

ETIF |



UNIVERSITÀ  
CATTOLICA  
del Sacro Cuore

Digital Compliance Hub

# RESEARCH INSIGHT

Report 2022

## INDICE DEI CONTENUTI

EXECUTIVE SUMMARY	3
1. CETIF RESEARCH SCENARIO	5
2. LA FUNZIONE COMPLIANCE	9
3. DIGITAL COMPLIANCE	17
BIBLIOGRAFIA	23
APPENDICE METODOLOGICA	25

### AUTORI:

Aurora Dania  
Chiara Frigerio  
Paolo Gatelli  
Giovanni Gatti  
Federico Rajola

Pubblicato nel mese di Dicembre 2022  
Copyright © Cetif. Tutti i diritti riservati.  
Ogni utilizzo o riproduzione anche parziale  
del presente documento non è consentita senza  
previa autorizzazione di Cetif.

**DISCLAIMER:** Cetif assicura che il presente documento è stato realizzato con la massima cura e con tutta la professionalità acquisita nel corso della sua lunga attività. Tuttavia, stante la pluralità delle fonti d'informazione e nonostante il meticoloso impegno da parte di Cetif affinché le informazioni contenute siano esatte al momento della pubblicazione, né Cetif né i suoi collaboratori possono promettere o garantire (anche nei confronti di terzi) esplicitamente o implicitamente l'esattezza, l'affidabilità o la completezza di tali informazioni. Cetif, pertanto, declina qualsiasi responsabilità per eventuali danni, di qualsiasi tipo, che possano derivare dall'uso delle informazioni contenute nel presente rapporto.

Si evidenzia, inoltre, che il presente rapporto potrebbe contenere proiezioni future o altre dichiarazioni in chiave prospettica, circostanza che comporta rischi e incertezze. Si avvisano pertanto i lettori che tali affermazioni sono solamente previsioni e potrebbero quindi discostarsi in modo considerevole dagli effettivi riscontri ed eventi futuri. Cetif declina fin d'ora qualsiasi responsabilità e garanzia in relazione a tali proiezioni.

## EXECUTIVE SUMMARY

La Funzione Compliance per il mercato finanziario costituisce un fondamentale presidio per la tutela del consumatore e il rispetto della buona governance. Il framework regolamentare è in continua evoluzione e la sfida per le istituzioni è divicolarsi e interpretare al meglio questo progresso. Indagando l'impatto che le principali normative hanno sui prodotti finanziari, in termini di controlli e KPI di compliance, il mercato ritiene che **GDPR e ESG sono le due normative più impattanti sull'operatività finanziaria**, mentre quelle meno impattanti per il momento sono ritenute l'Artificial Intelligence Act e la DORA.

Ogni singola istituzione finanziaria investe molto nei processi e nelle competenze di tale funzione che si caratterizza per alta complessità del ruolo e forte coordinamento con il business. Sul fronte del dimensionamento, **si osserva che il mercato finanziario impiega per compiti di Compliance in media 1,78 risorse ogni 100.000 clienti**, con una marcata differenza tra banche e imprese assicurative. Infatti, **le istituzioni bancarie impiegano 4 volte più risorse** delle imprese assicurative, a causa del perimetro più ampio che solitamente ricopre la Compliance bancaria per via delle normative AML. Gli occupati sono distribuiti abbastanza equamente per genere, anche se all'aumentare dell'inquadramento aumentano proporzionalmente le risorse di genere maschile. E' infatti ancora presente un **elevato gender gap per le posizioni dirigenziali**, con gli uomini che arrivano a rappresentare quasi il 75% del totale.

Le risorse di Compliance sono distribuite su ambiti e aree diverse. Inoltre, **la Compliance bancaria opera su aree più numerose di quelle della Compliance assicurativa**, sempre a causa del perimetro più ampio della Compliance bancaria, anche se vi sono anche risorse destinate ai mercati. Per le imprese assicurative una buona porzione di occupati lavora su temi legati alla POG e alla distribuzione assicurativa, così come sulla vigilanza, sui rapporti con le istituzioni e sulla *corporate governance*. Lo stesso settore è ancora molto legato a competenze tradizionali, essendo l'analisi normativa la competenza prevalente. Al contrario, nel settore bancario sebbene prevalgano competenze di verifica e il controllo, cominciano ad emergere anche competenze legate all'IT e al digitale.

