POLITECNICO DI TORINO

Corso di Laurea Magistrale
in Ingegneria Gestionale LM-31

Tesi di Laurea Magistrale

Gestione di Progetti di Adeguamento normativo in ambito ICT nel settore Financial Services

Relatore/i

prof. Alberto De Marco

prof. Massimo Rebuglio

Candidato

Alessandro Panero – s292867

Anno Accademico 2023-2024

Sommario

1 L'evoluzione delle metodologie di Project Management

1.1 Fondamenti storici e strumenti iniziali

L'evoluzione delle metodologie di gestione dei progetti nel mondo Information and Communications Technology rappresenta un affascinante viaggio di adattamento e innovazione. Sebbene le radici della disciplina risiedano nei progetti di costruzione e ingegneria dei primi anni del XX secolo, la sua applicazione all'ICT ha sviluppato caratteristiche uniche che affrontano le sfide e le necessità distintive dell'implementazione innovativa e tecnologica che sempre più risulta essere imprevedibile e con parecchie variabili e stakeholders per ogni singolo progetto.

I primi approcci sistematici alla gestione dei progetti emersero negli anni '50 con lo sviluppo del Critical Path Method (CPM) da parte di DuPont e della Program Evaluation and Review Technique (PERT) da parte della Marina degli Stati Uniti. Queste tecniche introdussero concetti fondamentali che ancora influenzano gli strumenti moderni di gestione dei progetti. L'attenzione del CPM sull'identificazione delle attività critiche alla corretta riuscita del progetto e delle loro interdipendenze fornì ai project manager un approccio strutturato alla pianificazione e all'allocazione delle risorse durante ogni fase progettuale. La forza della tecnica risiedeva nella sua capacità di evidenziare quali attività non potevano essere ritardate senza influire sulla data di completamento del progetto, consentendo un'allocazione delle risorse più efficace e incentrata sulla gestione del rischio risultante da eventuali ritardi sulle attività che fanno parte del Critical Path.

PERT, nel frattempo, ha introdotto tecniche di stima probabilistica, riconoscendo l'incertezza intrinseca alle attività di progetto. Incorporando stime di durata ottimistiche, pessimistiche e più probabili, PERT ha fornito un approccio più sfumato alla pianificazione dei progetti rispetto al modello deterministico del CPM. Tuttavia, entrambe le tecniche condividevano una limitazione comune: assumevano un ambiente di progetto relativamente stabile con attività e dipendenze ben definite – un'assunzione che si sarebbe rivelata sempre più problematica nei progetti del futuro che sempre più spesso risentono di avvenimenti esterni sia economici sia macro politici, ed inoltre necessitano di un livello di competenze sempre più alto per il raggiungimento del corretto svolgimento delle attività, soprattutto nel più dinamico mondo della gestione dei progetti in ambito ICT.

1.2 L'Era del Waterfall: Controllo Strutturato e Documentazione

L'introduzione della metodologia Waterfall nel 1970 ha segnato un'evoluzione significativa negli approcci alla gestione dei progetti. Questa metodologia ha portato con sé una serie di strumenti di documentazione e controllo che sarebbero diventati standard nel settore del project management. Le matrici di tracciabilità dei requisiti sono emerse come strumenti cruciali per garantire che i deliverable del progetto fossero allineati alle specifiche iniziali. I comitati di controllo delle modifiche e i modelli di documentazione formale hanno fornito struttura al processo di gestione dei progetti, mentre i diagrammi di Gantt sono diventati lo standard de facto per visualizzare il programma di esecuzione delle singole attività di progetto.

La forza di questi strumenti risiedeva nella loro capacità di fornire una chiara visibilità sul progresso del progetto e di mantenere una documentazione completa. Tuttavia, la loro efficacia dipendeva fortemente dalla stabilità dei requisiti iniziali – una condizione raramente soddisfatta nei moderni progetti ICT. La natura rigida degli strumenti di Waterfall spesso portava a quello che divenne noto come il fenomeno del "requirements freeze", dove le esigenze aziendali in continuo cambiamento non potevano essere accolte senza una significativa interruzione delle attività a piano, necessaria alla ripianificazione dei singoli task di progetto.

1.3 Approcci Iterativi: Bilanciare Struttura e Flessibilità

L'emergere di approcci iterativi negli anni '80, in particolare il modello a Spirale, ha introdotto nuovi strumenti focalizzati sulla gestione del rischio e sullo sviluppo incrementale. Le matrici di valutazione del rischio e i quadri di valutazione dei prototipi sono diventati componenti essenziali della cassetta degli attrezzi del project manager. Questi strumenti rappresentavano un significativo avanzamento rispetto all'approccio centrato sulla documentazione del modello Waterfall, fornendo meccanismi per la valutazione e l'aggiustamento continui.

L'enfasi del modello a Spirale sull'analisi del rischio ha portato allo sviluppo di strumenti di gestione del rischio più sofisticati. Questi includevano tecniche quantitative di valutazione del rischio e alberi decisionali per valutare gli approcci tecnici. A differenza degli strumenti relativi alla modalità di gestione Waterfall, che si concentravano principalmente sul monitoraggio del progresso rispetto a un piano fisso, questi nuovi strumenti aiutavano i project manager a prendere decisioni informate sulla direzione del progetto basandosi su prove empiriche delle iterazioni di sviluppo precedenti.

1.4 La Trasformazione Agile: Strumenti per la Collaborazione e la Consegna

Il movimento Agile ha portato a un cambiamento fondamentale non solo nella metodologia ma anche negli strumenti utilizzati per gestire i progetti. La lavagna delle attività fisica, forse lo strumento più semplice e potente introdotto dai metodi Agile, ha rivoluzionato il modo in cui i team visualizzavano e gestivano il lavoro ed è stato seguito presto da equivalenti digitali come JIRA e Trello, che hanno mantenuto la semplicità delle lavagne fisiche aggiungendo funzionalità per i team distribuiti e reportistica automatizzata per facilitare la gestione e il monitoraggio delle attività e dunque minimizzare il rischio relativo alle singole attività.

La metodologia Scrum, come il framework Agile più ampiamente adottato, ha introdotto il proprio set di strumenti e artefatti. Il Burndown Chart dello sprint forniva un mezzo semplice ma efficace per tracciare i progressi all'interno delle iterazioni, mentre le misurazioni della velocità offrivano un approccio alla futura pianificazione basato sui dati. Questi strumenti segnarono una notevole deviazione dagli strumenti tradizionali di project management, concentrandosi sulla produttività del team e sulla consegna di valore piuttosto che sulla conformità a un piano prestabilito.

1.5 Analisi Comparativa degli Approcci Metodologici

Quando si confrontano questi approcci metodologici, dobbiamo considerare la loro efficacia in diversi contesti. Gli strumenti tradizionali del modello Waterfall eccellono in ambienti dove i requisiti sono stabili e la documentazione di conformità è cruciale. La loro forza risiede nel fornire tracce di audit chiare e documentazione completa, rendendoli particolarmente preziosi nei settori regolamentari ma la loro rigidità spesso porta a costi aumentati quando i requisiti cambiano, poiché gli strumenti offrono un supporto limitato per incorporare modifiche una volta completata una fase di progetto.

Le metodologie iterative e gli strumenti associati offrono un migliore supporto per la gestione del rischio e l'evoluzione dei requisiti. La capacità di aggiustare il corso delle attività in base al feedback delle iterazioni precedenti rende questi approcci più adatti a progetti con significative incertezze tecniche e che dipendono da nuove tecnologie che sono in continua evoluzione e necessitano di adattamento quando debbono collaborare allo stesso fine. Tuttavia, il sovraccarico di mantenere più tracce parallele di sviluppo e documentazione può rendere questi metodi più dispendiosi in termini di risorse, soprattutto dedicate al continuo monitoraggio e alla gestione della documentazione di dettaglio, rispetto agli approcci più semplici e lineari.

Gli strumenti Agile, al contrario, danno priorità alla semplicità e alla flessibilità rispetto alla documentazione completa. La loro forza risiede nel supportare una rapida adattabilità ai cambiamenti

dei requisiti e nel mantenere il focus del team sulla consegna del valore e non di un risultato prestabilito. Questa flessibilità può rendere più difficile mantenere il tipo di documentazione dettagliata richiesta in ambienti fortemente regolamentati e dunque le organizzazioni di dimensioni spesso si trovano spesso a integrare gli strumenti Agile con processi di documentazione aggiuntivi per soddisfare i requisiti di conformità e/o regolamentari.

1.6 Approcci Ibridi Moderni: Integrare Strumenti e Tecniche

Il riconoscimento che nessuna metodologia unica si adatta a tutti i progetti ha portato all'emergere di approcci ibridi che combinano strumenti da diverse tradizioni metodologiche dando alla luce le più moderne piattaforme di gestione dei progetti come Azure DevOps e GitLab che riflettono questa natura ibrida, offrendo capacità che spaziano dalla gestione tradizionale delle attività, al coordinamento dei team Agile, e all'automazione DevOps.

Queste piattaforme dimostrano come la gestione dei progetti ICT moderni si sia evoluta oltre le divisioni metodologiche per concentrarsi sull'efficacia pratica. Vengono dunque utilizzate Kanban board a supporto della gestione delle attività quotidiane insieme ai diagrammi di Gantt per la pianificazione a lungo termine e integrano il controllo del codice sorgente con le pipeline di integrazione continua. Questa integrazione di strumenti provenienti da tradizioni metodologiche diverse consente alle grandi organizzazioni di adattare il loro approccio di gestione dei progetti in base alle esigenze specifiche del progetto ICT, mantenendo al contempo la coerenza alla loro infrastruttura di strumenti in utilizzo.

1.7 L'Impatto degli Strumenti Moderni sul Successo dei Progetti

L'evoluzione degli strumenti di gestione dei progetti ha influenzato significativamente i risultati dei progetti e grazie agli strumenti moderni hanno migliorato la visibilità sui progressi del progetto, facilitato una migliore collaborazione tra team distribuiti e consentito approcci più sofisticati alla gestione dei rischi introducendo però nuove sfide riguardanti l'integrazione degli strumenti e la coerenza dei dati tra diverse piattaforme.

L'analisi dei tassi di successo dei progetti suggerisce che le organizzazioni più efficaci sono quelle che mantengono un elevato livello di equilibrio tra la sofisticazione degli strumenti e l'utilità pratica. Sebbene le suite di strumenti complete offrano capacità potenti, la loro efficacia dipende fortemente dalla maturità dell'organizzazione nell’adottare tali moderne pratiche di gestione dei progetti e dalla capacità dei team multidisciplinari che fanno parte del progetto di utilizzare questi strumenti in modo efficace.

1.8 Tendenze future negli strumenti di gestione dei progetti

Guardando al futuro, vediamo diverse tendenze emergenti negli strumenti e nelle tecniche di gestione dei progetti. Nuove tecnologie quali intelligenza artificiale e machine learning stanno iniziando a influenzare la gestione dei progetti attraverso l'analisi predittiva e l'ottimizzazione automatizzata della pianificazione che risultano più efficaci quando costruite su una base di pratiche sane di gestione dei progetti e una chiara comprensione metodologica.

Il futuro degli strumenti di gestione dei progetti ICT sembra muoversi verso una maggiore integrazione di diversi approcci metodologici, con un'enfasi sul supporto delle pratiche di gestione dei progetti adattive che rispondano alle necessità per quanto riguarda sia la flessibilità sia la coerenza richiesta.

1.9 Il Project Management nei Servizi Finanziari ICT

1.9.1 Introduzione

Negli ultimi anni, il settore dei Financial Services ha subito una profonda trasformazione guidata dai rapidi progressi nelle tecnologie dell'Information and communications technology (ICT). Questi sviluppi hanno portato a cambiamenti significativi nel modo in cui le istituzioni finanziarie gestiscono le loro operazioni, interagiscono con i clienti e rispettano i requisiti normativi. Al centro di tale evoluzione c'è il ruolo del Project Management nell'orchestrare le varie iniziative ICT che sono diventate con il passare degli anni fondamentali per il settore dei Financial Services e per i servizi che le società del settore erogano verso i propri clienti. Poiché le istituzioni finanziarie si affidano sempre più a infrastrutture digitali sofisticate, la necessità di solidi framework di Project Management a supporto e coordinamento dell'operatività è diventata più critica che mai. Questa sezione esplora l'evoluzione delle metodologie di ICT Project Management nel settore dei Financial Services, le sfide poste dalla trasformazione digitale e l'importanza crescente della governance tecnologica e della conformità normativa in questo settore.

1.9.2 Evoluzione delle metodologie di gestione dei progetti ICT

Storicamente, la gestione dei progetti nel settore dei Financial Services seguiva approcci tradizionali e lineari come il modello Waterfall, che enfatizzava una pianificazione dettagliata iniziale e fasi di sviluppo sequenziali con punti di controllo intermedi. Questa metodologia era particolarmente adatta alla natura conservatrice del settore finanziario, dove stabilità, prevedibilità e conformità a rigide normative erano fondamentali. Tuttavia, con l'integrazione sempre maggiore della tecnologia avanzata nei servizi finanziari, le limitazioni dell'approccio Waterfall sono diventate evidenti. La sua struttura rigida e la mancanza di flessibilità spesso non riuscivano a soddisfare le esigenze frenetiche

dei progetti ICT moderni, specialmente in un ambiente in cui le aspettative dei clienti, la situazione normativa e la tecnologia stessa erano in continua evoluzione.

Il passaggio verso metodologie di gestione dei progetti più dinamiche e adattabili, come Agile e Scrum, ha segnato un punto di svolta significativo per il settore. Questi approcci, che danno priorità allo sviluppo iterativo, alla collaborazione cross-funzionale e al miglioramento continuo, sono meglio adatti alla natura complessa e in rapida evoluzione dei progetti ICT in tale settore. Le metodologie Agile permettono un feedback più frequente, consentendo ai team operativi di adattarsi rapidamente ai cambiamenti nei requisiti aziendali o nei vincoli normativi dovuti al proliferare di nuovi prodotti da offrire alla clientela e alle problematiche legate a temi di sicurezza informatica. Questa flessibilità è particolarmente importante nel settore dei servizi finanziari, dove le scadenze di conformità regolamentare e la necessità di soluzioni innovative rivolte ai clienti spesso vanno di pari passo.

Nonostante i loro numerosi vantaggi, l'adozione delle metodologie Agile non è stata priva di sfide. Le istituzioni finanziarie operano in un ambiente altamente regolamentato e qualsiasi modifica ai loro sistemi deve aderire a rigorosi standard di governance e gestione del rischio. Questo ha portato allo sviluppo di modelli ibridi che combinano elementi sia dell'approccio Agile che della gestione tradizionale dei progetti, spesso chiamati "Agile con uno strato di governance". Questi modelli mantengono l'agilità necessaria per l'innovazione e la rapidità di applicazione della stessa assicurando al contempo che i controlli di compliance normativa necessari siano in atto per soddisfare le richieste degli enti regolatrici nazionali e sovranazionali che anno dopo anno acuiscono il controllo sull’operatività dei dipartimenti di erogazione dei servizi ICT interni agli istituti finanziari.

Il passaggio verso la trasformazione digitale ha anche reso necessario ripensare il modo in cui le istituzioni finanziarie affrontano la gestione dei progetti. Mentre banche, assicurazioni e altre entità finanziarie come prestatori di servizi di pagamento adottano più piattaforme e servizi digitali, si trovano ad affrontare una serie di nuove sfide. La trasformazione digitale nei servizi finanziari non è semplicemente una questione di aggiornare i sistemi legacy o lanciare nuovi prodotti digitali; essa, infatti, rappresenta un cambiamento fondamentale nel modo in cui queste istituzioni operano sul mercato. I progetti ICT non riguardano più solo la tecnologia, bensì si tratta di guidare la trasformazione aziendale, migliorare l'esperienza del cliente e arricchire il pacchetto di prodotti offerto alla propria customer base, sia differenziando i canali di vendita aggiungendo nuove offerte digitali, sia differenziando la gestione dei servizi ICT interni ed esterni senza perdere d’occhio gli obblighi di conformità normativi in costante evoluzione.

1.9.3 Sfide della Trasformazione Digitale nelle Istituzioni Finanziarie

Il settore dei Financial Services è caratterizzato dalla sua dipendenza dalla fiducia, stabilità e sicurezza. Tali principi sono profondamente radicati nell'operatività delle principali istituzioni finanziarie e qualsiasi interruzione o incident ai propri sistemi ICT può avere conseguenze di vasta portata con importanti ripercussioni sulla loro credibilità e dunque sulla loro produzione economica. La trasformazione digitale, pur offrendo significative opportunità di crescita e innovazione, introduce anche una serie di sfide che devono essere gestite con attenzione tramite una efficace gestione dei progetti di sviluppo ICT così da permettere la messa in produzione di servizi ICT che garantiscano un livello di servizio verso il cliente finale soddisfacente per la fiducia che il cliente ripone nelle banche e nelle assicurazioni a cui si affida.

Una delle sfide più significative è l'integrazione dei nuovi sistemi digitali con l'infrastruttura legacy esistente. La totalità delle principali istituzioni finanziarie si affidano ancora a sistemi core obsoleti, alcuni dei quali in uso da decenni quali tecnologie Mainframe o Cobol. Questi sistemi, sebbene stabili e affidabili, sono spesso inadatti a gestire le esigenze dei servizi digitali moderni. Integrare nuove tecnologie come il cloud computing, l'intelligenza artificiale e la blockchain con questi sistemi legacy è un processo complesso che richiede una pianificazione attenta, coordinamento e gestione dei rischi. Gli Project Manager in ambito ICT devono affrontare le difficoltà tecniche, operative e normative associate a tali integrazioni, garantendo che i nuovi sistemi non compromettano la stabilità e la sicurezza delle operazioni esistenti.

