli anni compresi tra il 2002 e il 2004 furono di grande importanza; nel 2002, l'Istituto di Credito ottenne l'autorizzazione per l'esercizio dell'attività bancaria, segnando una svolta significativa nella sua storia, cambiando così la propria ragione sociale. Nello stesso anno, la Banca aderì al *Factor Chain International*, un'importante rete mondiale di società di factoring che consente di operare su scala internazionale, espandendo così la propria presenza all'estero, in particolare dopo l'apertura dei presidi aperti in Romania e Polonia. Nel 2003, l'istituto venne ammesso al *Mercato Telematico Azionario* (MTA) della Borsa di Milano, un passo cruciale che ne sancì la rilevanza nel panorama finanziario italiano ed esattamente un anno dopo la quotazione in Borsa, nel 2004, la Banca raggiunse un ulteriore traguardo significativo entrando a far parte del segmento STAR (*Segmento Titoli con Alti Requisiti*) di Borsa Italiana[7]. Quest'ultimo è noto per essere il segmento di Borsa Italiana più selettivo in termini di trasparenza e informativa agli investitori, infatti le società partecipanti devono presentare una capitalizzazione compresa tra 40 milioni di euro e 1 miliardo di euro, flottante minimo al 35% e obbligo del rispetto di particolari requisiti di eccellenza, quali

[7] Borsa Italiana (s.d.), Glossario Finanziario - *Segmento Titoli con Alti Requisiti (STAR)*, Borsa Italiana, URL: Segmento Titoli con Alti Requisti (STAR) - Glossario Finanziario - Borsa Italiana

ad esempio: elevati standard di trasparenza informativa, standard internazionali di governance e liquidità, compresa la nomina di un operatore specialista.

Durante gi anni compresi tra il 2008 e il 2013 gli eventi furono guidati da due obiettivi in particolare: crescita e diversificazione. La Banca entra a far parte del segmento retail attraverso il lancio di un conto deposito online ad alto rendimento ed entra nel mercato dei NPLs (*Non Performing Loans*, ovvero crediti, vantati dalle banche, che i debitori non sono più in grado di pagare). Dal 2016 si susseguirono diverse acquisizioni ed eventi che portarono, nel 2023, la Banca a celebrare i suoi primi 40 anni.

Oggi, la Banca ricopre una posizione di spicco all'interno del panorama bancario italiano, distinguendosi sia nel finanziamento alle imprese sia nella gestione dei crediti deteriorati. Accanto a queste attività principali, l'Istituto di Credito offre servizi specialistici dedicati alla clientela privata, rafforzando la propria presenza e il proprio ruolo di rilievo nel settore finanziario. Elementi caratteristici sono la velocità e la flessibilità, garantiti dal modo unico che la Banca ha di operare grazie alla propria struttura snella. I valori sui quali la Banca ha sempre fondato il suo operato, dal 1983 ad oggi, sono:

- Integrità;
- Eccellenza;
- Competenza;
- Trasparenza.

Fornire un supporto concreto ai propri clienti tramite servizi e prodotti d'eccellenza, che generano un impatto positivo sull'economia e creano valore per il territorio: questa è la missione che la Banca si impegna a perseguire ad oggi.

CAPITOLO 2

2.1 INFORMATION TECHNOLOGY E FINANCIAL SERVICE INDUSTRY

2.1.1 Il ruolo strategico dell'IT nel settore finanziario

Nel corso degli ultimi anni, l'**Information Technology** (IT) ha assunto un ruolo centrale e insostituibile nel settore dei servizi finanziari, diventando non solo un solido supporto per le operazioni quotidiane, ma anche un fattore strategico in grado di trasformare profondamente il modo in cui le istituzioni finanziarie operano, competono e instaurano relazioni con i propri clienti. La crescente digitalizzazione dei processi bancari, l'emergere di nuove tecnologie e la necessità di rispondere a un contesto normativo sempre più complesso hanno reso l'IT un componente essenziale per il successo e la sostenibilità delle banche e delle altre istituzioni finanziarie[8]. In questo contesto, è fondamentale comprendere l'importanza e il ruolo dell'IT all'interno del settore finanziario, esplorare l'evoluzione storica della sua adozione nelle banche e analizzare la sua rilevanza strategica per la competitività delle istituzioni finanziarie nel mercato globale.

L'Information Technology ricopre, ad oggi, un ruolo che va ben oltre il semplice supporto tecnologico: è il motore che permette alle banche di sviluppare nuove offerte, migliorare l'esperienza del cliente e ottimizzare la gestione interna. L'automazione dei processi operativi ha consentito alle banche di ridurre significativamente i tempi di esecuzione delle transazioni, minimizzare gli errori umani e abbattere i costi operativi. Questi miglioramenti non solo aumentano l'efficienza complessiva delle operazioni bancarie, ma permettono anche alle istituzioni finanziarie di focalizzarsi su attività a maggiore valore aggiunto, quali, ad esempio, lo sviluppo di nuove opportunità di mercato.

L'IT svolge un ruolo cruciale anche in altri ambiti, come la gestione del rischio e la sicurezza informatica, due aree che suscitano crescente preoccupazione per le istituzioni finanziarie. Le moderne tecnologie di analisi dei dati, supportate da strumenti di intelligenza artificiale e machine learning, permettono di monitorare e analizzare enormi volumi di dati in tempo reale, in maniera tale da identificare potenziali rischi e prevenire eventuali frodi. La sicurezza dei dati e delle transazioni è essenziale per mantenere la fiducia dei clienti e la reputazione dell'istituzione

[8] Brynjolfsson, E., & McAfee, A. (2014), *The Second Machine Age: Work, Progress, and Prosperity in a Time of Brilliant Technologies*, W. W. Norton & Company

finanziaria, ecco perché, in un contesto in cui le minacce informatiche sono sempre più sofisticate, l'IT offre soluzioni indispensabili per salvaguardare le risorse digitali e assicurare il rispetto delle normative sulla protezione dei dati[9].

2.1.2 Evoluzione storica

L'adozione dell'Information Technology nel settore bancario è il risultato di un complesso processo evolutivo che ha attraversato diverse fasi storiche. Nei primi anni della digitalizzazione bancaria le tecnologie informatiche venivano utilizzate principalmente per l'automazione di operazioni di back-office, come la gestione dei conti e l'elaborazione delle transazioni. Negli anni '60 e '70, mediante l'introduzione dei mainframe, le banche iniziarono a centralizzare le proprie operazioni e ciò portò alla creazione di sistemi di elaborazione dati su larga scala che permettevano una gestione più efficiente delle operazioni quotidiane. Un vero e proprio cambiamento si verificò negli anni '80 e '90, con l'avvento dei personal computer e delle reti di telecomunicazioni. Durante questa fase si ebbe l'introduzione di sistemi di core banking che centralizzarono le operazioni bancarie su piattaforme unificate, migliorando così l'efficienza e riducendo i costi operativi. Le banche iniziarono a sviluppare sistemi di home banking, permettendo ai clienti di accedere ai propri conti e di effettuare operazioni bancarie da casa ed in modo semplice, segnando così l'inizio di una nuova era di servizi bancari digitali. Gli anni a seguire, ovvero gli anni 2000, furono caratterizzati dall'espansione dell'internet banking e, successivamente, del mobile banking. Le banche iniziarono a offrire una vasta gamma di servizi online, permettendo ai clienti di effettuare transazioni, richiedere prestiti e gestire investimenti direttamente dal proprio computer o dispositivo mobile. Questa evoluzione migliorò la convenienza per i clienti e contribuì a ridurre i costi operativi per le banche, consentendo loro di servire un numero maggiore di clienti evitando il conseguente aumento della presenza fisica tramite filiali.

Oggi l'Information Technology (IT) è considerato come un fattore abilitante cruciale per l'innovazione nel settore finanziario, poiché tecnologie emergenti come il cloud computing, la blockchain e l'intelligenza artificiale offrono nuove opportunità per la creazione di prodotti finanziari personalizzati, la semplificazione delle operazioni e la trasformazione dei modelli di

[9] Laudon, K. C., & Laudon, J. P. (2020), *Management Information Systems: Managing the Digital Firm* (16ª ed.), Pearson

business tradizionali. Negli ultimi anni queste innovazioni hanno ricevuto un'ulteriore spinta permettendo alle banche di differenziarsi dai concorrenti, innovare i propri modelli di business, introdurre nuovi prodotti e servizi, e migliorare al contempo la sicurezza e la conformità alle normative. Le banche che adottano rapidamente queste tecnologie possono quindi offrire servizi più efficienti, sicuri e orientati al cliente, consolidando la loro posizione competitiva all'interno del mercato[10].

2.1.3 Automazione e centralizzazione dei sistemi bancari

Come precedentemente accennato, l'implementazione di **sistemi di core banking centralizzati** rappresenta una delle innovazioni più rivoluzionarie all'interno del settore bancario moderno. Essi sono definiti come piattaforme informatiche che gestiscono in modo integrato tutte le operazioni bancarie fondamentali, come la gestione dei conti correnti, i depositi, i prestiti, i pagamenti e le transazioni finanziarie, come mostrato graficamente in Fig. 2.1. A differenza dei modelli operativi precedenti, caratterizzati da sistemi decentralizzati e spesso frammentati tra diverse filiali e dipartimenti, i sistemi di core banking centralizzati consentono alle banche di consolidare la totalità delle loro operazioni su un'unica piattaforma. Questo approccio ha rivoluzionato il modo in cui le banche gestiscono le proprie attività, consentendo una visione unificata e integrata di tutte le operazioni finanziarie[11].

La centralizzazione dei sistemi bancari ha avuto un impatto significativo sull'espansione globale delle banche poiché ha consentito loro di operare in modo più efficiente e coerente su scala internazionale. Ciò è stato possibile in quanto i sistemi centralizzati permettono alle banche di standardizzare le loro operazioni su diversi mercati, offrendo ai clienti un'esperienza omogenea e coerente indipendentemente dalla loro ubicazione geografica. Tale discorso è particolarmente rilevante per le banche multinazionali che devono gestire operazioni in più paesi con legislazioni diverse e aspettative dei clienti variabili. È possibile affermare quindi che la centralizzazione dei sistemi bancari offre numerosi vantaggi significativi per le istituzioni finanziarie, rendendo questa strategia altamente attrattiva.

[10] Deloitte, (2012), *IT Playbook_2012*
[11] Deloitte (s.d.), *Digital transformation hits core banking, Deloitte*, URL: Bank-Thoughtware-EN.pdf (deloitte.com)

I principali **benefici** includono:

- *Aumento dell'efficienza operativa:* la centralizzazione consente l'automazione delle operazioni quotidiane, riducendo la necessità di interventi manuali e minimizzando gli errori umani. Ciò accelera i processi interni e permette di riassegnare le risorse umane a compiti legati all'aspetto strategico e di maggior valore aggiunto;

- *Riduzione dei costi operativi*: gestire un unico sistema centralizzato è generalmente più economico rispetto alla gestione di molteplici sistemi decentralizzati, poiché vengono ridotti, ad esempio, i costi derivanti dall'aggiornamento, dalla manutenzione e dalla sicurezza. Inoltre, la centralizzazione permette di ottenere economie di scala, ovvero permette di ridurre i costi medi di produzione in relazione all'aumento del volume di produzione, ottimizzando l'allocazione delle risorse IT e abbattendo i costi associati all'infrastruttura e alle licenze software;

- *Velocità delle transazioni*: i sistemi centralizzati di core banking permettono di processare le transazioni in tempo reale o quasi reale, migliorando la fluidità delle operazioni e aumentando la rapidità nell'esecuzione delle transazioni per i clienti. In un mercato globale in cui la velocità è essenziale per rimanere competitivi nel mercato e soddisfare i clienti, questa capacità costituisce un vantaggio competitivo e strategico fondamentale per il successo aziendale, favorendo l'incremento continuo dei ricavi e la fidelizzazione dei clienti.

Nonostante i numerosi vantaggi, come spesso accade, l'adozione di sistemi di core banking centralizzati presenta anche diverse **sfide e complessità**, di seguito sono elencati alcuni esempi:

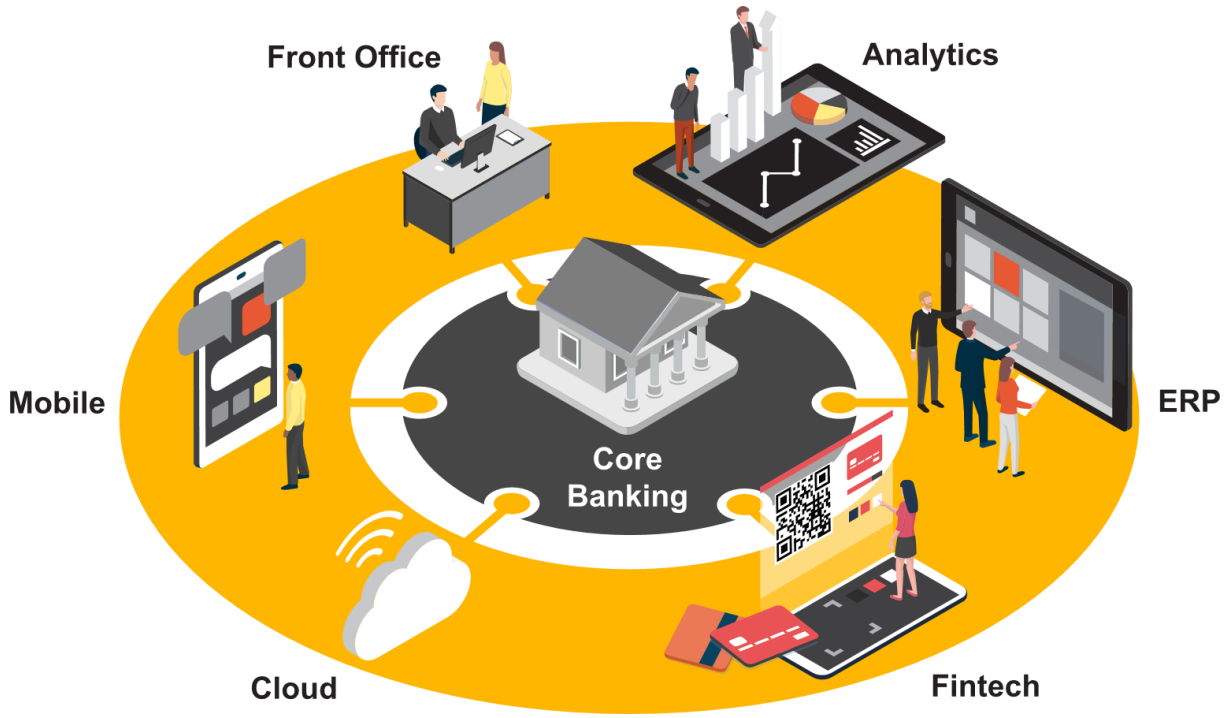
- *Complessità tecnica e operativa*: la migrazione da sistemi decentralizzati a una piattaforma centralizzata richiede una pianificazione accurata, ingenti investimenti in termini di tempo e risorse e una gestione efficace del cambiamento organizzativo. Questo processo può comportare interruzioni del servizio, problemi di integrazione e la necessità di aggiornare infrastrutture IT obsolete. È inoltre necessaria una costante formazione del personale al fine di acquisire nuove competenze operative e rimanere sempre aggiornati;

- *Sicurezza informatica*: un sistema centralizzato diventa un obiettivo attraente per i cybercriminali e, di conseguenza, la sua protezione richiede l'implementazione di misure di sicurezza avanzate, come crittografia dei dati, gestione degli accessi e monitoraggio continuo delle minacce.

È essenziale garantire la conformità alle normative sulla protezione dei dati, come il GDPR, che impone standard rigorosi per la gestione delle informazioni sensibili;

- *Gestione del rischio*: la centralizzazione offre, da un lato, maggiore visibilità e controllo, dall'altro, introduce anche nuovi rischi, come la dipendenza da un'unica piattaforma. In caso di guasti tecnici o attacchi informatici, l'interruzione del servizio può avere un impatto significativo su tutte le operazioni della banca. Al fine di mitigare questi rischi, è necessario sviluppare piani di continuità operativa e disaster recovery per garantire la resilienza del sistema in caso di eventi avversi.

Figura 2.1 – Core Banking Transformation



FONTE: PwC, (2024), Core Banking Transformation, PwC,

URL: Core Banking Transformation | PwC Switzerland

2.1.4 Innovazioni tecnologiche nel settore finanziario

Tra le principali innovazioni che stanno attualmente plasmando il futuro del settore finanziario e già menzionate in precedenza, il cloud computing, l'intelligenza artificiale (AI), il machine learning, e la blockchain con la Distributed Ledger Technology (DLT) rappresentano le tecnologie più rilevanti. Quest'ultime stanno trasformando non solo l'infrastruttura IT delle banche, ma anche e soprattutto il modo in cui queste ultime interagiscono con i clienti, gestiscono il rischio e ottimizzano le operazioni[12].

Il **Cloud Computing** ha rivoluzionato il settore finanziario offrendo alle istituzioni la possibilità di scalare rapidamente le proprie operazioni, accedere a risorse computazionali su richiesta e ridurre significativamente i costi infrastrutturali. Per comprendere pienamente l'entità dell'innovazione introdotta, è indispensabile compiere una breve analisi retrospettiva: prima dell'avvento del Cloud, le banche dovevano investire in maniera massiccia in hardware e software allo scopo di costruire e mantenere le proprie infrastrutture IT e questi investimenti comportavano non solo alti costi iniziali, ma anche costi continui legati alla manutenzione, agli aggiornamenti e alla gestione delle risorse IT. Oggi il Cloud Computing consente alle banche di superare queste sfide attraverso l'adozione di un modello di servizio su richiesta[13]. Le risorse IT, come il calcolo, l'archiviazione e le applicazioni software, vengono fornite attraverso internet da provider di servizi cloud quali, ad esempio, Amazon Web Services (AWS, vedi Fig. 2.2) Microsoft Azure e Google Cloud Platform. Questo modello offre alle banche una *flessibilità* senza precedenti, permettendo loro di adattarsi rapidamente alle variazioni della domanda da parte dei clienti e di scalare le risorse IT in base a quelle che sono le reali esigenze operative. Ad esempio, durante i periodi di picco, come ad esempio il Black Friday o il fine anno fiscale, le banche possono aumentare temporaneamente le capacità computazionali per gestire l'aumento del volume delle transazioni, senza la necessità di dover investire in hardware aggiuntivo che potrebbe poi risultare sottoutilizzato durante i periodi normali.

[12] PwC (2020), *Financial Services Technology 2020 and Beyond: Embracing Disruption*, PwC, URL: Financial Services Technology 2020 and Beyond: Embracing disruption (pwc.com)
[13] Accenture (2021), *The Cloud Imperative for Banking - Growth Markets*, Accenture, URL: CLOUD_V6 (accenture.com)

Figura 2.2 – AWS Cloud Computing

FONTE: R. Johnz (2024), What is AWS Cloud Computing? A Comprehensive Guide for Understanding Demystifying AWS Cloud Computing, Medium,

URL: [What is AWS Cloud Computing: A Comprehensive Guide for Understanding Demystifying AWS Cloud Computing | by Remi Johnz | Medium]

Oltre alla scalabilità ed elasticità, il cloud computing offre anche significativi vantaggi in termini di *economicità*. Le banche possono ridurre i costi legati all'acquisto e alla manutenzione dell'hardware, oltre ai costi energetici associati al funzionamento dei data center interni. Inoltre, il modello di pagamento basato sull'utilizzo ("pay-as-you-go") permette alle istituzioni finanziarie di pagare solo per le risorse effettivamente utilizzate, migliorando così l'efficienza dei costi e riducendo gli sprechi. Un altro aspetto molto rilevante riguarda il concetto della *sicurezza*: i provider di servizi cloud investono notevolmente in misure di sicurezza avanzate spesso superiori

a quelle che molte banche potrebbero implementare internamente ed in maniera autonoma. I servizi cloud generano una copia di backup dei dati archiviati per evitare qualsiasi forma di perdita di informazioni e dati, in questa maniera, in caso di malfunzionamento o perdita di dati su un server, la copia di backup può essere recuperata da un altro server. Questa funzionalità è particolarmente utile, ad esempio, quando diversi utenti collaborano su un unico file in tempo reale e si verifica un'improvvisa corruzione del file che risulta quindi danneggiato.

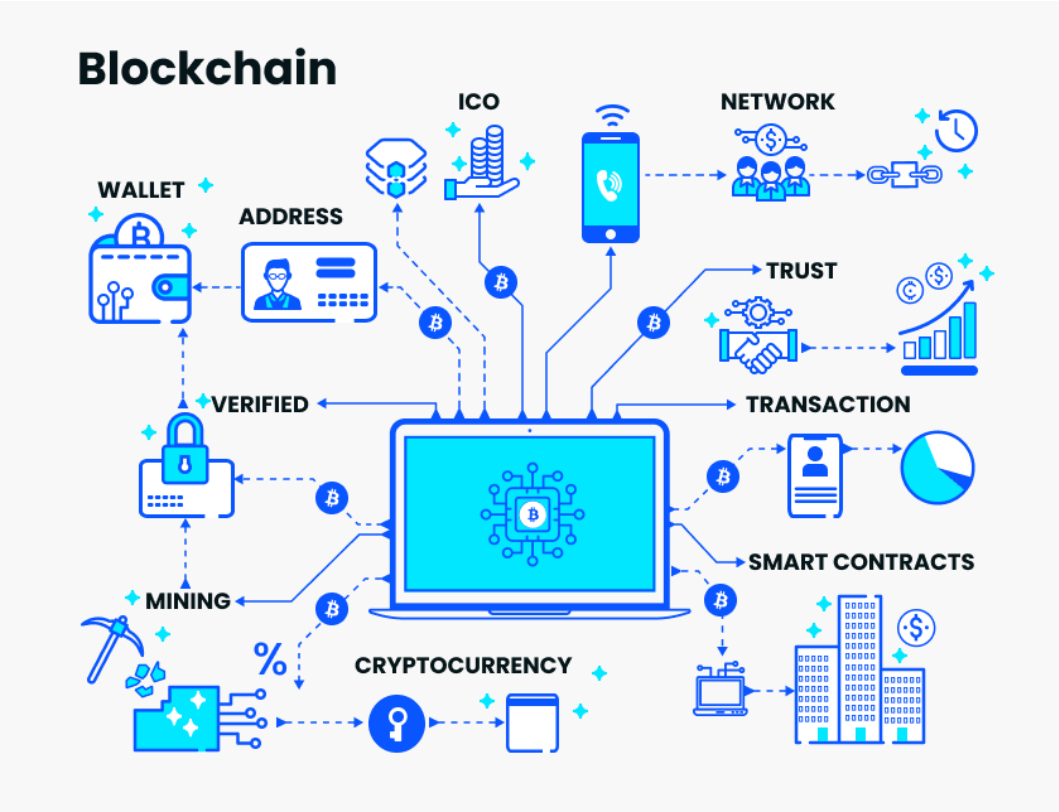
L'**Intelligenza Artificiale** (AI) e il **Machine Learning** sono tecnologie che, negli ultimi anni, hanno esercitato un'influenza profonda sul modo in cui le istituzioni finanziarie gestiscono il rischio, personalizzano i servizi e automatizzano i processi decisionali. Queste tecnologie consentono alle banche di analizzare grandi volumi di dati in tempo reale, individuando schemi ed anomalie che potrebbero sfuggire alle tecniche di analisi tradizionali. Nel campo della *gestione del rischio*, ad esempio, gli algoritmi di Machine Learning possono esaminare dati storici e in tempo reale per rilevare comportamenti anomali indicativi di attività fraudolente. Inoltre, l'AI viene impiegata per affinare la precisione dei modelli di rischio di credito, permettendo una valutazione più accurata e tempestiva della solvibilità dei clienti. Un'altra area in cui l'AI sta apportando significativi miglioramenti è la *personalizzazione dei servizi*: le banche possono utilizzare l'Intelligenza Artificiale per analizzare i comportamenti e le preferenze dei clienti, offrendo prodotti e servizi personalizzati che rispondono alle esigenze specifiche di ciascun individuo. Ad esempio, gli algoritmi di Machine Learning analizzano i dati delle transazioni dei clienti per identificare le loro preferenze di spesa e suggerire i prodotti finanziari più affini al loro profilo. Inoltre, l'AI migliora l'esperienza del cliente attraverso l'uso di assistenti virtuali e chatbot, che forniscono supporto e consulenza continua, rispondendo a domande e risolvendo problemi in modo rapido ed efficiente. Infine, l'*automazione delle decisioni* rappresenta un ulteriore campo in cui l'AI e il Machine Learning hanno un impatto rilevante. Le banche possono sfruttare queste tecnologie per automatizzare processi decisionali complessi, riducendo i tempi di risposta e incrementando l'efficienza operativa. Ad esempio, l'AI può essere utilizzata per automatizzare l'approvazione dei prestiti, analizzando in tempo reale tutta la documentazione e i dati relativi al cliente al fine di poter prendere decisioni corrette ed immediate. Ciò non solo accelera il processo di erogazione del credito, ma riduce anche il rischio di errori umani.