In molti casi la funzione Compliance di una stessa istituzione svolge l'attività per più *legal entity* riferibili al medesimo gruppo. In particolare emerge come mediamente **la funzione Compliance svolga l'attività per 4,4 legal entity dello stesso gruppo bancario o assicurativo**. Ciò richiede che la Compliance sia organizzativamente ben strutturata, con un modello organizzativo ben formalizzato. In questo caso, le preferenze fra banche ed assicurazioni divergono, in quanto **il modello organizzativo che le imprese assicurative preferiscono è solitamente di tipo accentrato, mentre le banche convergono maggiormente su un modello di tipo misto**.

Ma la crescita dimensionale della funzione va di pari passo con la digitalizzazione dei processi. Come precedentemente descritto, la funzione Compliance si sta velocemente trasformando verso la Digital Compliance. Questo richiede la creazione di unità organizzative interne dedicate, come l'IT Compliance e l'unità organizzativa che si occupa di monitorare lo sviluppo di soluzioni di Digital compliance e gestione dati. In tal senso, **le banche risultano meglio strutturate, avendo previsto un modello formalizzato per entrambe le unità, al contrario delle imprese assicurative che prevalentemente non hanno un modello**

**formalizzato**.

L'implementazione delle nuove tecnologie per la Digital Compliance è un processo ancora in corso, su cui le istituzioni stanno concentrando i loro sforzi, soprattutto in termini di investimento. **Questo trend negli ultimi due anni risulta essere in costante crescita, con il settore bancario che avanza in maniera più sostenuta, rispetto al settore assicurativo**. In particolare, **nel 2022 il 40% di istituzioni bancarie e il 27% di imprese assicurative hanno previsto di investire oltre il 25% in più, rispetto all'anno precedente**. La differenza nel livello di investimenti si riflette sull'effettiva implementazione delle tecnologie, in quanto emerge che il settore bancario ha conseguentemente un livello di maturità più elevato, anche in termini di impatto di mercato, rispetto alle imprese assicurative. Quest'ultime hanno accumulato un gap tecnologico importante, che però sembrano intenzionate a colmare aumentando ulteriormente i propri investimenti. Inoltre, i progetti sviluppati in Digital Compliance si sono avvalsi principalmente di tecnologie di Business Intelligence e Reporting, piuttosto che di tecniche di Advanced Analytics, o di Artificial Intelligence,

**Lo stesso livello di investimento in Digital Compliance è fortemente correlato all'adozione di tecniche di Advanced Analytics**, ad evidenza dell'efficacia dell'investimento effettuato. In sostanza, **gli istituti che hanno effettuato maggiori investimenti in Digital Compliance negli ultimi anni, sono anche coloro i quali hanno un livello di maturità più elevato delle tecniche di Advanced**. Allo stesso modo, è stata rilevata un'elevata correlazione fra l'adozione dell'Advanced Analytics, rispetto al modello organizzativo di quell'unità interna alla Compliance che si occupa di monitorare lo sviluppo della stessa tecnologia. Le istituzioni con **un modello organizzativo formalizzato (in particolare accentrato) possiedono sono le stesse che possiedono un livello di adozione delle tecniche di Advanced Analytics più elevato**. Al contrario, le organizzazioni che non hanno modelli organizzativi formalizzati nello sviluppo di soluzioni di Advanced Analytics per la Compliance, riscontrano maggiori difficoltà nell'adozione della tecnologia.

Rispetto alle modalità di realizzazione dei progetti di Digital Compliance vi sono diverse soluzioni individuate dalle istituzioni. In particolare, il mercato sembra preferire le **partnership esterne con enti terzi, insieme a modalità di sviluppo interno (in house)**. Solo una parte marginale dei progetti è stata effettuata **attraverso la collaborazione con FinTech o RegTech (l'8% dei progetti)** degli ultimi 2 anni), soprattutto a causa di alcune criticità che hanno riguardato **l'integrazione con i sistemi legacy, la scarsa maturità tecnologica delle Fintech disponibili, ma anche la mancanza effettiva di prodotti pronti all'uso per la funzione Compliance**.

Per concludere, **il processo di trasformazione digitale per l'area Compliance è pienamente in corso**. Le istituzioni stanno adeguando in forma digitale i processi tradizionali, attraverso l'utilizzo delle nuove tecnologie, soprattutto di Advanced Analytics. Nonostante ciò, **persistono alcune criticità che rallentano o impediscono lo sviluppo dei progetti di Digital Compliance** e che il mercato deve particolarmente attenzionare, come: **il framework normativo in evoluzione e frammentato, la difficile collaborazione con le FinTech, nonché la difficoltà nell'assumere e ricercare personale adeguatamente formato** per le nuove necessità, apportate dalla rivoluzione digitale.