Un'altra sfida è il crescente ritmo di innovazione nel settore Fintech, le aziende emergenti in tale settore sono spesso non gravate dai vincoli normativi delle istituzioni finanziarie tradizionali e sono dunque in grado di innovare rapidamente, offrendo nuovi servizi ai clienti con consistenti impatti migliorativi che convincono soprattutto la clientela giovanile a spostarsi verso tali operatori e risultando quindi un competitor molto pericoloso per i principali player del mercato. In risposta a tale minaccia, le banche e le assicurazioni predominanti sono spesso sotto pressione per accelerare i propri sforzi di trasformazione digitale per rimanere competitive a livello tecnologico e contrastare l'insorgere di tali new entry del mercato. Tuttavia, questa necessità di velocità deve essere bilanciata con la necessità di una rigorosa gestione del rischio e conformità normativa. Gli ICT Project Manager devono garantire che le nuove iniziative digitali vengano implementate in modo efficiente e competitivo senza compromettere la capacità delle istituzioni finanziari di soddisfare i requisiti normativi che sono sempre più sotto controllo da parte delle autorità regolatrici nazionali e sovrannazionali (es. Banca d'Italia, IVASS, EBA, etc.).

La sicurezza informatica è un'altra sfida critica legata alla trasformazione digitale nei servizi finanziari erogati. Man mano che le istituzioni finanziarie adottano più piattaforme e servizi digitali, diventano

sempre più vulnerabili agli attacchi informatici sempre più frequenti negli ultimi anni, soprattutto verso società, come quelle del settore dei Financial Services, che tengono al loro interno un'imponente mole di dati personali dei loro clienti sia anagrafici sia legati alle abitudini di spesa. I Project Manager in tale settore devono lavorare a stretto contatto con i team di sicurezza ICT per garantire che misure di cybersecurity robuste siano integrate in tutti i progetti ICT sin dall'inizio e con importanza focale. Questa necessità richiede un approccio proattivo alla gestione del rischio, con valutazioni regolari e aggiornamenti dei protocolli di sicurezza repentini necessari a tenere il passo con le minacce quotidianamente emergenti.

Un'ulteriore sfida sta nella gestione dei dati personali che le istituzioni finanziarie devono affrontare nei loro percorsi di trasformazione digitale. La quantità di dati generati dai servizi finanziari è cresciuta esponenzialmente negli ultimi anni, e gestire efficacemente questi dati è un componente chiave di qualsiasi strategia di trasformazione digitale data l'importanza focale dei dati per il corretto svolgimento dell'operatività del settore dei Financial Services. Gli ICT Project Manager devono garantire che siano in atto framework di Data Governance per proteggere le informazioni sensibili, rispettare le normative sulla privacy dei dati come il GDPR (General Data Protection Regulation – Regulation (EU) 2016/679) e ottimizzare l'uso dei dati ai fini reportistici come input per le decisioni aziendali.

Infine, la conformità normativa rimane una preoccupazione costante nel settore dei servizi finanziari. Con l'adozione di nuove tecnologie digitali, i regolatori stanno introducendo nuovi requisiti per garantire la sicurezza, la stabilità e la resilienza delle istituzioni finanziarie nell'utilizzo della tecnologia applicata ai loro core business. Queste normative spesso variano tra le diverse giurisdizioni, aggiungendo un ulteriore livello di complessità ai progetti ICT. Gli ICT Project Manager devono essere ben informati sul panorama normativo e lavorare a stretto contatto con i team di conformità e gestione del rischio informatico per garantire che tutti i progetti rispettino gli standard necessari così da poter rispondere in maniera ottimale alle richieste dei clienti a cui si rivolgono.

1.9.4 ICT Governance e conformità normativa

La crescente dipendenza dalle tecnologie digitali nei servizi finanziari ha sottolineato l'importanza di solidi framework di ICT Governance. L'ICT Governance si riferisce ai processi, politiche e strutture che garantiscono una gestione efficace dell'ambito ICT all'interno di un'organizzazione. Nel contesto dei Financial Services, l'ICT Governance è strettamente legata alla conformità normativa, poiché le istituzioni devono garantire che i loro sistemi ICT aderiscano a rigorosi standard normativi e che garantiscano un livello di servizio elevato necessario a mantenere un'alta fiducia da parte dei clienti finali.

Un’ICT Governance efficace aiuta le istituzioni finanziarie a gestire i rischi associati ai progetti ICT, garantendo che questi progetti siano allineati con gli obiettivi strategici e gli obblighi normativi dell'organizzazione. Un componente chiave della governance tecnologica è l'istituzione di ruoli e responsabilità chiari per la gestione dei progetti e processi ICT. Questo include la definizione di chi è responsabile della supervisione dell'implementazione delle nuove tecnologie e di eventuali ICT incident risultati, della garanzia del rispetto dei requisiti normativi e della gestione dei rischi legati alla cybersicurezza, alla privacy dei dati e ai fornitori di servizi terzi.

Uno dei quadri normativi più significativi emersi negli ultimi anni è il Regolamento DORA - Digital Operational Resilience Act (Regulation (EU) 2022/2554) . DORA è un regolamento dell'Unione Europea che mira a rafforzare la resilienza dei sistemi ICT delle istituzioni finanziarie contro le interruzioni operative. Secondo DORA, le istituzioni finanziarie sono tenute a implementare quadri completi di gestione del rischio ICT, sono tenute a condurre regolari test di resilienza operativa digitale, gestire i rischi legati ai fornitori di servizi ICT erogati da terze parti e segnalare e gestire gli ICT incident in modo tempestivo e standardizzato.

Gli ICT Project Manager nel settore Financial Services devono essere pienamente consapevoli dei requisiti imposti dal Regolamento DORA e dagli altri quadri normativi vigenti, poiché svolgono un ruolo cruciale nel garantire che i progetti e i processi ICT siano conformi sin dall'inizio della loro esecuzione. Ciò richiede una stretta collaborazione tra i team ICT Project Management, i team operativi in ambito ICT, gli specialisti del rischio tecnologico e gli esperti di conformità normativa. Insieme, devono garantire che tutti gli aspetti del ciclo di vita del progetto ICT, dalla pianificazione e progettazione all'implementazione e al monitoraggio continuo, siano allineati agli standard normativi oltre che rispettare gli standard operativi necessari a mantenere un elevato livello di servizio.

Oltre a soddisfare i requisiti normativi, le istituzioni finanziarie devono anche dimostrare di avere i controlli necessari per gestire i rischi associati ai loro sistemi ICT. Questo include la conduzione di audit interni regolari, la continua implementazione di misure di cybersecurity robuste e il mantenimento di registri dettagliati degli incidenti ICT e della loro gestione e risoluzione. Il mancato rispetto di questi requisiti può comportare sanzioni significative, danni reputazionali e significative interruzioni operative.

In conclusione, la gestione dei progetti ICT in ambito Financial Services è evoluta significativamente in risposta alla trasformazione digitale del settore. L'adozione di metodologie più flessibili come Agile, insieme all'importanza crescente dell’ICT Governance e della conformità normativa, ha rimodellato il modo in cui le istituzioni finanziarie affrontano i progetti ICT. Mentre queste istituzioni continuano a navigare le sfide della trasformazione digitale, una gestione efficace dei progetti ICT sarà fondamentale

per garantire che rimangano competitive, conformi e resilienti in un panorama tecnologico in continua evoluzione.

2 Introduzione al Regolamento DORA

2.1 Contesto e requisiti di resilienza ICT

Il Digital Operational Resilience Act (DORA) rappresenta un significativo avanzamento normativo nel settore dei servizi finanziari, particolarmente in risposta alla natura sempre più digitalizzata dell'industria. Infatti, man mano che le istituzioni finanziarie continuano ad abbracciare la tecnologia per snellire le operazioni, migliorare l'esperienza dei clienti e aumentare l'efficienza, diventano anche più dipendenti da sistemi complessi di tecnologia dell'informazione e della comunicazione (ICT) e questa dipendenza espone le istituzioni a una vasta gamma di rischi, che vanno dalle minacce di sicurezza informatica alle interruzioni operative. DORA è stato introdotto dall'Unione Europea (UE) per affrontare questi rischi stabilendo un quadro normativo completo che mira a rafforzare la resilienza operativa digitale delle istituzioni finanziarie e delle loro infrastrutture ICT critiche.

Il settore dei Financial Services è stato a lungo uno dei più regolamentati, data la sua importanza cruciale nell'economia globale e per i suoi clienti. Tuttavia, i quadri normativi esistenti si sono concentrati principalmente sui rischi finanziari, come i rischi di liquidità, di mercato e di credito, con minore enfasi sui rischi associati alle tecnologie digitali da cui le istituzioni finanziarie moderne dipendono sempre più ed essendo il settore arrivato ad un livello evolutivo elevato, sono aumentate anche le minacce che deve affrontare, incluse attacchi informatici, violazioni dei dati e interruzioni dei sistemi. Questi rischi non si limitano alle sole istituzioni finanziarie, ma si estendono all'ecosistema finanziario più ampio, incluse le terze parti fornitori di servizi ICT.

L'introduzione di DORA segna un cambiamento di paradigma nel modo in cui le istituzioni finanziarie sono tenute a gestire e mitigare i rischi legati ai servizi ICT. DORA riconosce esplicitamente che la resilienza operativa – definita come la capacità di un'organizzazione di prevenire, rispondere, riprendersi e imparare dalle interruzioni operative – è diventata una componente critica della gestione del rischio nell'era digitale, anche per una società del settore Financial Services. Secondo DORA, le istituzioni finanziarie sono tenute a sviluppare solidi quadri di gestione del rischio ICT che garantiscano il funzionamento continuo e affidabile dei loro sistemi critici, anche di fronte a interruzioni significative.

Una delle forze trainanti dietro l'implementazione di DORA è la crescente preoccupazione per i rischi sistemici posti dai fallimenti su larga scala delle funzionalità ICT che potrebbero paralizzare il settore finanziario. La crisi finanziaria del 2008 ha evidenziato la natura interconnessa del sistema finanziario, dove il fallimento di una singola istituzione potrebbe avere effetti a catena su tutto il settore. Allo stesso modo, un grave fallimento delle funzioni ICT in una grande istituzione finanziaria – o in un fornitore di servizi terzi che supporta più istituzioni – potrebbe avere conseguenze devastanti per la

stabilità finanziaria di un paese e dunque anche dell'Unione Europea. DORA mira a mitigare questi rischi garantendo che tutte le istituzioni finanziarie, indipendentemente dalle dimensioni, abbiano le misure necessarie per mantenere la continuità operativa di fronte a interruzioni legate alle funzioni ICT.

2.2 DORA Key Pillars

DORA è costruito su diversi pillar chiave che collettivamente mirano a migliorare la resilienza operativa digitale delle istituzioni finanziarie e che forniscono un quadro completo per gestire i rischi ICT e garantire che le istituzioni siano attrezzate per affrontare le sfide di un ambiente sempre più digitale. Questi pillar includono quadri di gestione del rischio ICT, sistemi e componenti ICT critici, test di resilienza operativa digitale, gestione del rischio di terze parti ICT e segnalazione degli incidenti ICT e condivisione delle informazioni.

2.2.1 Quadri di gestione del rischio ICT

La pietra angolare dell'approccio normativo di DORA è il requisito per le istituzioni finanziarie di implementare quadri di gestione del rischio ICT completi che devono essere integrati nelle strategie di gestione del rischio più ampie dell'istituzione e dovrebbero coprire tutti gli aspetti delle operazioni ICT, inclusi hardware, software, reti e dati. L'obiettivo è garantire che i rischi ICT siano identificati, valutati, mitigati e monitorati su base continuativa.

Le istituzioni finanziarie devono stabilire strutture di governance chiare per supervisionare la gestione del rischio ICT. Questo include l'assegnazione di responsabilità specifiche alla direzione senior e al consiglio di amministrazione, assicurando che siano attivamente coinvolti nella supervisione dei rischi ICT e nella resilienza operativa dell'istituzione. In pratica, questo significa che la gestione del rischio ICT non è più una funzione isolata relegata al dipartimento ICT e che diventa così un componente essenziale del quadro complessivo di gestione del rischio e di governance dell'istituzione.

Inoltre, le istituzioni sono tenute a condurre valutazioni regolari dei rischi per identificare le potenziali vulnerabilità nella loro infrastruttura ICT. Queste valutazioni dovrebbero considerare sia le minacce interne sia esterne, inclusi attacchi informatici, disastri naturali, guasti di sistema ed errori umani. Basandosi su queste valutazioni, le istituzioni devono implementare controlli appropriati per mitigare i rischi identificati e rivedere regolarmente questi controlli per garantirne l'efficacia nel tempo.

2.2.2 Sistemi e Componenti ICT Critici

DORA pone particolare enfasi sulla protezione dei sistemi e dei componenti ICT valutati critici. Questi sono i sistemi e le infrastrutture essenziali per il funzionamento di un'istituzione finanziaria e, per

estensione, per la stabilità dell'intero settore finanziario. Esempi includono i sistemi di elaborazione dei pagamenti, le piattaforme di trading, le piattaforme di emissione polizze per il settore assicurativo e i sistemi di archiviazione dei dati dei clienti.

Le istituzioni finanziarie sono tenute a identificare quali dei loro sistemi e componenti ICT sono considerati critici ed implementare misure aggiuntive per proteggere questi sistemi dalle interruzioni. Ciò include garantire che i sistemi critici siano resilienti ad un'ampia gamma di potenziali minacce, dagli attacchi informatici ai danni fisici causati da disastri naturali. DORA impone alle istituzioni di stabilire sistemi di backup e misure di ridondanza per garantire che le funzioni critiche possano continuare anche in caso di guasto del sistema.

Per proteggere ulteriormente le infrastrutture ICT critiche, DORA richiede alle istituzioni di implementare meccanismi di monitoraggio e segnalazione robusti che consentano loro di rilevare e rispondere a potenziali minacce o interruzioni in tempo reale, riducendo il rischio di interruzioni prolungate che potrebbero avere conseguenze significative per i clienti e per l'intero sistema finanziario nazionale e sovrannazionale.

2.2.3 Test di Resilienza Operativa Digitale

Un componente chiave del quadro normativo di DORA è il requisito per le istituzioni finanziarie di condurre regolari test di resilienza operativa digitale. Questo comporta la simulazione di vari incidenti legati alle funzioni ICT, come attacchi informatici o interruzioni di sistema, per valutare la capacità dell'istituzione di rispondere efficacemente. L'obiettivo è identificare le debolezze nei sistemi e nei processi dell'istituzione e apportare i miglioramenti necessari per garantire che possano resistere a interruzioni nel mondo reale.

I test della resilienza operativa digitale devono essere condotti regolarmente e dovrebbero includere una gamma di scenari, da incidenti minori a interruzioni su larga scala. Si prevede che le istituzioni finanziarie collaborino con tester di terze parti, inclusi hacker etici, per condurre test di penetrazione e altre forme di valutazioni della sicurezza. Questi test aiutano a identificare le vulnerabilità che potrebbero non essere evidenti durante le normali operazioni e forniscono preziose intuizioni su come l'istituzione può migliorare la propria resilienza operativa.

Oltre ai test interni, DORA richiede alle istituzioni finanziarie di partecipare a esercizi di resilienza a livello di settore quale lo stress test imposto dall’autorità vigente EBA (European Banking Authority) nei primi mesi del 2024. Questi esercizi sono progettati per testare la resilienza dell'intero ecosistema finanziario, comprese le interconnessioni tra le istituzioni e i loro fornitori di servizi terzi. Partecipando a questi esercizi, le istituzioni possono ottenere una migliore comprensione dei rischi più ampi per il sistema finanziario e di come possono collaborare con altri stakeholders per gestire questi rischi.

2.2.4 Gestione dei rischi ICT di terze parti

Uno degli aspetti più significativi di DORA è il suo focus sui rischi associati ai fornitori di servizi ICT di terze parti. Infatti, le istituzioni finanziarie fanno sempre più affidamento su fornitori esterni per una gamma di servizi ICT, inclusi cloud computing, archiviazione dati e soluzioni di cybersecurity e sebbene questi fornitori offrano servizi preziosi, introducono anche nuovi rischi, poiché qualsiasi interruzione delle loro operazioni può avere un impatto diretto sulle istituzioni finanziarie che dipendono da loro.

Secondo DORA, le istituzioni finanziarie sono tenute a implementare solidi quadri di gestione del rischio di terze parti che garantiscano il controllo sui loro sistemi ICT, anche quando si affidano a fornitori esterni. Ciò include condurre una rigorosa due diligence prima di collaborare con fornitori terzi, valutare la loro resilienza operativa e garantire che soddisfino gli stessi standard di sicurezza e resilienza dell'istituzione finanziaria stessa.

Le istituzioni devono anche stabilire contratti chiari con fornitori terzi che includano accordi dettagliati a riguardo dei livelli di servizio (SLA) che delineano le responsabilità del fornitore in caso di interruzione. Questi accordi dovrebbero specificare la rapidità con cui il fornitore deve rispondere agli incidenti, le procedure per segnalare gli incidenti e le sanzioni per il mancato rispetto dei livelli di servizio concordati.

Inoltre, DORA richiede alle istituzioni finanziarie di monitorare continuamente le prestazioni dei loro fornitori terzi e di eseguire valutazioni regolari per garantire che rimangano conformi ai requisiti normativi ed è particolarmente importante per i servizi ICT critici, dove qualsiasi interruzione potrebbe avere conseguenze di vasta portata per l'istituzione e i suoi clienti.

2.2.5 Segnalazione degli incidenti ICT e condivisione delle informazioni

DORA introduce nuovi requisiti per la segnalazione degli incidenti ICT, garantendo che le istituzioni finanziarie siano in grado di rispondere rapidamente ed efficacemente alle interruzioni e condividere le informazioni pertinenti con i regolatori e altri stakeholder. Le istituzioni finanziarie sono tenute a stabilire processi per identificare, segnalare e rispondere agli incidenti ICT, con un focus sulla minimizzazione dell'impatto di questi incidenti sui clienti e sul sistema finanziario più ampio.

In caso di un incidente ICT significativo, le istituzioni devono segnalare l'incidente alle autorità di regolamentazione competenti entro un tempo specificato con aggiornamenti intermedi e a fine dell’impatto legato all’incidente ICT. Questo assicura che i regolatori siano informati sui potenziali rischi per il sistema finanziario e possano prendere le misure appropriate se necessario. DORA incoraggia anche le istituzioni finanziarie a condividere informazioni sugli incidenti ICT con altre istituzioni, specialmente se l'incidente ha il potenziale di impattare più stakeholder promuovendo un

approccio collaborativo alla gestione dei rischi ICT e migliorando la resilienza complessiva del settore finanziario.