La **Blockchain** e la **Distributed Ledger Technology** (DLT), innovazioni dirompenti all'interno del settore finanziario, offrono nuove modalità per eseguire transazioni in maniera sicura,

trasparente e senza la necessità di intermediari. La Blockchain è una forma di DLT nella quale le transazioni vengono registrate in blocchi concatenati tra loro seguendo un ordine cronologico, creando una catena di blocchi che è immutabile e resistente alle frodi, vedi Fig. 2.3. Ogni partecipante alla rete possiede una copia identica del registro delle transazioni e ciò permette di garantire la trasparenza e l'integrità dei dati; ecco perché, di conseguenza, uno dei principali vantaggi della Blockchain è la *sicurezza delle transazioni*. Grazie alla crittografia avanzata e alla natura decentralizzata della Blockchain, le transazioni sono altamente sicure e praticamente immuni da manipolazioni o eventuali attacchi informatici. La *riduzione degli intermediari* è un altro beneficio chiave offerto dalla Blockchain e dalla DLT; tradizionalmente, molte transazioni finanziarie richiedono l'intervento di intermediari, come banche, notai o broker, al fine di garantire la sicurezza e l'integrità delle operazioni, tuttavia, la blockchain consente di eseguire queste transazioni direttamente tra le due o più parti coinvolte e questo non solo riduce i costi associati alle commissioni degli intermediari, ma accelera anche il processo di transazione e aumenta, ancora una volta, la trasparenza[14].

[14] B. Carson, G. Romanelli, P. Walsh, A. Zhumaev (2018), *Blockchain beyond the hype: What is the strategic business value?*, McKinsey Digital, URL: The strategic business value of the blockchain market | McKinsey

Figura 2.3 – Blockchain Technology



FONTE: A. Edge (2023), Concept of blockchain technology and its potential applications in various sectors, Analytics Vidhya, Astha Edge, URL: Concept of blockchain technology and its potential applications in various sectors - Kenta Fast Blog (asthaedge.com)

Dopo aver analizzato l'impatto cruciale del Cloud computing, della Blockchain e dell'Intelligenza Artificiale nel settore finanziario, diventa fondamentale esplorare altre innovazioni emergenti che stanno ulteriormente trasformando questo ambito. Tecnologie come l'Internet of Things (IoT) stanno aprendo nuove prospettive, offrendo opportunità senza precedenti per l'automazione, la personalizzazione dei servizi e la gestione dei rischi. Questi sviluppi, insieme ad altre tecnologie emergenti, stanno ridisegnando il futuro dei servizi finanziari, rendendolo sempre più interconnesso e orientato ai dati, con importanti implicazioni per le strategie operative delle istituzioni finanziarie.

Con il termine **Internet of Things** (IoT) si fa riferimento all'insieme di tecnologie e applicazioni che consentono alla rete di dispositivi connessi a Internet di raccogliere e scambiare dati in tempo reale. Esso sta rapidamente trasformando vari settori, e il settore finanziario non fa eccezione;

infatti, una delle applicazioni più immediate dell'IoT nel settore finanziario riguarda la personalizzazione dei servizi bancari e assicurativi. Attraverso l'uso di sensori e dispositivi intelligenti, le banche possono raccogliere dati in tempo reale sui comportamenti dei clienti, le loro abitudini di spesa e le loro esigenze finanziarie. Questi dati possono essere utilizzati per offrire servizi personalizzati, ad esempio, un dispositivo IoT installato in un'auto potrebbe monitorare lo stile di guida di un cliente e permettere alla compagnia assicurativa di offrire un premio più accurato e personalizzato basato sul rischio effettivo. L'IoT può anche migliorare la gestione dei rischi per le banche. Ad esempio, i sensori IoT possono monitorare le condizioni ambientali di un impianto industriale o di un'area geografica, fornendo dati in tempo reale che le banche possono in un secondo momento utilizzare per valutare i rischi associati ai prestiti o agli investimenti in quelle determinate aree. Questo potrebbe portare a una valutazione del rischio più precisa e a decisioni di prestito più informate.

2.1.5 Sicurezza informatica e Cybersecurity

Come visto fin ora, in un contesto in cui le operazioni bancarie e finanziarie sono sempre più digitalizzate, garantire la sicurezza dei sistemi e delle informazioni è essenziale non solo per proteggere gli asset dell'istituzione, ma anche per mantenere un elevato livello di fiducia da parte dei clienti e la conformità alle normative[15]. Questo paragrafo esplora le principali minacce informatiche e vulnerabilità che affliggono il settore finanziario, le soluzioni avanzate di Cybersecurity implementate per mitigare questi rischi, e l'importanza della protezione dei dati sensibili (e.g., informazioni personali identificative, dettagli del conto bancario, documenti legali e finanziari, informazioni di contatto, ecc.). Il settore finanziario è uno dei bersagli principali per i cybercriminali a causa della natura altamente lucrativa delle potenziali incursioni e la quantità significativa di dati sensibili gestiti dalle istituzioni[16]. Tra le **minacce informatiche** più comuni, che colpiscono questo settore e non solo, vi sono:

[15] European Central Bank (ECB) (2018), *Cyber Resilience Oversight Expectations for Financial Market Infrastructures*, ECB, URL: Cyber resilience oversight expectations for financial market infrastructures (europa.eu)
[16] National Institute of Standards and Technology (2024), *The NIST Cybersecurity Framework (CSF) 2.0*, NIST, URL: The NIST Cybersecurity Framework (CSF) 2.0

- *Phishing*: i criminali informatici inviano e-mail o messaggi ingannevoli per indurre gli utenti a fornire informazioni sensibili, come le credenziali di accesso o i dettagli della carta di credito. Una volta ottenute, queste informazioni possono essere utilizzate per accedere ai conti bancari delle vittime, sottrarre fondi o eseguire altre svariate attività fraudolente;
- *Malware:* può assumere diverse forme, tra cui virus, trojan, e spyware, ed è spesso utilizzato per compromettere i sistemi informatici delle banche, rubare dati, o interrompere le operazioni. I ransomware sono una forma specifica di malware e risultano essere particolarmente pericolosi poiché bloccano l'accesso ai dati critici delle istituzioni finanziarie, richiedendo un riscatto per ripristinarne l'accesso;
- *Attacchi DDoS:* sono progettati per sovraccaricare i sistemi informatici delle banche, rendendo i servizi inaccessibili per gli utenti legittimi. Questi attacchi possono paralizzare le operazioni delle banche, causando disagi ai clienti e perdite finanziarie considerevoli.

Per contrastare le minacce informatiche e proteggere i loro sistemi, le istituzioni finanziarie hanno adottato una serie di **soluzioni avanzate di Cybersecurity**, di seguito un breve elenco di esempi e relative descrizioni. Queste tecnologie sono fondamentali per garantire la sicurezza dei dati e delle operazioni finanziarie, nonché per assicurare la conformità con le normative vigenti.

- La *crittografia* è una delle tecniche maggiormente efficaci nella protezione dei dati sensibili in quanto essa trasforma le informazioni in un formato illeggibile per chiunque non possieda la chiave di decrittazione, rendendo quindi impossibile per i cybercriminali accedere ai dati protetti, nonostante riescano ad intercettarli. Nel settore finanziario, la crittografia viene utilizzata per proteggere i dati in transito (come le transazioni online) e i dati a riposo (archiviati nei database), garantendo che solo le parti autorizzate possano accedere alle informazioni sensibili;
- La *gestione degli accessi* è un'altra componente critica della cybersecurity nelle istituzioni finanziarie. Con l'aumento delle operazioni digitali e la necessità di accedere ai sistemi da diverse località e dispositivi, è essenziale che le banche implementino soluzioni robuste di gestione delle identità e degli accessi (Identity and Access Management, IAM). Queste soluzioni garantiscono che solo gli utenti autorizzati possano accedere ai sistemi e ai dati sensibili, attraverso l'uso di autenticazione a più fattori (MFA), controlli di accesso basati sui ruoli (RBAC), e politiche di accesso molto rigorose;

- Il *monitoraggio continuo* delle minacce è essenziale nella strategia di Cybersecurity delle istituzioni finanziarie, poiché permette di rilevare e rispondere tempestivamente agli attacchi informatici. Questo processo si basa su tecnologie avanzate e una sorveglianza ininterrotta del traffico di rete e delle attività digitali. Le banche utilizzano sistemi di rilevamento delle intrusioni (IDS) e sistemi di prevenzione delle intrusioni (IPS) al fine di monitorare, con cadenza regolare, il traffico di rete. In particolare, gli IDS identificano e segnalano attività sospette che potrebbero indicare un tentativo di intrusione, analizzando i dati alla ricerca di anomalie. Gli IPS, invece, vanno oltre la semplice rilevazione, bloccando attivamente le minacce una volta individuate, come ad esempio durante un attacco DDoS. Questi sistemi sono potenziati da soluzioni di analisi delle minacce basate su intelligenza artificiale (AI) e Machine Learning, che migliorano l'efficacia del rilevamento. La rapidità con cui le minacce evolvono rappresenta una sfida significativa, motivo per cui molte banche collaborano con fornitori di servizi di sicurezza gestita (MSSP), i quali offrono monitoraggio e gestione della sicurezza.

2.1.6 Compliance e regolamentazione tecnologica

All'interno del contesto sempre più complesso e digitalizzato del settore finanziario, la conformità alle normative (spesso indicata con il nome di "compliance") e la regolamentazione tecnologica sono diventate aspetti cruciali che le istituzioni finanziarie devono gestire con la massima attenzione. La rapida evoluzione delle tecnologie e l'aumento delle minacce informatiche hanno spinto i legislatori a sviluppare un quadro normativo rigoroso al fine di proteggere i dati sensibili dei clienti, garantire la sicurezza delle transazioni e promuovere una concorrenza leale nel mercato. In particolare, regolamenti come il GDPR e la PSD2 hanno avuto un impatto significativo sul settore finanziario, richiedendo alle banche di adattare le loro strategie IT per garantire la conformità e sfruttare le nuove opportunità di mercato.

Il **Regolamento Generale sulla Protezione dei Dati** (GDPR), entrato in vigore in data 25 maggio 2018, è attualmente una delle normative più rilevanti per quanto riguarda la protezione dei dati personali all'interno dell'Unione Europea. Il GDPR ha stabilito standard rigorosi per la raccolta, l'elaborazione, la conservazione e la gestione dei dati personali, imponendo alle organizzazioni, comprese le istituzioni finanziarie, obblighi significativi per proteggere la privacy dei loro clienti. Uno dei principi fondamentali del GDPR è quello della "*Privacy by design*", che richiede alle

istituzioni di integrare la protezione dei dati fin dalla fase di progettazione dei sistemi e delle applicazioni. Questo principio implica che le banche devono implementare misure di sicurezza adeguate, come la crittografia e l'anonimizzazione, per proteggere i dati personali, e garantire che vengano raccolti e trattati solo i dati strettamente necessari. Il GDPR introduce anche il concetto di "*Diritto all'oblio*", che permette ai cittadini dell'UE di richiedere la cancellazione dei propri dati personali dalle banche e da altre organizzazioni. Le banche devono quindi essere in grado di rispondere tempestivamente a tali richieste e di garantire che i dati siano rimossi da tutti i sistemi e le copie di backup. Inoltre, il GDPR impone obblighi rigorosi in caso di violazione dei dati, richiedendo alle organizzazioni di notificare tempestivamente le autorità di controllo e tutti i soggetti direttamente interessati, minimizzando in questo modo i danni e proteggendo la fiducia dei clienti[17].

Oltre al GDPR, altre normative globali hanno imposto requisiti rigorosi per la protezione dei dati personali nel settore finanziario, ad esempio, negli Stati Uniti, la Gramm-Leach-Bliley Act (GLBA) richiede alle istituzioni finanziarie di divulgare le proprie pratiche di raccolta e condivisione dei dati e di proteggere le informazioni personali dei clienti. In Asia, paesi come il Giappone, Singapore e Hong Kong hanno introdotto normative simili, riflettendo l'importanza globale della protezione dei dati personali. Tali normative sulla protezione dei dati hanno costretto le banche a rivedere e rafforzare le loro pratiche di gestione dei dati, investendo in tecnologie di Cybersecurity avanzate, come spiegato precedentemente, e sviluppando politiche di protezione dei dati conformi alle normative internazionali. La non conformità può comportare sanzioni severe, quali multe significative e danni reputazionali, che possono compromettere la fiducia dei clienti, la stabilità finanziaria dell'istituzione e la competitività all'interno del mercato.

La **direttiva sui servizi di pagamento** (*Payment Service Directive* - PSD2), entrata in vigore in data 13 gennaio 2018 e resa attuativa in data 14 novembre 2019, è un altro regolamento cruciale che ha trasformato, in maniera radicale, il panorama dei pagamenti in Europa. La PSD2 è stata progettata per promuovere l'innovazione, aumentare la concorrenza e migliorare la sicurezza dei pagamenti digitali, aprendo il mercato dei servizi di pagamento a nuovi attori, come le fintech e i fornitori di servizi di terze parti (*Third Party Payment Services Provider* - TPP). Uno degli aspetti

[17] Parlamento Europeo e Consiglio dell'Unione Europea (2016), *Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali e alla libera circolazione di tali dati*, Gazzetta ufficiale dell'Unione europea, URL: REGOLAMENTO (UE) 2016/ 679 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO

più rivoluzionari della PSD2 è l'introduzione del concetto di "*Open banking*": tale direttiva obbliga le banche tradizionali a fornire accesso alle informazioni sui conti dei clienti e ai servizi di pagamento ai TPP tramite interfacce di programmazione delle applicazioni (API). Questo consente ai clienti di autorizzare le TPP a gestire i propri conti bancari, effettuare pagamenti e offrire servizi finanziari innovativi, come l'aggregazione di conti e il budgeting personalizzato. L'open banking ha ampliato significativamente le opportunità di innovazione nel settore dei pagamenti, permettendo a nuove aziende di entrare nel mercato e offrire soluzioni su misura che rispondono meglio alle esigenze dei clienti. Tuttavia, ha anche creato nuove sfide per le banche tradizionali, le quali devono adattarsi a un ambiente competitivo più dinamico e collaborare con i nuovi attori del mercato. Per rimanere competitive, le banche hanno dovuto investire nello sviluppo di API sicure e in strategie di collaborazione con le fintech, sfruttando le nuove opportunità offerte dalla PSD2 per migliorare i propri servizi e attrarre nuovi clienti. La PSD2 ha inoltre introdotto requisiti rigorosi in materia di autenticazione forte del cliente (*Strong Customer Authentication*, SCA) e gestione dei rischi, al fine di rafforzare la sicurezza delle transazioni elettroniche. La SCA prevede l'utilizzo di almeno due dei tre fattori di autenticazione (i.e., conoscenza, possesso e inerenza) per autorizzare i pagamenti digitali, riducendo così il rischio di frodi. Le banche sono quindi chiamate a implementare soluzioni di autenticazione avanzate, come l'autenticazione biometrica o i token di sicurezza, per conformarsi a tali requisiti e garantire la sicurezza delle transazioni[18].

La conformità normativa non è più solo una questione di adempimento legale, bensì è diventata una componente strategica che può influenzare la competitività e l'innovazione delle istituzioni finanziarie. Tuttavia, è emerso fin qui che l'adattamento alle nuove normative comporta quasi sempre l'insorgere di sfide significative, le banche devono bilanciare la necessità di conformità con la necessità di innovare e rimanere competitive in un mercato in rapida evoluzione. Questo trade-off richiede una gestione attenta delle risorse, un costante aggiornamento delle competenze del personale IT, e una collaborazione efficace tra i dipartimenti legali, di conformità e tecnologici.

[18] Parlamento Europeo e Consiglio dell'Unione Europea (2015), *Direttiva (UE) 2015/2366 del Parlamento Europeo e del Consiglio del 25 novembre 2015 relativa ai servizi di pagamento nel mercato interno (PSD2)*, Gazzetta ufficiale dell'Unione europea, URL: Direttiva (UE) 2015/ del Parlamento europeo e del Consiglio, del 25 novembre 2015

2.2 IT GOVERNANCE

2.2.1 Introduzione e norma ISO/IEC 38500

È possibile definire l'**IT Governance** come un insieme critico di pratiche e procedure il cui utilizzo è volto ad assicurare che le tecnologie informatiche siano impiegate in maniera efficace per sostenere gli obiettivi e le strategie aziendali. Essa si colloca nel punto di intersezione tra la gestione IT e la governance aziendale, con l'obiettivo primario di garantire che gli investimenti nell'ambito IT generino valore aggiunto per l'azienda e di mitigare i rischi associati alle tecnologie emergenti.

La **norma ISO/IEC 38500** rappresenta un punto di riferimento cruciale per la governance IT in quanto offre un quadro normativo che guida le aziende nell'uso responsabile delle tecnologie informatiche. Questa norma internazionale, elaborata dall'International Organization for Standardization (ISO) e dalla International Electrotechnical Commission (IEC), è stata progettata allo scopo di aiutare le organizzazioni di tutte le dimensioni, compresi gli enti pubblici e le aziende private, a governare i propri sistemi IT in modo efficace, efficiente e in linea con le esigenze etiche e normative. Tale norma si basa su **sei principi fondamentali**, di seguito elencati, che delineano le responsabilità del consiglio di amministrazione e della direzione esecutiva riguardo alla gestione delle risorse IT.

1. *Responsabilità*: questo principio sottolinea l'importanza di avere chiarezza sui ruoli e le responsabilità all'interno dell'organizzazione riguardo all'IT in quanto ogni individuo deve comprendere e accettare le proprie responsabilità relativamente all'offerta e alla domanda di IT. Coloro che sono responsabili delle azioni devono avere anche l'autorità necessaria per compierle, garantendo così che le decisioni siano prese in modo informato e responsabile;
2. *Strategia*: la strategia aziendale deve considerare le capacità attuali e future dell'IT. Questo significa che le pianificazioni per l'uso dell'IT devono soddisfare le esigenze attuali e future dell'organizzazione;
3. *Acquisizione*: le acquisizioni di IT devono essere effettuate per motivi validi e basate su un'analisi appropriata e continua. Le decisioni devono essere trasparenti, con un equilibrio adeguato tra benefici, opportunità, costi e rischi, sia a breve che a lungo termine;

4. *Performance*: questo principio si concentra sulla necessità di monitorare e valutare le prestazioni delle risorse IT. Le organizzazioni devono stabilire metriche e indicatori chiave di prestazione per garantire che l'IT stia contribuendo in modo efficace agli obiettivi aziendali al fine di identificare possibili aree di miglioramento e a garantire che le risorse siano utilizzate in modo efficiente;
5. *Conformità*: le organizzazioni devono garantire che l'uso dell'IT sia conforme a tutte le normative, leggi e obblighi contrattuali in vigore. Questo principio è fondamentale per ridurre i rischi legali e reputazionali e proteggere l'organizzazione da potenziali sanzioni e danni;
6. *Comportamento umano*: le organizzazioni devono considerare come le persone interagiscono con la tecnologia e come le loro decisioni e azioni possono influenzare l'uso dell'IT. È essenziale promuovere una cultura di responsabilità e consapevolezza riguardo all'uso dell'IT, affinché tutti i membri dell'organizzazione contribuiscano a una governance efficace.

Per assistere le organizzazioni nell'implementazione di questi principi, la norma ISO/IEC 38500 fornisce un modello di governance definibile come un approccio olistico che aiuta le organizzazioni a gestire l'IT in modo strategico e responsabile. Attraverso una chiara struttura di governance, processi di acquisizione ben definiti, monitoraggio delle prestazioni, gestione dei rischi e coinvolgimento degli stakeholder, le organizzazioni possono massimizzare i benefici delle loro risorse IT e garantire che queste siano allineate con gli obiettivi aziendali complessivi. Una buona governance dell'IT offre numerosi vantaggi alle organizzazioni, contribuendo a migliorare le loro prestazioni complessive e a garantire un uso responsabile e strategico delle risorse IT. Ecco alcuni dei principali **benefici**:

- *Innovazione nei servizi e nei mercati*: una governance efficace dell'IT promuove l'innovazione, consentendo alle organizzazioni di sviluppare nuovi servizi e prodotti migliorando la loro competitività sul mercato;
- *Allineamento dell'IT con le esigenze aziendali*: la governance dell'IT assicura che le strategie IT siano allineate con gli obiettivi e le esigenze dell'organizzazione;
- *Implementazione e operazione appropriata delle risorse IT*: ciò include la pianificazione, l'acquisizione, l'implementazione e la manutenzione delle tecnologie, assicurando che siano utilizzate in modo ottimale per massimizzare i benefici;

- *Chiarezza di responsabilità e accountability*: la governance dell'IT stabilisce chiare responsabilità e ruoli all'interno dell'organizzazione garantendo che ci sia una responsabilità definita per le decisioni relative all'IT, il che facilità la rendicontazione;
- *Continuità e sostenibilità aziendale*: assicurare che le organizzazioni siano in grado di affrontare le interruzioni e di mantenere le operazioni anche in situazioni di crisi.

In un contesto aziendale sempre più digitalizzato e interconnesso, la norma ISO/IEC 38500 assume una rilevanza ancora maggiore in quanto al giorno d'oggi le organizzazioni sono chiamate a gestire una crescente complessità tecnologica e a rispondere proattivamente alle evoluzioni del panorama sia tecnologico che normativo. In un ambiente molto dinamico, una governance IT ben strutturata può fornire il necessario supporto strategico per supportare attivamente non solo la competitività, ma anche la sostenibilità a lungo termine delle pratiche aziendali[19].

2.2.2 Funzioni principali dell'IT Governance

Qual è il ruolo che l'IT Governance ricopre nel reparto IT di un'organizzazione? L'IT Governance ricopre una posizione di rilievo nel dipartimento IT di ciascuna azienda in quanto è una guida concreta il cui ruolo risulta indispensabile per assicurare che le decisioni nell'ambito IT siano allineate e coerenti con gli obiettivi strategici aziendali e che le soluzioni tecnologiche adottate facilitino il raggiungimento degli obiettivi prefissati. Attraverso una governance IT efficace, il reparto IT ha le potenzialità per trasformare sé stesso da un centro di costi a un vero e proprio motore di valore, stimolando l'innovazione e promuovendo il vantaggio competitivo dell'azienda. Uno degli aspetti principali del ruolo della IT Governance è la capacità di creare un ponte tra la tecnologia e le esigenze del business, tutto ciò richiede l'istituzione di processi decisionali trasparenti e l'attribuzione di responsabilità ben definite per la pianificazione, l'attuazione e il monitoraggio delle tecnologie all'interno dell'organizzazione[20]. Questa sezione ha l'obiettivo di illustrare in modo approfondito alcuni esempi rappresentativi delle principali funzioni dell'IT Governance.

[19] International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) (2015), *ISO/IEC 38500:2015 - Information technology – Governance of IT for the organization*, ISO, Ginevra
[20] Weill, P., & Ross, J. W. (2004), *IT Governance: How Top Performers Manage IT Decision Rights for Superior Results*, Harvard Business School Press, Boston

Allineamento strategico

L'allineamento strategico è fondamentale per la governance IT poiché rappresenta il punto di collegamento tra le strategie IT e le strategie aziendali, garantendo che gli investimenti tecnologici siano direttamente correlati agli obiettivi a lungo termine dell'organizzazione. Questo processo va oltre la semplice coordinazione, richiedendo un'integrazione profonda delle agende IT e di Business attraverso una pianificazione congiunta e un impegno continuo da parte dei leader aziendali.

La definizione degli obiettivi comuni tra IT e Business è il primo passo per un efficace allineamento strategico; infatti, questo step richiede che i leader IT siano coinvolti sin dalle fasi iniziali della formulazione della strategia aziendale, assicurando che le proposte tecnologiche siano rilevanti per le esigenze del business, sia attuali che future, in maniera tale che la tecnologia non solo supporti, ma anche abiliti nuove opportunità di business. Un efficace allineamento strategico dipende da innumerevoli variabili, tra cui la comunicazione aperta e continua tra il dipartimento IT e gli altri settori dell'organizzazione, ecco spiegato perché riunioni regolari, workshop e canali di comunicazione dedicati sono elementi fondamentali per scambiare idee tramite sessioni di brainstorming, discutere i progressi e adeguare le strategie in risposta alle mutevoli condizioni del mercato o ad eventuali ostacoli di natura interna all'azienda. Un aspetto essenziale al fine di trasformare le strategie in azioni concrete è la pianificazione integrata tra IT e business; in questo contesto, l'elaborazione di roadmap tecnologiche che riflettano le priorità strategiche del business consente una più stretta correlazione tra investimenti IT e obiettivi aziendali, garantendo che ogni iniziativa tecnologica sia finalizzata a migliorare specifici risultati di business.

L'allineamento strategico non può essere considerato un processo statico o definitivo in quanto richiede un continuo processo di adattamento per garantirne l'efficacia nel corso del tempo. Infatti, la sua natura dinamica detta la necessità di effettuare regolari revisioni delle strategie IT, che devono essere realizzate in collaborazione con il management aziendale con l'obiettivo di rivedere e riorganizzare le priorità legate all'IT in funzione dei cambiamenti del mercato, delle nuove esigenze aziendali e degli obiettivi strategici che l'organizzazione intende perseguire nel lungo termine[21].

[21] Galliers, R. D., & Leidner, D. E. (2014), *Strategic Information Management: Challenges and Strategies in Managing Information Systems* (4ª ed.), Routledge

Gestione delle risorse

La gestione delle risorse nell'ambito dell'IT Governance è un ulteriore aspetto cruciale in quanto garantisce che gli investimenti tecnologici come, ad esempio, hardware, software e competenze umane siano utilizzati in modo ottimale ed efficiente, ciò vuol dire massimizzare il valore di queste risorse cercando allo stesso tempo di minimizzare i costi e ridurre gli sprechi, il che è ottenibile mediante l'uso di un approccio organizzato e mirato. In parole semplici, il processo di valutazione delle necessità tecnologiche è un processo continuo che permette alle organizzazioni di definire quali investimenti sono necessari per mantenere o migliorare la propria infrastruttura IT. Ad esempio, una società di servizi finanziari potrebbe analizzare le proprie operazioni IT con cadenza annuale per determinare se sia necessario aggiornare i propri server migliorando così la capacità di elaborazione dei dati o rinnovare le licenze software per rafforzare la sicurezza informatica. Una volta identificate le possibili esigenze, segue la fase di acquisizione di nuove tecnologie e la manutenzione dell'infrastruttura già esistente, step altrettanto essenziali al fine di prevenire malfunzionamenti e/o interruzioni del servizio che possono avere un impatto negativo sulle operazioni aziendali. Inoltre, in un contesto del genere, investire nella formazione e nello sviluppo del personale IT è fondamentale per garantire che il reparto tecnologico possa continuare a supportare le necessità dell'azienda di fronte a rapidi cambiamenti tecnologici.