# 1. CETIF RESEARCH SCENARIO

## LE PRIORITÀ DELLA DIGITAL COMPLIANCE

**Il digitale nelle istituzioni finanziarie spinge anche la Compliance ad adottare tecniche e strumenti, per poter meglio mitigare i rischi di non conformità alle norme e di buona condotta**

### • IL DIGITALE E I CAMBIAMENTI ORGANIZZATIVI

Negli ultimi anni le istituzioni finanziarie si sono impegnate a favorire lo sviluppo delle nuove tecnologie all'interno delle proprie organizzazioni, sia in termini di investimento, che attraverso un cambiamento della cultura aziendale. **L'uso avanzato del dato e l'introduzione dell'AI, volti a supportare l'operatività tradizionale, spesso richiedono un cambiamento della cultura aziendale e delle strutture organizzative**, anche inserendo nuove figure professionali, formate internamente o esternamente. Pertanto, assume sempre più rilevanza la ricerca di un mix di skill e competenze, combinato ad un nuovo modo di lavorare più agile e collaborativo. Inoltre, nel raggiungimento dell'obiettivo di arrivare al dato come prodotto, spesso è richiesto l'impegno di tutta l'organizzazione, all'interno della quale ogni singolo lavoratore deve sentirsi ingaggiato e culturalmente pronto al cambiamento. In questo senso, un fattore di successo può rivelarsi la creazione di team variegati, con figure professionali completamente diverse l'una dall'altra, volte a superare eventuali problemi di mindset e di contrasto al cambiamento che possono sorgere.

### • SFIDE E RISCHI DELLA DIGITAL COMPLIANCE

Il cambiamento culturale ed organizzativo può rivelarsi fonte di valore, sebbene comporti **numerosi rischi** che la Compliance è chiamata a mitigare, **soprattutto attraverso la creazione di una funzione che fa uso di digitale (la Digital Compliance)**. Infatti, le numerose applicazioni di Intelligenza Artificiale e di Advanced Analytics, implementate in diversi processi, fanno emergere la necessità per il sistema di concentrarsi sui rischi ad essi connessi, tenendo in considerazione fattori fondamentali, quali: la **privacy**, essenziale nel trattamento dei dati (*GDPR compliant*); la **trasparenza**, (ad esempio nel caso di *«black box algorithm»*, in cui non si intuisce chiaramente la relazione fra le variabili e il loro impatto); **l'assenza di bias discriminatori** nell'analisi dei dati, sia in fase di input, che nel loro ciclo di vita; **un elevato standard di robustezza dei modelli; un'elevata accountability**. La stessa automatizzazione dei processi può comportare diversi rischi, ad esempio, l'utilizzo in termini prescrittivi di dati provenienti da processi automatizzati, può rivelarsi difficoltoso e rischioso, come nell'AFC. In questo caso, quando vengono segnalati degli alert, vi possono essere dei falsi positivi, per cui risulta difficile capire in capo a chi ricade la responsabilità dell'errore.

Una pratica ideale per utilizzare **l'Intelligenza Artificiale in ambito Compliance, al fine di gestire i rischi dell'AI stessa**, è una forte contestualizzazione dei dati, senza cui è difficile creare un buon modello di gestione, adeguato agli scopi della funzione. Inoltre, può rivelarsi fondamentale avere un'analisi dettagliata dei rischi legati all'uso del digitale, utilizzando una documentazione strutturata, ma non burocratizzata, in cui poter designare alcune linee guida che permettano di non perdere il fine ultimo dell'adozione dell'AI in Compliance, capire pienamente gli strumenti adottati e la direzione intrapresa. Questo processo può, inoltre, aiutare a creare maggiore sicurezza ed elevata affidabilità nei confronti di chi utilizza l'AI, in quanto il rischio è costantemente gestito e monitorato.

Persistono talvolta delle **criticità legate allo sviluppo di strumenti di Intelligenza Artificiale per la funzione Compliance**, tra queste vi è il tema del **rapporto con gli ICT**, i quali sono solitamente **più focalizzati sul business** (evoluzione software e sviluppo prodotti), che sui controlli di Compliance. Altre riguardano la **difficoltà di cambiare la cultura aziendale**, per orientarla alla centralità del dato; nonché **come utilizzare il dato stesso quale motore di incrocio fra funzioni di business diverse**.