2.3 Tempistiche di Implementazione e Impatto Istituzionale

L'implementazione di DORA sta avendo un impatto profondo sulle istituzioni finanziarie, richiedendo loro di fare significativi investimenti nella loro infrastruttura ICT e nelle capacità di gestione del rischio. La regolamentazione include una tempistica di implementazione graduale, dando alle istituzioni il tempo di adattarsi ai nuovi requisiti. Tuttavia, la complessità dei cambiamenti richiesti significa che le istituzioni devono iniziare a prepararsi per DORA ben prima delle scadenze regolatorie fissate per il 17 Gennaio 2025.

Per molte istituzioni, soprattutto quelle appartenenti al settore assicurativo, l'implementazione di DORA comporterà una revisione completa dei loro sistemi ICT esistenti, dei framework di gestione del rischio e delle relazioni con terze parti. Le istituzioni dovranno valutare se i loro sistemi attuali soddisfano i requisiti di resilienza stabiliti da DORA e apportare eventuali aggiornamenti necessari per garantire la conformità e questo potrebbe includere investimenti in nuove tecnologie, come strumenti avanzati di monitoraggio e reportistica, oltre a migliorare le loro capacità di cybersecurity.

L'impatto istituzionale di DORA va oltre la conformità e rappresenta un'opportunità per le istituzioni finanziarie di migliorare la loro resilienza operativa complessiva e proteggersi meglio contro i crescenti rischi associati alla trasformazione digitale. Rafforzando i loro sistemi ICT e i quadri di gestione del rischio, le istituzioni possono migliorare la loro capacità di rispondere alle interruzioni e mantenere la continuità delle operazioni, salvaguardando infine la fiducia dei loro clienti e stakeholders.

In conclusione, DORA è una regolamentazione fondamentale che affronta i rischi unici posti dalla digitalizzazione del settore dei servizi finanziari. Il suo focus sulla resilienza operativa, la gestione del rischio di terze parti e la segnalazione degli incidenti riflette l'importanza crescente delle tecnologie ICT nella stabilità del sistema finanziario. Mentre le istituzioni finanziarie lavorano per implementare i requisiti di DORA, non solo miglioreranno la loro postura di conformità, ma rafforzeranno anche la loro capacità di prosperare in un mondo sempre più digitale.

3 Obiettivi della tesi

3.1 Governance di Progetti DORA

Lo scopo di questa tesi è di esaminare l'intersezione tra la gestione dei progetti ICT e la conformità normativa nel settore dei servizi finanziari, concentrandosi in particolare sulle sfide associate all'attuazione del Digital Operational Resilience Act (DORA). Poiché le istituzioni finanziarie devono affrontare un crescente controllo normativo e la pressione per migliorare la loro resilienza operativa, devono adattare le loro pratiche di gestione dei progetti per garantire che le loro infrastrutture tecnologiche e i loro processi siano in linea con i severi requisiti del DORA. Questa ricerca cerca di offrire spunti pratici su come le istituzioni finanziarie possano gestire efficacemente l'adozione del DORA attraverso solidi framework di gestione dei progetti ICT che integrino le considerazioni sulla conformità normativa in ogni fase della realizzazione del progetto.

Il problema centrale affrontato in questa tesi è come gli istituti finanziari possono gestire le complessità dell'implementazione del DORA mantenendo l'efficienza operativa e il corretto approccio all'innovazione. Il DORA introduce una serie di requisiti rigorosi volti a garantire la resilienza operativa delle istituzioni finanziarie, che coprono aree quali la gestione del rischio ICT, la supervisione dei fornitori di servizi terzi e la segnalazione degli incidenti ICT. Queste nuove normative richiedono un approccio strategico alla gestione dei progetti ICT in grado di bilanciare la conformità normativa con la necessità di portare avanti le iniziative di trasformazione digitale.

Le istituzioni finanziarie fanno sempre più affidamento su infrastrutture ICT complesse, che spesso coinvolgono un'ampia gamma di sistemi interni e fornitori di servizi esterni. Il processo per garantire che questi sistemi ICT soddisfino gli standard DORA richiede un approccio coordinato e interfunzionale alla gestione dei progetti ICT. Inoltre, l'ambito di applicazione del DORA si estende ai fornitori terzi, il che significa che le istituzioni devono gestire non solo i propri sforzi di conformità, ma anche quelli dei loro partner esterni. Ciò introduce un ulteriore livello di complessità nella gestione dei progetti ICT, in quanto gli istituti finanziari devono garantire che queste relazioni di terzi siano soggette agli stessi standard di resilienza operativa e di gestione del rischio delle loro operazioni interne.

La ricerca analizzerà come i project manager possono guidare l'integrazione del DORA nei progetti ICT, affrontando sfide chiave come l'allineamento delle tempistiche del progetto con le scadenze normative, la gestione delle risorse tra più dipartimenti e la garanzia che tutti gli stakeholder rilevanti, sia interni che esterni, siano coinvolti nel processo di conformità. Un'attenzione particolare sarà rivolta

allo sviluppo di quadri di gestione dei progetti che consentano alle istituzioni di raggiungere la conformità normativa mantenendo la flessibilità delle loro iniziative ICT.

3.2 Ambito e limitazioni della ricerca

La ricerca si concentrerà sulle istituzioni finanziarie dell'Unione Europea, in quanto la DORA è una normativa rivolta principalmente a queste entità. Tuttavia, i risultati possono avere implicazioni più ampie anche per le istituzioni finanziarie al di fuori dell'UE che sono interessate dalle normative europee o che si affidano a fornitori di servizi con sede nell'UE. La ricerca coprirà una gamma di istituzioni di diverse dimensioni, dalle grandi banche globali alle piccole società finanziarie regionali, esplorando il modo in cui le diverse organizzazioni approcciano la gestione dei progetti nel contesto dell'adozione del DORA.

L'ambito dei progetti ICT presi in considerazione comprenderà sia le iniziative di trasformazione digitale in corso sia quelle nuove che coinvolgono sistemi ICT critici, come le piattaforme bancarie di base, i sistemi di pagamento e le infrastrutture di cybersecurity. La ricerca analizzerà come le metodologie di gestione dei progetti possano essere adattate per garantire che questi progetti soddisfino i requisiti della DORA per la resilienza operativa, la gestione del rischio ICT e la segnalazione degli incidenti.

Sebbene la ricerca miri a fornire una visione completa della gestione dei progetti per la conformità al DORA, vi sono alcuni limiti. Una limitazione è l'attenzione esclusiva alle istituzioni finanziarie dell'UE, che potrebbe limitare l'applicabilità dei risultati in contesti extra-UE. Inoltre, la ricerca si concentra su progetti TIC su larga scala, il che significa che le istituzioni o i progetti più piccoli potrebbero trovarsi ad affrontare sfide diverse, non completamente coperte da questo studio. Inoltre, la natura in rapida evoluzione del contesto normativo fa sì che possano emergere nuove regole o linee guida che potrebbero avere un impatto sui risultati.

Nonostante queste limitazioni, la ricerca si propone di fornire spunti di riflessione utili ai project manager, ai responsabili della compliance e ai leader tecnologici degli istituti finanziari che hanno il compito di supervisionare l'adozione del DORA.

4 Servizi di consulenza in progetti ICT e regolamentari

Le società di consulenza in ambito Technology Advisory Services svolgono un ruolo critico nell'aiutare le istituzioni finanziarie a navigare le sfide della gestione dei progetti ICT e della conformità normativa, in particolare alla luce delle normative in evoluzione come il Digital Operational Resilience Act (DORA). L'approccio delle società di consulenza alla consegna dei progetti ICT si basa su una profonda esperienza, un robusto quadro di gestione dei progetti e una comprensione sfumata delle esigenze normative, rendendolo un caso di studio ideale per esaminare come le istituzioni finanziarie possano integrare con successo l'innovazione tecnologica con i requisiti di conformità.

Nel settore dei servizi finanziari, i servizi di consulenza sono progettati per colmare il divario tra trasformazione tecnologica e governance ICT regolamentare e questa è una sfida significativa per molte istituzioni finanziarie, che sono sotto costante pressione per innovare, ottimizzare le operazioni e migliorare le esperienze dei clienti, il tutto rispettando requisiti normativi stringenti. I Servizi di Consulenza Tecnologica delle principali società del settore consulenza sono particolarmente rilevanti poiché offrono un approccio olistico che affronta non solo gli aspetti tecnici dei progetti ICT ma anche le dimensioni strategiche, operative e regolamentari. L'esperienza di tali aziende nel navigare ambienti normativi complessi come quelli imposti da DORA, combinata con le sue metodologie strutturate di gestione dei progetti, fornisce una roadmap per come le istituzioni finanziarie possono raggiungere la conformità mentre guidano la trasformazione digitale.

4.1 Quadro di consegna dei progetti ICT

Uno dei punti di forza principali dei servizi di consulenza tecnologica delle principali società di consulenza è il quadro di gestione dei progetti strutturato che impiegano per fornire soluzioni ICT, specificamente adattato al settore dei servizi finanziari, consente l'esecuzione sistematica dei progetti ICT, dalla pianificazione iniziale fino all'implementazione finale e alla revisione. Il quadro di consegna dei progetti delle società di consulenza è progettato per garantire che ciascuna fase di un progetto ICT sia eseguita in modo efficiente, con una forte attenzione al raggiungimento degli obiettivi aziendali e al rispetto dei requisiti normativi.

Al centro del framework di delivery dei progetti ICT delle società di consulenza c'è il loro focus sull'allineamento degli obiettivi del progetto con la strategia organizzativa. Le istituzioni finanziarie spesso intraprendono progetti ICT su larga scala, come iniziative di trasformazione digitale o l'implementazione di nuovi sistemi di gestione dei dati, con l'obiettivo di migliorare l'efficienza operativa, il coinvolgimento del cliente o il posizionamento competitivo. Tuttavia, senza un chiaro

allineamento tra gli obiettivi tecnici di questi progetti e gli obiettivi strategici più ampi dell'istituzione, c'è il rischio di un'allocazione errata delle risorse, un aumento incontrollato dello scope, o il fallimento nel raggiungere i KPI di progetto e aziendali. Il framework delle società di consulenza mitiga questi rischi assicurando che tutti gli stakeholder, inclusi i project manager, i team ICT e i leader aziendali, siano allineati sugli obiettivi di progetto sin dall'inizio.

La metodologia di gestione dei progetti imposta dalle società di consulenza enfatizza anche le pratiche agili, riconoscendo che la flessibilità è fondamentale per gestire le complessità dei progetti ICT nel settore finanziario. Le istituzioni finanziarie operano in un ambiente in rapida evoluzione, dove aggiornamenti normativi, progressi tecnologici e dinamiche di mercato possono influenzare l'ambito e la direzione di un progetto ICT. L'approccio agile di tali società consente uno sviluppo iterativo, in cui i team di progetto possono adattarsi rapidamente ai cambiamenti senza compromettere le tempistiche o la qualità del progetto. Questo è particolarmente importante nel contesto della conformità normativa, dove nuove linee guida possono richiedere adeguamenti ai sistemi o ai processi ICT a metà di un progetto.

Inoltre, il framework di consegna dei progetti ICT è altamente collaborativo, favorendo una stretta interazione tra gli stakeholder interni (come l'ufficio di gestione dei progetti, gli specialisti ICT e i team di conformità) e gli stakeholder esterni (come i fornitori terzi e gli enti regolatori). La collaborazione è essenziale per il successo dei progetti ICT, in particolare quando più team multidisciplinari devono lavorare insieme per integrare nuove tecnologie, gestire i dati e garantire la conformità normativa. Tale framework facilita questa collaborazione attraverso processi di ICT governance strutturati, comunicazione regolare e una comprensione condivisa degli obiettivi e delle tappe di questa tipologia di progetto.

La struttura di governance all'interno del framework di consegna dei progetti di PwC garantisce responsabilità in ogni fase del progetto. Questo viene realizzato tramite ruoli e responsabilità ben definiti, processi decisionali chiari e un rigoroso controllo. Ad esempio, ogni fase del progetto – che sia progettazione, sviluppo, test o implementazione – ha dei responsabili designati che sono incaricati di supervisionare il completamento delle attività chiave e di riferire sui progressi. Questa struttura non solo mantiene il progetto sulla buona strada, ma garantisce anche che eventuali rischi o problemi siano identificati e affrontati tempestivamente, riducendo la probabilità di ritardi o superamenti dei costi.

La gestione del rischio è un altro componente critico del framework di consegna dei progetti ICT e nel settore dei servizi finanziari, i rischi associati ai progetti ICT sono sfaccettati e possono variare da rischi tecnologici, come guasti ai sistemi o attacchi informatici, a rischi operativi, come interruzioni dei processi o violazioni dei dati, e rischi normativi, come la non conformità con DORA. Le società di

consulenza adottano un approccio proattivo alla gestione del rischio, incorporando valutazioni dei rischi e strategie di mitigazione durante l'intero ciclo di vita del progetto. Identificando i potenziali rischi in anticipo e sviluppando piani di contingenza, tali società aiutano le istituzioni finanziarie a evitare costose interruzioni e garantire la resilienza dei loro sistemi ICT.

4.2 Approccio di Consulenza sulla Conformità Normativa

I servizi di consulenza per la conformità normativa sono parte integrante delle più ampie offerte di Technology Advisory, in particolare nel settore dei servizi finanziari, dove le richieste normative stanno diventando sempre più rigorose. Una delle principali sfide che le istituzioni finanziarie affrontano oggi è la necessità di rimanere conformi a complessi quadri normativi, come DORA, perseguendo al contempo la trasformazione digitale. L'approccio delle principali società di consulenza alla conformità normativa si basa su una profonda comprensione del panorama normativo, combinata con un'esperienza pratica nell'aiutare le istituzioni a implementare soluzioni di conformità efficaci e sostenibili.

DORA, in particolare, presenta una serie unica di sfide per le istituzioni finanziarie a causa del suo focus completo sulla gestione del rischio ICT, la resilienza operativa e la supervisione di terze parti. I servizi di consulenza per la conformità normativa sono progettati per aiutare le istituzioni ad allinearsi a questi requisiti fornendo soluzioni personalizzate che affrontano sia gli aspetti tecnici che quelli di governance della conformità. L'approccio di tali società non riguarda solo assicurarsi che le istituzioni soddisfino i requisiti normativi minimi ma si tratta di aiutarle a costruire una resilienza robusta e a lungo termine nei loro sistemi e processi ICT.

Uno degli elementi chiave dell'approccio consulenziale alla conformità normativa è il suo focus sulla gestione del rischio ICT. Secondo DORA, le istituzioni finanziarie sono tenute a implementare quadri di gestione del rischio ICT completi che coprano tutti gli aspetti della loro infrastruttura digitale, inclusi hardware, software, reti e dati. Le società di consulenza assistono le istituzioni nello sviluppo di questi quadri conducendo valutazioni dettagliate del rischio, identificando potenziali vulnerabilità e raccomandando controlli appropriati. Questo processo spesso comporta una stretta collaborazione con vari stakeholder all'interno dell'istituzione, inclusi team ICT, responsabili della conformità e alta dirigenza, per garantire che tutti i rischi siano correttamente identificati e affrontati.

Le società di consulenza forniscono anche indicazioni sull'implementazione dei test di resilienza operativa digitale, che sono un requisito critico secondo DORA. Le istituzioni finanziarie sono tenute a condurre test regolari sui loro sistemi ICT per garantire che possano resistere a una vasta gamma di potenziali interruzioni, dagli attacchi informatici ai guasti di sistema. I servizi di consulenza aiutano le

istituzioni a progettare ed eseguire questi test, fornendo approfondimenti sulle aree in cui la resilienza può essere migliorata. Questo include sia test tecnici, come test di penetrazione e simulazioni di recupero di emergenza, sia esercizi più ampi di resilienza operativa che coinvolgono più dipartimenti e stakeholder.

La gestione del rischio di terze parti è un'altra area in cui i servizi di consulenza sulla conformità normativa sono particolarmente preziosi. DORA pone una forte enfasi sulla necessità per le istituzioni finanziarie di gestire i rischi associati ai loro fornitori di servizi ICT, in particolare quelli che forniscono servizi critici come il cloud computing o la cybersecurity. Le società di consulenza aiutano le istituzioni a sviluppare solidi framework di gestione del rischio di terze parti che garantiscono che i loro fornitori di servizi soddisfino gli stessi standard di resilienza e sicurezza dell'istituzione stessa. Questo comporta condurre una due diligence approfondita sui potenziali fornitori di servizi, sviluppare contratti chiari e accordi sul livello di servizio (SLA), e implementare meccanismi di monitoraggio e supervisione continui.

Oltre ad aiutare le istituzioni a conformarsi al DORA, i servizi di consulenza sulla conformità normativa si estendono anche ad altri quadri normativi rilevanti, come il Regolamento Generale sulla Protezione dei Dati (GDPR) e la Direttiva sui Servizi di Pagamento 2 (PSD2). Questo approccio olistico garantisce che le istituzioni finanziarie siano in grado di navigare l'intero spettro dei requisiti normativi mantenendo la flessibilità necessaria per innovare e crescere. La profonda esperienza nella conformità normativa sviluppata dalle principali società di consulenza, unita alla loro conoscenza tecnica dei sistemi e dei processi ICT, consente loro di fornire soluzioni complete che rispondano sia alle esigenze immediate che a quelle a lungo termine delle istituzioni finanziarie.

I servizi di consulenza sottolineano anche l'importanza della segnalazione regolamentare e della condivisione delle informazioni, che sono componenti critici di DORA. Le istituzioni finanziarie sono tenute a segnalare agli enti regolatori gli incidenti ICT significativi e a condividere informazioni rilevanti con altre istituzioni per contribuire a mitigare i rischi sistemici e a tal proposito le società di consulenza assistono i propri clienti nello sviluppo dei meccanismi di segnalazione e dei flussi di lavoro necessari, garantendo che siano in grado di soddisfare qu esti requisiti in modo tempestivo ed efficiente. Questo spesso comporta l'integrazione di strumenti di segnalazione regolamentare nell'infrastruttura ICT più ampia dell'istituzione, consentendo la rilevazione, la segnalazione e la risoluzione automatizzata degli incidenti.