Misurazione delle prestazioni

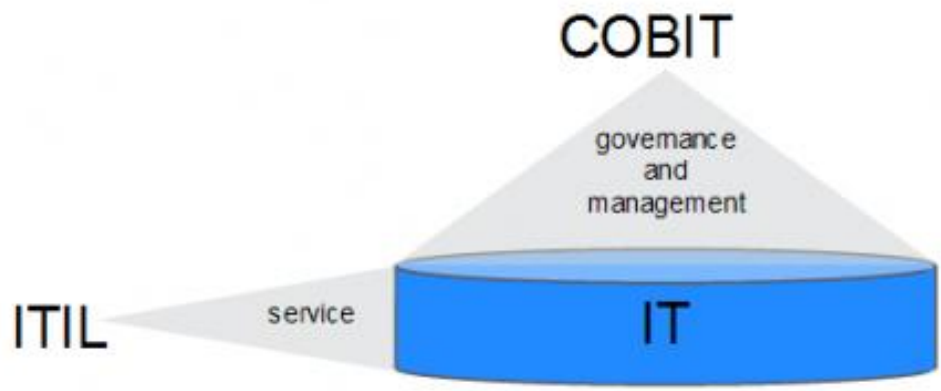
La misurazione delle prestazioni è una funzione, particolarmente importante, che utilizza una serie di indicatori di prestazione chiave (KPI) per monitorare vari aspetti delle operazioni IT, dalla sicurezza alla soddisfazione dell'utente, dall'uptime dei sistemi alla loro capacità di supportare le operazioni aziendali, ecc. L'uso costante di un set strutturato di KPI aiuta non solo a identificare possibili aree di forza e di debolezza nel panorama IT mediante una misurazione oggettiva delle prestazioni, ma è utile anche per garantire la trasparenza in quanto promuove un ambiente di responsabilità all'interno dell'intera area aziendale.

L'insieme di queste funzioni dell'IT Governance, nel caso in cui siano integrate in maniera efficace, permettono alle organizzazioni di sfruttare al meglio le loro risorse IT e di garantire che le decisioni tecnologiche siano prese con una chiara comprensione del loro impatto strategico, operativo e finanziario.

2.2.3 Best Practice

Alla luce di quanto esposto nei paragrafi precedenti, appare evidente che la governance IT necessiti di un approccio strutturato e metodico per garantire che gli investimenti tecnologici producano valore aggiunto, riducendo contestualmente i rischi correlati. In Figura 2.4 sono mostrati due dei principali framework utilizzati a livello globale per implementare una governance IT efficace, ovvero **ITIL** *(Information Technology Infrastructure Library)* e **COBIT** *(Control Objectives for Information and Related Technology);* essi non solo assistono le aziende nella gestione e nel monitoraggio delle attività IT, ma offrono anche direttive fondamentali per le attività di audit e conformità normativa[22].

Figura 2.4 – ITIL e COBIT a confronto



FONTE: Shobhit Mehta*, (2019), Lessons Learnt While Combining COBIT 5 & ITIL, URL:* Lessons learnt from combining COBIT 5 & ITIL – Governance, Risk, & Compliance (grcmusings.com)

Best Practice - ITL

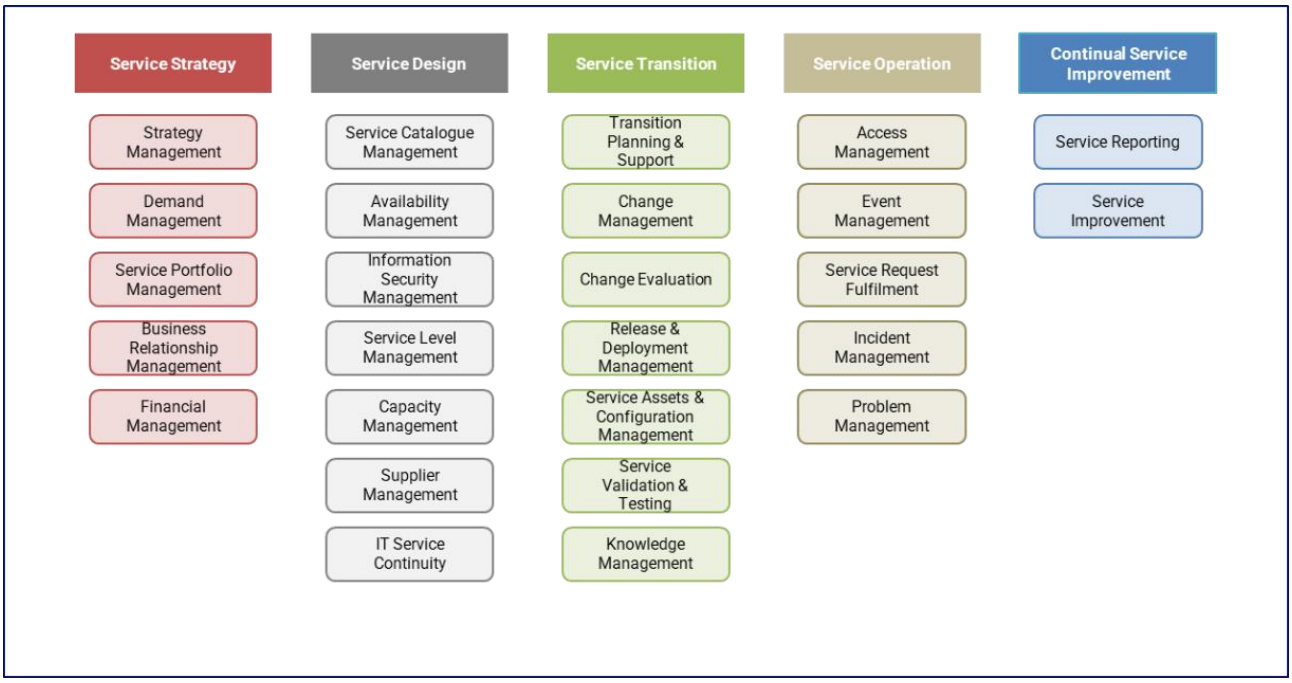
ITIL fu sviluppato dal governo britannico in risposta alla necessità, fatta presente da molte organizzazioni, di migliorare l'efficienza nella gestione dei servizi IT in quanto esse stavano affrontando sfide significative legate alla crescente complessità dei sistemi informatici e al costante

[22] Deloitte, (2012), *IT Playbook_2012*

bisogno di fornire servizi di qualità sempre crescente. Nel dettaglio, il tutto ebbe inizio alla fine degli anni ’80 e inizi anni ’90, quando l'Office of Government Commerce (OGC), un'agenzia del governo britannico responsabile della gestione degli acquisti e dei servizi IT nel settore pubblico, cominciò a documentare il modo in cui le migliori organizzazioni gestivano i loro servizi IT, per poi arrivare alla creazione di una serie di testi di riferimento, noti come IT Infrastructure Library (ITIL), i quali raccolsero le pratiche più consolidate del settore. Mentre inizialmente la diffusione di ITIL rimase geograficamente limitata alla Gran Bretagna, la creazione di veri e proprio manuali di riferimento stimolò un interesse crescente da parte di una comunità globale di professionisti e organizzazioni.

La *prima versione* di ITIL si concentrò principalmente su processi e pratiche di base per la gestione dei servizi IT; nei primi anni 2000 venne poi pubblicata la *seconda versione*, orientata verso attività strettamente connesse alla fornitura e al supporto dei servizi. A metà del 2007 l'OGC rilasciò un terzo aggiornamento, noto come *ITIL v3*, che, seppur simile alla versione precedente, introdusse un approccio più olistico ed enfatizzò l'importanza del ciclo di vita del servizio, suddividendolo in cinque fasi principali, ciascuna delle quali è, ancora oggi, composta da sottocategorie di processi, per un totale di 26 processi che coprono così l'intera organizzazione IT, vedi Fig. 2.5. L'obiettivo di ITIL v3 è migliorare la gestione e la fornitura dei servizi IT attraverso un approccio sistematico e strutturato, nell’ottica di utilizzare l’IT come figura di supporto per il business e per il raggiungimento di determinati obiettivi.

Figura 2.5 – Framework ITIL v3



FONTE: elaborazione interna all'impresa di consulenza

Sebbene il ciclo di vita sia suddiviso in cinque fasi distinte, di seguito descritte in maniera dettagliata, queste non sono da intendere come fasi isolate né richiedono una sequenza specifica per la loro esecuzione. La natura dell'approccio del Service Lifecycle risiede proprio nel fatto che ogni fase interagisce strettamente con le altre, formando un processo iterativo e multidimensionale. In aggiunta, per garantire l'efficacia di questo modello, la fase di miglioramento continuo del servizio è incorporata in ciascuna delle altre fasi.

- La fase di **Service Strategy** è fondamentale nel framework ITIL poiché stabilisce le basi per la gestione dei servizi IT allineandoli alle esigenze e agli obiettivi del business. Essa si concentra sulla definizione di come un'organizzazione può utilizzare i servizi IT per raggiungere i risultati desiderati e ottenere un vantaggio competitivo ponendosi i seguenti obiettivi: assicurare che i servizi IT siano progettati e gestiti in modo da supportare gli obiettivi strategici dell'organizzazione (i.e., allineamento con il Business), definire in che modo i servizi possono fornire valore ai clienti soddisfacendo le loro esigenze e aspettative,

creare e mantenere un portafoglio di servizi che rappresenti le offerte dell'organizzazione e le opportunità di mercato[23];

- Nella fase successiva, nota come **Service Design**, i servizi IT vengono progettati e pianificati per rispondere alle esigenze del business emerse nella precedente fase strategica. Alcuni esempi degli obiettivi che questa fase si prefigge di raggiungere includono: ottimizzazione dell'utilizzo delle risorse al fine di risparmiare tempo, denaro e ridurre i rischi operativi, soddisfare le esigenze di mercato creando servizi capaci di rispondere alle necessità attuali e future dei client e infine si impegna nell'attività di miglioramento della qualità dei servizi IT in generale, garantendo che essi raggiungano elevati standard qualitativi e rispettino i requisiti richiesti[24];
- La fase di **Service Transition** costituisce una componente essenziale del ciclo di vita dei servizi secondo il framework ITIL in quanto è interamente dedicata alla pianificazione e all'implementazione di nuovi servizi o alle modifiche di quelli esistenti. In particolare, questa fase si concentra nell'assicurare che l'introduzione dei servizi nell'ambiente operativo avvenga in modo controllato, minimizzando l'impatto sui servizi già in produzione e garantendo la continuità operativa. Inoltre, si pone l'accento sulla gestione del cambiamento, coordinando le modifiche ai servizi e ai processi di gestione per garantire un allineamento costante con le esigenze del business e migliorando la capacità dell'organizzazione di gestire un elevato volume di cambiamenti in modo efficace, rafforzando la flessibilità e l'adattabilità dell'azienda in un contesto in continua evoluzione[25];
- La fase di **Service Operations** è incaricata della gestione quotidiana dei servizi IT e della loro erogazione agli utenti finali, garantendo che le operazioni siano gestite in conformità con i livelli di servizio concordati ed eventualmente coordinando le operazioni necessarie per affrontare possibili incidenti o problemi che possano insorgere. Un altro aspetto cruciale è il monitoraggio delle prestazioni, che implica la raccolta sistematica di dati sulle performance dei servizi e l'utilizzo di queste informazioni per migliorare costantemente l'efficacia e l'efficienza delle operazioni nel continuo[26];

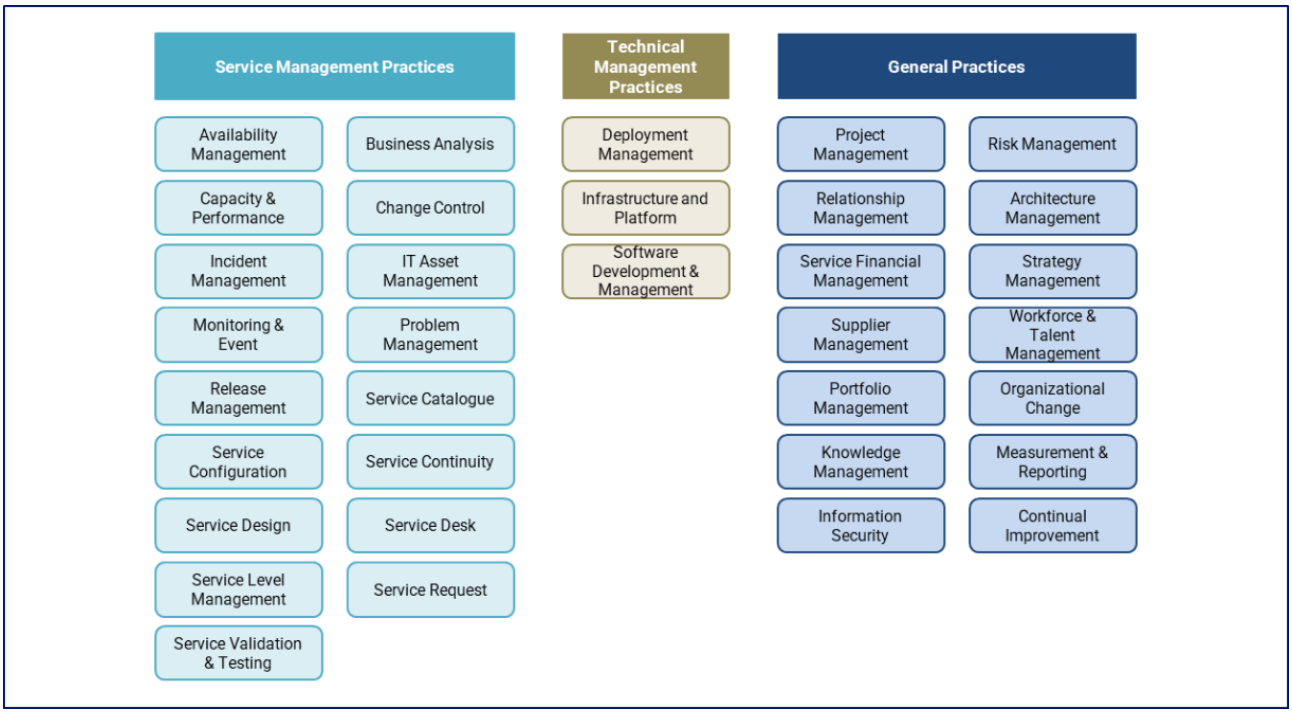
[23] Office of Government Commerce, (2011). *ITIL V3 - Service Strategy_1*
[24] Office of Government Commerce, (2011). *ITIL V3 - Service Design_2*
[25] Office of Government Commerce, (2011). *ITIL V3 - Service Transition_3*
[26] Office of Government Commerce, (2011). *ITIL V3 – Service Operation_4*

- L'ultima fase del ciclo di vita del servizio IT, conosciuta come **Continual Service Improvement (CSI)**, è dedicata al perfezionamento costante della qualità dei servizi IT e alla massimizzazione del valore offerto ai clienti ottenibili mediante un'analisi approfondita delle prestazioni dei servizi esistenti, utilizzando metriche e feedback per identificare possibili aree di miglioramento. Attraverso l'implementazione di strategie mirate, il CSI si propone di ottimizzare i servizi esistenti e di apportare modifiche che rispondano alle esigenze in costante evoluzione del business e del mercato, adottando un approccio flessibile che permette di adattare rapidamente i servizi e i processi operativi ai cambiamenti del contesto aziendale, assicurando così che l'organizzazione rimanga competitiva. In questo modo, il CSI non solo garantisce una risposta efficace alle esigenze attuali, ma prepara l'organizzazione ad affrontare le sfide future, mantenendo un vantaggio competitivo duraturo nel tempo[27].

Ed infine, l'ultima versione attualmente disponibile è nota come *ITIL 4* e supera il modello delle cinque fasi del Service Lifecycle andando a considerare tre macrocategorie, le quali definiscono a loro volta un totale di 34 pratiche di gestione IT, vedi Fig. 2.6. L'obiettivo di ITIL 4 è fornire un approccio flessibile alla gestione dei servizi IT, integrando metodologie moderne, come Agile e DevOps, e principi guida in modo da migliorare la creazione condivisa di valore, l'efficienza e la capacità di adattarsi ai cambiamenti. La diversa connotazione che ITIL 4 dà all'IT permette un maggiore coinvolgimento del business, il cliente stesso diventa parte del team.

[27] Office of Government Commerce, (2011). *ITIL V3 - Service Improvement_5*

Figura 2.6 – Framework ITIL 4



FONTE: elaborazione interna all'impresa di consulenza

Negli ultimi anni, **in Italia** molte aziende hanno iniziato a integrare le pratiche ITIL nei loro processi di gestione dei servizi IT a causa della crescente necessità di migliorare la qualità del servizio, ottimizzare i costi e rispondere in modo più efficace alle esigenze dei clienti. Le organizzazioni stanno riconoscendo sempre di più che l'adozione di best practice può portare a una gestione più strutturata e professionale dei servizi IT. A differenza di altri paesi però, in Italia non esiste un obbligo di certificazione per l'adozione di ITIL, ciò vuol dire che le aziende possono scegliere di implementarne le pratiche in modo volontario, senza la necessità di seguire uno standard ufficiale. Sebbene a primo impatto questa flessibilità possa essere vista come un vantaggio, essa potrebbe anche portare a una variabilità nella qualità dell'implementazione poiché alcune aziende potrebbero adottare solo alcune delle pratiche omettendo un approccio sistematico, il che comprometterebbe i potenziali benefici. Un altro fattore cruciale per l'implementazione del framework ITIL in Italia, e non solo, è la formazione; infatti, molte aziende stanno investendo nella formazione del personale per garantire che i dipendenti comprendano e possano applicare le pratiche previste dalla best practice in maniera ottimale. Nonostante i progressi, ci sono ancora sfide significative da affrontare, quali, ad esempio, la resistenza al cambiamento, la carenza di risorse e la difficoltà nell'integrare le pratiche ITIL con i processi esistenti, i quali potrebbero

ostacolarne l'adozione. È quindi essenziale che le organizzazioni valutino attentamente come adattare le pratiche ITIL alle loro specifiche esigenze e contesti, solo così possono massimizzare i benefici e migliorare la loro efficienza da un punto di vista operativo, e non solo.

Best Practice - COBIT

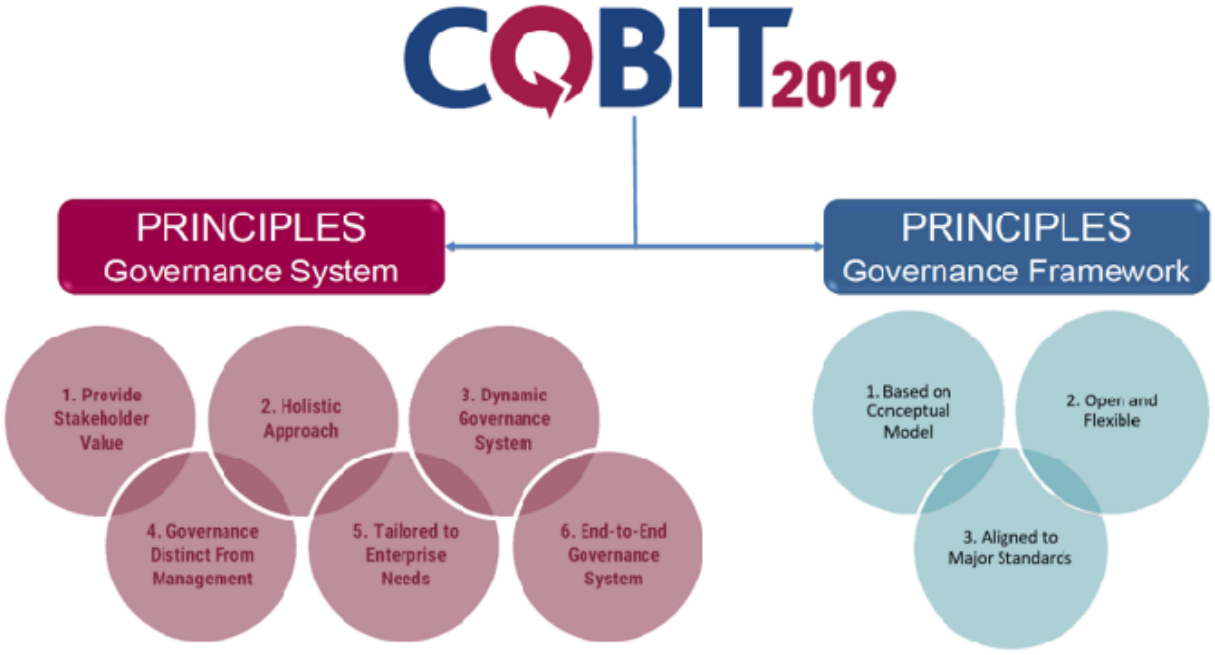
Fondata nel 1969, ISACA (*Information Systems Audit and Control Association*) è un'associazione professionale internazionale che si dedica a supportare gli esperti nel campo della governance, del controllo, della sicurezza, dell'audit e dell'assicurazione dei sistemi informativi. L'associazione è nota per lo sviluppo di certificazioni professionali e di framework, come COBIT, per i quali fornisce materiale educativo che aiuta numerosi professionisti a gestire efficacemente rischi, problemi di conformità e altre sfide legate all'immenso ambito dell'IT. COBIT, acronimo di "Control Objectives for Information and related Technology", è un framework di governance e gestione delle informazioni e della tecnologia, sviluppato nel 1996 per aiutare gli auditor finanziari a comprendere e gestire i rischi legati ai sistemi informativi[28]. Con l'evoluzione delle esigenze aziendali e l'avanzamento delle tecnologie, divenne evidente che il framework doveva andare oltre l'audit e, di conseguenza, nel 1998 COBIT 2.0 ampliò il suo ambito per includere una più ampia gestione dell'IT. L'edizione del 2000 di COBIT, la terza, continuò questa tendenza espansiva introducendo una struttura organizzativa più definita e criteri informativi che hanno aiutato le organizzazioni a valutare la qualità delle informazioni. COBIT 4.0, rilasciato nel 2005, consolidò ulteriormente il legame tra le pratiche di governance e le normative di conformità, enfatizzando l'importanza di una gestione IT che supporti in maniera attiva gli obiettivi strategici dell'azienda. Il salto più significativo avvenne nel 2012 con l'introduzione di COBIT 5, che riuscì a fornire un approccio completo alla governance sottolineando anche l'importanza di trattare l'informazione come un asset chiave per l'azienda, spostando quindi il focus dalla tecnologia all'informazione stessa[29].

La più recente iterazione, COBIT 2019, introduce oggi miglioramenti significativi per aumentare la flessibilità del framework, ovvero offre linee guida dettagliate, processi e/o procedure applicabili direttamente dalle organizzazioni[30]. Quest'ultima versione del framework permette inoltre un

[28] ISACA (2024), *COBIT—An ISACA Framework*, ISACA, URL: COBIT | Control Objectives for Information Technologies | ISACA
[29] D. D'Agostini, A. Piva, A. Rampazzo, (2012), *Governance IT - Continua evoluzione dei modelli per gestirla*, Triveneta, URL: Rubrica 1_piva_impaginato (aicqna.it)
[30] ISACA (2018), *COBIT 2019 Framework: Governance and Management Objectives*, ISACA

elevato livello di personalizzazione mantenendo una struttura aperta che si aggiorna facilmente con nuovi standard IT e normative. COBIT 2019 fu sviluppato seguendo due distinte serie di principi, di seguito descritti e mostrati in Fig. 2.7.

Figura 2.7 – COBIT



Fonte: BITIL (2024), COBIT 2019, Modello di IT Governance, BITIL*,*

URL: CobiT 2019 - BITIL.COM

I primi sei principi mirano a descriverei requisiti fondamentali di un *sistema di governance* (Governance System), quali:

1. Necessità di un sistema di governance robusto per rispondere ai bisogni degli stakeholders;
2. Composizione olistica del sistema di governance;
3. Dinamicità del sistema di governance per adattarsi rapidamente ai cambiamenti, strategici e/o tecnologici;
4. Chiara distinzione tra governance e gestione;
5. Personalizzazione del sistema di governance utilizzando fattori di progettazione personalizzati per definire le priorità e configurare i componenti del sistema;
6. Copertura end-to-end dell'organizzazione mediante un approccio globale che si estenda oltre la funzione IT.

In aggiunta, tre principi per definire un *quadro di governance* (Governance Framework) che può essere utilizzato per costruire un sistema di governance per l'organizzazione, di seguito elencati:

1. Fondazione del quadro di governance su un modello concettuale che identifichi chiaramente i componenti essenziali e le loro interrelazioni;
2. Apertura e flessibilità per permettere l'integrazione di nuovi contenuti e l'adattamento a sfide emergenti senza compromettere l'integrità e la coerenza del sistema;
3. Allineamento con normative e standard rilevanti per garantire che l'organizzazione rispetti le best practice e le direttive regolamentari più pertinenti.