### • LA DIGITAL COMPLIANCE PER L'EVOLUZIONE REGOLAMENTARE

**Lo sviluppo di un modello di digital Compliance**, con una funzione Compliance completamente permeata dall'Intelligenza Artificiale, oltre ad **aiutare** le istituzioni a mitigare i rischi legati all'uso delle nuove tecnologie e a velocizzare processi tradizionali, può fornire un grosso aiuto nel **divincolarsi nel mare magnum della complessità normativa**. L'interpretazione normativa, anche e soprattutto in ambito digitale, rappresenta oggi un tema di fondamentale importanza per la Compliance. In particolare, la continua evoluzione normativa fa sorgere l'esigenza di **traguardare una Smart Regulation**, intesa come un ripensamento dei processi regolatori, affinché siano maggiormente funzionali a una Compliance automatizzata.

L'evoluzione regolamentare è un fenomeno tuttora in atto. Il sistema sta cercando di disciplinare l'utilizzo delle nuove tecnologie in ambito finanziario, attraverso una serie di normative che sono entrate in vigore negli ultimi mesi, o lo saranno nei prossimi. Fra queste, **è in fase di negoziazione una proposta di regolamentazione dell'AI, l'Artificial Intelligence Act (AIA), che nasce da un'esigenza**, avvertita a livello europeo, come processo bottom-up, **derivante dalla crescita di applicazioni di AI** e che sarà fondamentale per assicurare il funzionamento degli strumenti di Intelligenza Artificiale. **Fino ad oggi, l'utilizzo dell'AI è invece stato regolamentato attraverso regole di soft law**: principi etici che devono guidare l'applicazione dell'intelligenza artificiale, affinché l'AI sia giusta, spiegabile e responsabile, sicura, trasparente e documentata. Talvolta, tali principi si sono rivelati essere però troppo generici. Da qui è sorta l'esigenza di affiancare una nuova regolamentazione, sebbene nuove norme potrebbero essere troppo o troppo poco stringenti.

L'entrata in vigore della normativa è ancora incerta, si ipotizza possa essere applicata a partire dal 2024. Certamente si conoscono **le linee guida che da un lato si basano su quelle legate all'Ethics for AI e dall'altro riguardano una suddivisione degli applicativi per livelli di rischio** (tra cui potrebbero essere ritenuti di livello inaccettabile il social scoring e il rilevamento biometrico). In particolare, potranno essere ritenuti rischiosi alcuni processi tradizionali, come ad esempio l'uso del metodo statistico, uno dei principi cardine per le imprese assicurative e che potrebbe complicare il business tradizionale. Pertanto, l'impatto dell'AIA sarà sicuramente forte sui sistemi ad alto rischio e la Compliance avrà un ruolo centrale, soprattutto in ambito assicurativo, dove sistemi e applicativi di AI possono inficiare il consumatore finale.

Come precedentemente descritto, le linee guida che fanno riferimento all'etica AI (Ethics for AI) saranno centrali all'interno dell'AI Act, legati soprattutto alla trasparenza nell'iter decisionale che deve essere tutelata e su cui la Compliance può giocare un ruolo determinante. **L'obiettivo** della normativa resta comunque quello di **promuovere l'innovazione, tutelando però i diritti fondamentali**, per una innovazione fortemente sostenibile. La sfida normativa sarà dunque, trovare una composizione ottimale del trade-off composto da tutela dei diritti e promozione dell'innovazione. Inoltre, tecnologicamente, **la nuova disciplina** sarà quanto più neutra possibile, con un **approccio risk-based e innovation friendly, cercando di evitare la overregulation**.

Prevedendo una grande invasività dell’AIA, può diventare **importante sfruttare le sandbox regolamentari per trovare degli spazi di collaborazione** anche con le autorità, **attraverso sperimentazioni ecosistemiche** che aiutino a comprendere e a valutare meglio i rischi legati ai sistemi di AI. Ad oggi, comunque, per il mercato è difficile misurare l’effettivo impatto dell’AIA sulla propria operatività finanziaria, data l’incertezza dei contenuti della normativa. Infatti per il momento le istituzioni sembrano porre maggiore attenzione verso altre normative, come la GDPR e l’ESG, ma anche la DORA, focalizzata sui processi di governance IT e che richiede una grande collaborazione con gli organi di vigilanza.

Infatti, analizzando l’impatto che le diverse normative avranno sui principali prodotti bancari e assicurativi, in termini di controlli e KPI di Compliance, **le normative GDPR e ESG, con la DORA, risultano essere quelle a impatto più elevato**, come mostrato dalla tabella in basso.