Nel complesso, l'approccio consulenziale materia di conformità normativa è progettato per aiutare le istituzioni finanziarie non solo a soddisfare i loro obblighi normativi attuali, ma anche a costruire la resilienza necessaria per prosperare in un ambiente sempre più digitale e regolamentato. Combinando

la sua esperienza nella gestione di progetti ICT con una profonda comprensione dei requisiti normativi e le società di consulenza sono in grado di fornire alle istituzioni finanziarie gli strumenti e le strategie di cui hanno bisogno per avere successo di fronte alle sfide in evoluzione.

5 Analisi degli Stakeholder

Nel campo della gestione dei progetti ICT e della conformità normativa nei servizi finanziari, il successo di qualsiasi iniziativa dipende in gran parte da una gestione efficace degli stakeholder. Data la complessità e la scala di questi progetti – che spesso comportano trasformazioni tecnologiche significative e una rigorosa supervisione normativa – l'identificazione, il coinvolgimento e la collaborazione dei principali stakeholder sono cruciali. Questa sezione esplora sia gli stakeholder interni alle società di consulenza sia gli stakeholder esterni nelle organizzazioni finanziari clienti, esaminando i loro ruoli, responsabilità e il valore che apportano alla consegna dei progetti ICT.

5.1 Stakeholder Interni

Gli stakeholder interni alle società di consulenza sono fondamentali per l'esecuzione di successo dei progetti ICT, in particolare quando si tratta di garantire che questi progetti siano conformi ai requisiti normativi come il Digital Operational Resilience Act (DORA). L'approccio multidisciplinare delle società di consulenza significa che una varietà di team e individui contribuiscono con la loro esperienza nelle diverse fasi del ciclo di vita del progetto. Ognuno di questi stakeholders apporta competenze specializzate e prospettive diverse, permettendo alle società di consulenza di offrire soluzioni complete che affrontano sia le sfide tecnologiche che quelle normative affrontate dalle istituzioni finanziarie.

5.1.1 Project Management Office (PMO)

Il Project Management Office (PMO) è al centro del framework di gestione dei progetti ICT delle società di consulenza. Serve come hub centrale per la pianificazione, il coordinamento e la supervisione dell'intero progetto, garantendo che tutte le attività siano completate in tempo, entro l'ambito e secondo il budget prestabilito. La principale responsabilità del PMO è fornire struttura al progetto, facilitando la comunicazione tra i diversi team coinvolti e garantendo che il progetto aderisca agli obiettivi e ai tempi stabiliti.

Nei progetti ICT per i servizi finanziari, dove la conformità normativa è un fattore critico, il PMO deve anche garantire che tutte le attività siano allineate con i quadri normativi pertinenti, incluso DORA. Questo spesso comporta una stretta collaborazione con i team di compliance per garantire che i protocolli di gestione del rischio, le misure di governance dei dati e le procedure di risposta agli incidenti siano integrati nel progetto sin dall'inizio. Inoltre, il PMO è responsabile dell'identificazione dei potenziali rischi e sfide, dello sviluppo di strategie di mitigazione e dell'assicurare che gli stakeholders del progetto siano informati sui progressi e su eventuali aggiustamenti necessari.

Il PMO svolge anche un ruolo chiave nell'allocazione delle risorse, assicurando che la giusta combinazione di competenze tecniche, di compliance e di business sia disponibile in ogni fase del progetto. Questo include il coordinamento con fornitori terzi, la supervisione degli obblighi contrattuali e l'assicurazione che il team di progetto abbia accesso agli strumenti e alle tecnologie necessarie per raggiungere gli obiettivi del progetto.

5.1.2 ICT Risk Specialist

Gli specialisti del rischio ICT all'interno delle società di consulenza sono responsabili di identificare, valutare e gestire i rischi associati ai componenti tecnologici dei progetti ICT. Nel contesto dei servizi finanziari, questi rischi sono sfaccettati e possono includere minacce informatiche, guasti di sistema, violazioni dei dati e mancanze di conformità. Date le stringenti richieste di DORA, che impone solidi framework di gestione del rischio ICT, gli specialisti del rischio tecnologico svolgono un ruolo fondamentale nell'assicurare che tutti gli aspetti del progetto aderiscano alle migliori pratiche di gestione del rischio.

Gli specialisti di ICT Risk lavorano a stretto contatto sia con i team tecnici che con i team di compliance per garantire che tutti i sistemi e i processi ICT siano progettati tenendo conto della mitigazione del rischio. Questo comporta la conduzione di valutazioni dei rischi approfondite, l'implementazione di misure di controllo e il monitoraggio continuo delle potenziali vulnerabilità durante l'intero ciclo di vita del progetto. Ad esempio, in un progetto che prevede l'implementazione di un nuovo sistema basato su tecnologie cloud, gli specialisti del rischio tecnologico valuterebbero i rischi associati alla migrazione dei dati, alle vulnerabilità di sicurezza e all'integrazione di servizi di terze parti.

Oltre a gestire rischi specifici, gli specialisti ICT Risk contribuiscono anche alla resilienza complessiva dei sistemi ICT. DORA pone una forte enfasi sulla resilienza operativa, richiedendo alle istituzioni finanziarie di avere sistemi robusti in grado di resistere e riprendersi da eventi dirompenti. Gli ICT Risk Specialist delle società di consulenza garantiscono che queste misure di resilienza siano integrate nella progettazione e nell'esecuzione dei progetti ICT, aiutando le istituzioni a soddisfare i requisiti normativi proteggendo al contempo le loro operazioni.

5.1.3 ICT Architecture Expert

Gli esperti di ICT Architecture sono responsabili della progettazione e dell'implementazione dell'infrastruttura tecnologica che supporta le operazioni delle istituzioni finanziarie. Nei progetti ICT su larga scala, questa tipologia di esperti svolgono un ruolo cruciale nel garantire che i sistemi sviluppati siano scalabili, sicuri e allineati sia con gli obiettivi aziendali che con i requisiti normativi. La loro

esperienza è essenziale per integrare nuove tecnologie – come il cloud computing, l'intelligenza artificiale e la blockchain – nelle infrastrutture esistenti senza interrompere le operazioni in corso.

All'interno dei team di progetto delle società di consulenza, gli esperti di architettura ICT collaborano strettamente con gli specialisti del rischio tecnologico e i team di conformità per garantire che i sistemi che progettano non solo soddisfino le specifiche tecniche ma aderiscano anche agli standard normativi. Questo è particolarmente importante nel contesto di DORA, che richiede alle istituzioni finanziarie di implementare solidi framework di gestione del rischio ICT e garantire la resilienza operativa dei loro sistemi critici.

Questi esperti svolgono anche un ruolo cruciale nell'ottimizzare le prestazioni dei sistemi ICT, assicurando che possano gestire i grandi volumi di dati e transazioni tipici dei servizi finanziari. Questo comporta la selezione del giusto mix di tecnologie, la progettazione di architetture di sistema efficienti e sicure, e assicurando che tutti i componenti siano pienamente integrati.

5.1.4 Team di ICT Compliance & Governance

I team di ICT Compliance & Governance delle società di consulenza sono essenziali per garantire che i progetti ICT soddisfino i requisiti normativi imposti alle istituzioni finanziarie. Questi team possiedono una profonda competenza nel panorama normativo, inclusi framework come DORA, il Regolamento generale sulla protezione dei dati (GDPR) e la Direttiva sui servizi di pagamento (PSD2). Il loro ruolo è garantire che tutti gli aspetti del progetto ICT, dalla progettazione del sistema alla gestione dei dati e supervisione di terze parti, siano conformi alle normative pertinenti.

Nel contesto di DORA, i team di compliance e governance normativa collaborano strettamente sia con il PMO che con gli specialisti di ICT Risk per garantire che i progetti ICT includano adeguate misure di gestione del rischio, meccanismi di segnalazione degli incidenti e protocolli di testing della resilienza. Inoltre, si interfacciano con le autorità di regolamentazione per garantire che l'istituzione sia preparata per eventuali audit o ispezioni che potrebbero essere richiesti come parte del processo normativo.

Inoltre, i team di ICT Compliance & Governance forniscono una supervisione continua durante l'implementazione dei progetti ICT, garantendo che tutte le pratiche di gestione, archiviazione e trasmissione dei dati aderiscano agli standard normativi. Questo è particolarmente importante per le istituzioni finanziarie, dove il rischio di violazioni dei dati o non conformità può comportare significative sanzioni finanziarie e danni reputazionali.

5.2 Stakeholder del Cliente

Oltre agli stakeholder interni alle società di consulenza, anche gli stakeholder esterni dell'organizzazione della società del settore Financial Services cliente svolgono un ruolo cruciale nel

successo della consegna dei progetti ICT. Questi stakeholders rappresentano tipicamente una gamma di dipartimenti, ciascuno con le proprie priorità, obiettivi e aree di competenza. Una collaborazione efficace tra i team di progetto della società di consulenza e gli stakeholder del cliente è essenziale per garantire che il progetto soddisfi sia i requisiti aziendali sia normativi.

5.2.1 DSI – Direzione Sistemi Informativi

La direzione Sistemi Informativi all'interno delle organizzazioni dei clienti è spesso il punto di contatto principale per i team di progetto delle società di consulenza. I dipartimenti che compongono la DSI sono responsabili della gestione quotidiana dei sistemi ICT dell'istituzione e il loro coinvolgimento è essenziale per garantire che il progetto sia in linea con l'infrastruttura, i processi e le capacità tecniche esistenti dell'istituzione.

La DSI fornisce preziose intuizioni sull'attuale infrastruttura ICT dell'istituzione finanziaria, aiutando i team di progetto della società di consulenza a comprendere le sfide e le opportunità associate all'implementazione di nuovi sistemi o all'aggiornamento di quelli esistenti. Inoltre, svolgono un ruolo chiave nell'identificazione dei potenziali rischi e nel garantire che i requisiti tecnici del progetto siano soddisfatti.

Inoltre, la DSI è spesso responsabile della supervisione dell'integrazione dei servizi di terze parti, come i fornitori di cloud o le aziende di cybersecurity. Data l'enfasi di DORA sulla gestione del rischio di terze parti, una stretta collaborazione tra i team di consulenza e la DSI del cliente è essenziale per garantire che tutti i servizi esterni soddisfino gli standard richiesti di sicurezza e resilienza.

5.2.2 Team di Sicurezza delle Informazioni

I team di sicurezza delle informazioni all'interno delle organizzazioni dei clienti sono incaricati di proteggere i dati e i sistemi dell'istituzione dalle minacce informatiche. Nel contesto di un progetto ICT, il loro ruolo è garantire che tutti i nuovi sistemi, processi e tecnologie soddisfino i requisiti di sicurezza dell'istituzione finanziaria. Questo è particolarmente importante nei servizi finanziari, dove le violazioni dei dati e gli attacchi informatici possono avere gravi conseguenze sia per l'istituzione sia per i suoi clienti.

I team di sicurezza informatica lavorano a stretto contatto con gli specialisti di ICT Risk delle società di consulenza per identificare potenziali vulnerabilità e implementare misure di sicurezza appropriate. Questo include tutto, dalla crittografia e i controlli di accesso alle procedure di risposta agli incidenti e ai piani di recupero in caso di disastro. I team di sicurezza informatica svolgono anche un ruolo chiave nell'assicurare che il progetto sia conforme ai requisiti normativi pertinenti, come quelli stabiliti in DORA, che impone rigorosi standard di sicurezza per i sistemi ICT delle istituzioni finanziarie.

5.2.3 Funzioni di Risk & Compliance

Le funzioni di Risk & Compliance delle organizzazioni clienti sono responsabili di assicurare che l'istituzione aderisca ai requisiti normativi e gestisca efficacemente i rischi operativi e in un progetto ICT, il loro ruolo è garantire che i nuovi sistemi e processi implementati siano allineati con il quadro di gestione del rischio più ampio dell'istituzione e soddisfino gli standard di conformità necessari.

Le funzioni di rischio e conformità collaborano sia con i team compliance delle società di consulenza sia con gli stakeholder interni del cliente per garantire che il progetto includa misure appropriate di gestione del rischio, come test di resilienza, segnalazione di incidenti e supervisione di terze parti. Forniscono anche input preziosi su come dovrebbe essere strutturato il progetto per minimizzare il rischio normativo e garantire che l'istituzione sia preparata per eventuali audit o ispezioni richieste da quadri come DORA.

5.2.4 Team ICT Operations

I team ICT Operations all'interno delle organizzazioni dei clienti sono responsabili della supervisione delle attività quotidiane dell'istituzione, compresi i suoi sistemi ICT. Nel contesto di un progetto ICT, il loro ruolo è garantire che il progetto non interrompa le operazioni in corso dell'istituzione e che i nuovi sistemi implementati migliorino, piuttosto che ostacolino, l'efficienza operativa.

I team ICT Operations lavorano a stretto contatto con l'ufficio di gestione dei progetti delle società di consulenza per garantire che il progetto venga eseguito senza intoppi e che eventuali interruzioni siano ridotte al minimo. Forniscono inoltre contributi preziosi su come i nuovi sistemi possano essere integrati nei processi esistenti dell'istituzione, aiutando a garantire una transizione senza soluzione di continuità una volta completato il progetto.

5.3 Quadro di raccolta e analisi dei dati

Il quadro di raccolta e analisi dei dati è fondamentale per sviluppare un sistema ICT completo, efficiente e resiliente, conforme ai quadri normativi come la DORA. All'interno delle istituzioni finanziarie, l'allineamento dei sistemi ICT agli standard normativi richiede un esame approfondito dell'attuale panorama tecnologico, un'analisi rigorosa delle lacune di conformità e un piano di implementazione ben strutturato in grado di apportare i cambiamenti necessari. Inoltre, la gestione efficace di questo processo attraverso le pratiche di project management è fondamentale per garantire l'adozione tempestiva e di successo di nuove tecnologie e processi.

Questa sezione delinea quattro aree chiave che costituiscono la spina dorsale del processo di raccolta e analisi dei dati per allineare i sistemi ICT ai requisiti normativi: Valutazione dell'infrastruttura ICT,

analisi dei gap normativi, approccio alla pianificazione dell'implementazione e gestione del progetto di implementazione.

5.3.1 Valutazione dell'infrastruttura ICT

Il punto di partenza per garantire la conformità normativa di un istituto finanziario è una valutazione dettagliata della sua attuale infrastruttura ICT. Il panorama dei sistemi ICT è in genere una complessa rete di sistemi legacy, soluzioni basate su cloud e integrazioni di terze parti che consentono il regolare funzionamento di servizi quali l'elaborazione delle transazioni, la gestione dei dati, il monitoraggio dei rischi e la gestione delle relazioni con i clienti. La comprensione di questo panorama è essenziale non solo per mantenere l'efficienza operativa, ma anche per identificare le vulnerabilità che potrebbero rappresentare un rischio ai sensi dei severi requisiti di resilienza ICT di DORA.

Una valutazione del panorama dei sistemi ICT comporta la mappatura di tutti gli asset tecnologici di un'organizzazione. Ciò include un inventario dettagliato di hardware, software, database e reti che costituiscono l'ambiente ICT di base. La valutazione si estende anche all'identificazione dei sistemi ICT critici che supportano le funzioni di core business, come i sistemi di pagamento, le piattaforme di trading, i sistemi necessari all'emissione di polizze e la gestione dei dati dei clienti. Comprendendo i componenti chiave e l'architettura di questi sistemi, gli istituti possono posizionarsi meglio per soddisfare gli standard di resilienza operativa imposti dalla DORA.

Oltre alla semplice catalogazione degli asset ICT, la valutazione deve considerare anche i punti di integrazione dei sistemi. Si tratta di punti critici in cui sistemi diversi interagiscono e scambiano dati. Ad esempio, gli istituti finanziari spesso si affidano a più fornitori di servizi terzi per funzioni quali l'archiviazione in cloud, l'analisi dei rischi e il monitoraggio della cybersecurity. Comprendere il flusso di dati tra questi sistemi, sia interni che esterni, è fondamentale per garantire che operino in modo continuo e sicuro.

Una valutazione efficace dell'infrastruttura ICT deve anche valutare le prestazioni e la scalabilità dei sistemi attuali. Con l'evoluzione dei requisiti normativi e delle esigenze aziendali, la capacità dell'infrastruttura ICT di un istituto di adattarsi e scalare diventa un fattore critico per mantenere la resilienza operativa. I sistemi che non sono in grado di gestire i crescenti volumi di dati, l'aumento della velocità delle transazioni o l'evoluzione delle minacce informatiche possono non essere conformi e mettere a rischio l'organizzazione. Per questo motivo, un'analisi dei colli di bottiglia delle prestazioni, della capacità del sistema e della scalabilità futura è essenziale per identificare le aree di miglioramento.

5.3.2 Analisi dei gap normativi

Una volta mappato e valutato il panorama dei sistemi ICT, il passo successivo è quello di condurre un'analisi dei gap normativi. Questo processo prevede la valutazione dei sistemi, dei processi e delle pratiche attuali rispetto ai requisiti normativi specifici delineati dalla DORA. L'obiettivo di un'analisi delle lacune è quello di individuare le aree in cui l'infrastruttura ICT e le misure di resilienza operativa dell'istituto non sono all'altezza degli standard normativi e di identificare i passi necessari per colmare tali lacune.

Una componente fondamentale di questa analisi è l'identificazione dei requisiti normativi che si applicano ai diversi aspetti dell'infrastruttura ICT. In base alla DORA, gli istituti finanziari sono tenuti a soddisfare linee guida rigorose sulla gestione del rischio ICT, sui test di resilienza operativa digitale, sulla gestione del rischio di terzi e sulla segnalazione degli incidenti. Ognuna di queste aree ha criteri specifici che devono essere rispettati e l'analisi delle lacune aiuta a evidenziare dove le pratiche attuali si discostano da questi standard.