L'adozione di COBIT offre numerosi vantaggi per le organizzazioni che mirano a ottimizzare la gestione e la governance dell'IT, tra i quali vi è, come spesso visto in precedenza, l'allineamento strategico, che garantisce una coerenza tra le strategie IT e gli obiettivi aziendali ed è essenziale per creare sinergia tra il reparto IT e le altre funzioni aziendali. In aggiunta, COBIT fornisce un framework strutturato che eleva la governance dell'IT, incentivando la responsabilità e la trasparenza, facilita anche la gestione dei rischi, permettendo alle aziende di identificare e mitigare efficacemente i rischi associati all'IT. Un ulteriore vantaggio è il miglioramento delle prestazioni, ottenuto attraverso la valutazione e l'ottimizzazione dei processi, che porta a un conseguente incremento dell'efficienza operativa.

Tuttavia, l'implementazione di COBIT può presentare delle sfide dovute, ad esempio, alla complessità del framework e ai costi associati alla formazione del personale e alle consulenze esterne, i quali possono rappresentare una barriera per alcune organizzazioni. Inoltre, come ogni cambiamento importante nelle prassi organizzative, l'introduzione di COBIT, allo stesso modo di ITIL, spesso incontra resistenza interna, caratterizzata da inerzie e reticenze del personale.

2.2.4 IT Governance Maturity Assessment

L'analisi dettagliata della Governance IT e dei relativi aspetti trattati nei paragrafi precedenti consente ora di comprendere appieno la natura di un IT Governance Maturity Assessment. È un processo sistematico largamente impiegato per valutare il livello di maturità delle pratiche di governance IT all'interno di un'organizzazione, fondamentale per comprendere quanto efficacemente le politiche e i processi di IT Governance supportino gli obiettivi strategici aziendali.

Questo processo mira a fornire una valutazione quantitativa e qualitativa del grado di formalizzazione e ottimizzazione delle pratiche di governance IT di un'organizzazione con l'intento di offrire una visione chiara del livello attuale di governance IT, facilitando il riconoscimento delle aree nelle quali è possibile implementare miglioramenti per incrementare l'efficacia delle funzioni IT[31]. Il processo di valutazione in un IT Governance Maturity Assessment segue tipicamente diverse fasi chiave, quali:

- **Preparazione**: definizione degli obiettivi dell'assessment, selezione del modello di maturità appropriato e schedulazione di un piano di lavoro ben dettagliato in attività e sotto-attività;
- **Raccolta dati e valutazione:** raccolta e analisi delle informazioni relative alle pratiche correnti di IT Governance attraverso questionari, interviste e revisioni documentali;
- **Analisi**: confronto delle pratiche osservate con i criteri del modello di maturità scelto per determinare il livello di maturità attuale;
- **Reportistica**: elaborazione di un rapporto dettagliato che evidenzia i risultati dell'assessment e fornisce raccomandazioni per il miglioramento, basate sui gap identificati tra il livello attuale e il livello desiderato di maturità.

Un IT Governance Maturity Assessment ben progettato e realizzato da esperti del settore non si limita a scattare una "fotografia" statica della situazione corrente, ma agisce come un catalizzatore per la trasformazione organizzativa. Attraverso l'identificazione e l'analisi approfondita delle pratiche esistenti, esso fornisce un quadro chiaro del livello di maturità dei processi IT costituenti il framework aziendale, facilitando l'implementazione di interventi mirati per colmare eventuali gap. Questo approccio supporta l'evoluzione continua delle funzioni IT, promuovendo l'integrazione armoniosa tra reparto IT e Business, rafforzando la capacità dell'organizzazione di adattarsi in un contesto dinamico. In tal modo, la maturità della governance IT diventa un indicatore critico per la sostenibilità e l'innovazione a lungo termine, garantendo che l'organizzazione non solo reagisca ai cambiamenti del mercato, ma li anticipi, mantenendo un vantaggio competitivo molto rilevante.

[31] Deloitte, (2012), *IT Playbook_2012*

CAPITOLO 3

3.1 Panoramica del progetto di IT Governance Maturity Assessment

Il progetto sviluppato e portato avanti durante il periodo di tirocinio, che rappresenta il nucleo centrale della presente tesi, nasce, in un primo momento, dalla necessità di adeguarsi ai nuovi requisiti normativi, analizzati nel dettaglio all'interno del paragrafo successivo, i quali impongono rigorosi standard a livello trasversale su molteplici processi interni agli istituti di credito. In risposta a tale esigenza, anche l'ufficio di IT Strategy & Value Management della Banca esaminata nel primo capitolo ha avviato un'indagine dettagliata su tutti i propri processi in ambito IT. Questo esame meticoloso ha dapprima portato all'elaborazione di un framework complesso di processi IT, progettato per allinearsi con le best practice e i benchmark di settore riconosciuti a livello internazionale, il che non ha rappresentato solo una misura per garantire la conformità alle normative vigenti, ma ha anche offerto l'opportunità di consolidare le fondamenta per un controllo più efficace e responsabile delle risorse IT di cui dispone l'istituto di credito in questione, anche in ottica futura. Una volta individuati i processi costituenti il cuore pulsante dell'ambito IT della Banca, gli stessi sono stati conseguentemente classificati secondo un livello di priorità, consentendo di focalizzare l'attenzione sulle aree più critiche in un primo momento e, successivamente, sui restanti processi definiti "non prioritari" per specifiche esigenze emerse internamente alla Banca. Questo sistema di priorità ha facilitato l'allocazione ottimale delle risorse e ha permesso di indirizzare gli sforzi verso i punti più nevralgici della struttura IT.

Il presente capitolo si propone quindi di analizzare, in maniera approfondita, l'implementazione del processo di IT Governance Maturity Assessment, condotto da Deloitte Consulting per l'istituto di credito in esame, focalizzandosi non solo sulle conformità raggiunte e sulle misure di adeguamento adottate in ambito normativo, ma esplorerà anche le potenziali lacune e le aree suscettibili di miglioramento. Mediante questa analisi dettagliata, infatti, l'intento è quello di elaborare strategie per potenziare la governance IT, abilitando la Banca non solo a rispondere con prontezza, ma anche a prevedere attivamente le evoluzioni del mercato finanziario e a prepararsi efficacemente per sfide future. Tale approccio strategico è essenziale per rafforzare e preservare la posizione competitiva dell'istituto di credito in un ambiente che è costantemente soggetto a innovazioni tecnologiche e cambiamenti normativi.

3.2 Il quadro normativo nel settore bancario: DORA e Circolare n. 285

La **Circolare n. 285** della Banca d'Italia e **DORA**, acronimo di *Digital Operational Resilience Act*, rappresentano due pilastri fondamentali del panorama normativo che regola il settore finanziario: affrontando sfide diverse ma al contempo complementari, esse condividono l'obiettivo di assicurare la stabilità e la sicurezza del sistema finanziario, integrando misure che vanno dalla gestione dei rischi tradizionali alla protezione contro i rischi tecnologici emergenti, in un contesto sempre più complesso e interconnesso.

DORA, emanata dalla Commissione Europea, si propone di rafforzare la resilienza digitale delle entità finanziarie tramite l'imposizione di standard elevati per la gestione dei rischi informatici e la continuità operativa, mirando a garantire che banche, assicurazioni e, in generale, altre istituzioni finanziarie siano in grado di prevenire, affrontare e riprendersi rapidamente da eventuali disservizi tecnologici o attacchi informatici che potrebbero compromettere la stabilità dell'intero sistema finanziario. Tra le principali disposizioni introdotte da DORA, spiccano l'obbligo per le entità finanziarie di adottare un quadro strutturato di gestione dei rischi legati alle tecnologie dell'informazione e della comunicazione (ICT - *Information and Communication Technology*) e la necessità di sviluppare piani di resilienza operativa dettagliati e continuamente aggiornati. Questi ultimi, devono essere testati con cadenza regolare affinché ne sia verificata l'efficacia e devono inoltre includere misure specifiche per garantire la continuità delle operazioni essenziali anche in caso di gravi emergenze. Un ulteriore elemento distintivo della suddetta direttiva è la gestione dei rischi associati ai fornitori terzi di servizi ICT, quali, ad esempio, i provider di cloud computing, ai quali viene richiesto di rispettare standard stringenti di sicurezza e affidabilità. Oltre a ciò, DORA introduce rigorosi obblighi di segnalazione degli incidenti legati all'ICT affinché le autorità competenti possano intervenire tempestivamente per mitigarne eventuali effetti negativi. È possibile affermare quindi che tale normativa introduce un sistema di vigilanza estremamente rigoroso, il quale consente l'imposizione di sanzioni e l'adozione di misure correttive nei confronti delle entità che risultano essere non conformi, assicurando così un'applicazione uniforme delle disposizioni in tutto il territorio dell'Unione Europea[32].

[32] Parlamento Europeo e Consiglio dell'Unione Europea (2022), *Regolamento (UE) 2022/2554 del Parlamento Europeo e del Consiglio del 14 dicembre 2022 relativo alla resilienza operativa digitale per il settore finanziario (Digital Operational Resilience Act - DORA)*, Gazzetta ufficiale dell'Unione Europea, URL: Publications Office (europa.eu)

Parallelamente, la **Circolare n. 285** della Banca d'Italia fornisce un quadro di riferimento dettagliato per la regolamentazione prudenziale delle banche e dei gruppi bancari italiani. Emanata nel dicembre 2013 e aggiornata svariate volte nel corso degli anni, tale circolare si propone di assicurare che le banche adottino strutture di governance solide, sistemi di controllo interno efficaci e un'adeguata gestione dei rischi. In particolare, essa fornisce indicazioni dettagliate sul modo in cui le banche debbano valutare la propria esposizione a diverse tipologie di rischi (e.g., di credito, di mercato, operativi e di liquidità) e stabilisce requisiti patrimoniali rigorosi, conformi agli standard internazionali di Basilea III. Quest'ultimo è un insieme di riforme introdotto dal Comitato di Basilea allo scopo di rafforzare la regolamentazione, la supervisione e la gestione del rischio nel settore bancario; elaborato in risposta alla crisi finanziaria del 2007-2008, esso mira a migliorare la resilienza delle banche, ovvero garantire che le banche siano meglio preparate a fronteggiare crisi economiche, imponendo requisiti patrimoniali più elevati e di migliore qualità, introducendo nuovi coefficienti di liquidità e un coefficiente di leva finanziaria per limitare l'eccessivo indebitamento. In aggiunta a quanto sopra spiegato, la Circolare n. 285 pone particolare attenzione anche alla trasparenza e alla responsabilità degli istituti bancari nei confronti degli investitori e del pubblico, richiedendo loro di fornire informazioni quanto più complete possibili sulle loro condizioni finanziarie e sulle politiche di governance adottate. Un altro aspetto cruciale è rappresentato dalle politiche di remunerazione, che devono essere strettamente allineate agli obiettivi di sostenibilità della banca, al fine di evitare incentivi che possano favorire comportamenti rischiosi. Qualora si verifichino situazioni di non conformità, la Banca d'Italia è autorizzata a intervenire applicando sanzioni e adottando misure correttive, assicurando così che le banche operino nel rispetto dei principi di sana gestione[33].

In altre parole, mentre DORA pone l'accento sulla resilienza operativa digitale e sulla protezione dalle minacce informatiche, la Circolare n. 285 si concentra sulla stabilità e sulla gestione prudenziale delle banche italiane, con particolare attenzione alla governance, alla gestione dei rischi e alla trasparenza. Come detto all'inizio del paragrafo, queste due normative, sebbene diverse per scopo e ambito di applicazione, si completano reciprocamente, contribuendo a creare un quadro normativo integrato che garantisce un elevato livello di stabilità del sistema finanziario, proteggendolo dai rischi sia tradizionali che emergenti.

[33] Banca d'Italia (2013), *Circolare n. 285 del 17 dicembre 2013 - Disposizioni di vigilanza prudenziale per le banche (testo integrale al 49° aggiornamento)*, URL: Circ_285_Testo_integrale_al_49_aggto.pdf (bancaditalia.it)

La complessità delle nuove normative permette di comprendere maggiormente uno dei motivi fondamentali che ha spinto l'istituto di credito a collaborare con Deloitte, che è una delle principali società di consulenza e revisione a livello globale. Questa collaborazione mira a sviluppare un approccio strutturato affinché la Banca possa analizzare, ottimizzare e monitorare i propri processi IT, rafforzando così la propria capacità di adattamento e resilienza in un contesto normativo e tecnologico in continua evoluzione.

3.3 Set-up progetto e benchmark di settore

Nel corso della seconda metà di maggio 2024, sono state avviate le prime attività relative al progetto oggetto della tesi, a beneficio dell'istituto di credito italiano precedentemente presentato, il quale rappresenta uno dei principali clienti di Deloitte S.r.l. S.B., con cui l'azienda collabora da diversi anni e in merito a numerose iniziative. Come già accennato, il progetto in questione rientra in un contesto di cooperazione strategica, mirato a supportare l'istituto di credito nel miglioramento delle proprie strutture operative e di governance in ambito IT.

Durante le prime fasi del progetto, che hanno coperto circa le prime 2-3 settimane, sono state svolte attività cruciali per l'avvio strutturato dei lavori. In primis, è stato redatto un **piano di lavoro** estremamente dettagliato che ha delineato tutte le attività e sotto-attività necessarie, mediante l'utilizzo del diagramma di **Gantt**, il quale è uno strumento fondamentale per la pianificazione e il monitoraggio delle attività che permette di rappresentare graficamente la sequenza temporale delle attività, evidenziando le loro interdipendenze e la durata prevista. Questo strumento, molto usato nell'ambito del Project Management, è stato utilizzato per definire e coordinare le varie fasi del progetto, facilitando l'allocazione delle risorse e il controllo dello stato di avanzamento. Una delle prime macro-attività è stata l'**analisi delle normative**: il team ha condotto un confronto approfondito (i.e., analisi delta) tra le normative vigenti e quelle già fornite dalla Banca in occasione di un precedente progetto. Questa attività ha permesso di identificare eventuali discrepanze, portando alla richiesta formale della documentazione mancante e all'aggiornamento del versioning delle normative esistenti nei database Deloitte. Parallelamente, è stato predisposto un repository di progetto (i.e., è stato creato un canale dedicato su Microsoft Teams, dove sono state caricate tutte le normative richieste), assicurando che le informazioni fossero facilmente accessibili e organizzate per tutti i membri del team e facilitando così la collaborazione tra i vari stakeholder del progetto.

Successivamente, è stata avviata la governance del progetto, con la definizione di meeting di confronto ricorrenti tra il team Deloitte e la Project Manager dell'azienda cliente, volti a monitorare lo stato di avanzamento delle attività, discutere eventuali criticità e allineare le strategie operative. Successivamente, è stata condotta un'analisi dettagliata su ciascuna normativa raccolta, valutando attentamente il contesto regolamentare di riferimento e verificando se le disposizioni fossero pertinenti all'ambito IT. Questa valutazione, protrattasi per diversi giorni, ha permesso di comprendere appieno l'applicabilità di ogni normativa, facilitandone l'integrazione nel piano di progetto e garantendo che tutte le componenti tecnologiche fossero allineate agli obblighi regolamentari previsti. Lo svolgimento di tutte queste attività iniziali ha posto le basi per una gestione coordinata del progetto, assicurando che tutte le informazioni necessarie fossero correttamente aggiornate e che il team fosse allineato sugli obiettivi e le aspettative, permettendo così una transizione fluida alle fasi successive del progetto.

La seconda macro-attività del progetto ha riguardato la definizione di un framework per i processi IT dell'istituto bancario, attività preceduta da un'analisi comparativa approfondita, comunemente nota come **benchmarking**. Quest'ultimo è un processo strutturato che consente di misurare le prestazioni, i prodotti o i servizi di un'organizzazione rispetto a quelli di aziende leader nel settore o rispetto a standard riconosciuti nel mercato di riferimento. È essenziale per identificare le migliori pratiche, rilevare eventuali aree di miglioramento e adottare strategie volte a colmare i gap prestazionali rispetto ai migliori competitor o standard del settore.

Il benchmarking può essere di diverse tipologie, tra cui il benchmarking competitivo, che confronta le performance aziendali con quelle dei concorrenti diretti, il benchmarking funzionale, che analizza i processi di aziende operanti in settori diversi ma con funzioni simili, oppure il benchmarking tecnico, utilizzato per confrontare le capacità tecniche di prodotti o servizi rispetto agli standard di eccellenza. Ognuno di queste tre tipologie di benchmarking richiede una pianificazione meticolosa, inclusa la definizione degli obiettivi, la selezione dei partner di benchmarking, la raccolta dei dati e l'analisi delle differenze di performance per individuare possibili interventi migliorativi.

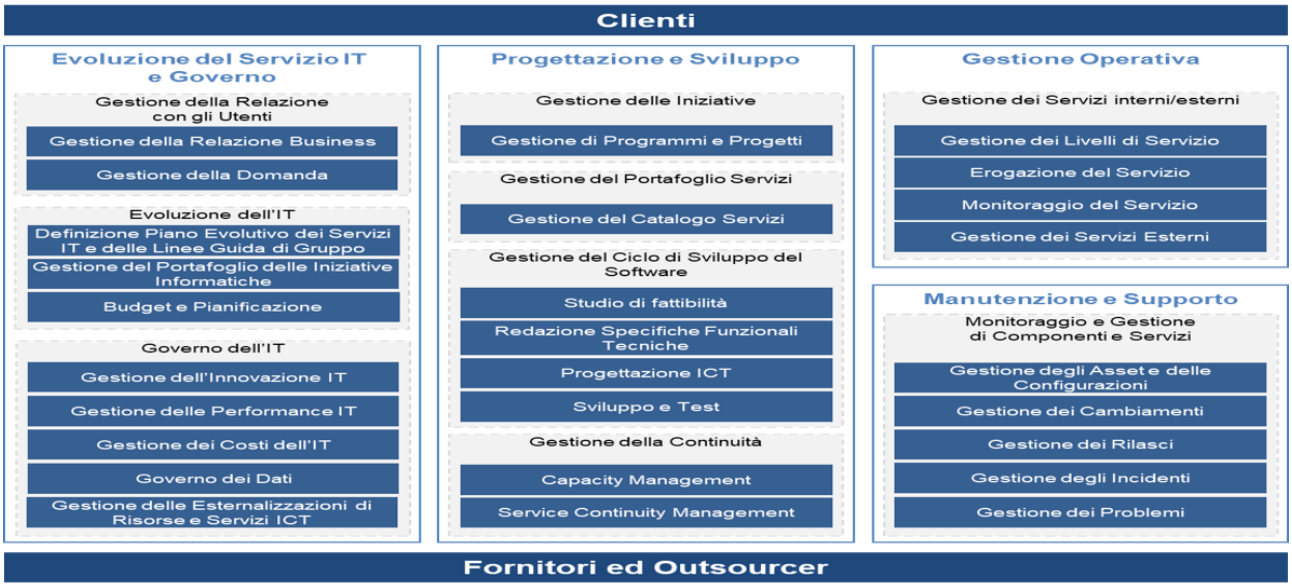
Nel contesto del progetto, è stato condotto un benchmarking competitivo su quattro principali player del settore dei servizi finanziari, il cui dettaglio viene fornito nelle sezioni successive, con l'obiettivo di individuare le best practice relative alla gestione dei processi IT. Come affrontato nel secondo capitolo della presente tesi, lato processi IT esistono diversi framework utili alla

formalizzazione degli stessi quali, ad esempio, COBIT e ITIL; quest'ultimo però è sicuramente quello più di ampio respiro e utilizzato a livello internazionale, oltre che ad essere il più adottato tra le realtà FSI. In particolare, dai risultati ottenuti dal benchmark, è emerso che la versione ITIL v3 rappresenta la prassi più adottata per la definizione dei framework dei processi IT, è stato riscontrato inoltre che la maggior parte degli istituti esaminati ha implementato un numero coerente e significativo di processi IT, ma quasi tutti hanno scelto di escludere dal framework i processi a presidio delle funzioni di controllo (i.e., IT Security, IT Risk, IT Compliance). Questa scelta strategica mira a mantenere una chiara separazione tra le attività operative e le funzioni di controllo, garantendo una gestione più indipendente dei rischi tecnologici e della conformità normativa. Grazie al benchmarking, è stato possibile delineare un framework personalizzato per l'istituto bancario, assicurando che i processi IT fossero allineati con le migliori pratiche del settore e adeguatamente integrati nelle strutture operative e di controllo già esistenti.

3.3.1 Benchmark di settore – IT Maturity Assessment Banca italiana n°1

Il **primo player bancario** analizzato durante il processo di benchmarking ha implementato un modello di gestione dei processi IT, mostrato in Fig. 3.1, basato sulle best practice internazionali **ITIL v3** e **COBIT** e strutturato in conformità con la tassonomia dei processi delineata da AbiLab. Quest'ultimo è un consorzio italiano, dedicato alla promozione della standardizzazione e dell'innovazione tecnologica nel settore bancario e prevede una suddivisione dei processi IT in quattro macrocategorie principali, quali: "Evoluzione del servizio IT e Governo", "Gestione operativa", "Progettazione e sviluppo" e "Manutenzione e supporto".

Figura 3.1 – Framework processi IT Banca italiana n°1



FONTE: elaborazione interna all'impresa di consulenza

Tale modello si dimostra completo e integrato, con un approccio estensivo alla gestione dei servizi IT, quasi interamente supportato dalla piattaforma intelligente ServiceNow, il che garantisce un elevato livello di integrazione tra i diversi processi, contribuendo a una gestione più efficiente e coordinata delle attività IT.

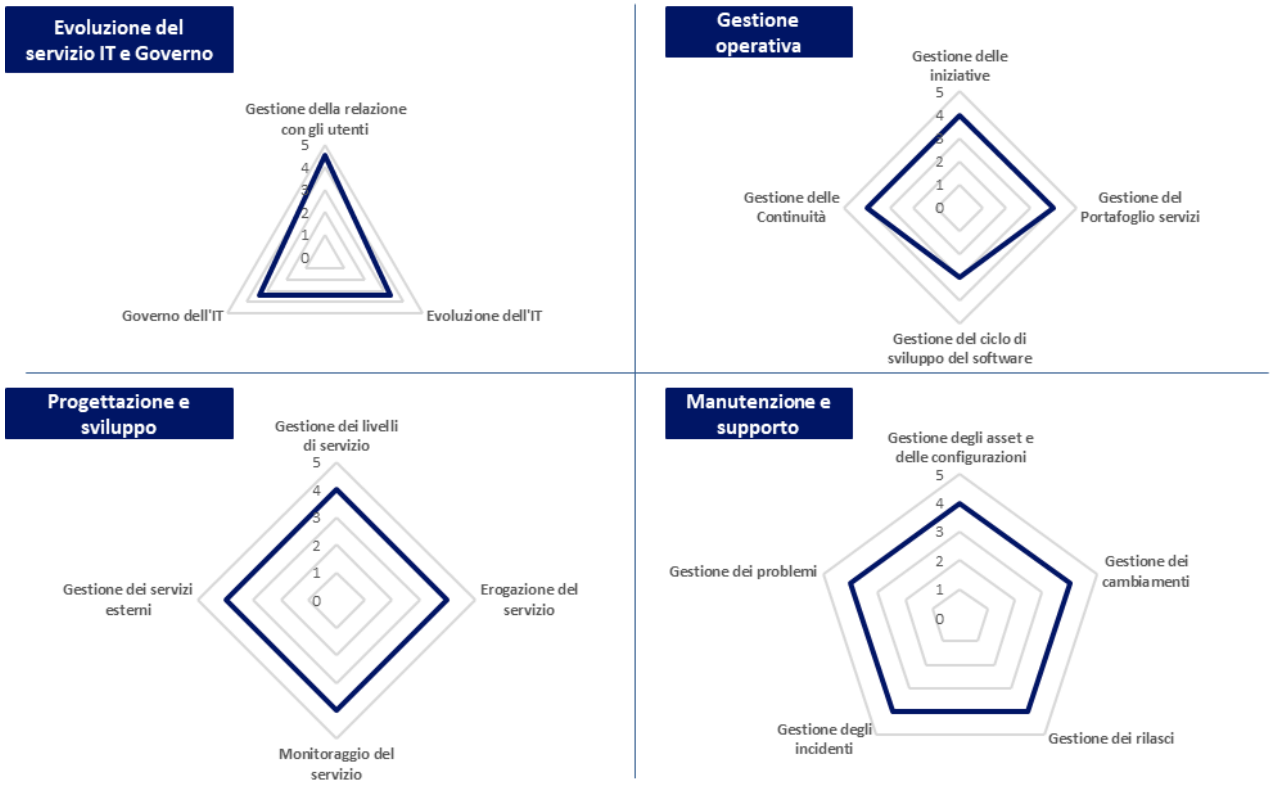
Tuttavia, nonostante il buon livello di maturità riscontrato in tutte le macroaree, emergono alcune criticità. La gestione del Cost Management, ad esempio, presenta un elevato grado di manualità e manca di un modello strutturato di Cost Allocation, sebbene siano stati effettuati interventi di integrazione con il CMDB (*Configuration Management Database*). Esso è un repository centrale che raccoglie informazioni dettagliate su tutti gli asset IT e le loro interrelazioni e viene utilizzato per tenere traccia delle configurazioni dei componenti tecnologici, come hardware, software, reti e applicazioni, e per supportare i processi di gestione del cambiamento, risoluzione dei problemi e pianificazione delle risorse. In altre parole, il CMDB funge da base dati di riferimento per la gestione e il monitoraggio dell'infrastruttura IT, consentendo una visione aggiornata delle risorse disponibili e delle loro dipendenze, facilitando così un approccio proattivo nella gestione operativa. Di conseguenza, la lacuna sopracitata può limitare la capacità dell'organizzazione di allocare con precisione i costi e ottimizzare le risorse. Analogamente, anche il processo di budget e pianificazione è gestito manualmente, il che potrebbe introdurre inefficienze e aumentare i margini di errore nella previsione e gestione delle risorse finanziarie.