Ad esempio, la DORA impone la creazione di solidi quadri di gestione del rischio ICT che consentano agli istituti di identificare, valutare e mitigare i rischi nel loro ambiente tecnologico. A tal proposito un'analisi delle carenze normative dovrebbe valutare se i processi di gestione del rischio attualmente in atto sono sufficienti e se sono necessari miglioramenti ed analogamente, la DORA richiede test periodici di resilienza dei sistemi ICT critici per garantire che possano resistere e riprendersi da attacchi informatici, guasti al sistema e altre interruzioni. L'analisi delle lacune dovrebbe esaminare se tali test sono già in corso e se soddisfano la frequenza, la portata e il rigore richiesti dalla normativa.

Inoltre, l'analisi dovrebbe concentrarsi sulla capacità dell'istituto di gestire i rischi di terzi. Le istituzioni finanziarie si affidano sempre più spesso a fornitori di servizi terzi per le funzioni ICT chiave e il DORA richiede che questi rapporti siano gestiti in modo da garantire la resilienza operativa. L'analisi delle lacune dovrebbe valutare se le attuali pratiche di gestione dei fornitori, i contratti e gli accordi sui livelli di servizio sono allineati con i requisiti del DORA.

Conducendo un'approfondita analisi delle lacune normative, gli istituti finanziari possono creare una chiara tabella di marcia per affrontare le carenze dei loro sistemi ICT. Questa tabella di marcia è fondamentale per la fase successiva del processo: la pianificazione e l'implementazione delle modifiche necessarie per raggiungere la conformità.

5.3.3 Approccio alla pianificazione dell'implementazione

Dopo aver individuato le lacune nella conformità normativa, gli istituti finanziari devono sviluppare un piano di implementazione completo per colmare tali carenze e allineare i propri sistemi ICT ai requisiti

della DORA e tale pianificazione non riguarda solo le modifiche tecniche necessarie per aggiornare o sostituire i sistemi obsoleti, ma anche i più ampi cambiamenti organizzativi necessari per supportare un ambiente ICT più resiliente, sicuro e conforme.

Un piano di implementazione di successo inizia con la definizione delle priorità delle lacune identificate. Alcune carenze possono rappresentare un rischio maggiore per l'organizzazione rispetto ad altre, soprattutto se riguardano sistemi o funzioni critiche. Ad esempio, le lacune nelle difese di sicurezza informatica o nei protocolli di verifica della resilienza dovrebbero essere affrontate con la massima priorità, dato il potenziale impatto degli attacchi informatici sulla resilienza operativa dell'istituto. Al contrario, questioni meno critiche, come piccole inefficienze nella gestione di terzi, possono essere affrontate in fasi successive del processo di implementazione.

Il passo successivo consiste nello sviluppare un piano d'azione dettagliato per affrontare ogni lacuna. Ciò comporta l'identificazione delle modifiche specifiche da apportare, sia che si tratti di aggiornare i sistemi esistenti, di implementare nuove tecnologie o di rivedere le politiche e le procedure interne. Il piano d'azione dovrebbe anche includere una tempistica per l'implementazione, delineando le tappe fondamentali e le scadenze per ogni fase del progetto. Data la complessità della maggior parte dell'infrastruttura ICT, potrebbe essere necessario suddividere il processo di implementazione in progetti più piccoli e gestibili, da completare in sequenza o in parallelo.

Per ogni progetto, è importante stabilire dei KPIs di progetto. Queste metriche aiuteranno a monitorare i progressi e a garantire che i cambiamenti implementati stiano ottenendo i risultati desiderati. I KPIs più comuni per i progetti ICT includono il tempo di attività del sistema, la riduzione degli incidenti, il miglioramento dei tempi di risposta e la maggiore soddisfazione degli utenti. Per i progetti di conformità normativa, per misurare il successo si possono utilizzare anche altri parametri, come i risultati degli audit, il numero di violazioni normative e la tempestività dei rapporti.

Una comunicazione efficace e il coinvolgimento degli stakeholder sono fondamentali anche durante la fase di implementazione. Gli stakeholder di tutta l'organizzazione, tra cui la direzione ICT, la compliance, la gestione del rischio e l'alta dirigenza, devono essere tenuti al corrente dei progressi compiuti e delle potenziali sfide che potrebbero sorgere. Aggiornamenti regolari, rapporti sullo stato di avanzamento e cicli di feedback aiutano a mantenere lo slancio e a garantire che il progetto rimanga in linea.

5.3.4 Gestione della fase di implementazione

Un approccio ben strutturato alla gestione del progetto è essenziale per garantire il successo dell'implementazione delle modifiche necessarie per diventare conformi al DORA. La gestione del

progetto di implementazione prevede la supervisione dell'esecuzione del piano d'azione, il coordinamento delle risorse, la gestione delle tempistiche e la garanzia che tutti i compiti vengano portati a termine in modo tempestivo ed efficiente.

Il primo passo nella gestione del progetto di implementazione è stabilire una struttura di governance del progetto. Ciò include l'assegnazione di ruoli e responsabilità per i membri chiave del team, come i project manager, i responsabili tecnici e i responsabili della compliance. Una chiara struttura di governance aiuta a garantire l'efficienza dei processi decisionali e la responsabilità per ogni aspetto del progetto.

Successivamente, il team di progetto deve sviluppare un piano di progetto dettagliato che includa compiti specifici, tappe e scadenze per ogni fase del processo di implementazione. Questo piano deve anche tenere conto dei potenziali rischi e delle sfide che possono sorgere durante il progetto, come i ritardi nell'acquisto di nuove tecnologie o i problemi con i contratti dei fornitori. Anticipando queste sfide e sviluppando piani di emergenza, il team di progetto può ridurre al minimo le interruzioni e mantenere il progetto nei tempi previsti.

Uno dei componenti chiave della gestione dei progetti è la gestione delle risorse. Si tratta di garantire la disponibilità del personale, della tecnologia e delle risorse finanziarie necessarie per portare a termine il progetto. In alcuni casi, ciò può richiedere l'assunzione di personale aggiuntivo o di consulenti esterni con competenze specialistiche in aree quali la cybersecurity o la conformità normativa. Può anche comportare l'allocazione di budget per nuovi investimenti tecnologici, come servizi cloud, strumenti di test di resilienza o software di monitoraggio della conformità.

Durante l'intero processo di implementazione, il project manager deve mantenere una stretta sorveglianza dei progressi e delle prestazioni. Ciò comporta la revisione regolare dei rapporti sullo stato del progetto, il monitoraggio degli indicatori chiave di prestazione (KPIs) e la risoluzione di eventuali problemi. Nei casi in cui il progetto sia in ritardo rispetto alla tabella di marcia o si trovi di fronte a ostacoli imprevisti, il project manager deve intervenire rapidamente per mitigare questi problemi e rimettere il progetto in carreggiata.

Infine, una volta completato il progetto di implementazione, è importante condurre una revisione post-implementazione. Si tratta di valutare il successo del progetto rispetto alle metriche di successo predefinite e di identificare le aree di miglioramento rimanenti. La revisione dovrebbe anche catturare le lesson learned, che possono essere utilizzate per migliorare i futuri progetti ICT o gli sforzi di conformità normativa.

Seguendo un approccio strutturato alla gestione dei progetti, gli istituti finanziari possono assicurarsi di colmare con successo le lacune normative identificate durante il processo di valutazione, aggiornare

i propri sistemi ICT per soddisfare i requisiti della DORA e mantenere la resilienza operativa a lungo termine.

6 BPMN in Ambito DORA ICT Project Management

6.1 Gestione del Progetto di Adempimento al Regolamento DORA in Ambito ICT

Il seguente diagramma BPMN, l'obiettivo principale è la gestione delle Attività di Progetto di Adempimento al Regolamento DORA in Ambito ICT. Le attività coinvolte includono tipicamente:

- **Analisi della Situazione As-Is**: Gap Analysis rispetto alle richieste imposte dal Regolamento DORA in Ambito ICT;
- **Definizione e Pianificazione Attività di Progetto**: Messa a terra del piano di iniziative necessarie a portare la società ad essere DORA Compliant;
- **Approvazione della Pianificazione**: Processo approvativo nei diversi livelli di Alta Direzione come supervisori della progettualità, cruciale per la società;
- **Svolgimento delle Attività di Adeguamento**: Adeguamento delle strutture ICT, dei processi operativi e formazione del personale;
- **Reporting e Monitoraggio delle Attività**: Controllo delle operazioni e reporting settimanale e mensile dello Stato di Avanzamento dei Lavori.

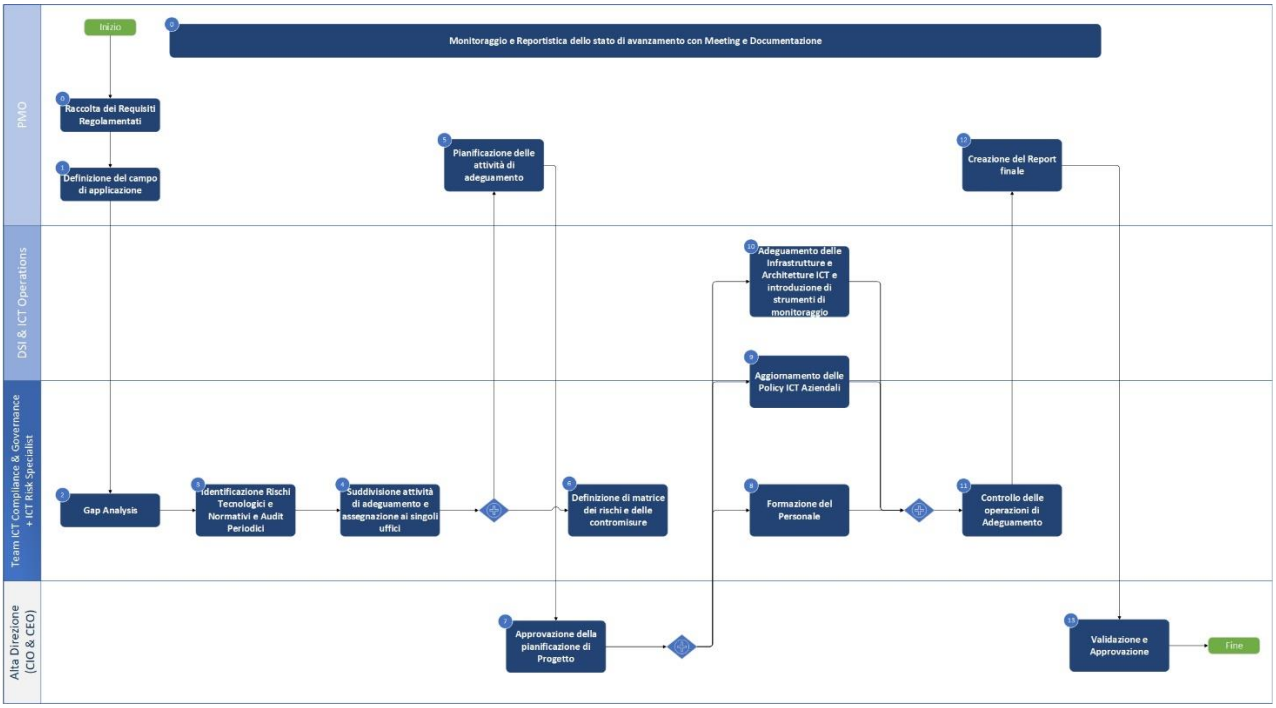

Figura 1 – Gestione del Progetto di Adeguamento al Regolamento DORA in Ambito ICT

6.2 Processo di Gestione degli Incidenti ICT

Il seguente diagramma BPMN si concentra sull'identificazione, la risposta e il recupero dagli incidenti, specificamente all'interno del quadro ICT. I compiti tipici includono:

- **Rilevazione degli Incidenti** Identificare un problema, come una violazione della sicurezza, un guasto del sistema o una corruzione dei dati;
- **Classificazione degli Incidenti**: Classificare la gravità dell'incidente in base al potenziale impatto sulle operazioni e sulla conformità normativa;
- **Risposta agli Incidenti**: Attivare i team necessari (ICT, sicurezza, rischio e conformità) per rispondere al problema e mitigare ulteriori danni;
- **Processo di Recupero**: Avviare le procedure di recupero, ripristinando la funzionalità del sistema e l'integrità dei dati;
- **Segnalazione degli Incidenti**: Segnalare l'incidente ai soggetti interni, alle autorità di regolamentazione (come richiesto da DORA) e ai clienti interessati, se applicabile.

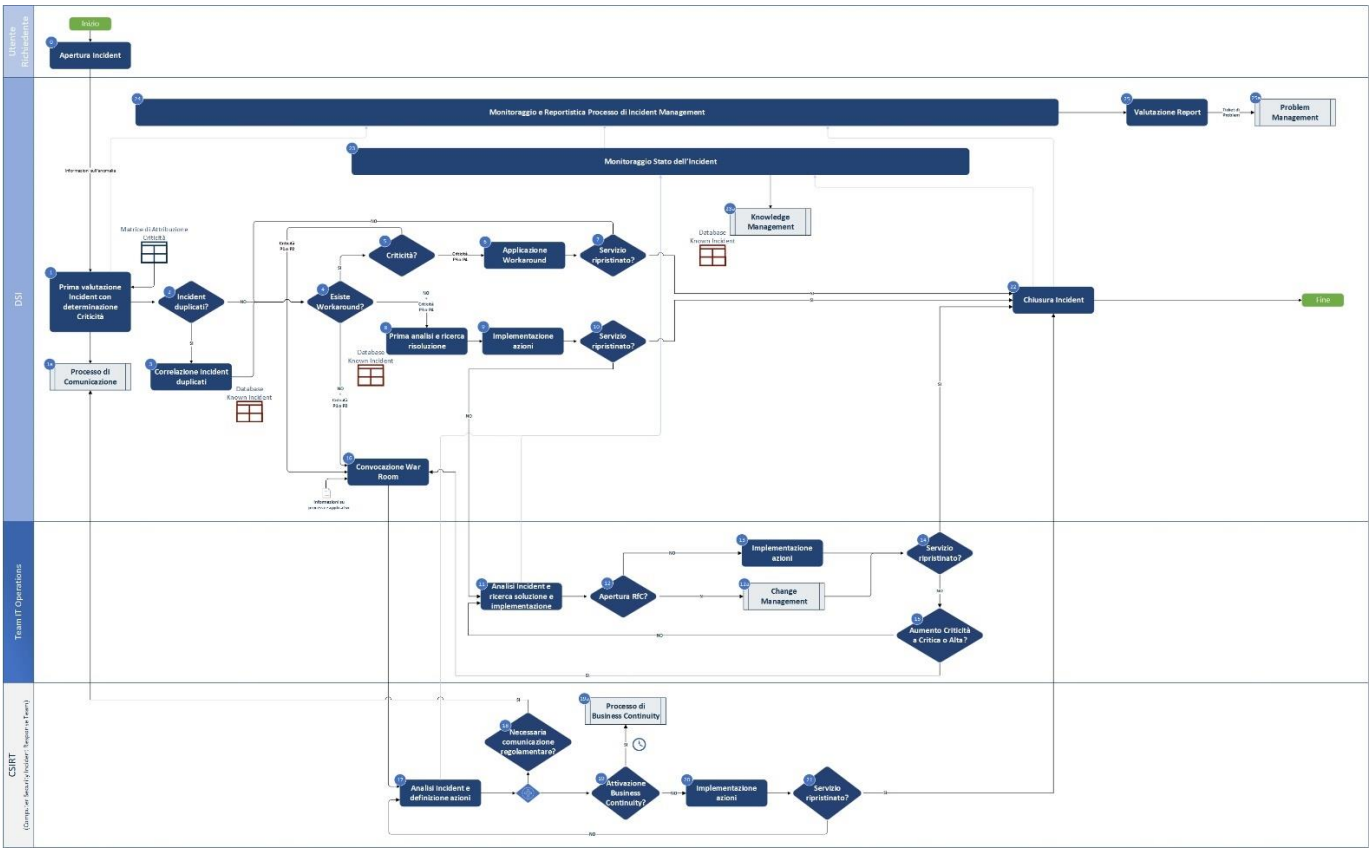

Figura 2 – Processo di Gestione degli Incidenti ICT

6.3 Gestione del Rischio ICT di Terze Parti

Il seguente diagramma BPMN evidenzia i processi relativi alla valutazione e alla gestione dei rischi posti dai servizi ICT di terze parti. Le attività includono:

- **Valutazione del Fornitore**: Valutare i fornitori terzi prima dell'integrazione, valutando le loro capacità, la conformità alle normative (come DORA) e l'esposizione al rischio;
- **Monitoraggio del Livello di Servizio**: Monitorare continuamente le prestazioni della terza parte per garantire la conformità ai livelli di servizio concordati;
- **Revisione del Rischio della Terza Parte**: Condurre valutazioni regolari del rischio per valutare eventuali cambiamenti nel profilo di rischio del fornitore terzo;
- **Gestione degli Incidenti della Terza Parte**: Se un servizio di terze parti subisce un incidente, assicurarsi che vengano prese le adeguate misure di escalation e mitigazione, in coordinamento con il fornitore;
- **Reportistica della Terza Parte**: Fornire report ai team interni di gestione del rischio e conformità, e condividere le informazioni rilevanti con le autorità di regolamentazione, se necessario.

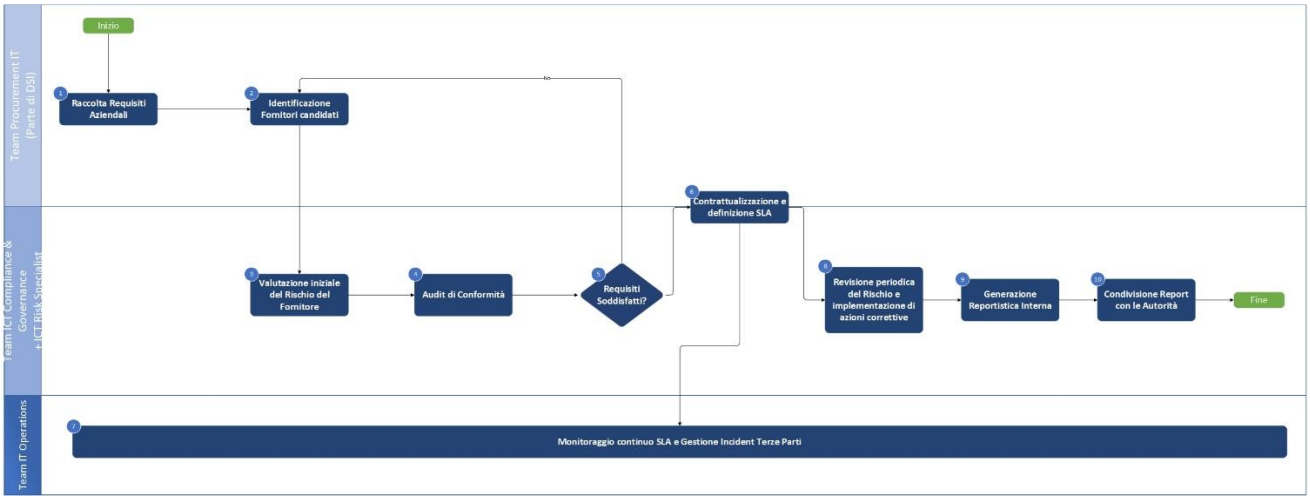

Figura 3 – Gestione del Rischio ICT di Terze Parti

6.4 Gestione delle Modifiche ICT – ICT Change Management

Il seguente diagramma BPMN si concentra sulla gestione e sull'implementazione delle modifiche ai sistemi e ai processi ICT. Le principali task includono:

1. **Presentazione della Richiesta di Modifica**: Proporre modifiche all'infrastruttura ICT, come aggiornamenti di sistema, nuove integrazioni o ottimizzazioni dei processi;

2. **Valutazione dell'Impatto**: Valutare l'impatto potenziale della modifica proposta sui sistemi esistenti, sui flussi di dati e sulla conformità normativa;
3. **Approvazione della Modifica**: Ottenere l'approvazione dagli stakeholder rilevanti, come i team ICT, di conformità e gestione dei rischi;
4. **Implementazione della Modifica**: Distribuire la modifica approvata, assicurandosi che sia adeguatamente testata e validata prima della messa in produzione;
5. **Revisione Post-Implementazione**: Esaminare l'efficacia della modifica e assicurarsi che non vi siano impatti negativi sulle operazioni del sistema o sullo stato di conformità.

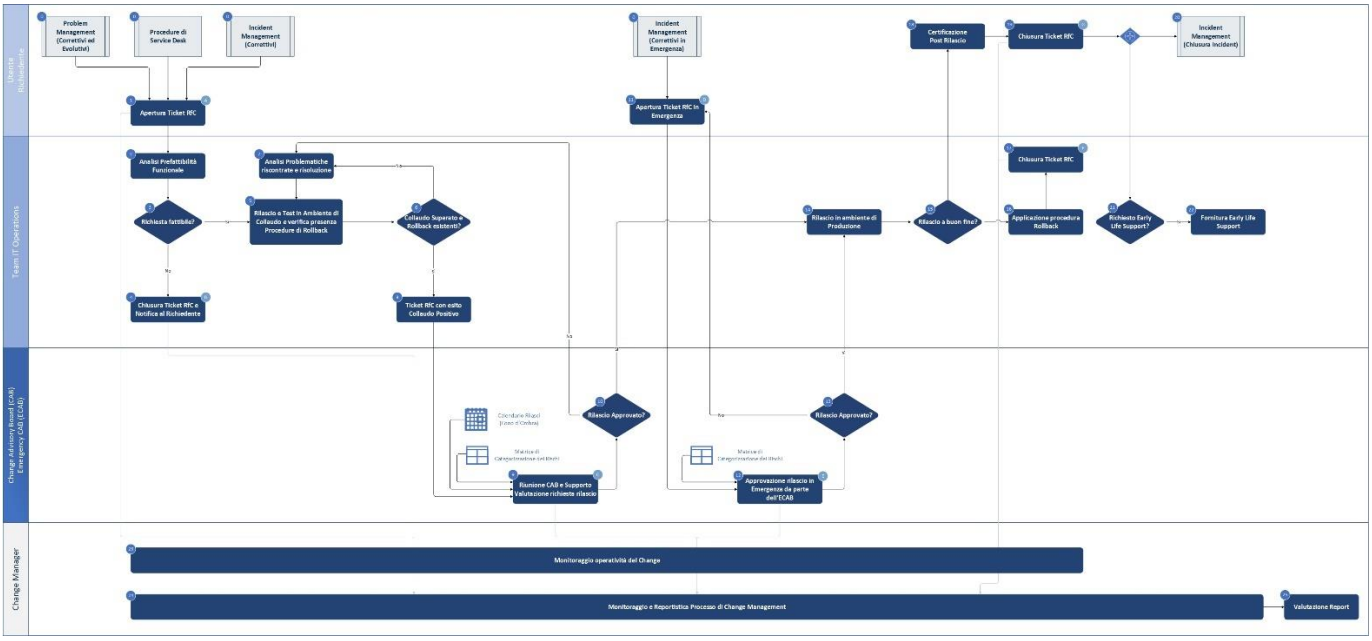

Figura 4 – Gestione delle Modifiche ICT – ICT Change Management

7 Analisi del Modello Attuale

Nel contesto della gestione dei progetti ICT e dei framework di compliance, in particolare nel settore dei servizi finanziari, una valutazione approfondita del modello attuale rivela sia punti di forza sostanziali sia aree di miglioramento. Il framework, progettato per garantire sia l'efficienza operativa sia l'allineamento normativo, incarna principi cruciali per navigare nei complessi scenari digitali e normativi. Tuttavia, come con qualsiasi sistema complesso, ci sono opportunità per affinare i processi e migliorare l'efficacia complessiva del framework.

7.1 Punti di forza

Uno dei punti di forza più degni di nota dell'attuale framework di gestione dei progetti ICT e conformità è la sua copertura completa del ciclo di vita del progetto. Dall'inizio alla pianificazione, esecuzione, monitoraggio e chiusura, il modello è progettato per affrontare ogni fase con rigore. Questo approccio approfondito garantisce che nulla venga trascurato, in particolare per quanto riguarda la conformità normativa, che è una preoccupazione pressante nei servizi finanziari a causa di regolamenti come il DORA. L'inclusione di quadri di gestione del rischio ICT, meccanismi di segnalazione degli incidenti e pratiche di gestione del rischio di terze parti garantisce che il quadro copra non solo gli aspetti tecnici della consegna del progetto, ma anche le esigenze di governance e compliance del settore.

Questa completezza è strettamente legata al coinvolgimento degli stakeholders, che è un altro punto di forza notevole. Nei servizi finanziari, dove il controllo normativo è intenso e le conseguenze di un fallimento sono gravi, la necessità di un coinvolgimento attivo da parte dei vari stakeholders interni ed esterni è fondamentale. Il modello attuale incorpora un coinvolgimento strutturato con i principali stakeholders, inclusi i team IT, i dipartimenti di compliance, i responsabili del ICT Risk e gli auditor esterni. Favorendo la collaborazione tra questi gruppi, il framework garantisce che vengano considerate prospettive diverse, il che aiuta a mitigare i rischi e garantisce l'allineamento sia con gli obiettivi aziendali sia con i requisiti normativi.

Inoltre, il focus del modello sull'integrazione dei processi è particolarmente prezioso nel panorama ICT moderno. La capacità di integrare senza soluzione di continuità i processi relativi alla governance ICT, alla gestione del rischio e alla compliance crea un sistema che non solo funziona in modo efficiente ma risponde anche dinamicamente alle sfide emergenti. Ad esempio, l'integrazione dei test di resilienza operativa digitale all'interno del framework consente l'identificazione e la mitigazione proattiva dei rischi, garantendo che i sistemi siano robusti contro le potenziali interruzioni.

Inoltre, l'allineamento con i quadri normativi come DORA, PSD2 e GDPR è un punto di forza cruciale. Il framework garantisce che le istituzioni finanziarie non solo possano soddisfare, ma anche superare i

requisiti normativi, il che non solo protegge da multe e sanzioni, ma migliora anche la reputazione dell'organizzazione in termini di compliance e resilienza. Gli aggiornamenti regolari per incorporare i cambiamenti nel panorama normativo dimostrano l'adattabilità del modello, permettendogli di rimanere rilevante ed efficace anche quando emergono nuove sfide normative.

7.2 Aree di miglioramento

Sebbene l'attuale framework dimostri significativi punti di forza, ci sono anche aree in cui il miglioramento potrebbe portare a una maggiore efficienza e valore. Una delle aree più rilevanti è l'efficienza dei processi. Nonostante la natura completa del modello, spesso ci sono inefficienze nell'esecuzione dei compiti, in particolare nella transizione tra le diverse fasi del progetto. Ad esempio, durante il passaggio dalla fase di pianificazione a quella di esecuzione, possono verificarsi ritardi dovuti a disallineamenti tra l'ufficio di project management e i team tecnici. Questi colli di bottiglia sono spesso aggravati da complessi processi di approvazione che, sebbene necessari per la compliance, a volte possono rallentare i progressi del progetto e ridurre l'efficienza complessiva. Snellire queste transizioni senza compromettere la governance e la compliance è un'area critica per il miglioramento.

Ottimizzazione dello stack tecnologico è un'altra area in cui il modello potrebbe evolversi. Man mano che le istituzioni finanziarie attraversano la trasformazione digitale dipendono sempre più da infrastrutture ICT sofisticate che devono essere ottimizzate per gestire grandi volumi di dati, supportare analisi avanzate e fornire capacità di reportistica in tempo reale. Tuttavia, in molti casi, i sistemi legacy svolgono ancora un ruolo significativo nei progetti ICT, creando sfide di integrazione e inefficienze. Modernizzare lo stack tecnologico per supportare meglio la gestione del flusso di dati, l'automazione e i test di resilienza digitale è cruciale per migliorare sia i risultati dei progetti sia la compliance normativa. Inoltre, sfruttare tecnologie emergenti come l'IA e il machine learning per la valutazione predittiva del rischio potrebbe trasformare la capacità del framework di gestire i rischi operativi e di conformità.

Un'altra area di miglioramento è la gestione della qualità dei dati. Nei servizi finanziari, dove l'integrità dei dati è fondamentale sia per il successo operativo sia per la conformità, gestire la qualità dei dati attraverso sistemi disparati è una sfida significativa. I processi attuali di validazione e assicurazione della qualità dei dati spesso comportano controlli manuali, che sono dispendiosi in termini di tempo e soggetti a errori. L'implementazione di strumenti di governance automatizzata dei dati potrebbe migliorare l'accuratezza e la tempestività della reportistica dei dati, migliorando così sia l'efficienza dei progetti ICT che la qualità delle sottomissioni regolamentari. Affrontando i problemi di qualità dei dati

alla fonte – durante l'inserimento, l'integrazione e l'elaborazione dei dati – il framework può ridurre la probabilità di violazioni della conformità e interruzioni operative.

Assegnazione delle risorse presenta anche un'opportunità critica di miglioramento. I progetti ICT nei servizi finanziari richiedono spesso competenze specializzate in aree come la cybersecurity, la compliance normativa e il cloud computing. Tuttavia, le risorse non sono sempre allocate in modo ottimale, risultando in team sovraccarichi o lacune nelle competenze durante le fasi chiave del progetto. Implementare un sistema di gestione delle risorse più dinamico che adatti le allocazioni in base alle necessità del progetto e alle valutazioni dei rischi migliorerebbe la consegna complessiva del progetto. Inoltre, sviluppare team interdisciplinari con sia competenze tecniche sia normative potrebbe ridurre la dipendenza dai consulenti esterni, abbassando così i costi e migliorando la conservazione delle conoscenze all'interno dell'organizzazione.

La gestione delle relazioni con terze parti potrebbe anche essere migliorata, in particolare per quanto riguarda la gestione del rischio poiché le istituzioni finanziarie dipendono sempre più da fornitori di servizi terzi per il cloud computing, la cybersecurity e la gestione dei dati e i rischi associati a queste relazioni diventano più pronunciati. Il modello attuale tiene conto del rischio dei fornitori terzi, ma i processi per monitorare e valutare questi rischi potrebbero essere più robusti e in particolare, il monitoraggio continuo delle prestazioni dei fornitori terzi rispetto ai livelli di servizio concordati e agli standard di conformità potrebbe essere migliorato attraverso l'uso di strumenti di monitoraggio avanzati e sistemi di reportistica automatizzati. Questo non solo migliorerebbe i tempi di risposta ai potenziali problemi, ma fornirebbe anche una visione più trasparente del rischio dei servizi forniti da società terze in tutta l'organizzazione.

Infine, l’analisi delle lacune normative è un'area in cui si possono apportare miglioramenti e sebbene l'attuale quadro sia progettato per garantire la conformità alle normative esistenti, la natura dinamica dei cambiamenti normativi nel settore dei servizi finanziari richiede che le istituzioni siano proattive nell'identificare potenziali lacune. Implementare un sistema di monitoraggio normativo più lungimirante, supportato da analisi predittive, potrebbe quindi aiutare le istituzioni a rimanere al passo con i cambiamenti normativi e garantire che i loro processi di gestione dei progetti ICT siano sempre allineati con i requisiti più recenti.

8 Best Practices di Settore

La gestione efficace dei progetti ICT nel settore dei Financial Services dipende dall'adozione e dall'integrazione delle migliori pratiche del settore. Queste pratiche sono progettate non solo per garantire che i progetti siano consegnati in tempo e nel rispetto del budget stanziato, ma anche per mantenere una rigorosa compliance ai requisiti normativi e minimizzare i rischi. Sfruttando framework e metodologie ben consolidati, le istituzioni finanziarie possono navigare meglio nel complesso panorama ICT. Di seguito, esploriamo alcuni dei più efficaci framework di governance ICT, metodologie di gestione dei progetti, approcci di gestione del rischio e strumenti di monitoraggio della conformità attualmente utilizzati in questo settore.

8.1 Framework di ICT Governance

I framework di ICT governance forniscono la base strutturale per la gestione delle risorse tecnologiche e dei processi all'interno di un'organizzazione. Nel settore dei servizi finanziari, dove i sistemi ICT sono profondamente intrecciati con la conformità normativa e la gestione del rischio, questi framework giocano un ruolo cruciale nell'assicurare l'allineamento tra le iniziative tecnologiche e gli obiettivi aziendali più ampi.

Uno dei framework più noti in questo ambito è COBIT (Control Objectives for Information and Related Technologies). Sviluppato originariamente da ISACA, COBIT offre un quadro completo per la gestione e il governo dell'ICT aziendale. L'enfasi di COBIT sia sulla governance sia sulla gestione lo rende particolarmente adatto per i servizi finanziari, in quanto assicura che gli investimenti in ICT supportino gli obiettivi aziendali affrontando al contempo rischi e obblighi normativi. Tale framework aiuta le istituzioni ad allineare la loro strategia ICT con i requisiti normativi come DORA, GDPR, e PSD2, fornendo linee guida chiare per la gestione del rischio tecnologico, il mantenimento dell'integrità dei dati, e la garanzia della resilienza operativa.

Un altro framework chiave è l'ITIL (Information Technology Infrastructure Library), che si concentra sull'ottimizzazione della gestione dei servizi ICT. L'approccio del ciclo di vita di ITIL alla gestione dei servizi IC

T si allinea con la necessità nei servizi finanziari di garantire un'integrazione senza soluzione di continuità dei sistemi ICT con le operazioni aziendali. I processi ITIL, che includono la gestione degli incidenti, la gestione dei problemi e la gestione dei livelli di servizio, sono inestimabili per mantenere la resilienza e l'affidabilità dei servizi ICT, in particolare in un ambiente in cui i tempi di inattività o le interruzioni possono avere impatti finanziari e reputazionali significativi.

Oltre a COBIT e ITIL, ISO/IEC 27001 è ampiamente adottato per il suo focus sulla gestione della sicurezza delle informazioni. Data la sensibilità dei dati gestiti dalle istituzioni finanziarie, l'implementazione degli standard ISO 27001 garantisce che siano in atto misure appropriate per proteggere i beni informativi dalle minacce, che provengano da attacchi informatici, violazioni dei dati o fallimenti operativi. Il framework aiuta le istituzioni a implementare un robusto sistema di gestione della sicurezza delle informazioni (ISMS), che è fondamentale per la compliance normativa e la mitigazione del rischio.

8.2 Metodologie di Gestione dei Progetti

La gestione dei progetti nei servizi finanziari, in particolare per i progetti ICT, richiede un approccio strutturato che possa bilanciare la necessità di agilità con l'imperativo di una rigorosa governance e controllo. La scelta della metodologia di gestione dei progetti può influenzare significativamente il successo di un progetto ICT, influenzando come vengono gestiti i rischi, come vengono allocati le risorse e come vengono monitorati i deliverable.

Una delle metodologie più ampiamente adottate nel settore è Waterfall, un approccio lineare e sequenziale alla gestione dei progetti. Nel Waterfall, i progetti avanzano attraverso fasi distinte – raccolta dei requisiti, progettazione, implementazione, test e distribuzione – ognuna delle quali deve essere completata prima che inizi la fase successiva. L'approccio Waterfall è preferito per i progetti in cui i requisiti sono ben definiti dall'inizio e difficilmente cambiano, rendendolo particolarmente adatto per i progetti che sono fortemente orientati alla compliance, come l'implementazione di nuovi sistemi di reportistica normativa o aggiornamenti alle infrastrutture ICT critiche. La sua natura strutturata garantisce una documentazione e un test approfonditi, essenziali per l'auditabilità e l'approvazione normativa.