Un aspetto positivo è la presenza di un'unità organizzativa dedicata alla guida di progetti di Digital Innovation; in particolare, all'interno del processo di BRM (*Business Relationship Management)*, è stata definita una metodologia che prevede l'implementazione di Business Case al fine di valutare tematiche innovative. Questo approccio strutturato consente di affrontare in modo sistematico le opportunità di innovazione, integrando valutazioni finanziarie e strategiche per orientare meglio le decisioni aziendali.

Per quanto riguarda l'ambito dello sviluppo software, i processi relativi al ciclo di vita dello sviluppo (SDLC - *Software Development Lifecycle Management*) sono stati regolamentati attraverso l'introduzione di una policy e di una guida operativa, che supportano i team nell'adozione di linee guida specifiche e nell'utilizzo degli strumenti previsti dalla toolchain. Tuttavia, nonostante la formalizzazione di queste procedure, il livello di adozione effettiva dei processi risulta inferiore al 30%, indicando una necessità di rafforzamento nella formazione e nella diffusione delle pratiche definite per garantire una maggiore uniformità operativa.

In sintesi, il modello di gestione dei processi IT adottato dal primo player bancario analizzato presenta una struttura solida e ben articolata, in linea con le migliori prassi internazionali nonostante vi sono alcune aree che necessitano di miglioramenti, in particolare nella gestione dei costi e nell'adozione delle politiche di sviluppo software, affinché l'organizzazione possa raggiungere un livello di eccellenza ancora più elevato. Di seguito, nella figura 3.2, vengono riportati, mediante l'utilizzo di grafici a ragnatela, i dati che supportano e illustrano quanto esposto fin ora.

Figura 3.2 - IT Maturity Assessment Banca italiana n°1

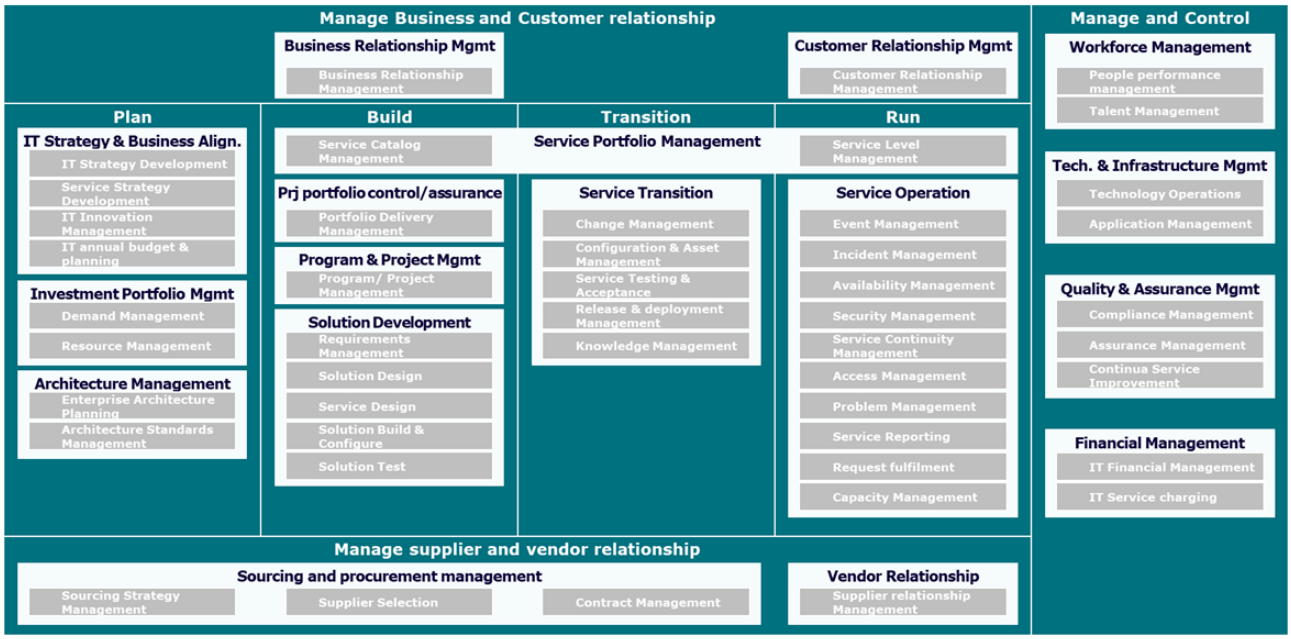


FONTE: elaborazione interna all'impresa di consulenza

3.3.2 Benchmark di settore – IT Maturity Assessment Banca italiana n°2

Il **secondo player bancario** analizzato ha adottato un framework dei processi IT, mostrato in Fig. 3.3, basato sulle best practice internazionali di **ITIL v3**, il quale organizza i processi IT in categorie specifiche, ovvero: "Manage Business & Plan", "Build", "Transition", "Run", "Manage & Control" e "Manage Supplier and Vendor Relationship". L'adozione di queste categorie riflette un approccio strutturato alla gestione dei servizi IT, che si basa su una metodologia consolidata a livello internazionale per garantire un efficiente coordinamento e allineamento delle attività tecnologiche con gli obiettivi aziendali.

Figura 3.3 – Framework processi IT Banca italiana n°2



FONTE: elaborazione interna all'impresa di consulenza

Dall'analisi delle evidenze emerse, sintetizzate graficamente in Fig. 3.4, è stato rilevato che l'organizzazione raggiunge un buon livello di maturità nelle macroaree di "Transition", "Run" e "Manage Supplier and Vendor Relationship" e ciò indica che la Banca è in grado di gestire in maniera efficace il passaggio dalle fasi di sviluppo a quelle operative, assicurando una continuità del servizio e una gestione ottimale dei fornitori e delle relazioni con i partner commerciali.

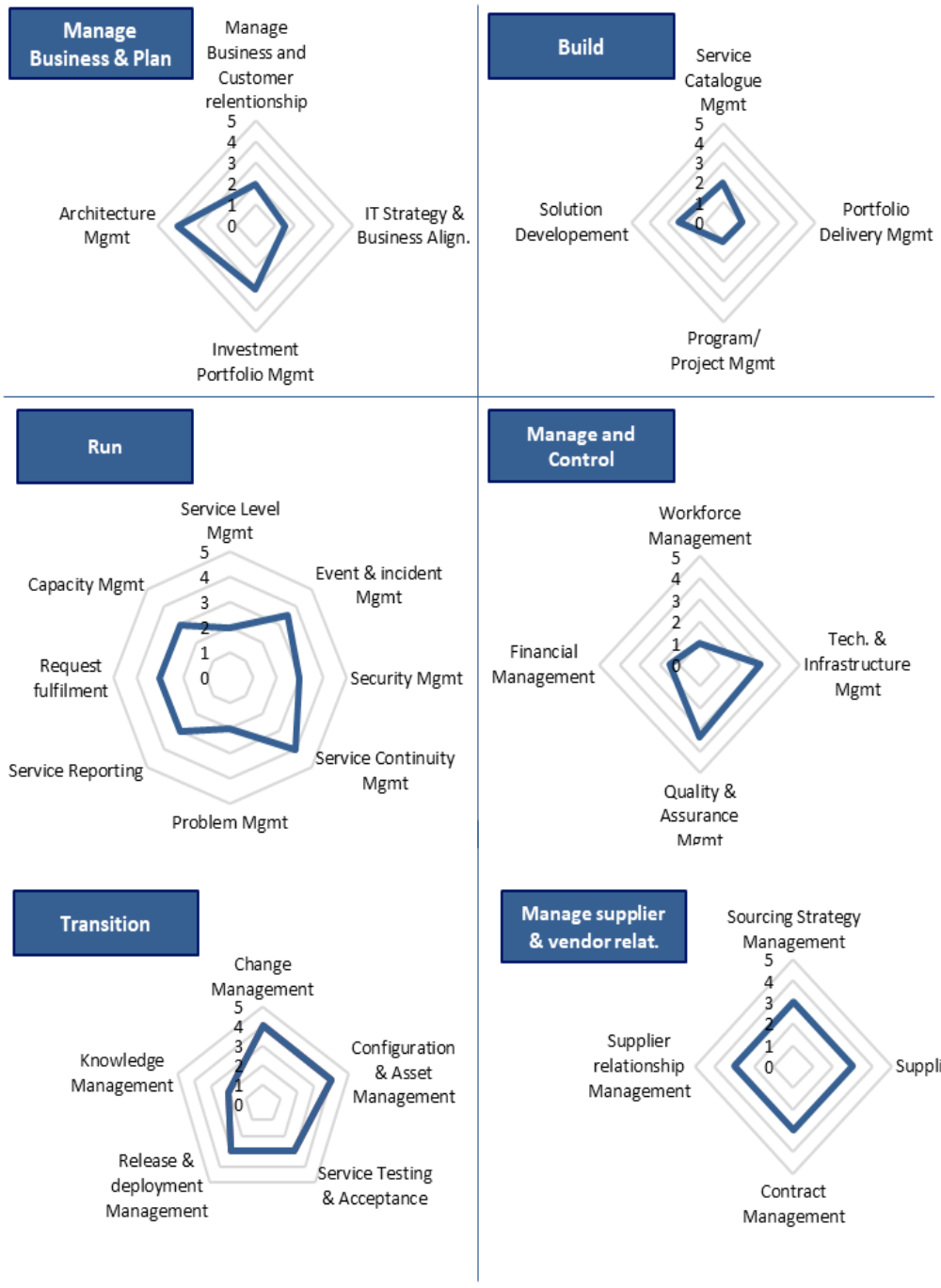
Tuttavia, sono stati individuati alcuni aspetti critici nelle altre aree del modello, che necessitano di interventi di potenziamento e miglioramento. In particolare, per quanto riguarda il l'area "Business Relationship Management", è stata rilevata l'assenza di una struttura formalizzata che si occupi della gestione delle relazioni con le varie unità di business, e ciò potrebbe ostacolare la capacità dell'IT di comprendere pienamente le esigenze strategiche dell'azienda e di fornire un supporto adeguato nella definizione e realizzazione dei progetti tecnologici. Inoltre, l'area di "IT Strategy & Business Alignment" presenta processi non completamente definiti e non eseguiti in modo indipendente, evidenziando quindi una mancanza di integrazione tra la pianificazione strategica dell'IT e le esigenze complessive del business; questo disallineamento potrebbe portare a inefficienze nella gestione delle priorità e nell'allocazione delle risorse.

Anche l'area di “Solution Development” risulta poco matura: in particolare, si osservano difficoltà significative nella pianificazione delle risorse e nelle stime dell'effort richiesto per i progetti. Questi problemi possono compromettere la capacità dell'istituto di rispettare le tempistiche e i budget previsti, riducendo l'efficacia complessiva del ciclo di sviluppo delle soluzioni IT. La mancanza di processi strutturati in questa area suggerisce la necessità di implementare pratiche di Project Management più rigorose e metodologie di sviluppo che facilitino una pianificazione e una gestione più accurate dei progetti.

Infine, l'area di “Financial Management” appare carente in termini di maturità, principalmente a causa dell'assenza di un processo di contabilità strutturato e della difficoltà nel collegare in modo chiaro i costi e i ricavi relativi ai vari componenti dei servizi offerti. Questa carenza limita la capacità dell'azienda di analizzare e controllare efficacemente la redditività delle diverse iniziative IT e di supportare decisioni finanziarie informate. L’implementazione di un modello di cost accounting più dettagliato e la definizione di metriche precise per il monitoraggio dei costi e dei benefici associati ai servizi IT sono quindi essenziali per migliorare la governance finanziaria dell’area tecnologica.

In poche parole, sebbene il modello adottato dal secondo player bancario presenti punti di forza significativi in alcune macroaree, persistono diverse criticità che richiedono interventi mirati per potenziare l’efficacia complessiva della gestione dei processi IT e per garantire un allineamento più stretto con le esigenze strategiche e operative dell’organizzazione.

Figura 3.4 - IT Maturity Assessment Banca italiana n°2

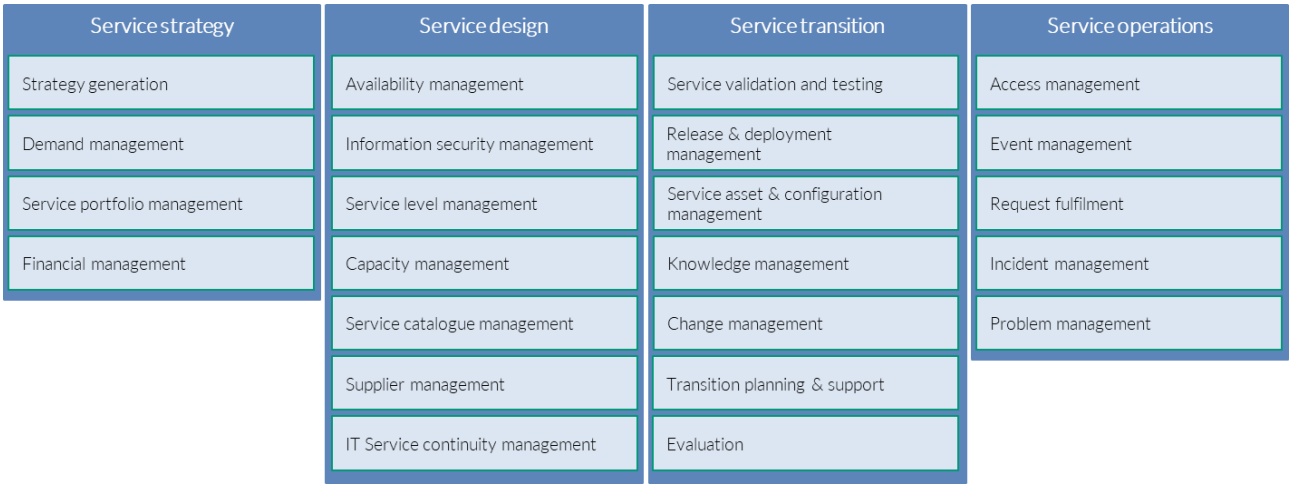


FONTE: elaborazione interna all'impresa di consulenza

3.3.3 Benchmark di settore – IT Maturity Assessment Assicurazione

Il **player** successivo, non più bancario bensì **assicurativo**, ha adottato integralmente il framework proposto da **ITIL v3**, suddividendo i processi IT nelle quattro principali categorie di "Service Strategy", "Service Design", "Service Transition" e "Service Operation", vedi Fig. 3.5.

Figura 3.5 – Framework processi IT Assicurazione



FONTE: elaborazione interna all'impresa di consulenza

Dall'esame delle informazioni raccolte, sintetizzate in maniera grafica in Fig. 3.6, è stato rilevato un buon livello di maturità nelle macroaree di "Service Strategy" e "Service Operation", dimostrando che l'azienda possiede una solida strategia di gestione dei servizi e una buona capacità operativa. In particolare, la macroarea di "Service Strategy" evidenzia che l'azienda è in grado di pianificare e definire strategie di servizio allineate con gli obiettivi di business, supportando un efficace decision-making a livello strategico. Analogamente, la macroarea di "Service Operation" mostra una buona capacità di gestione delle operazioni quotidiane, garantendo un'erogazione del servizio stabile e reattiva alle esigenze degli utenti.

Tuttavia, le macroaree di "Service Design" e "Service Transition" risultano meno mature, suggerendo la necessità di ulteriori interventi per migliorare la progettazione e la transizione dei servizi IT. La limitata maturità in queste aree può comportare inefficienze nella fase di definizione dei requisiti dei servizi e nella loro implementazione, influenzando negativamente la capacità dell'organizzazione di rispondere in maniera tempestiva e adeguata alle mutevoli esigenze del mercato e dei clienti.

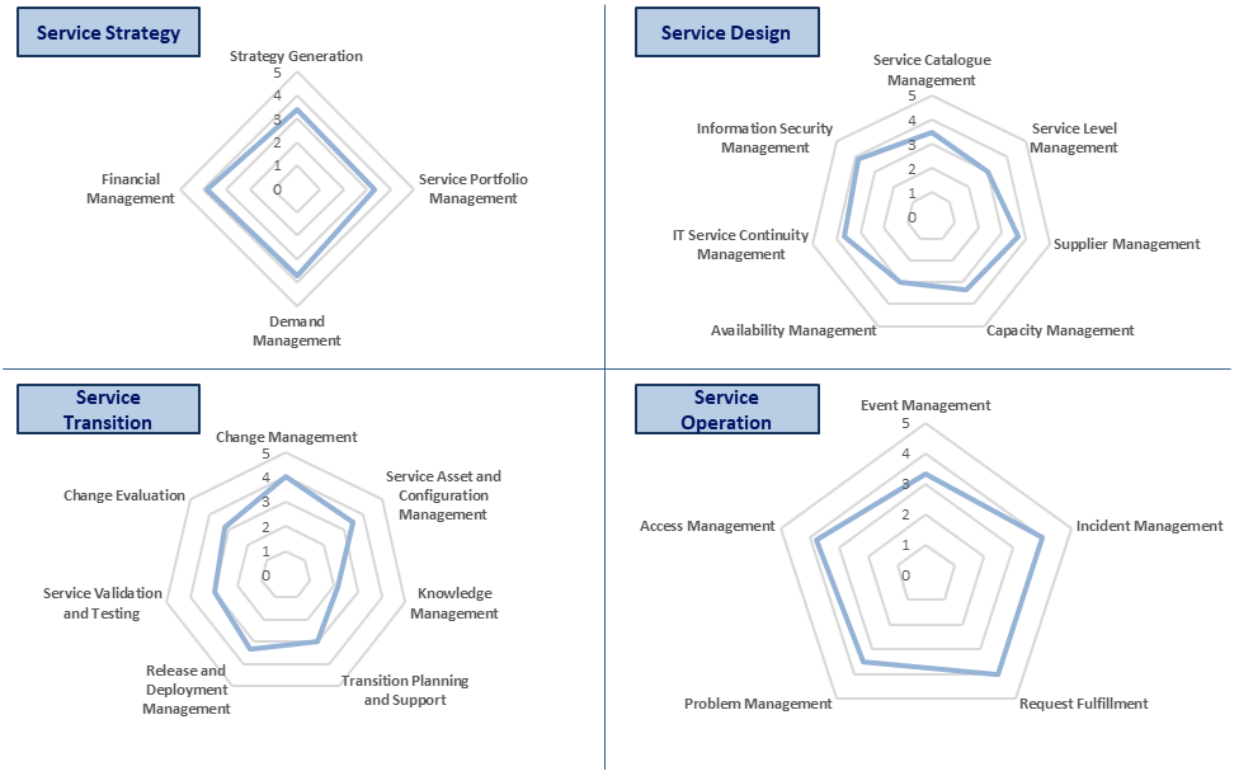
La valutazione del livello di maturità è stata condotta attraverso un'autovalutazione periodica basata su sei dimensioni chiave, quali: maturità, ruoli, attività, formalizzazione, documentazione, KPI e applicazioni a supporto. Questo approccio multidimensionale ha permesso di ottenere una panoramica dettagliata e strutturata dello stato dei processi IT, evidenziando sia le aree di eccellenza sia quelle che richiedono un ulteriore sviluppo. In generale, il player assicurativo presenta un livello di maturità complessivo positivo, con diverse aree che mostrano potenziale di miglioramento.

Per quanto riguarda i singoli processi, i risultati più rilevanti riguardano il Change Management e il Problem Management, i quali sono stati implementati efficacemente utilizzando lo strumento aziendale ServiceNow. Le attività relative a questi processi sono state formalizzate e documentate in modo rigoroso tramite un apposito regolamento, raggiungendo il livello target previsto dal framework ITIL v3. Questo risultato dimostra l'efficacia delle iniziative messe in atto per garantire una gestione strutturata e trasparente delle modifiche e dei problemi all'interno dell'organizzazione.

Parallelamente, i processi di Demand Management, Incident Management e Request Fulfillment hanno beneficiato di attività di miglioramento specifiche, con l'introduzione di KPI per la valutazione dell'efficienza del processo, nonché con la formalizzazione di regolamenti che ne disciplinano l’esecuzione. Tali iniziative hanno consentito di aumentare il livello di controllo e monitoraggio delle prestazioni, favorendo un miglioramento continuo nella gestione delle richieste e degli incidenti.

Le attività attualmente in corso sono finalizzate al potenziamento dei processi rimanenti, tra cui Strategy Generation, Service Validation and Testing, Service Level Management e Knowledge Management. In particolare, si sta lavorando per rafforzare la capacità di generare strategie IT efficaci e per migliorare il processo di validazione e testing dei servizi, assicurando che tutti i requisiti siano soddisfatti ancor prima dell'implementazione. Analogamente, l'ottimizzazione del Service Level Management è volta a garantire un monitoraggio costante della qualità del servizio erogato, mentre il miglioramento del Knowledge Management mira a una gestione più efficiente delle informazioni, promuovendo una cultura di condivisione della conoscenza all'interno dell'organizzazione.

Figura 3.6 – IT Maturity Assessment Assicurazione

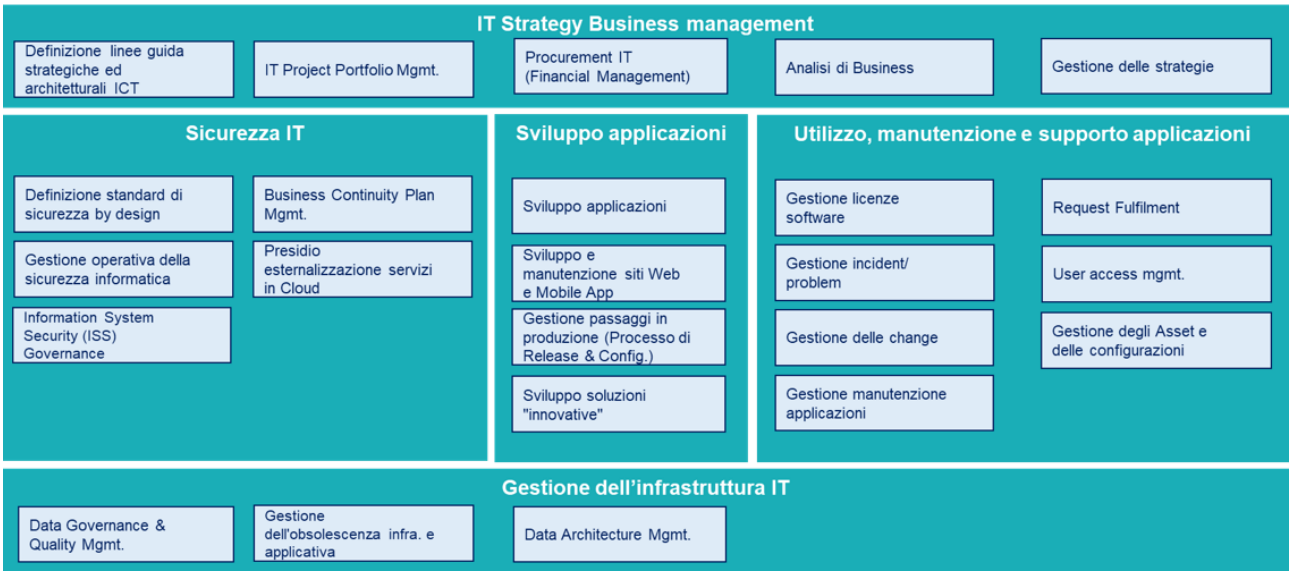


FONTE: elaborazione interna all'impresa di consulenza

3.3.4 Benchmark di settore – IT Maturity Assessment Finanziaria

Per quanto concerne il **player finanziario** oggetto di analisi, è attualmente in corso un IT Maturity Assessment dei processi IT, con l'obiettivo di valutare la maturità e l'efficacia operativa delle diverse aree funzionali. I processi IT, rappresentati in Fig. 3.7, sono stati classificati in cinque macrocategorie: "IT Strategy Business Management", "IT Security", "Infrastructure Management", "Software Development" e "Application Support & Maintenance". Tale valutazione si propone non solo di misurare il livello di maturità attuale, ma anche di supportare la definizione di un framework strutturato per i processi IT, in linea con le best practice di settore.

Figura 3.7 – Framework processi IT Finanziaria



FONTE: elaborazione interna all'impresa di consulenza

L'assessment è stato condotto attraverso un'autovalutazione svolta dall'ufficio di IT Governance, la quale ha evidenziato che l'istituzione finanziaria presenta un livello medio di maturità complessiva; ciò significa che, pur avendo implementato processi IT strutturati, esistono aree che necessitano di miglioramenti significativi per raggiungere un livello di eccellenza, vedi Fig. 3.8 per maggiori dettagli. Nell'ultimo anno, sono state intraprese diverse iniziative volte a migliorare la maturità dei processi nell'area di IT Operations, con particolare attenzione a "Incident Management" e "Problem Management". Questi interventi hanno contribuito a una maggiore efficienza nella gestione degli incidenti e nella risoluzione dei problemi, migliorando la capacità dell'organizzazione di rispondere rapidamente alle criticità operative.

Tuttavia, il processo di "Change Management", sebbene venga eseguito, non è ancora formalizzato adeguatamente e tale lacuna limita la possibilità di monitorare l'efficacia del processo, e potrebbe ostacolare l'implementazione coerente di cambiamenti tecnologici all'interno dell'organizzazione. Inoltre, sono state riscontrate carenze significative nella "Gestione e Configurazione dell'Asset": nonostante le attività di miglioramento intraprese durante l'ultimo anno, il livello di maturità di questa area non è ancora sufficiente. La gestione degli asset e delle configurazioni è essenziale per garantire una visibilità completa delle risorse tecnologiche e per supportare una gestione strategica delle infrastrutture IT.