Tuttavia, le metodologie Agile hanno guadagnato trazione negli ultimi anni, in particolare per progetti che coinvolgono lo sviluppo software o dove la flessibilità è fondamentale. In contrasto con la struttura rigida di Waterfall, Agile enfatizza lo sviluppo iterativo, dove i team di progetto consegnano piccoli pezzi funzionali del progetto in brevi cicli incrementali (chiamati sprint). Agile consente una maggiore adattabilità, rendendolo ideale per progetti in cui i requisiti possono evolversi nel tempo o dove il feedback degli stakeholder è cruciale per il successo. Nei servizi finanziari ICT, Agile è spesso impiegato per progetti legati alla trasformazione digitale, dove vengono integrate nuove tecnologie e l'istituzione deve rimanere reattiva ai cambiamenti normativi o di mercato emergenti.

La metodologia Scrum, un sottoinsieme di Agile, è stata ampiamente adottato per la sua capacità di gestire progetti software complessi. Il focus di Scrum sui team cross-funzionali e l'uso di cicli di sviluppo brevi e delimitati nel tempo lo rendono un modo efficace per gestire sia l'ambito del progetto che le

aspettative degli stakeholder in un ambiente dinamico. È particolarmente utile nella gestione dello sviluppo continuo e del deployment di sistemi ICT, come applicazioni di mobile banking o piattaforme rivolte ai clienti, dove i rapidi cicli di feedback e i miglioramenti incrementali sono essenziali.

8.3 Approcci di ICT Risk

Nel settore dei servizi finanziari, una gestione efficace del ICT Risk è fondamentale, dato l'alto rischio coinvolto nell'assicurare la resilienza operativa, la sicurezza dei dati e la conformità normativa. I progetti ICT, che spesso introducono nuove tecnologie e processi, sono intrinsecamente rischiosi. Pertanto, adottare approcci robusti di gestione del rischio è essenziale per garantire che questi progetti non espongano l'istituzione a rischi indebiti.

Uno degli approcci più ampiamente riconosciuti nella gestione del rischio è l'Enterprise Risk Management (ERM), che adotta una visione olistica dei rischi nell'intera organizzazione. Nel contesto dei progetti ICT, l'ERM garantisce che i rischi legati alla tecnologia, alle operazioni, alla conformità e alle minacce esterne siano identificati e gestiti proattivamente. Integrando la gestione del rischio nel quadro complessivo della governance del progetto, le istituzioni finanziarie possono assicurarsi che i rischi siano considerati in ogni fase del ciclo di vita del progetto, dalla pianificazione all'esecuzione e oltre.

Una tecnica specifica spesso impiegata nella gestione del rischio dei progetti ICT è il Registro dei Rischi, che fornisce un modo sistematico per documentare, valutare e prioritizzare i rischi sia operativi sia in ambito ICT. Mantenendo un registro dei rischi, i project manager possono tracciare i rischi nel tempo, assegnare responsabilità e sviluppare strategie di mitigazione. Ad esempio, i rischi legati ai fornitori terzi – come ritardi nella consegna del servizio o violazioni del contratto – possono essere identificati precocemente e gestiti attraverso l'implementazione di piani di contingency o un maggior controllo dei contratti.

L'analisi quantitativa dei rischi, come le simulazioni Monte Carlo o l'analisi degli alberi decisionali, è un'altra best practice per valutare l'impatto potenziale dei rischi sui progetti ICT. Questi metodi permettono alle istituzioni finanziarie di modellare la probabilità e la gravità potenziale dei rischi, consentendo decisioni più informate e una migliore allocazione delle risorse.

Inoltre, la gestione del rischio informatico è diventato un punto focale nei Financial Services, data la crescente frequenza e sofisticazione degli attacchi informatici. Framework come il Cybersecurity Framework del NIST aiutano le istituzioni a identificare, proteggere, rilevare, rispondere e recuperare dalle minacce informatiche. Dato il focus normativo sulla resilienza digitale, adottare un approccio

strutturato alla gestione del rischio informatico è essenziale sia per la compliance sia per la protezione dei dati finanziari sensibili.

8.4 Strumenti di Monitoraggio della Compliance

Garantire la conformità normativa continua è una sfida costante per le istituzioni finanziarie, in particolare man mano che gli ambienti normativi evolvono. Per affrontare questa sfida, le istituzioni hanno adottato una gamma di strumenti di monitoraggio della conformità che aiutano ad automatizzare e semplificare il processo di tracciamento, segnalazione e assicurazione dell'adesione agli standard normativi.

Uno degli strumenti più ampiamente utilizzati in questo ambito è il software GRC (Governance, Risk, and Compliance) che integra molteplici aspetti di governance, Risk Management e compliance in un'unica piattaforma. Consolidando queste funzioni, gli strumenti GRC permettono alle istituzioni finanziarie di mantenere una visibilità in tempo reale sulla loro posizione di conformità, garantendo che i requisiti normativi siano soddisfatti senza ritardi inutili o processi manuali. Questi strumenti offrono anche dashboard che consentono alla direzione di monitorare le metriche di conformità, valutare l'esposizione al rischio e rispondere ai problemi man mano che si presentano.

Un altro strumento importante è il RegTech (Regulatory Technology), una categoria di tecnologia che si concentra sull'aiutare le istituzioni finanziarie a soddisfare i requisiti di conformità attraverso l'automazione e l'analisi. Le soluzioni RegTech, come i sistemi di reportistica automatizzata e gli strumenti di monitoraggio delle transazioni in tempo reale, riducono il carico della conformità garantendo che i dati siano raccolti, elaborati e riportati in linea con i requisiti normativi. Nel contesto della gestione dei progetti ICT, gli strumenti RegTech sono spesso utilizzati per monitorare i cambiamenti del sistema, tracciare i flussi di dati e garantire che qualsiasi modifica all'infrastruttura ICT non comprometta la conformità normativa.

Infine, strumenti per il test della resilienza operativa digitale, come il penetration testing e le valutazioni delle vulnerabilità, sono fondamentali per garantire che i sistemi ICT rimangano conformi a regolamenti come DORA. Questi strumenti simulano attacchi o interruzioni reali per valutare la resilienza dei sistemi ICT, fornendo preziose informazioni su potenziali debolezze e aree di miglioramento. Testando regolarmente la resilienza dei loro sistemi, le istituzioni finanziarie possono non solo soddisfare i requisiti normativi, ma anche migliorare la loro capacità di resistere e riprendersi da attacchi informatici o guasti operativi.

L'adozione delle migliori pratiche del settore nella governance delle ICT, nella gestione dei progetti, nella gestione del rischio e nel monitoraggio della conformità è fondamentale per le istituzioni

finanziarie che mirano a navigare nelle complessità degli ambienti normativi moderni. Sfruttando framework consolidati come COBIT e ITIL, adottando metodologie Agile in combinazione con metodologie Waterfall, implementando approcci olistici alla gestione del rischio e utilizzando strumenti avanzati di monitoraggio della conformità, le istituzioni finanziarie possono garantire che i loro progetti ICT vengano consegnati con successo, mantenendo al contempo un forte focus sulla compliance normativa e sulla mitigazione del rischio. Queste pratiche non solo supportano l'efficienza operativa, ma posizionano anche le istituzioni per un successo a lungo termine in un mondo sempre più digitale e regolamentato.

9 Punti di miglioramento

Poiché le istituzioni finanziarie continuano a operare in un contesto normativo sempre più complesso, migliorare la gestione dei progetti ICT e allinearsi a quadri normativi come DORA è essenziale per mantenere la resilienza operativa. Le seguenti raccomandazioni affrontano aree chiave di ottimizzazione dei processi, miglioramento della tecnologia e misurazione delle prestazioni per migliorare l'efficacia complessiva della governance ICT e della gestione della conformità.

9.1 Ottimizzazione dei processi

La gestione efficace dei progetti è il pilastro delle iniziative ICT di successo ma ci sono sempre opportunità per migliorare l'efficienza, ridurre le ridondanze e garantire flussi di lavoro più fluidi. L'ottimizzazione dei processi comporta il perfezionamento dei passaggi coinvolti nella gestione dei progetti ICT per migliorare la velocità di consegna, l'allocazione delle risorse e la supervisione della conformità. Diverse strategie possono essere impiegate per raggiungere questi obiettivi.

In primo luogo, implementare l'automazione nelle attività di gestione dei progetti può ridurre significativamente i carichi di lavoro manuali ed eliminare l'errore umano. Strumenti come il software di gestione dei progetti che automatizzano le attività di routine, come la pianificazione, la rendicontazione dello stato e il monitoraggio dei rischi, possono liberare tempo prezioso per i project manager affinché possano concentrarsi su decisioni strategiche di livello superiore. Inoltre, automatizzare le attività legate alla conformità – come generare tracce di controllo o garantire l'integrità dei dati tra i sistemi – può assicurare che i requisiti normativi siano continuamente rispettati senza ritardi inutili.

In secondo luogo, adottare metodologie Agile può introdurre maggiore flessibilità e reattività nei processi di gestione dei progetti. Le pratiche Agile consentono uno sviluppo iterativo e un coinvolgimento regolare degli stakeholder, particolarmente vantaggioso nel settore dei servizi finanziari in rapida evoluzione. Invece di aderire rigidamente a modelli Waterfall sequenziali, Agile incoraggia un feedback continuo, assicurando che i progetti rimangano allineati con le esigenze aziendali, i cambiamenti normativi e i paesaggi tecnologici in evoluzione. Le revisioni e le retrospettive degli Sprint aiutano i team a identificare inefficienze di processo in tempo reale e a effettuare le regolazioni necessarie.

Terzo, focalizzandosi sulla collaborazione cross-funzionale all'interno dei progetti ICT è cruciale. La natura a compartimenti stagni di molte istituzioni finanziarie spesso porta a interruzioni della comunicazione e inefficienze nei processi. Promuovendo una collaborazione più forte tra i dipartimenti – particolarmente tra i team ICT, compliance e risk – le organizzazioni possono assicurarsi che gli

obiettivi del progetto siano allineati sin dall'inizio. Una comunicazione regolare attraverso workshop congiunti o dashboard di progetto integrate può aiutare a eliminare questi compartimenti, promuovendo un approccio più unificato alla gestione dei progetti ICT.

Infine, adottando i principi del Lean management può aiutare a semplificare i processi rimuovendo le attività che non aggiungono valore. Lean si concentra sul migliorare il flusso di valore eliminando gli sprechi – che si tratti di documentazione eccessiva, approvazioni non necessarie, o ritardi nel prendere decisioni. Esaminando l'intero ciclo di vita dei progetti ICT, le istituzioni finanziarie possono identificare e rimuovere inefficienze, riducendo così il tempo di immissione sul mercato e migliorando i risultati dei progetti.

9.2 Roadmap per il Potenziamento della Tecnologia

Nel contesto dei requisiti normativi come DORA, garantire che lo stack tecnologico sia robusto, scalabile e conforme è essenziale per la resilienza operativa. La seguente roadmap delinea i passaggi chiave per aggiornare l'infrastruttura tecnologica di un'istituzione per soddisfare i requisiti di resilienza ICT di DORA migliorando al contempo la capacità tecnologica complessiva.

- **Valutazione dello Stack Tecnologico Attuale**: Prima di implementare qualsiasi miglioramento, è necessaria una valutazione approfondita della tecnologia esistente. Ciò comporta la mappatura di tutti i sistemi ICT critici, infrastrutture e software attualmente in uso e l'identificazione di eventuali sistemi legacy che possono rappresentare rischi per la compliance o la continuità operativa. L'obiettivo è valutare i sistemi attuali rispetto ai requisiti di DORA per la resilienza operativa, concentrandosi su aree come la sicurezza dei dati, la disponibilità e la scalabilità.

- **Migrazione a Soluzioni Basate su Cloud**: La tecnologia cloud offre significativi vantaggi in termini di scalabilità, sicurezza e resilienza. Le istituzioni finanziarie dovrebbero dare priorità alla transizione a soluzioni basate su cloud ove appropriato. I servizi cloud offrono vantaggi intrinseci, come il Disaster Recovery, gli aggiornamenti automatici e i protocolli di sicurezza avanzati. Tuttavia, è importante garantire che i fornitori di servizi cloud soddisfino standard di sicurezza e conformità rigorosi, e le istituzioni devono stabilire solidi accordi sul livello del servizio (SLA) e meccanismi di monitoraggio per i fornitori terzi per rispettare i requisiti di gestione del rischio ICT di terze parti di DORA.

- **Integrazione di Analisi Avanzata e AI**: Per migliorare sia l'efficienza operativa sia la conformità normativa, le istituzioni finanziarie dovrebbero investire in analisi avanzata e intelligenza artificiale (AI). Gli strumenti guidati dall'AI possono migliorare la gestione del rischio rilevando

automaticamente le anomalie, identificando le potenziali minacce e offrendo intuizioni predittive sulle prestazioni dei sistemi ICT. Inoltre, l'AI e il machine learning possono ottimizzare i processi di reportistica normativa analizzando grandi dataset in tempo reale, garantendo che le istituzioni rimangano conformi ai requisiti di reportistica normativa e gestione degli incidenti secondo il DORA.

- **Rafforzare le misure di cybersecurity**: DORA pone un forte accento sulla resilienza operativa, in particolare in relazione alla cybersecurity. Per soddisfare queste esigenze, le istituzioni devono investire in soluzioni di cybersecurity di nuova generazione. Questo include l'implementazione di protocolli di sicurezza multilivello, come la crittografia, l'autenticazione multi-fattore e i sistemi di rilevamento delle intrusioni. Le istituzioni dovrebbero anche considerare l'implementazione di architetture zero-trust, il che presuppone che ogni richiesta, sia interna sia esterna alla rete, debba essere verificata prima di concedere l'accesso. Questi miglioramenti garantiscono che i sistemi siano protetti contro le minacce interne ed esterne.
- **Stabilire il Monitoraggio e la Reportistica in Tempo Reale**: Infine, integrare sistemi di monitoraggio e reportistica in tempo reale sarà essenziale per garantire la conformità continua ai requisiti di segnalazione degli incidenti ICT di DORA. Le istituzioni dovrebbero implementare strumenti che forniscano una visibilità continua delle prestazioni del sistema, identificando potenziali interruzioni prima che influenzino le operazioni. Questi sistemi di monitoraggio dovrebbero essere in grado di generare report in tempo reale per fornire aggiornamenti immediati ai regolatori durante gli incidenti, garantendo la compliance alle rigorose linee guida di gestione degli incidenti di DORA.

9.3 Metriche di Successo e KPI

Per garantire che la gestione dei progetti ICT e le iniziative di conformità stiano ottenendo i risultati desiderati, è essenziale definire e monitorare i Key Performance Indicators (KPIs). Queste metriche forniscono un modo tangibile per misurare il successo, garantire la responsabilità e identificare aree di ulteriore miglioramento. I seguenti KPIs sono fondamentali per tracciare il successo dei progetti ICT e degli sforzi di conformità normativa all'interno delle istituzioni finanziarie.

- **Tempo di Consegna del Progetto**: Questo KPI traccia il tempo impiegato per completare un progetto ICT dall'inizio alla consegna. Monitorando i tempi di consegna dei progetti, le istituzioni possono valutare se i loro processi di gestione dei progetti sono efficienti o se si verificano ritardi in determinate fasi. Concentrarsi sulla riduzione dei tempi di consegna – senza compromettere la qualità – indica una riuscita ottimizzazione dei processi di gestione dei progetti.

- **Variazione del Budget**: La varianza del budget misura la differenza tra il budget stimato del progetto e le spese effettive. Questo KPI aiuta i project manager a garantire che i progetti ICT siano realizzati entro le risorse finanziarie allocate, il che è particolarmente importante in ambienti altamente regolamentati dove i superamenti dei costi possono portare a sanzioni per non conformità o vincoli di risorse. Monitorare la varianza del budget può anche rivelare inefficienze nell'allocazione delle risorse e negli acquisti.

- **Frequenza degli incidenti di conformità**: La frequenza degli incidenti di conformità – come le violazioni dei requisiti normativi o gli audit falliti – funge da KPI critico per misurare l'efficacia dei processi di gestione della conformità di un'istituzione. Una bassa frequenza di incidenti di conformità indica che i processi e i miglioramenti tecnologici dell'istituzione stanno mitigando con successo i rischi e mantenendo l'allineamento normativo. Al contrario, una frequenza crescente di incidenti suggerisce la necessità di ulteriori miglioramenti nella gestione dei rischi o nell'ottimizzazione dei processi.

- **Tempo di inattività del sistema e disponibilità**: Monitorare il tempo di inattività del sistema fornisce informazioni sulla resilienza dell'infrastruttura ICT dell'istituzione. Sotto DORA, la resilienza operativa è fondamentale e ridurre al minimo il tempo di inattività del sistema è un indicatore chiave di successo. Questo KPI misura il tempo in cui i sistemi ICT critici non sono disponibili ed evidenzia le aree in cui le capacità di ridondanza o failover potrebbero dover essere potenziate.

- **Punteggi di Valutazione del Rischio delle Parti Terze**: Poiché i fornitori di ICT di terze parti svolgono un ruolo sempre più importante nei servizi finanziari, monitorare i risultati delle valutazioni del rischio delle parti terze è essenziale. Questo KPI valuta la performance dei fornitori nel soddisfare gli obblighi contrattuali, aderire ai protocolli di sicurezza e garantire la continuità del servizio. Un punteggio elevato nelle valutazioni del rischio delle parti terze indica che l'istituzione ha processi di gestione dei fornitori solidi e sta mitigando con successo i rischi relativi, in linea con i requisiti di DORA.

- **Punteggi di Soddisfazione del Cliente**: Sebbene spesso trascurata negli sforzi di compliance normativa, la soddisfazione del cliente rimane un indicatore chiave del successo complessivo dei progetti ICT. Man mano che le istituzioni implementano nuovi sistemi o miglioramenti, monitorare il feedback dei clienti attraverso sondaggi di soddisfazione o Net Promoter Score (NPS) può fornire preziose informazioni sull'impatto di questi cambiamenti sull'esperienza dell'utente finale. Alti punteggi di soddisfazione del cliente suggeriscono che i sistemi ICT dell'istituzione sono facili da usare, affidabili e rispondenti alle esigenze dei clienti.

- **Tempo di risposta agli incidenti**: Il tempo di risposta agli incidenti misura il tempo impiegato per rilevare, rispondere e risolvere gli incidenti ICT. Una risposta rapida agli incidenti è fondamentale per ridurre al minimo l'impatto delle interruzioni sulle operazioni aziendali e garantire la conformità con i requisiti di segnalazione degli incidenti di DORA. Questo KPI aiuta le istituzioni a valutare l'efficacia dei loro processi di gestione degli incidenti e a identificare le aree di miglioramento nei protocolli di risposta.

Migliorare la gestione dei progetti ICT e la conformità normativa nei servizi finanziari richiede un approccio olistico che combini ottimizzazione dei processi, aggiornamenti tecnologici e un focus su risultati misurabili. Adottando processi di gestione dei progetti più efficienti, aggiornando lo stack tecnologico per migliorare la resilienza e la conformità, e monitorando il successo attraverso KPI chiari, le istituzioni finanziarie possono posizionarsi per avere successo in un ambiente sempre più regolamentato e guidato dalla tecnologia. Queste raccomandazioni non solo garantiscono l'allineamento con i requisiti normativi come DORA, ma supportano anche l'efficienza operativa a lungo termine, la mitigazione del rischio e la soddisfazione del cliente.

10 Conclusione

Nel settore dinamico e altamente regolamentato dei servizi finanziari, l'integrazione di solide strutture di gestione dei progetti ICT e strategie di conformità normativa è essenziale per mantenere la resilienza operativa, soprattutto alla luce del Digital Operational Resilience Act (DORA). La ricerca presentata in questa tesi fornisce approfondimenti completi su come le istituzioni finanziarie possono allineare le loro strategie ICT con i requisiti di DORA, snellire i processi di gestione dei progetti e garantire la stabilità tecnologica a lungo termine. Questa conclusione riassume i principali risultati, fornisce raccomandazioni pratiche per l'implementazione e identifica le future opportunità di ricerca che potrebbero ulteriormente migliorare l'intersezione tra il mondo ICT e la compliance normativa.

10.1 Sommario dei principali risultati

L'obiettivo principale di questa tesi è esplorare come le istituzioni finanziarie possano migliorare la gestione dei progetti ICT e i quadri di conformità per allinearsi meglio con DORA. I risultati chiave si concentrano sui seguenti aspetti:

- **Punti di forza dei modelli attuali**: I quadri di gestione dei progetti ICT e i sistemi di conformità esistenti all'interno delle istituzioni finanziarie sono completi, con protocolli ben consolidati per il coinvolgimento delle parti interessate e l'allineamento normativo. Molte istituzioni hanno già integrato team cross-funzionali, combinando funzioni ICT, compliance e gestione del rischio per garantire che i progetti restino sulla buona strada e all'interno dei limiti normativi.

- **Lacune nell'efficienza dei processi**: Nonostante i punti di forza, ci sono chiare opportunità per migliorare l'efficienza nei processi di gestione dei progetti ICT. Queste lacune spesso derivano dalla dipendenza da processi manuali e obsoleti che potrebbero essere automatizzati, portando a flussi di lavoro più snelli, tempi di consegna dei progetti più rapidi e una migliore allocazione delle risorse.

- **Ottimizzazione dello stack tecnologico**: La ricerca sottolinea la necessità per le istituzioni finanziarie di modernizzare la propria infrastruttura tecnologica, in particolare migrando a sistemi basati su cloud, integrando AI e analisi, e rafforzando le misure di sicurezza informatica. L'aggiornamento dello stack tecnologico non riguarda solo il rispetto dei requisiti di resilienza ICT di DORA, ma anche la preparazione dell'istituzione ai rischi tecnologici in evoluzione.

- **Monitoraggio e reportistica della compliance**: L'introduzione di strumenti di monitoraggio della conformità in tempo reale e analisi dei dati avanzate è essenziale per le istituzioni finanziarie che cercano di stare al passo con i requisiti di segnalazione regolamentare sempre

più rigorosi. Le istituzioni che investono in soluzioni di monitoraggio avanzate sono meglio attrezzate per gestire proattivamente i rischi di compliance e assicurare un allineamento continuo con gli standard regolamentari.

- **Raccomandazioni per il miglioramento dei processi e delle tecnologie**: La tesi fornisce diverse raccomandazioni pratiche per migliorare sia i processi di gestione dei progetti che l'infrastruttura tecnologica. Queste includono l'adozione di metodologie Agile, pratiche di gestione snella e strumenti di compliance automatizzati, così come l'implementazione di servizi cloud e protocolli avanzati di cybersecurity.

Nel complesso, i risultati indicano che le istituzioni finanziarie sono ben posizionate per soddisfare i requisiti di DORA, ma devono concentrarsi su aree specifiche di miglioramento per garantire un'efficienza ottimale e una compliance a lungo termine.

10.2 Considerazioni sull'implementazione

Sebbene le raccomandazioni fornite siano complete, le realtà pratiche dell'implementazione di questi cambiamenti devono essere attentamente considerate dalle istituzioni finanziarie. Un'implementazione di successo richiederà un approccio strategico e graduale, supportato da una pianificazione accurata e una solida comprensione delle sfide specifiche che ogni organizzazione deve affrontare. Le seguenti considerazioni sono critiche per un'implementazione efficace:

- **Allocazione delle risorse e budgeting**: Una delle sfide più significative nell'implementazione delle modifiche proposte è il costo associato all'aggiornamento dell'infrastruttura tecnologica e all'automazione dei processi. Le istituzioni finanziarie devono valutare attentamente le loro strategie di allocazione delle risorse, assicurandosi che il budget necessario sia destinato alla transizione ai servizi cloud, agli strumenti di compliance basati sull'intelligenza artificiale e alle misure avanzate di cybersecurity. La pianificazione del budget per questi cambiamenti richiederà un equilibrio tra i costi immediati e i risparmi a lungo termine derivanti dal miglioramento dell'efficienza e dalla riduzione dei rischi.

- **Change Management**: L'implementazione di nuovi processi e tecnologie spesso incontra resistenze all'interno dell'organizzazione. Devono essere impiegate strategie di Change Management per garantire transizioni fluide, inclusi piani di comunicazione, programmi di formazione e supporto continuo per il personale mentre si adatta ai nuovi sistemi. Il coinvolgimento della leadership è essenziale per guidare il cambiamento culturale, incoraggiando i team ad abbracciare le nuove tecnologie e processi come opportunità di miglioramento piuttosto che come ostacoli.

- **Allineamento Normativo e Gestione del Rischio**: Sebbene le raccomandazioni siano strettamente allineate con DORA, le istituzioni devono anche considerare come questi cambiamenti si inseriscono in altri quadri normativi, come il GDPR (Regolamento Generale sulla Protezione dei Dati) e il PSD2 (Direttiva sui Servizi di Pagamento II). Assicurare che questi vari requisiti normativi siano armonizzati nei sistemi ICT è cruciale per evitare lacune o sovrapposizioni nella compliance.

- **Gestione dei Fornitori e Rischio Terze Parti**: La migrazione ai servizi cloud o il ricorso a fornitori terzi per soluzioni ICT comporta rischi che devono essere gestiti con attenzione. Le istituzioni finanziarie devono sviluppare strategie robuste di gestione dei fornitori, includendo accordi dettagliati sul livello di servizio (SLA) e il monitoraggio continuo delle prestazioni dei fornitori terzi. Questo è particolarmente importante sotto DORA, che sottolinea la necessità per le istituzioni di gestire proattivamente i rischi ICT dei fornitori terzi.

- **Implementazione Graduale e Test Pilota**: Si raccomanda un approccio graduale all'implementazione per minimizzare le interruzioni alle operazioni in corso. Le istituzioni dovrebbero iniziare con programmi pilota per specifici dipartimenti o processi, permettendo test e aggiustamenti in tempo reale prima di estendere i cambiamenti a tutta l'organizzazione. Questo approccio aiuta a identificare potenziali problemi in anticipo, assicurando che le implementazioni su larga scala siano più fluide ed efficienti.

- **Formazione e Sviluppo dei Dipendenti**: Man mano che le istituzioni finanziarie adottano tecnologie più avanzate e strategie di ottimizzazione dei processi, è essenziale fornire una formazione continua ai dipendenti. I dipendenti devono essere dotati delle competenze necessarie per affrontare efficacemente questi cambiamenti sia che si tratti di padroneggiare le metodologie Agile sia che si tratti di capire come utilizzare strumenti di conformità basati su AI. Investire in programmi di formazione non solo faciliterà una implementazione più fluida, ma migliorerà anche la produttività complessiva della forza lavoro.

L'incorporazione di queste considerazioni di implementazione in un piano comprensivo aiuterà le istituzioni finanziarie a superare le potenziali barriere, assicurando che i miglioramenti proposti nella gestione dei progetti ICT e nella conformità normativa possano essere realizzati efficacemente.

10.3 Aree di Ricerca Future

Man mano che il settore dei Financial Services continua ad evolversi emergeranno nuove sfide e opportunità, in particolare nel contesto dei quadri normativi come DORA e il panorama tecnologico in

continua evoluzione. La ricerca futura dovrebbe concentrarsi su diverse aree chiave per rafforzare ulteriormente la gestione dei progetti ICT e le capacità di conformità:

- **Tendenze Normative Emergenti** : Le istituzioni finanziarie devono anticipare i cambiamenti normativi imminenti che potrebbero influenzare le operazioni ICT. La ricerca futura dovrebbe concentrarsi sulle normative previste, in particolare quelle relative alla privacy dei dati, alla sicurezza informatica e alla governance dell'IA. Poiché i governi e i regolatori rispondono ai progressi tecnologici e ai nuovi rischi, sarà fondamentale comprendere come queste normative possano influenzare la gestione dei progetti ICT e le strategie di conformità.

- **Il Ruolo dell'Intelligenza Artificiale nella Conformità**: Con la crescente diffusione delle tecnologie AI, il loro ruolo nella compliance normativa si espanderà. La ricerca futura dovrebbe esplorare come l'AI possa essere sfruttata per automatizzare compiti complessi di conformità, come il monitoraggio in tempo reale, la previsione dei rischi e la rendicontazione normativa. La ricerca in questo settore potrebbe fornire preziose intuizioni su come l'AI possa essere integrata nei sistemi ICT esistenti senza compromettere l'integrità normativa.

- **Blockchain e Tecnologie di Registro Distribuito**: La tecnologia blockchain ha il potenziale per rivoluzionare la gestione dei progetti ICT e la conformità, in particolare in aree come l'integrità dei dati, la trasparenza e la tracciabilità. Esplorare come la blockchain possa essere utilizzata per migliorare la sicurezza, automatizzare la gestione dei contratti e semplificare la rendicontazione normativa potrebbe fornire significativi benefici per le istituzioni finanziarie. La ricerca sulle potenziali applicazioni della blockchain nella gestione della conformità è ancora nelle prime fasi, ma questo è un settore con notevole promessa per future innovazioni.

- **Cybersecurity nella Post-Quantum Era**: Con lo sviluppo del calcolo quantistico, i protocolli di cybersecurity tradizionali potrebbero diventare obsoleti, presentando rischi significativi per le istituzioni finanziarie. La ricerca futura dovrebbe concentrarsi su come le istituzioni possono prepararsi a questo cambiamento, esplorando il potenziale della crittografia resistente ai quanti e altre misure avanzate di sicurezza. Man mano che i quadri normativi evolvono per affrontare questi rischi emergenti, le istituzioni dovranno rimanere al passo per garantire la conformità continua.

- **Impatto del Lavoro a Distanza sulla Resilienza delle ICT**: Il passaggio al lavoro a distanza, accelerato dalla pandemia globale, ha introdotto nuove sfide per la gestione dei progetti ICT e la conformità. È necessaria una ricerca sugli effetti a lungo termine del lavoro a distanza sull'infrastruttura ICT, il coinvolgimento dei dipendenti e la sicurezza informatica per comprendere come le istituzioni possano mantenere la resilienza operativa in questo nuovo

contesto. Questo sarà particolarmente importante per garantire che le politiche di lavoro a distanza siano allineate ai requisiti normativi come DORA.

- **Sovranità dei dati e conformità transfrontaliera**: Man mano che le istituzioni finanziarie espandono le loro operazioni globali devono navigare tra complesse leggi sulla sovranità dei dati che variano a seconda della regione. La ricerca futura dovrebbe concentrarsi su come le istituzioni possano gestire i flussi di dati transfrontalieri garantendo al contempo la conformità con le normative locali e internazionali. Questo comporterà la comprensione delle sfumature delle leggi sulla privacy dei dati, come il GDPR nell'area UE, e la loro interazione con i quadri di governance ICT nelle diverse giurisdizioni.

- **Sostenibilità e Green ICT**: Man mano che le preoccupazioni ambientali diventano più rilevanti, le ricerche future dovrebbero esplorare il ruolo delle pratiche ICT sostenibili nei servizi finanziari. Questo include investigare come le istituzioni possano ridurre la loro impronta di carbonio tramite data center efficienti dal punto di vista energetico, servizi cloud e tecnologie verdi. La ricerca in questo ambito potrebbe anche esaminare come gli obiettivi di sostenibilità possano essere integrati nei framework di gestione dei progetti ICT, allineandosi con le più ampie iniziative di responsabilità sociale d'impresa (Corporate Social Responsibility - CSR).

In conclusione, i risultati di questa tesi dimostrano che le istituzioni finanziarie hanno compiuto significativi progressi nell'allineare la gestione dei progetti ICT e i quadri di conformità ai requisiti normativi, come DORA. Tuttavia, ci sono ancora opportunità di miglioramento, in particolare nelle aree dell'efficienza dei processi, dell'ottimizzazione tecnologica e del monitoraggio della conformità. Adottando le raccomandazioni delineate in questo documento, come l'automazione dei processi, le metodologie Agile, la migrazione al cloud e le misure avanzate di cybersecurity, le istituzioni finanziarie possono garantire che i loro sistemi ICT siano resilienti, efficienti e pienamente conformi agli standard normativi.

Guardando al futuro, le istituzioni finanziarie devono rimanere agili e reattive alle tendenze regolamentari emergenti e ai progressi tecnologici. Investendo in ricerca e sviluppo continuo, le istituzioni possono continuare a migliorare i loro framework di governance ICT, assicurandosi di rimanere competitive in un ambiente sempre più digitale e regolamentato. L'integrazione di AI, blockchain e tecnologie resistenti ai quanti, insieme a un focus sulla sostenibilità, giocherà un ruolo critico nel plasmare il futuro della gestione dei progetti ICT e della conformità nel settore dei servizi finanziari.

Bibliografia e Sitografia

Massimo Messina, Ph.D. – Riflessioni sulla conformità al Digital Operational Resilience Act (DORA)

Autorità Bancaria Europea (EBA) – Informazioni ufficiali su DORA e aggiornamenti normativi.
https://www.eba.europa.eu

European Commission - DORA Overview – Presentazione dettagliata di DORA e dei relativi RTS.
https://ec.europa.eu

Regulatory Standards Updates by ESAs – Documenti tecnici pubblicati dalle ESA.
https://www.eiopa.europa.eu

PwC Advisory – Risorse sulla conformità a DORA e gestione dei fornitori ICT.
https://www.pwc.com

FSI Insights – Articoli e report sulla resilienza digitale secondo DORA.
https://www.fsi.fitchsolutions.com

PMI (Project Management Institute) – Guide e best practice su metodologie di project management applicate a progetti ICT.
https://www.pmi.org

Agile Alliance – Approccio Agile nel settore ICT finanziario.
https://www.agilealliance.org

Scrum.org – Dettagli sull'adozione di Scrum per progetti ICT.
https://www.scrum.org

CIO.com – Articoli sulle tecniche di gestione di progetti ICT nel contesto finanziario.
https://www.cio.com

ITIL Framework (AXELOS) – Linee guida per l'integrazione dei processi ICT.
https://www.axelos.com

ISACA - COBIT Framework – Il sito ufficiale di ISACA, l'organizzazione che sviluppa il framework COBIT, offre risorse approfondite su COBIT 5 e COBIT 2019, incluse guide per la governance IT, strumenti di implementazione, e riferimenti per la conformità normativa.
https://www.isaca.org/resources/cobit

Ringraziamenti

Desidero innanzitutto esprimere la mia profonda gratitudine al Professor Alberto De Marco e al Professor Massimo Rebuglio, che mi hanno accompagnato con competenza, pazienza e determinazione lungo il percorso di redazione di questa tesi. La loro disponibilità e la loro guida sono state fondamentali per affrontare le sfide di questo lavoro, trasformandole in opportunità di crescita e approfondimento.

Un ringraziamento dal profondo del mio cuore va alla mia famiglia, che con il suo sostegno incondizionato, la sua fiducia e la sua vicinanza mi ha permesso di affrontare il mio percorso di Laurea Magistrale con serenità e motivazione. Nello specifico ringrazio mia madre e mio padre, Gemma e Guido, per l'appoggio, la pazienza e la volontà che hanno messo nello starmi accanto dai primi passi scolastici fino ad oggi. Ai miei due fratelli, Matteo e Paolo, perché sono le due persone che più stimo e che sono sempre state pronte ad essermi accanto sia nei momenti belli ma soprattutto nei momenti più duri della vita.

Una menzione va sicuramente ai compagni degli anni universitari e a tutti gli amici che ci sono sempre stati per qualunque cosa, sia scolastica sia di vita, per cui ho sempre avuto bisogno del loro appoggio.

Un grande ringraziamento ai colleghi del Team Tech FS Insurance di PwC Italia per essere stati fonte di ispirazione e di accompagnamento nella redazione della tesi e nell'apprendimento di tutto quello che è il contenuto della tesi ma soprattutto il bagaglio che mi porterò per sempre dalla mia prima esperienza lavorativa post-universitaria. Nello specifico ringrazio in ordine temporale Daniele e Luca per il supporto che mi hanno dato nell'imparare il più possibile e costruire un roseo presupposto alla mia futura carriera.

Dulcis in fundo, un grazie di cuore va alla mia compagna, Sarah, che è la principale motivazione che ho avuto per la conclusione di questa Laurea e per giungere a questo punto. Spero che tu per prima sia soddisfatta di me e di quello che ho fatto.

Grazie a tutti voi.

Those who never change their mind
never change anything
[WINSTON CHURCHILL]