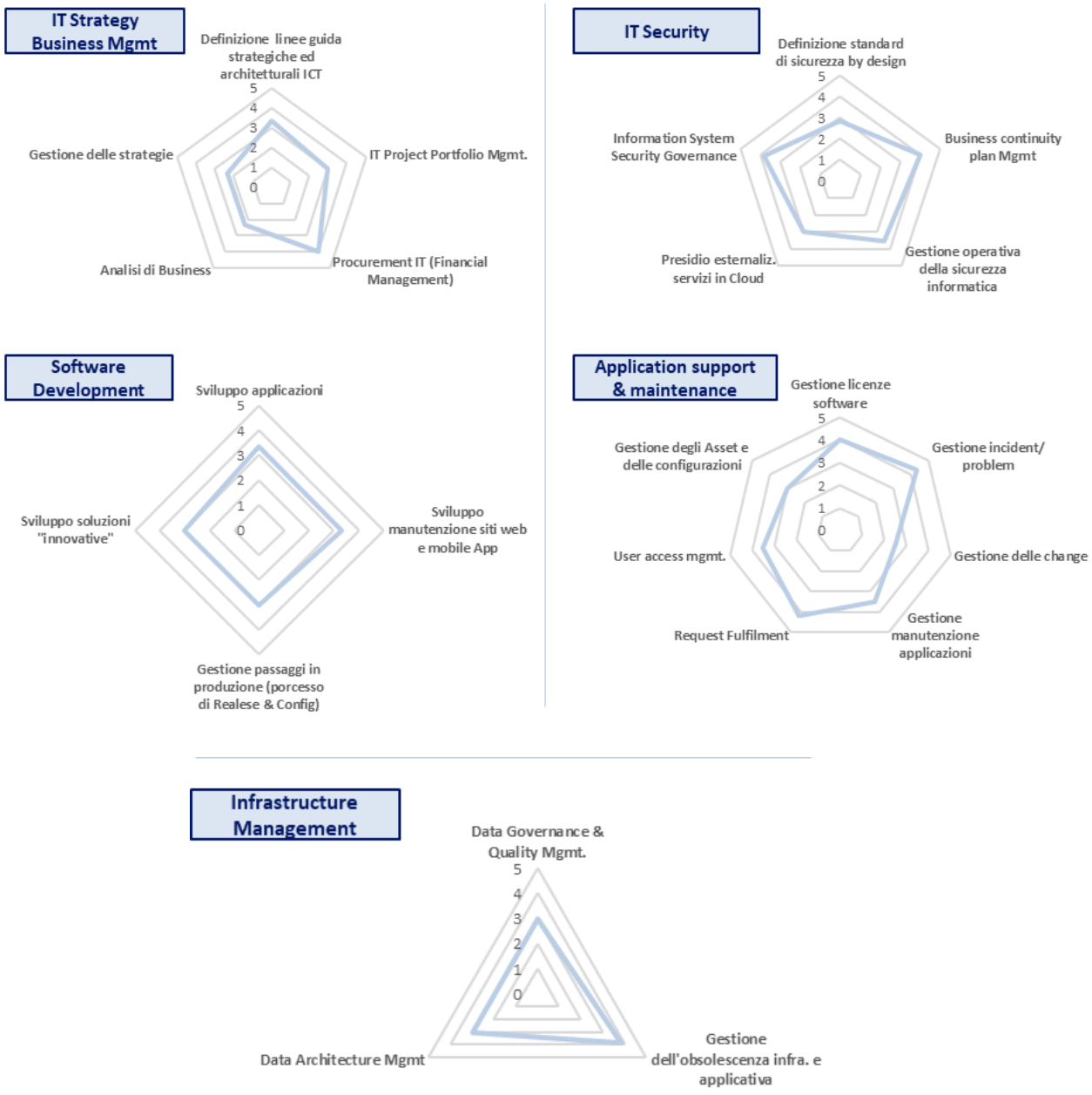
Parallelamente, è in fase di sviluppo un nuovo strumento per supportare il processo di Access Management che dovrebbe facilitare il controllo degli accessi alle risorse aziendali, contribuendo a una gestione più sicura e conforme delle autorizzazioni e dei privilegi utente. Tuttavia, nell'ambito della "Gestione della Strategia IT", è stato rilevato che, pur essendo presente un processo formalizzato relativo alla strategia commerciale, esso non indirizza in modo specifico la gestione strategica dell'IT. Questo deficit potrebbe comportare un disallineamento tra le priorità tecnologiche e gli obiettivi aziendali, compromettendo la capacità dell'organizzazione di sfruttare appieno il potenziale delle tecnologie emergenti.

Un'altra area che richiede attenzione è la struttura del BRM, la quale non include al suo interno il processo di Analisi del Business. Infatti, questo processo, che riveste un'importanza cruciale per comprendere le esigenze del business e tradurle in requisiti IT concreti, presenta un livello di maturità basso e non è formalizzato in alcuna normativa aziendale di riferimento, il che limita la capacità dell'organizzazione di gestire efficacemente le relazioni tra le unità IT e le altre funzioni aziendali, riducendo la capacità di risposta e di allineamento strategico.

L'analisi dei gap condotta sull'organizzazione, comparando le pratiche interne con le best practice di **ITIL 4**, ha evidenziato un buon livello di copertura nelle pratiche tecniche. Tuttavia, sono state riscontrate significative lacune nelle pratiche generali e in quelle legate ai servizi. In particolare, è emersa l'assenza di riferimenti specifici alle pratiche relative alla gestione degli asset e dei servizi, nonché alla definizione di una strategia IT integrata. Queste carenze indicano la necessità di sviluppare un quadro strategico più solido, che integri le esigenze operative con una visione a lungo termine delle priorità IT, assicurando una gestione proattiva e strategica delle risorse tecnologiche.

Quindi, sebbene l'organizzazione finanziaria abbia dimostrato un impegno significativo nel miglioramento dei propri processi IT, sono ancora presenti aree critiche che richiedono interventi mirati per elevare il livello di maturità complessivo. L'implementazione di strutture formali e di un framework coerente per la gestione strategica e operativa dell'IT sarà fondamentale per garantire una maggiore efficienza e allineamento con gli obiettivi aziendali.

Figura 3.8 – IT Maturity Assessment Finanziaria



FONTE: elaborazione interna all'impresa di consulenza

3.3.5 Framework Deloitte

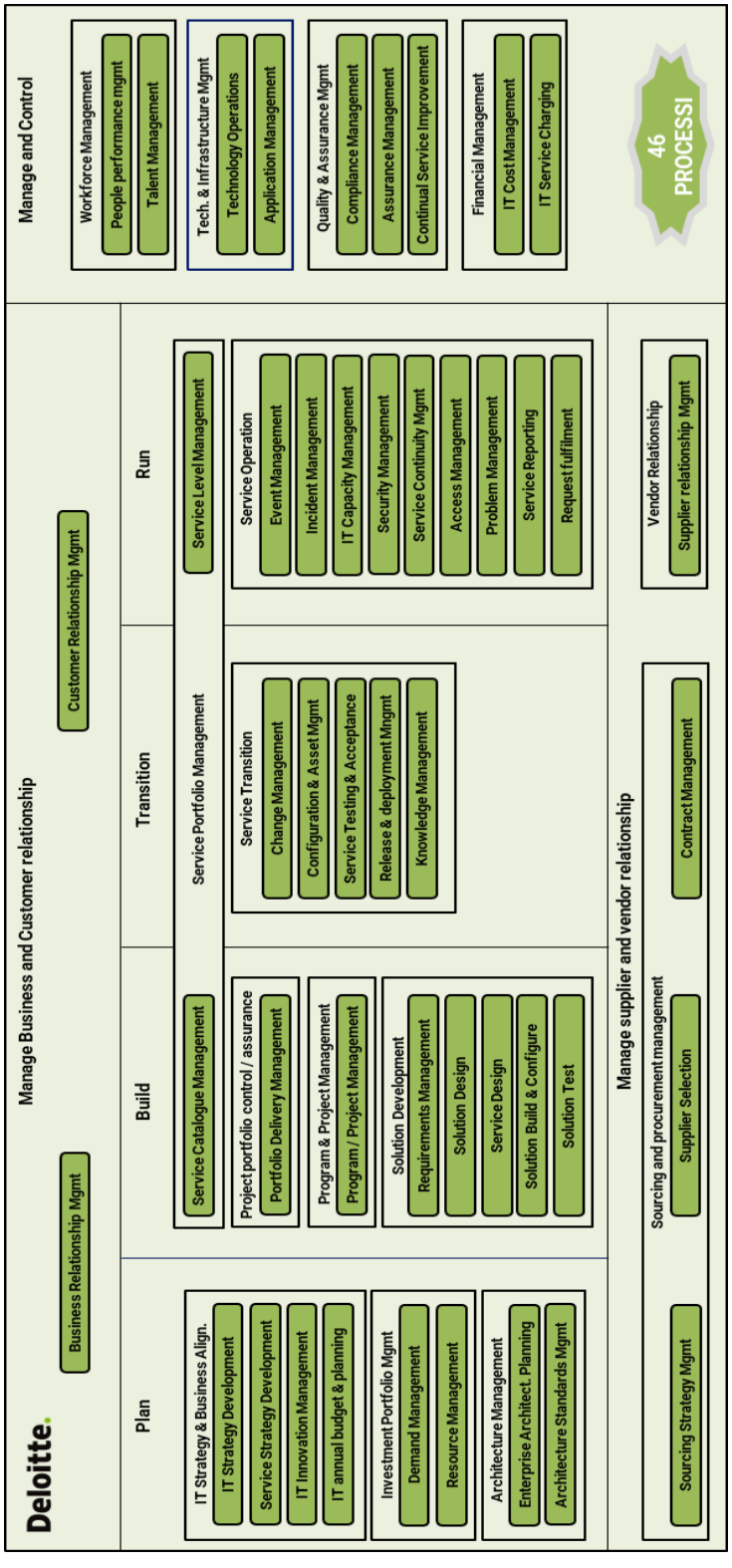
Il framework dei processi IT definito da Deloitte per le realtà operanti nell'industria dei servizi finanziari (FSI), mostrato in Fig. 3.9, è stato progettato con l'obiettivo di fornire un modello strutturato e coerente con le esigenze specifiche di queste organizzazioni. Tale framework,

coerentemente con il benchmark di settore, si fonda sulle best practice di **ITIL v3**, riconosciute a livello internazionale per la gestione ottimizzata dei servizi IT. Questa scelta strategica risponde alla necessità di molte organizzazioni di rafforzare e, in alcuni casi, attivare una rappresentazione chiara e dettagliata dei servizi IT in essere all'interno dell'azienda, sulla base di quanto indicato dalle best practice.

ITIL v3, in particolare, offre una logica di rappresentazione verticale dei singoli processi alla base di un'organizzazione IT, assicurando quindi una visione integrata e completa delle operazioni tecnologiche. Questo approccio permette di delineare con chiarezza le responsabilità e le interazioni tra i vari processi, facilitando la gestione e il miglioramento continuo dei servizi. Come già visto nel capitolo precedente, la rappresentazione verticale proposta da ITIL v3 si articola in una serie di processi distinti, ognuno dei quali è focalizzato su una specifica fase del ciclo di vita del servizio IT. L'adozione di questo framework offre numerosi vantaggi, tra cui una maggiore trasparenza nella gestione dei servizi IT, la possibilità di identificare e colmare eventuali lacune operative e/o strategiche, e la capacità di rispondere tempestivamente alle esigenze di business attraverso un modello di governance robusto. Inoltre, ITIL v3 fornisce una base solida per la misurazione delle performance, grazie all'adozione di KPI specifici per ogni processo, che consentono di monitorare costantemente l'efficienza delle attività svolte; questa misurazione puntuale è fondamentale per supportare il processo decisionale e per guidare le iniziative di miglioramento continuo, elementi essenziali per mantenere un vantaggio competitivo in un settore dinamico come quello finanziario e assicurativo.

La scelta di Deloitte di adottare ITIL v3 come riferimento per il proprio framework dei processi IT deriva anche dalla capacità di questo modello di adattarsi a contesti organizzativi complessi e diversificati, come quelli tipici delle realtà FSI. ITIL v3, infatti, non si limita a fornire una serie di linee guida per la gestione operativa, ma offre anche strumenti per il governo strategico dell'IT, facilitando l'allineamento tra gli obiettivi tecnologici e quelli di business, il che è cruciale per garantire che le iniziative IT non siano solo efficienti dal punto di vista operativo, ma anche efficaci nel supportare la crescita e l'innovazione aziendale.

Figura 3.9 – Framework processi IT Deloitte



FONTE: elaborazione interna all'impresa di consulenza

3.4 Definizione framework processi IT Banca

La definizione del framework dei processi IT della Banca ha rappresentato un'attività molto articolata, mirata a ottenere una mappatura precisa dei processi IT in essere, al fine di garantire una gestione efficace e allineata agli standard internazionali. Come visto fin ora, inizialmente è stata portata avanti un'analisi approfondita delle normative interne e dei processi IT, proseguendo con la costruzione di un modello personalizzato basato sul framework proposto da Deloitte (utilizzato quindi come input), ma adattato alle esigenze della Banca.

Di seguito una descrizione dettagliata dell'approccio metodologico utilizzato per la definizione del framework dei processi IT per l'azienda cliente:

1) La prima fase si è concentrata sulla **mappatura delle normative interne e dei processi IT**: questo passaggio è stato cruciale per ottenere una visione completa delle procedure normative e dei processi IT operativi all'interno dell'organizzazione. Di seguito l'elenco degli step operativi necessari allo sviluppo di questa prima fase:

   - *Rilevazione e raccolta delle normative*: un censimento dettagliato di tutte le procedure e i regolamenti interni all'istituto di credito, che ha permesso di creare un inventario aggiornato delle disposizioni esistenti;

   - *Analisi di alto livello delle normative e mappatura di queste ultime con i processi del framework Deloitte*: questa analisi ha permesso di identificare disallineamenti e lacune, fornendo una base solida per la successiva integrazione dei processi mancanti.

2) La seconda fase ha visto l'esecuzione di **valutazioni interne**, coordinate dall'ufficio IT Strategy con il supporto di Deloitte. Queste valutazioni hanno avuto come obiettivo l'identificazione di due categorie principali di processi IT:

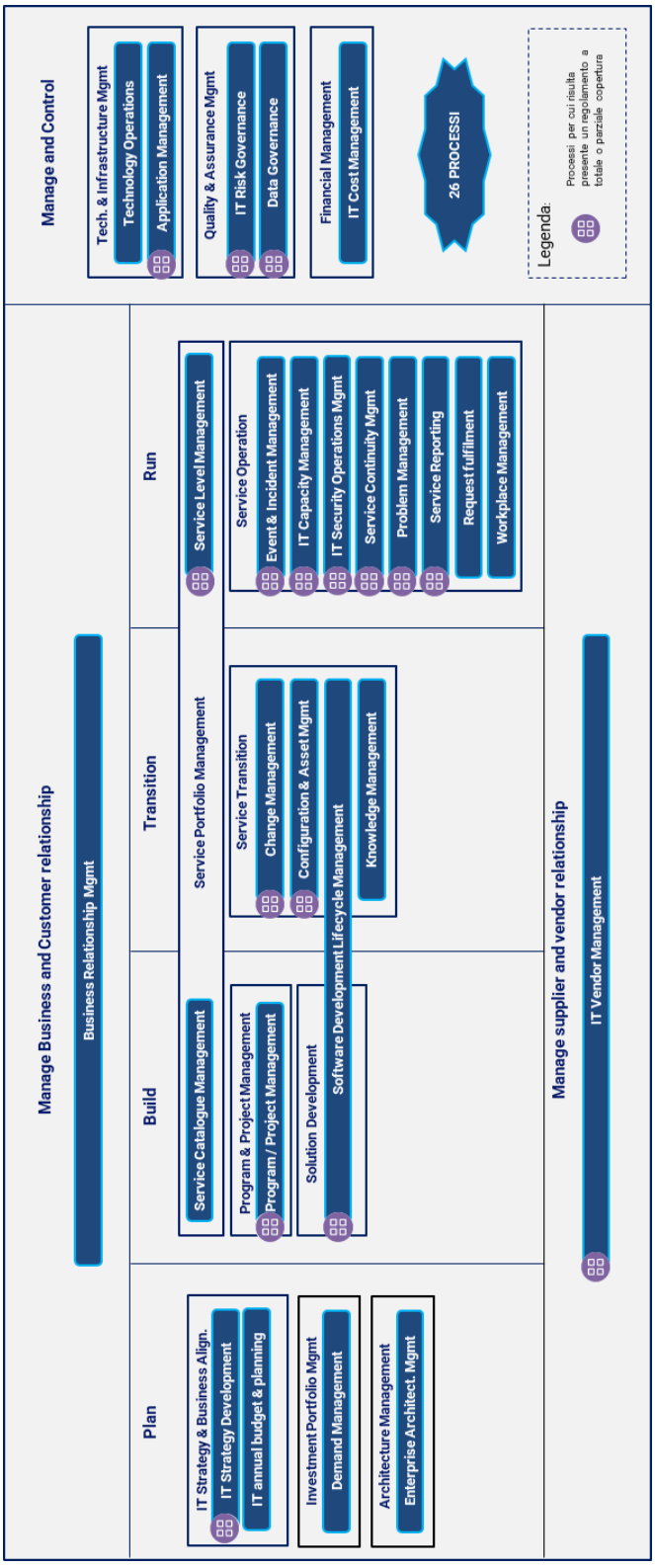
   - *Processi non ancora attivati*: si tratta di processi che, pur non essendo operativi, sono stati riconosciuti come fondamentali per lo sviluppo strategico dell'IT. La loro introduzione è considerata prioritaria per colmare le lacune e per garantire una gestione più integrata;

   - *Processi agiti ma non formalizzati*: ovvero processi che, sebbene operativi, non sono regolamentati attraverso normative aziendali specifiche. La mancanza di formalizzazione può generare inefficienze e incertezze nell'esecuzione delle attività, rendendo difficile il monitoraggio e l'ottimizzazione delle performance.

3) In parallelo, è stata condotta un'analisi degli **esiti del benchmark di settore**, analizzata nel dettaglio nei paragrafi precedenti, che ha permesso di confrontare i processi IT della Banca con quelli di altre realtà operanti nel settore finanziario. L'obiettivo principale era duplice: individuare eventuali processi comuni a realtà similari e non in essere presso la Banca e valutare l'effettiva attivazione di specifici processi.

All'esito dell'applicazione dei driver definiti nell'approccio metodologico sopra descritto, si rappresenta di seguito, in Fig. 3.10, il **framework** risultante **dei processi IT della Banca.** La rappresentazione risulta inoltre arricchita con l'indicazione dei processi oggetto di adeguamenti normativi recenti o in corso e per cui è presente un regolamento a totale o parziale copertura: quest'ultima non è da intendersi come una valutazione di maturità, destinata alla seconda fase del progetto.

Figura 3.10 – Framework processi IT Banca



FONTE: elaborazione interna all'impresa di consulenza

Per una maggiore chiarezza, viene presentato di seguito l'elenco completo con le descrizioni di ciascun processo IT incluso nel framework definito per la Banca:

- Fase: **Manage Business and Customer relationship**
  1. *Business Relationship Management***:** gestione della relazione con il Business al fine di garantire il soddisfacimento delle esigenze presenti e definire progetti che siano in linea con la strategia e abbiano un solido business case.

- Fase: **Plan**
  1. *IT Strategy Development:* definizione della strategia IT di medio-lungo termine volta a migliorare i servizi erogati nel rispetto delle esigenze di mercato/ dei Clienti e considerando aspetti chiave quali la tecnologia e i servizi di IT Operations;
  2. *IT annual budget & planning:* definizione del budget e controllo della spesa e dei costi sostenuti, nel rispetto della strategia IT. Include un ciclo di negoziazioni periodiche per la definizione del budget futuro e per il monitoraggio nel day-by-day del budget attuale;
  3. *Demand Management***:** analisi e valutazione dei requisiti di business definiti in merito a servizi IT esistenti/ nuovi al fine di garantire che le risorse disponibili siano in grado di coprire le esigenze attuali e future;
  4. *Enterprise Architecture Management:* pianificazione ed evoluzione costante dell'architettura complessiva a supporto delle iniziative di delivery e trasformazione attraverso creazione e adozione di standard tecnologici.

- Fase: **Manage supplier and vendor relationship**
  1. *IT Vendor Management:* processo atto a garantire una gestione e presidio efficace delle relazioni con i fornitori IT, con l'obiettivo di monitorare le prestazioni e definire di conseguenza un rating complessivo del fornitore che tenga in considerazione anche fattori esterni (dati societari, certificazioni, dipendenza del fornitore dal volume dei servizi erogati alla Banca, criticità dei servizi esternalizzati, sostenibilità, ecc.).

- Fase: **Build**
  1. *Service Catalogue Management:* processo atto a definire le pratiche utili a produrre e manutenere un catalogo di servizi IT preciso e completo, che contiene tutti i dettagli su tutti i servizi operativi e quelli in via di sviluppo o proposti;

2. *Program & Project Management:* gestione efficiente ed efficace dei progetti/ programmi tramite impiego di metodologie standard, conoscenze, competenze, tecniche e strumenti attraverso tutta l'organizzazione;
3. *Software Development Lifecycle Management* (in quanto ritenuto trasversale, fa parte di due fasi): gestione ottimale del Ciclo di sviluppo del software: gestione dei requisiti, disegno soluzione complessiva, servizi IT collegati, realizzazione soluzione e fasi di test.

- Fase: **Transition**
  1. *Change Management:* gestione del cambiamento al fine di minimizzare gli impatti della trasformazione sui Clienti finali;
  2. *Configuration & Asset Management:* definizione di un modello logico dell'infrastruttura IT al fine di identificare, monitorare e manutenere le versioni di tutti gli elementi di configurazione (Configuration Items) esistenti;
  3. *Knowledge Management:* formalizzazione, aggiornamento, conservazione e condivisione nel tempo delle informazioni e delle procedure presenti all'interno dell'organizzazione, incrementando l'efficienza e riducendo il rischio/ necessità di re-discovery della conoscenza.

- Fase: **Run**
  1. *Service Level Management*: processo atto a normare le modalità di definizione e negoziazione dei livelli di servizio con fornitori IT (SLA) e Business (OLA) nonché il monitoraggio e la misurazione degli stessi nel continuo;
  2. *Event & Incident Management:* definizione di procedure e processi relativi alla classificazione degli eventi per indirizzare le azioni relative, garantendo la gestione e il monitoraggio dei servizi; gestione degli Incident finalizzata al ripristino del corretto funzionamento nel minor tempo possibile e alla minimizzazione degli impatti generati sui Clienti;
  3. *IT Capacity Management:* processo che si occupa di ottimizzare l'utilizzo delle risorse IT, prevenire i problemi legati alla capacità e pianificare in modo proattivo per soddisfare le esigenze;

4. *IT Security Operations Management: g*estione dei processi per garantire la riservatezza, l'integrità e la disponibilità dei servizi, in conformità delle policy. Include il monitoraggio e l'applicazione di eventuali azioni correttive relative a violazioni di sicurezza;
5. *IT Service Continuity Management:* supporto al processo di Business Continuity Management per garantire il ripristino delle strutture IT entro i tempi stabiliti;
6. *Problem Management:* identificazione delle route cause al fine di identificare ed eliminare proattivamente incident ricorrenti, minimizzandone il relativo impatto;
7. Service Reporting: processo atto a descrivere le modalità di reporting dei servizi IT a 360° e a fornire periodicamente sintesi su performance dei servizi IT a livello operativo e direzionale;
8. *Request fulfilment:* gestione delle richieste di change minori/ standard o delle richieste di informazioni;
9. *Workplace Management:* processo atto a definire le regole per l'utilizzo delle postazioni di lavoro e dei servizi IT annessi al fine di garantire la sicurezza delle informazioni e delle risorse informatiche utilizzate per il loro trattamento.

- Fase: **Manage and Control**
  1. *Technology Operations***:** gestione, monitoraggio e valutazione continua dell'infrastruttura IT durante tutto il ciclo di vita dei servizi;
  2. *Application Management:* gestione degli applicativi nel corso dell'intero ciclo di vita;
  3. *IT Governance*: gestione dei controlli di I livello che vengono effettuati da IT ai fini di rilevazione del rischio associato ai servizi IT;
  4. *Data Governance*: processo atto a garantire la pianificazione, la supervisione e il controllo della gestione dei dati, il loro uso e quello delle fonti correlate;
  5. *IT Cost Management:* gestione dei requisiti di budget, accounting e tariffazione dei servizi IT.

3.4.1 Classificazione dei processi per priorità

Il framework dei processi IT della Banca è stato strutturato suddividendo i processi in due categorie: **prioritari** e **non prioritari**. Questa suddivisione è stata effettuata valutando in primo luogo se i processi in questione fossero stati oggetto di adeguamenti normativi in linea con le principali disposizioni regolamentari, come la Circolare 285, DORA o le linee guida EBA

(*European Banking Authority*). Inoltre, sono stati presi in considerazione i processi sottoposti a IT audit interni nell'ultimo anno e quelli oggetto di valutazione da parte del team di IT Risk.

Di seguito vengono analizzati nel dettaglio i tre driver utilizzati per la classificazione dei processi:

- **Adeguamenti normativi ed attenzione degli enti regolatori**: in questa categoria rientrano i processi che sono stati oggetto di adeguamenti alle normative di riferimento, identificati come critici dai regolatori durante le ispezioni o le verifiche periodiche. Tra le principali normative a cui i processi sono stati adeguati figurano:
  - Il 40° aggiornamento della Circolare 285, che, come già affrontato precedentemente, include importanti revisioni in materia di governance e gestione dei rischi IT;
  - DORA, anch'esso affrontato nei paragrafi precedenti, che introduce specifiche disposizioni per garantire la resilienza operativa digitale delle istituzioni finanziarie;
  - Le linee guida dell'EBA, che stabiliscono requisiti specifici per la gestione dei rischi legati all'IT e alla sicurezza informatica.

- **Audit interni**: questa categoria comprende i processi che sono stati sottoposti a verifiche interne durante l'ultimo anno. Gli Audit interni hanno il compito di valutare, in questo specifico caso, la conformità e l'efficienza dei processi IT rispetto alle normative interne e ai requisiti di governance dell'organizzazione. I risultati di tali verifiche rappresentano un indicatore importante della criticità e dell'efficacia dei processi esaminati, evidenziando le aree che richiedono interventi di miglioramento o revisione.

- **Valutazioni IT Risk**: processi che sono stati posti all'attenzione del team IT Risk nell'ambito delle attività di presidio e controllo del rischio. Tali processi sotto monitoraggio da parte dell'IT Risk sono considerati rilevanti in quanto possono avere un impatto significativo sulla sicurezza operativa e sulla gestione dei rischi tecnologici della Banca.

L'aderenza di un processo ad uno dei tre driver sopracitati costituisce il criterio principale per definire una prima lista di processi prioritari. Tuttavia, questa lista è stata ulteriormente affinata grazie alle valutazioni interne condotte dall'ufficio IT Strategy, che hanno avuto il compito di identificare i processi per cui, nonostante l'aderenza ad uno dei driver, è stato opportuno posticipare l'analisi di maturità; questo perché tali processi erano in quel periodo oggetto di progettualità in corso, le quali avrebbero potuto modificare in modo sostanziale la struttura operativa e la configurazione As-Is dei processi stessi. La declinazione dei processi in due differenti livelli di

priorità ha consentito di stabilire quali processi costituivano le due tranche previste per il processo di IT Maturity Assessment, con scadenze fissate rispettivamente al 30 settembre e al 30 novembre.

In particolare, a seguito dell'applicazione della prioritizzazione stabilita, i **processi** identificati come **prioritari** e analizzati in dettaglio nei successivi paragrafi della presente tesi sono **16**, ovvero: *IT Strategy Development, IT annual budget & planning, Service Catalogue Management, Program/Project Management, Change Management, Configuration & Asset Management, IT Capacity Management, Service Level Management, IT Vendor Management, IT Service Continuity Management, IT Security Operations Management, Application Management, IT Governance, Technology Operations, Service Reporting e Software Development Lifecycle Management.*

3.5 IT Maturity Assessment processi prioritari – Approccio metodologico

Dopo la definizione del framework dei processi IT della Banca, è stato avviato il vero e proprio processo di IT Governance Maturity Assessment per i processi considerati prioritari. Esso è iniziato con l'elaborazione di specifiche **checklist di valutazione**, progettate per analizzare in modo strutturato e approfondito ciascun processo IT agito all'interno dell'organizzazione. Ogni checklist, elaborata tramite lo strumento Excel, contiene una serie di domande di tipo booleano indirizzate a uno o più referenti di ciascun processo. La struttura delle checklist si basa su un modello articolato in cinque diverse categorie, ciascuna delle quali rappresenta un aspetto fondamentale per la valutazione del processo.

In particolare, le categorie utilizzate sono le seguenti:

1. **Regolamento di processo**: questa categoria verifica la presenza di linee guida centrali e la regolamentazione del processo attraverso politiche o procedure specifiche. L'obiettivo è garantire che le operazioni siano svolte in conformità agli standard e alle norme aziendali predefinite, assicurando una gestione conforme alle best practice;
2. **Attività operative**: si analizza l'effettiva esecuzione delle attività previste per ciascun processo, indipendentemente dalla presenza di regolamenti formali. Questa categoria permette di valutare l'efficienza operativa e di identificare eventuali discrepanze tra quanto pianificato e quanto effettivamente realizzato;
3. **Ruoli e responsabilità**: questa categoria mira a verificare la corretta definizione dei rappresentanti di processo e delle loro responsabilità, poiché una chiara definizione dei ruoli è

essenziale per una gestione efficace e per evitare sovrapposizioni o ambiguità nelle responsabilità operative;

4. **KPIs e reporting**: tale categoria esamina la presenza e la definizione KPI e della reportistica associata. I KPI rappresentano uno strumento fondamentale per monitorare la performance del processo, fornendo dati misurabili che consentono di valutare l'efficacia delle operazioni e di identificare aree di miglioramento;
5. **Tool**: si verifica la disponibilità e l'adeguatezza degli strumenti a supporto del processo, sia per il controllo che per l'automazione delle attività. L'utilizzo di tool adeguati è indispensabile per ottimizzare l'efficienza operativa e ridurre il rischio di errori manuali, facilitando la gestione e il monitoraggio delle attività.

Le domande booleane inserite nelle checklist sono state progettate per ottenere risposte chiare e univoche dai referenti di ciascun processo, in modo tale da avere una base oggettiva per valutare la maturità di ciascun processo in relazione alle diverse categorie analizzate. Il processo di raccolta e analisi delle risposte e delle opinioni fornite dai principali referenti interni alla Banca, svoltosi nell'arco di diverse settimane, ha permesso al team Deloitte di procedere allo step successivo; ogni categoria, valutata non solo sulla base delle risposte ottenute, ma anche attraverso approfondite considerazioni manageriali interne, è stata classificata utilizzando una **scala da 1 a 5**. Inoltre, a ciascuna delle categorie sopra descritte è stato assegnato un peso specifico, consentendo di calcolare un punteggio complessivo per ogni processo IT analizzato.

3.6 Esiti di dettaglio e aree di intervento identificate

Questo paragrafo ha lo scopo di presentare in dettaglio i risultati relativi ad alcuni dei 16 processi precedentemente identificati come prioritari. L'obiettivo è illustrare l'output del processo di IT Governance Maturity Assessment, evidenziando per ciascun processo IT le evidenze emerse dall'analisi dello stato attuale (as-is), le possibili aree di miglioramento e le proposte di action plan. In particolare, saranno illustrati a titolo esemplificativo gli esiti di 6 processi, ciascuno rappresentativo di una fase del ciclo di vita del servizio IT definito nel framework (i.e., plan, build, ecc.).

Il primo processo oggetto di analisi, appartenente alla fase "Plan", è stato il processo di **IT Strategy Development,** la cui valutazione ha portato all'assegnazione di un **punteggio complessivo di 4,1**,

segno di una buona formalizzazione del processo, anche se permangono alcune aree che richiedono miglioramenti e interventi mirati, vedi Fig. 3.11.

Tale processo risulta formalizzato attraverso un documento normativo ben strutturato, il quale viene revisionato periodicamente per garantirne la continua attualità e coerenza con le evoluzioni normative. Tuttavia, il documento presenta alcune aree di criticità che richiedono ulteriori interventi di miglioramento: in particolare, non è attualmente regolata in maniera formale l'integrazione del processo con il processo di IT Annual Budget & Planning, un passaggio essenziale per garantire la coerenza tra la pianificazione finanziaria annuale e gli obiettivi strategici IT. Inoltre, manca una regolamentazione adeguata per quanto riguarda l'analisi previsionale dei rischi IT, attività cruciale per valutare e anticipare eventuali criticità legate alla sicurezza informatica, all'affidabilità dei sistemi e alle vulnerabilità operative.

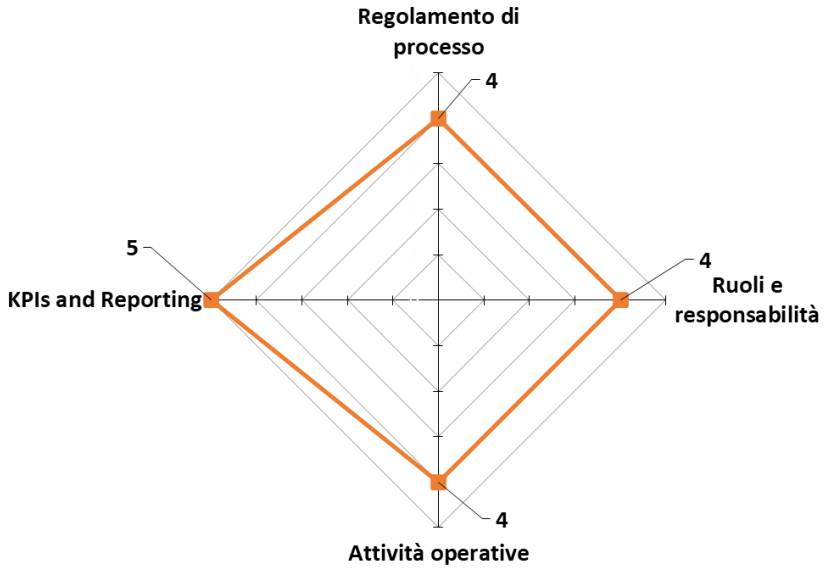
Un altro punto di forza del processo è la chiara definizione dei ruoli e delle responsabilità: i compiti relativi alla gestione e all'approvazione della strategia IT sono stati assegnati in maniera chiara ai vari attori coinvolti, come il CIO (*Chief Information Officer),* il COO (*Chief Operating Officer)* e l'AD (*Amministratore Delegato)*. Tuttavia, vi è una lacuna nella formalizzazione degli uffici e dei referenti che partecipano alla definizione della strategia IT.

Per quanto riguarda le attività operative, queste risultano allineate alle best practice del settore. La pianificazione strategica tiene conto delle principali dimensioni dell'IT e delle esigenze evolutive della banca; tuttavia, si rileva l'assenza di una sezione specifica dedicata all'analisi dei trend IT. Un'ulteriore lacuna riguarda la mancanza di sessioni di endorsement durante il percorso di approvazione del piano, che potrebbero rafforzare la validazione interna e garantire un più ampio coinvolgimento delle figure chiave della governance aziendale, quali membri del consiglio e del collegio sindacale.

Nonostante questi aspetti da migliorare, i KPI di processo sono stati definiti in modo chiaro, e rappresentano un valido strumento per monitorare il progresso e l'efficacia della strategia IT. È stato deciso di non valutare la sezione Tool in questo caso data la tipologia di processo, in quanto, a partire dalla fine del 2024, il processo sarà ulteriormente potenziato grazie all'introduzione del nuovo tool ServiceNow, una piattaforma basata su cloud progettata per automatizzare e semplificare vari processi aziendali attraverso l'integrazione di servizi digitali, che supporterà il monitoraggio delle attività e l'esecuzione della strategia IT. Grazie a questa implementazione, la

Banca potrà migliorare la gestione delle informazioni strategiche e operative, ottimizzando la tracciabilità dei processi e migliorando la capacità di reagire prontamente alle esigenze del contesto competitivo e tecnologico in continuo cambiamento.

Figura 3.11 – Livello di maturità IT Strategy Development



FONTE: elaborazione interna all'impresa di consulenza

Per quanto riguarda la fase di "Build", il processo di **Program & Project Management** è stato valutato con un **punteggio complessivo di 4,4**, indicativo di una gestione ben strutturata e formalizzata, ma che lascia spazio a ulteriori miglioramenti e ottimizzazioni, vedi Fig. 3.12.

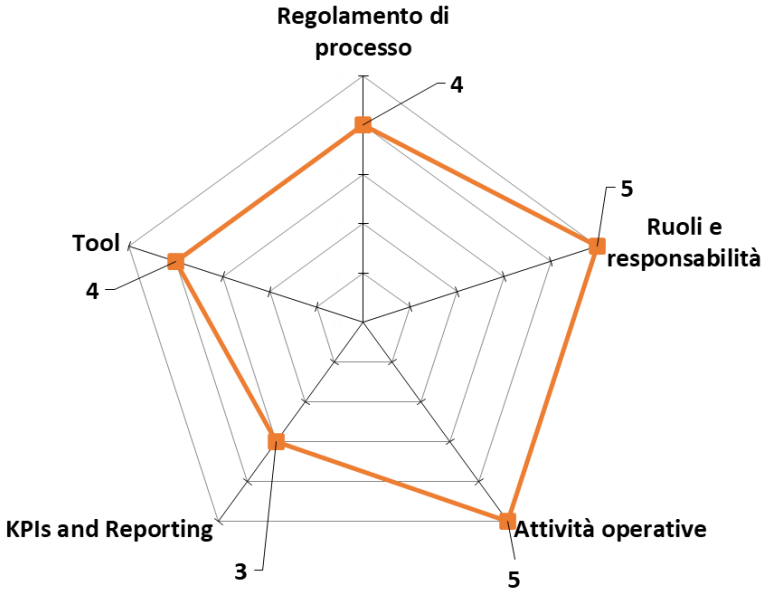
Il processo è formalizzato in appositi documenti normativi che vengono revisionati periodicamente, garantendo così che la gestione del programma e dei progetti resti allineata con gli obiettivi strategici della Banca e con l'evoluzione delle best practice nel settore. Per quanto riguarda la governance, i ruoli e le responsabilità sono definiti chiaramente, il che facilita una corretta attribuzione dei compiti e delle responsabilità tra i vari attori coinvolti nel processo.

Le attività operative risultano perfettamente allineate alle best practice, segno che il processo segue linee guida riconosciute e consolidate nel campo del Project Management. Questo allineamento

non solo facilita l'esecuzione delle attività, ma permette anche di ottimizzare le risorse e di garantire che i progetti vengano gestiti in maniera efficiente, con un focus sulla qualità e sulla tempistica.

Inoltre, sono stati definiti in modo chiaro KPI per il monitoraggio delle performance del processo, i quali vengono regolarmente riportati in specifici report e rendicontati alla direzione, offrendo così una visione trasparente e dettagliata dell'andamento del processo. Dal punto di vista degli strumenti di supporto, viene utilizzato Microsoft Teams come strumento di collaborazione, facilitando la comunicazione e la condivisione di informazioni tra i membri del team di progetto e i principali stakeholder. Jira viene invece impiegato per il caricamento e la gestione dei documenti ufficiali relativi ai vari progetti. Tuttavia, è previsto che questi documenti saranno progressivamente migrati sulla piattaforma ServiceNow, che offrirà una gestione centralizzata e maggiormente automatizzata della documentazione.

Figura 3.12 – Livello di maturità Program & Project Management



FONTE: elaborazione interna all'impresa di consulenza

Il processo di **Configuration & Asset Management**, appartenente alla fase "Transition", ha ottenuto un **punteggio complessivo di 3,6** a seguito di una valutazione che ha evidenziato aspetti

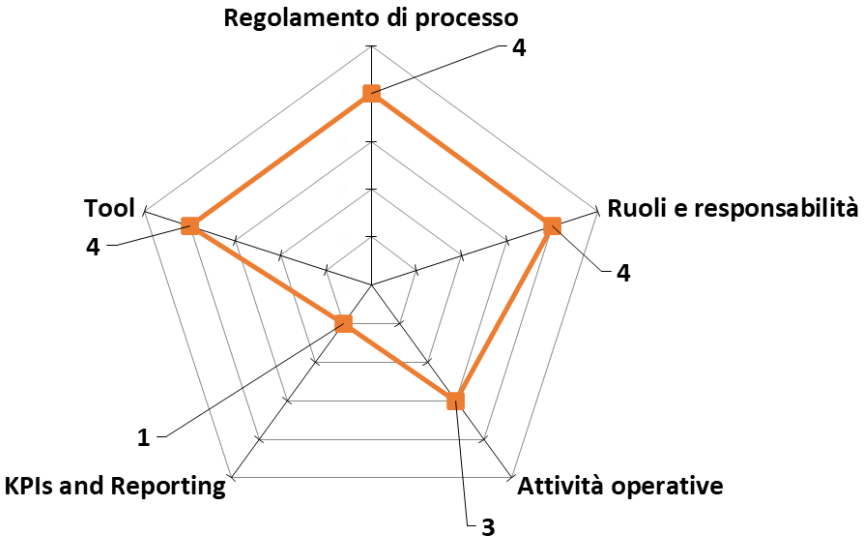
positivi ma anche diverse aree di miglioramento che necessitano di interventi specifici, vedi Fig. 3.13.

Il processo risulta formalizzato in un apposito documento normativo che definisce chiaramente la struttura e le modalità di gestione del catalogo degli asset. Tuttavia, non sono stati identificati momenti formali di revisione regolare del documento, un aspetto che limita la capacità di aggiornare la gestione degli asset in modo coerente con le evoluzioni infrastrutturali e tecnologiche.

Un'altra area critica è l'assenza di un owner di processo: sebbene siano stati definiti i responsabili delle informazioni e della manutenzione degli asset, non è stato individuato un owner specifico per il processo nel suo complesso. Per quanto riguarda la struttura del catalogo degli asset, essa risulta adeguata solo per la parte applicativa. Inoltre, vi è una significativa carenza nella definizione dei KPI e dei controlli di processo, che dovrebbero essere utilizzati per monitorare l'efficacia della gestione degli asset.

Per quanto riguarda gli strumenti di supporto, il tool attualmente impiegato per la gestione del processo è Jira. Sebbene risulti efficace per alcune delle attività connesse al processo, le informazioni relative agli asset infrastrutturali sono principalmente registrate in altri strumenti, come, ad esempio, Lansweeper, una piattaforma di gestione degli asset IT. Questa dispersione dei dati su diversi tool limita l'efficienza del processo, complicando l’accesso centralizzato alle informazioni e rendendo più complesso il monitoraggio e la gestione complessiva degli asset IT.

Figura 3.13 – Livello di maturità Configuration & Asset Management



FONTE: elaborazione interna all'impresa di consulenza

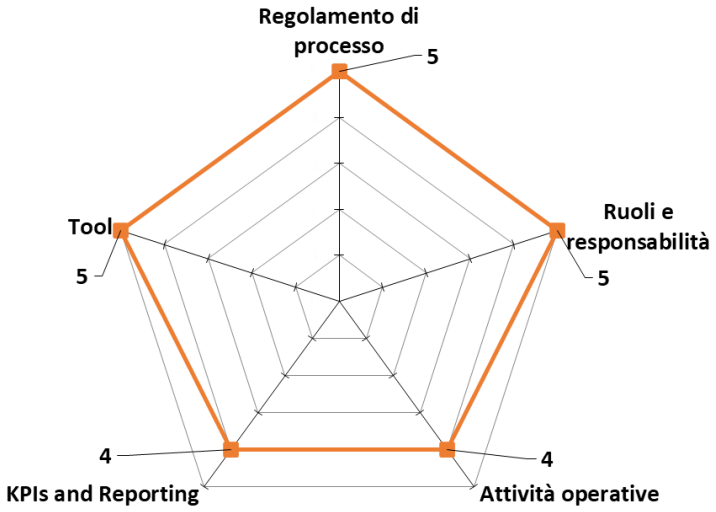
Per la fase di "Run", l'esempio riportato è rappresentato dal processo di **IT Service Continuity Management**, il quale ha ottenuto complessivamente un **punteggio di 4,5**, il che indica una gestione altamente strutturata e formalizzata, con particolare attenzione alla continuità operativa e al disaster recovery, vedi Fig. 3.14.

Il processo risulta formalizzato in un apposito documento normativo che disciplina le procedure da seguire per garantire la continuità dei servizi IT in caso di incidenti o eventi critici. Annualmente, vengono prodotti documenti specifici come il Piano di Continuità Operativa e il Disaster Recovery Plan, i quali sono fondamentali per garantire la prontezza operativa e la capacità dell'organizzazione di rispondere tempestivamente a eventuali disastri o interruzioni dei servizi IT.

Nel caso in cui vi sia una esternalizzazione dei servizi coinvolti, vengono previste clausole ad hoc per la gestione dei fornitori, assicurando che anche le terze parti rispettino gli standard di continuità operativa richiesti. Il processo è presidiato principalmente dall'ufficio Business Continuity, che ha il compito di coordinare tutte le attività operative correlate alla gestione della continuità del servizio IT e lavora a stretto contatto con i referenti sia del business che dell'IT per garantire un approccio integrato e allineato alla gestione della continuità operativa.

Sono state inoltre definite delle metriche specifiche per monitorare l'efficacia delle attività di test, che verificano la capacità delle procedure adottate di garantire la continuità operativa e che vengono regolarmente rendicontate alla direzione, permettendo un monitoraggio costante delle prestazioni del processo. Infine, dal punto di vista della toolistica, esiste una buona copertura tecnologica a supporto del presidio del processo. L'uso efficace degli strumenti tecnologici garantisce un controllo accurato e costante delle procedure operative, fornendo al team di Business Continuity le risorse necessarie per monitorare ed eventualmente intervenire in maniera rapida in caso di criticità.

Figura 3.14 – Livello di maturità IT Service Continuity Management



FONTE: elaborazione interna all'impresa di consulenza

Il processo di **Technology Operations**, per la fase "Manage and Control", ha ottenuto un **punteggio complessivo di 2,8**, indicando alcune criticità e carenze nella formalizzazione e nella gestione operativa, vedi Fig. 3.15.

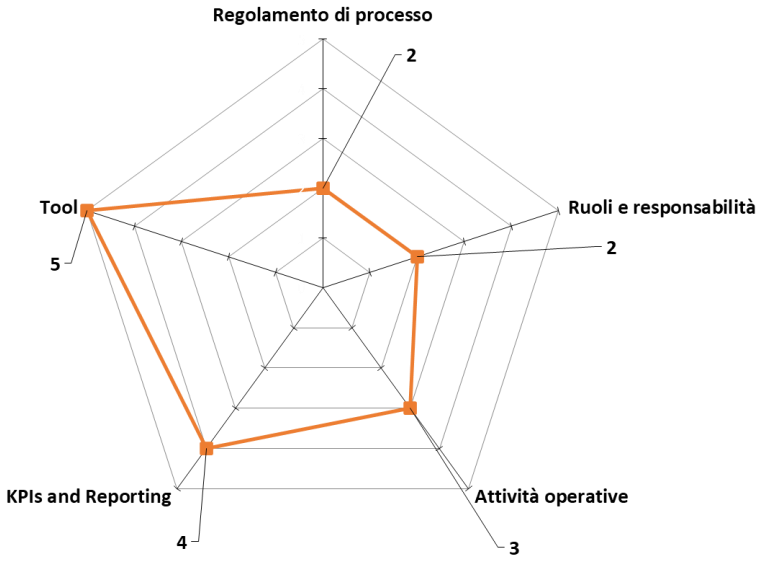
Il processo non è formalizzato in un documento normativo ufficiale e ciò rappresenta una lacuna significativa poiché l'assenza di un quadro normativo ben definito impedisce un'applicazione strutturata del processo. L'area Infrastructure della Banca è designata come owner del processo, con il supporto delle funzioni di IT Security Operations e Privacy & Security, dipartimenti che

attualmente collaborano nella gestione operativa, sebbene vi siano ancora delle aree critiche che richiedono attenzione.

Le attività di gestione del ciclo di vita degli asset infrastrutturali sono effettivamente svolte, ma presentano alcuni punti di attenzione, soprattutto per quanto riguarda il provisioning, l'installazione, la configurazione, l'aggiornamento e la dismissione degli asset IT. Le aree di intervento più rilevanti riguardano l'assenza di una definizione chiara della ownership della gestione del middleware e la mancanza di un processo strutturato per il Licensing Management, che attualmente viene gestito con un approccio basato sul "best effort", ciò vuol dire che non esiste una procedura formale per garantire che le licenze software siano gestite in modo efficace, comportando così rischi di non conformità e inefficienze operative.

Dal punto di vista dei tool e della produzione di reportistica, vi è una buona copertura, in linea con le best practice del settore. Gli strumenti utilizzati per la gestione e il monitoraggio delle attività IT permettono di avere un presidio adeguato sulle operazioni, sebbene rimangano alcune lacune nell'integrazione tra i vari sistemi e nella standardizzazione della gestione del middleware e delle licenze software.

Figura 3.15 – Livello di maturità Technology Operations



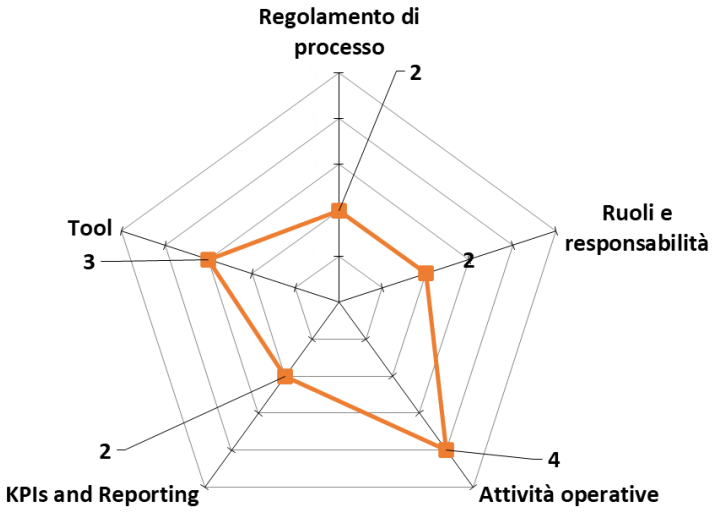
FONTE: elaborazione interna all'impresa di consulenza

Infine, l'ultimo esempio relativo agli esiti di dettaglio riguarda la fase "Manage supplier and vendor relationship", che include un solo processo, quello di **IT Vendor Management.** Esso ha ottenuto un **punteggio complessivo di 2,4**, risultato che evidenzia una gestione complessivamente insufficiente e la necessità di una formalizzazione e strutturazione più adeguata del processo, vedi Fig. 3.16.

Il processo, infatti, non è formalizzato attraverso un regolamento interno alla Banca, il che rappresenta una significativa debolezza per la governance della gestione dei fornitori IT, e, in aggiunta, attualmente non risultano definiti in maniera chiara i ruoli e le responsabilità all'interno del processo. Gli App Owner utilizzano linee guida interne per la gestione dei fornitori, ma senza una standardizzazione a livello di processo e ciò rende difficile garantire una valutazione coerente delle prestazioni dei fornitori. La funzione Procurement produce delle scorecard, ma queste permettono solo una valutazione qualitativa dei fornitori, senza includere indicatori quantitativi di performance, i quali sarebbero essenziali per una gestione più oggettiva e trasparente del servizio fornito.

L'elenco dei fornitori attivi è archiviato sui tool Jira e Jagger, ma questi strumenti non permettono di monitorare i KPI quantitativi relativi alla performance dei fornitori. L'assenza di un sistema di monitoraggio efficace, di conseguenza, impedisce alla Banca di avere una visione chiara delle performance dei propri fornitori IT e di identificare rapidamente eventuali criticità o problemi operativi. Un ulteriore aspetto critico riguarda la valutazione delle penali, che viene effettuata in maniera manuale; questa mancanza di automazione non solo aumenta il rischio di errori, ma rende il processo più lento e meno efficiente, con potenziali ricadute negative sulla tempestività degli interventi e delle correzioni.

Figura 3.16 – Livello di maturità IT Vendor Management

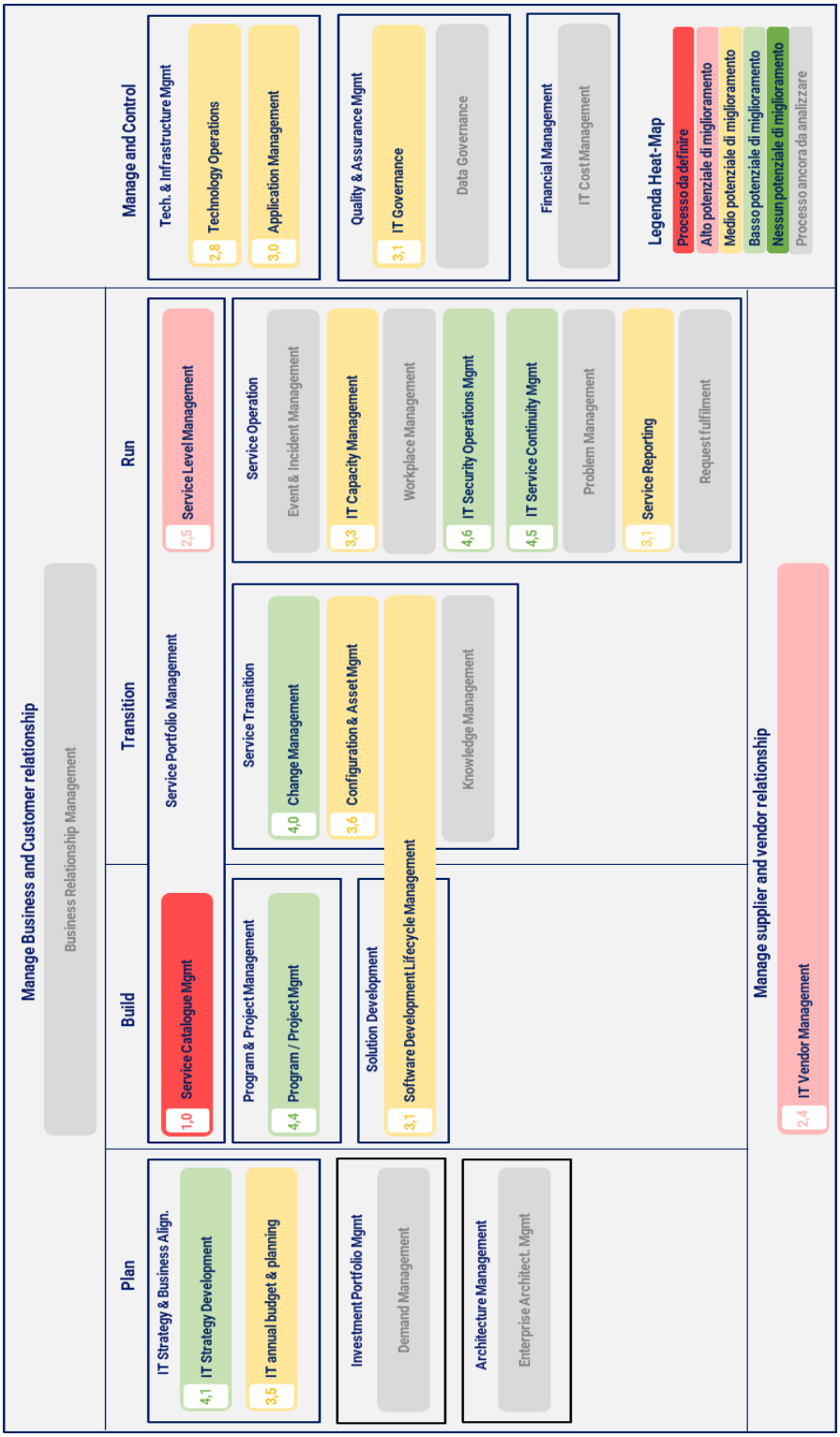


FONTE: elaborazione interna all'impresa di consulenza

3.7 Considerazioni generali ed esiti di sintesi

La prima Wave dell'IT Governance Maturity Assessment, i cui esiti complessivi sono mostrati in Fig. 3.17, ha rivelato che circa il 63% dei processi esaminati presenta numerose aree di intervento necessarie per un allineamento alle best practice. Questo dato sottolinea la necessità di miglioramenti per garantire che l'IT Governance risponda agli standard di eccellenza e ottimizzi la gestione dei servizi IT.

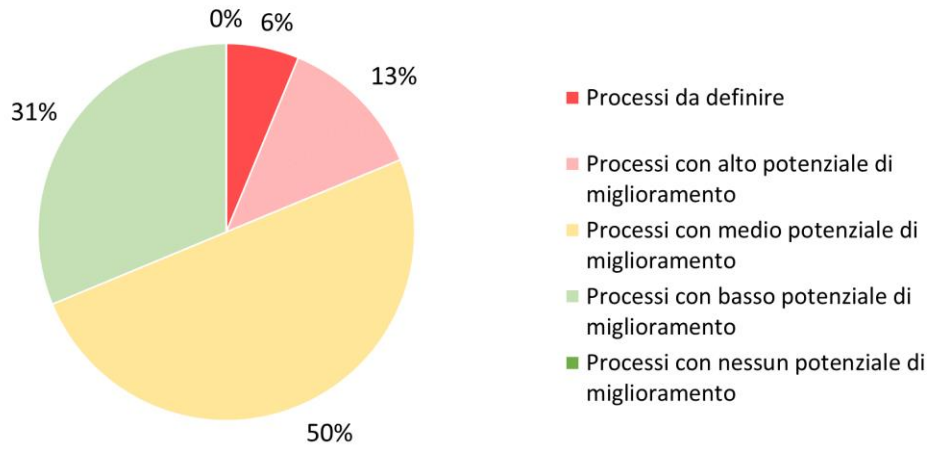
Figura 3.17 – Heatmap, esiti complessivi



FONTE: elaborazione interna all'impresa di consulenza

In termini percentuali, vedi Fig. 3.18 per una rappresentazione quantitativa degli esiti, la valutazione ha evidenziato che:

Figura 3.18 – Grafico esiti

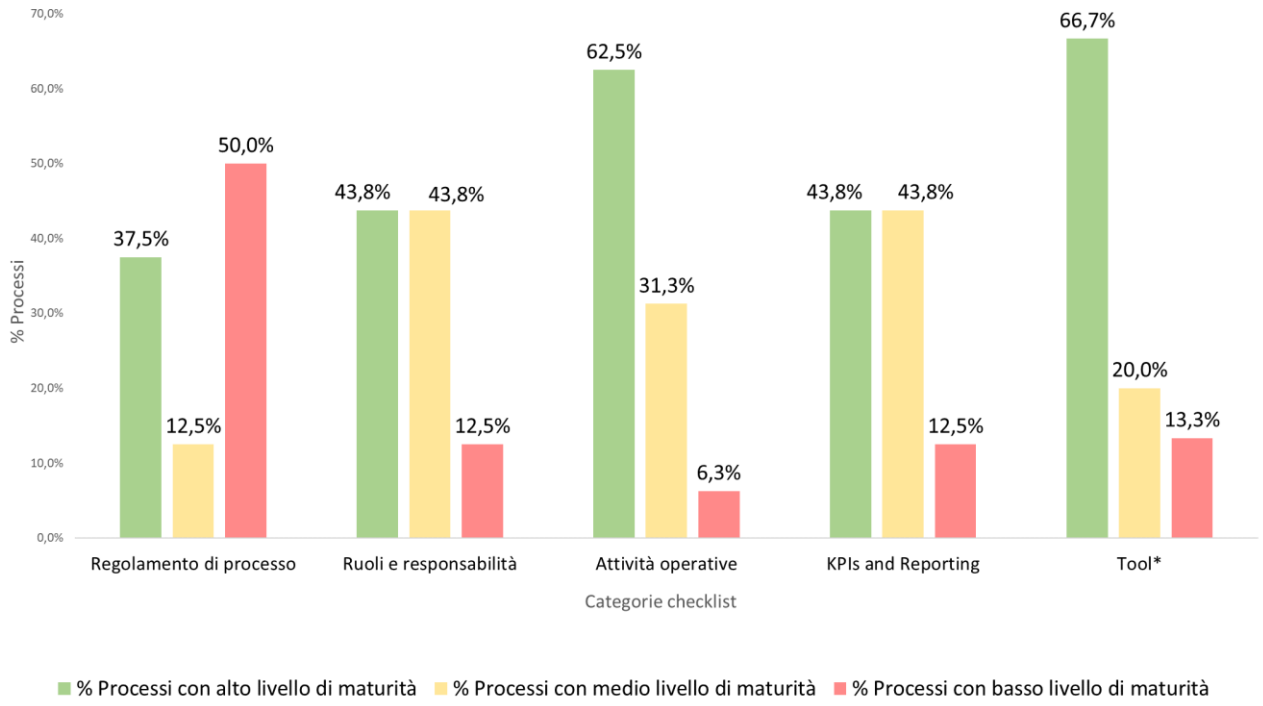


FONTE: elaborazione interna all'impresa di consulenza

- Il **31%** dei processi esaminati presenta un **basso potenziale di miglioramento,** il che significa che, nonostante siano già a un buon livello, con interventi limitati e mirati è possibile raggiungere livelli di eccellenza operativa;
- Il **50%** dei processi mostra un **medio potenziale di miglioramento**, suggerendo che molte delle pratiche in atto sono già in linea con gli standard, ma vi è ancora margine per ottimizzazioni mirate, in particolare per quanto riguarda la formalizzazione e l'implementazione di sistemi di controllo e monitoraggio;
- Il **13%** dei processi presenta un **alto potenziale di miglioramento**. Questo implica che le carenze rilevate richiedono interventi di natura strutturale e strategica per migliorare in modo significativo l'efficacia del processo;
- Solo un processo, il Service Catalogue Management, risulta non implementato, e quindi richiede un intervento completo per essere sviluppato e integrato nel framework IT.

I principali interventi identificati a seguito di questa analisi riguardano **due aree critiche**, vedi Fig. 3.19 per una rappresentazione grafica:

Figura 3.19 – Grafico livello di maturità per categoria



FONTE: elaborazione interna all'impresa di consulenza

1. **Formalizzazione delle linee guida di processo a livello di Banca**: attualmente, il 50% dei processi esaminati presenta un basso livello di maturità, mentre un ulteriore 12,5% raggiunge un livello medio. La formalizzazione delle linee guida permetterebbe di uniformare la gestione dei processi e garantirebbe una maggiore coerenza e conformità rispetto agli standard aziendali e normativi;
2. **Identificazione dei ruoli e implementazione di KPI per la misurazione delle performance**: attualmente, il 12,5% dei processi presenta un basso livello di maturità in quest'area, mentre il 43,8% presenta un livello medio. L'introduzione di metriche quantitative chiare e di responsabilità ben definite è essenziale per garantire un miglior controllo e una gestione più efficiente dei processi IT.

Nonostante la necessità di interventi strutturali, la maggior parte dei processi presenta comunque un buon livello di maturità, soprattutto per quanto riguarda le **attività operative**, con il **62,5%**dei

processi che risultano ben presidiati. Anche dal punto di vista della **toolchain** a supporto delle attività, il **66,7%** dei processi dispone di strumenti adeguati alla gestione e al monitoraggio, confermando una buona base tecnologica a disposizione dell'organizzazione.

Entrando più nel dettaglio, i processi che hanno mostrato il maggior livello di maturità sono:

- IT Strategy Development;
- Program & Project Management;
- Change Management;
- IT Security Operations Management;
- IT Service Continuity Management.

Questi processi sono ben strutturati e mostrano un alto grado di aderenza alle best practice del settore, il che conferisce all'organizzazione un buon livello di controllo e governance su queste aree.

Tuttavia, oltre alla necessità di implementare il Service Catalogue Management, sono stati rilevati processi con il livello di maturità più basso, tra cui il SLA Management e l'IT Vendor Management. Quest'ultimo è particolarmente rilevante, poiché è oggetto di intervento anche secondo la normativa DORA, che richiede adeguamenti specifici per garantire la resilienza e la sicurezza operativa del settore finanziario. Questi processi richiedono azioni correttive significative per colmare le lacune e migliorare l'efficacia complessiva dell'IT Governance aziendale.

CONCLUSIONI

In considerazione dei dettami normativi introdotti dalla DORA, con impatti verticali su processi quali Incident Management, IT Vendor Management, Risk Management e Configuration & Asset Management, l'ufficio IT Strategy & Value Management dell'Istituto di Credito ha ritenuto opportuno estendere il perimetro di osservazione a tutti i processi di IT Governance, secondo best practice di mercato, il che ha condotto, a partire dalla seconda metà di maggio 2024, all'avvio del progetto oggetto della presente tesi. In particolare, è stato sviluppato un framework che allinea i processi IT dell'Istituto alle migliori pratiche e ai benchmark di settore, con l'obiettivo di valutarne il livello di maturità. Grazie all'attività svolta durante il periodo di tirocinio presso Deloitte Consulting è stato possibile raggiungere questo obiettivo con successo, consolidando il processo di **IT Governance Maturity Assessment** e fornendo una base solida per il miglioramento continuo della governance IT.

Tuttavia, come accade di consueto, tale percorso non è risultato privo di difficoltà. Oltre alla complessità regolamentare rappresentata da normative come il Digital Operational Resilience Act e la Circolare n. 285, una delle sfide più rilevanti ha riguardato la **resistenza al cambiamento** manifestata da alcuni referenti interni all'Istituto di Credito. Durante i numerosi meeting tenuti nel corso del progetto, in particolare quelli dedicati alla compilazione delle checklist di autovalutazione per ciascun processo, è emersa una certa opposizione all'adozione di nuovi metodi operativi. La naturale inclinazione verso il mantenimento dello status quo ha, di conseguenza, rallentato in alcuni casi il processo di valutazione del livello di maturità, rendendo più complesso il coinvolgimento attivo del personale nelle iniziative di miglioramento. L'aspetto principale che ha contribuito ad incrementare tale resistenza nei referenti interni alla Banca, il quale ha contribuito quindi a rendere meno lineare lo svolgimento delle attività previste, è stato il timore diffuso tra i referenti interni che il processo di IT Governance Maturity Assessment fosse in realtà una valutazione delle loro prestazioni personali, piuttosto che un'analisi oggettiva dei processi aziendali. È stato quindi necessario chiarire fin dall'inizio che il focus del progetto fosse sui processi e non sulle persone, rassicurando i referenti sul fatto che l'obiettivo dell'assessment è quello di migliorare l'efficienza complessiva dell'organizzazione e non giudicare il loro operato. Affrontare queste difficoltà ha però rappresentato un'opportunità preziosa per comprendere meglio l'importanza della gestione del cambiamento in progetti, come questo, di trasformazione organizzativa e tecnologica. In particolare, due elementi si sono rivelati essenziali per il successo del progetto e il suo

proseguimento: una **comunicazione trasparente** e una **formazione continua**, indispensabili per superare i timori presenti, favorire una maggiore apertura verso i cambiamenti proposti e agevolare l'adozione delle soluzioni innovative all'interno dell'Istituto di Credito.

Da un punto di vista dei risultati ottenuti, il lavoro svolto ha portato all'elaborazione di una road map attuativa, in quanto sono emerse lacune significative su diversi fronti; in primo luogo, sono stati rilevati importanti gap nella percezione del ruolo dell'IT all'interno dell'organizzazione, evidenziando la mancanza di KPI adeguati e l'assenza di una reportistica strutturata ad hoc, aspetti che in realtà sono fondamentali per una gestione efficace e trasparente delle performance e dei processi IT. Inoltre, dal punto di vista della compliance interna, è emerso che molti processi, pur essendo implementati correttamente in alcune aree, non risultano formalizzati all'interno di un regolamento ufficiale. Tale mancanza rappresenta un rischio per l'organizzazione, poiché, senza una documentazione unificata e centralizzata che funga da guida operativa, si può incorrere in una frammentazione delle modalità di esecuzione delle attività operative e ciò potrebbe condurre a una disomogeneità nei comportamenti e nelle performance, con alcuni dipendenti che adottano pratiche più virtuose e altri che, al contrario, potrebbero non rispettare pienamente le best practice aziendali, come è emerso in alcune circostanze. Pertanto, è possibile affermare che, all'interno di un'organizzazione ben funzionante, la predisposizione di una documentazione regolamentare e di linee guida operative che siano accessibili e valide per tutte le unità operative è un aspetto essenziale: ciò non solo facilita una maggiore uniformità nell'applicazione delle procedure, ma consente anche di migliorare la trasparenza, la responsabilità e il monitoraggio delle attività, contribuendo in maniera decisiva al miglioramento continuo e alla riduzione dei rischi operativi.

In linea generale, comunque, il progetto è stato portato avanti con **successo**, raggiungendo pienamente tutti gli obiettivi prefissati e completando con esito positivo i deliverable previsti nel piano di lavoro delineato all'avvio dell'iniziativa. Oltre al raggiungimento degli obiettivi operativi, il progetto ha avuto un impatto strategico di grande rilievo in quanto ha stimolato un'ulteriore riflessione interna alla Banca, evidenziando l'importanza di continuare a investire nel miglioramento della governance IT. In particolare, sono state identificate nuove opportunità per ottimizzare uno dei processi IT inclusi nel framework, già oggetto di confronto tra il team di IT Strategy & Value Management della Banca e il team di Deloitte, in relazione all'avvio di una **nuova iniziativa** nel campo della Data Quality, la cui implementazione è prevista entro la fine del 2024.

Nel complesso, questa esperienza ha apportato un contributo significativo al processo di ottimizzazione della governance IT dell'azienda cliente, creando fondamenta solide per futuri interventi mirati al miglioramento continuo. L'auspicio è che il lavoro svolto possa rappresentare un punto di riferimento per tutti coloro che saranno coinvolti nella gestione della trasformazione digitale e nell'ottimizzazione della governance IT, specialmente in un contesto economico e normativo che si presenta sempre più complesso e competitivo. In tal senso, i risultati raggiunti rappresentano un primo passo fondamentale verso un'evoluzione continua, che permetterà all'Istituto non solo di rispondere efficacemente alle sfide tecnologiche future, ma anche di rafforzare la propria posizione di leadership nel panorama finanziario. Tuttavia, questo progetto non deve essere considerato un punto di arrivo, bensì un punto di partenza: solo attraverso una governance IT flessibile e in grado di adattarsi ai cambiamenti sarà possibile consolidare i risultati ottenuti, garantendo all'Istituto una capacità di risposta proattiva alle trasformazioni future e un vantaggio competitivo duraturo.

BIBLIOGRAFIA

- **DOCUMENTI PUBBLICI DELLA LETTERATURA SCIENTIFICA**

Accenture (2021), *The Cloud Imperative for Banking - Growth Markets*, Accenture, URL: CLOUD_V6 (accenture.com)

Banca d'Italia (2013), *Circolare n. 285 del 17 dicembre 2013 - Disposizioni di vigilanza prudenziale per le banche (testo integrale al 49° aggiornamento)*, URL: Circ_285_Testo_integrale_al_49_aggto.pdf (bancaditalia.it)

Brynjolfsson, E., & McAfee, A. (2014), *The Second Machine Age: Work, Progress, and Prosperity in a Time of Brilliant Technologies*, W. W. Norton & Company

D. D'Agostini, A. Piva, A. Rampazzo, (2012), *Governance IT - Continua evoluzione dei modelli per gestirla*, Triveneta, URL: Rubrica 1_piva_impaginato (aicqna.it)

Deloitte (s.d.), *Digital transformation hits core banking, Deloitte*, URL: Bank-Thoughtware-EN.pdf (deloitte.com)

European Central Bank (ECB) (2018), *Cyber Resilience Oversight Expectations for Financial Market Infrastructures*, ECB, URL: Cyber resilience oversight expectations for financial market infrastructures (europa.eu)

Galliers, R. D., & Leidner, D. E. (2014), *Strategic Information Management: Challenges and Strategies in Managing Information Systems* (4ª ed.), Routledge

Gazzetta Ufficiale della Repubblica Italiana (2015), *Legge di Stabilità 2016 - Legge n.208 del 28 dicembre 2015*, URL: Gazzetta Ufficiale

International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) (2015), *ISO/IEC 38500:2015 - Information technology – Governance of IT for the organization*, ISO, Ginevra

ISACA (2018), *COBIT 2019 Framework: Governance and Management Objectives*, ISACA

Laudon, K. C., & Laudon, J. P. (2020), *Management Information Systems: Managing the Digital Firm* (16ª ed.), Pearson

National Institute of Standards and Technology (2024), *The NIST Cybersecurity Framework (CSF) 2.0*, NIST, URL: The NIST Cybersecurity Framework (CSF) 2.0

Office of Government Commerce, (2011). *ITIL V3 - Service Design_2*

Office of Government Commerce, (2011). *ITIL V3 - Service Improvement_5*

Office of Government Commerce, (2011). *ITIL V3 - Service Operation_4*

Office of Government Commerce, (2011). *ITIL V3 - Service Strategy_1*

Office of Government Commerce, (2011). *ITIL V3 - Service Transition_3*

Parlamento Europeo e Consiglio dell'Unione Europea (2015), *Direttiva (UE) 2015/2366 del Parlamento Europeo e del Consiglio del 25 novembre 2015 relativa ai servizi di pagamento nel mercato interno (PSD2)*, Gazzetta ufficiale dell'Unione europea, URL: Direttiva (UE) 2015/ del Parlamento europeo e del Consiglio, del 25 novembre 2015

Parlamento Europeo e Consiglio dell'Unione Europea (2016), *Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali e alla libera circolazione di tali dati*, Gazzetta ufficiale dell'Unione europea, URL: REGOLAMENTO (UE) 2016/ 679 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO

Parlamento Europeo e Consiglio dell'Unione Europea (2022), *Regolamento (UE) 2022/2554 del Parlamento Europeo e del Consiglio del 14 dicembre 2022 relativo alla resilienza operativa digitale per il settore finanziario (Digital Operational Resilience Act - DORA)*, Gazzetta ufficiale dell'Unione Europea, URL: Publications Office (europa.eu)

PwC (2020), *Financial Services Technology 2020 and Beyond: Embracing Disruption*, PwC, URL: Financial Services Technology 2020 and Beyond: Embracing disruption (pwc.com)

Weill, P., & Ross, J. W. (2004), *IT Governance: How Top Performers Manage IT Decision Rights for Superior Results*, Harvard Business School Press, Boston

- **DOCUMENTI INTERNI AZIENDALI**

Deloitte, (2012), *IT Playbook_2012*

- **RISORSE WEB**

B. Carson, G. Romanelli, P. Walsh, A. Zhumaev (2018), *Blockchain beyond the hype: What is the strategic business value?*, McKinsey Digital, URL: The strategic business value of the blockchain market | McKinsey

Borsa Italiana (s.d.), *Glossario Finanziario - Segmento Titoli con Alti Requisiti (STAR)*, Borsa Italiana, URL: Segmento Titoli con Alti Requisti (STAR) - Glossario Finanziario - Borsa Italiana

Brand Finance (2024), *Deloitte - Making an impact that matters*, Brand Finance, URL: Deloitte: Making an Impact that Matters | Brand Finance

Daniele Fontana (2017), *La Deloitte Touche Tohmatsu*, Starting Finance, URL: La Deloitte Touche Tohmatsu | Starting Finance

Deloitte Italy (2022), *Deloitte diventa Società Benefit*, Deloitte, URL: Deloitte diventa Società Benefit | Deloitte Italy

Deloitte Italy (2024), *Deloitte Italia - Servizi professionali alle imprese*, Deloitte, URL: I nostri servizi | Deloitte

ISACA (2024), *COBIT—An ISACA Framework*, ISACA, URL: COBIT | Control Objectives for Information Technologies | ISACA

Treccani (2012), *Deloitte Touche*, Enciclopedia Treccani - Lessico del XXI Secolo, URL: Deloitte & touche - Enciclopedia - Treccani