L’impatto in termini di controlli e KPI di compliance che le norme indicate avranno nel 2023 sui principali prodotti finanziari

PRODOTTI \ NORMATIVE	AIA	MICA	AML	DORA	GDPR	ESG
CONTO CORRENTE/CARTE	Alto	Basso	Basso	Basso	Basso	Basso
FINANZIAMENTI	Basso	Basso	Basso	Basso	Basso	Basso
SERVIZI DI INVESTIMENTO	Basso	Basso	Basso	Basso	Basso	Alto
POLIZZE AUTO	Basso	Basso	Basso	Basso	Basso	Basso
POLIZZE CASA	Basso	Basso	Basso	Basso	Basso	Basso
POLIZZE SALUTE	Basso	Basso	Basso	Basso	Basso	Basso
POLIZZE VITA	Basso	Basso	Basso	Basso	Basso	Alto

Legenda: ■ Basso Impatto ■ Alto Impatto

Dalla tabella emerge la **grande attenzione che il mercato ripone verso la regolamentazione ESG**, sebbene la definizione, a livello europeo, delle diverse componenti E-S-G non sia ancora pienamente compiuta. In particolare, **la disciplina che riguarda il regolamento della classificazione delle attività ESG** (Reg. UE 2020/852), la trasparenza e informativa sulla sostenibilità dei servizi finanziari, (Reg. UE 2019/2088), l’integrazione dei rischi di sostenibilità nella governance (Reg. Delegato UE 2021/1256) e il target market, la distribuzione dei prodotti e l’adeguatezza ai criteri ESG **risulta ancora oggi un processo aperto e in fieri**. In questo caso, la vigilanza di Compliance deve svolgere un ruolo pro-attivo che esuli dall’esclusiva

diffusione di regolamenti e che faciliti l’accesso del consumatore alle informazioni in materia ESG e il loro utilizzo. È necessario aumentare la literacy dei consumatori, promuovendo formazione finanziaria e sviluppando campagne di informazione, mirate alla diffusione della consapevolezza di temi ESG; allo stesso tempo, occorre insistere sulla formazione dei dipendenti che devono essere in grado di alfabetizzare, fare consulenza e dare supporto ai clienti, soprattutto nell’indicazione delle proprie preferenze.

• IL RICORSO AL REGHTECH

**Nella realizzazione di progetti digitali** per la funzione Compliance il mercato può scegliere solitamente di **sviluppare soluzioni internamente, o avvalendosi di partnership esterne** con enti terzi, anche se talvolta tale **collaborazione risulta complessa**, soprattutto se si fa riferimento al mondo **FinTech e RegTech**.

**Il RegTech consiste nell’utilizzo di tecniche per risolvere l’attuazione dei requisiti regolamentari di compliance in maniera più efficace ed efficiente.** Esistono tre tipologie diverse di RegTech: Compliance-RegTech, quando gli intermediari finanziari sviluppano e acquisiscono tecnologie per rendere più efficiente la compliance; Sup-RegTech, quando l’Autorità di Vigilanza fa uso di una determinata tecnologia per agevolare la compliance, la vigilanza e l’enforcement; Reg-RegTech, quando permette di tradurre le regole direttamente in *machine readable language*, in cui gli obblighi di legge sono scritti con linguaggio leggibile dal digitale. **La criticità principale** nell’utilizzo di questo strumento riguarda il **buon funzionamento del RegTech**, in quanto il rischio di bias può provocare problemi relativi all’aderenza e all’adeguatezza degli strumenti che sono spesso forniti in outsourcing. **Lo stesso outsourcing** è generatore di rischi, in quanto può comportare problemi di concentrazione di mercato, inducendo abusi di dipendenza economica da parte dei fornitori e **facendo sorgere problemi di regulatory capture** (sia per la vigilanza, sia per i vigilati) e **di monitoring**. Inoltre, spesso c’è il rischio di dover avviare un’attività che non si limiti ad un controllo di secondo livello, ma evolva in una vera e propria attività di **consulenza di compliance Fintech**.

• IL CONTROLLO DELLE RETI

Un altro tema centrale nello sviluppo della digital compliance riguarda i sistemi di monitoraggio che si stanno evolvendo, dai controlli a campione, a continuous monitoring, attraverso l’utilizzo di *dashboard*, per raggiungere logiche *real time* e predittive e il supporto di tecniche advanced analytics. Inoltre, **efficaci strumenti di controllo a distanza possono contribuire a modificare il modello ispettivo sulle reti, diminuendo anche sensibilmente l’uso dello stesso strumento**. Per questo motivo, le istituzioni stanno cercando costantemente di migliorare il controllo delle reti a distanza, per cui è necessario dotarsi di nuove competenze analitiche, da ricercare sul mercato, o da formare internamente, così come una nuova *data culture* per la funzione Compliance.

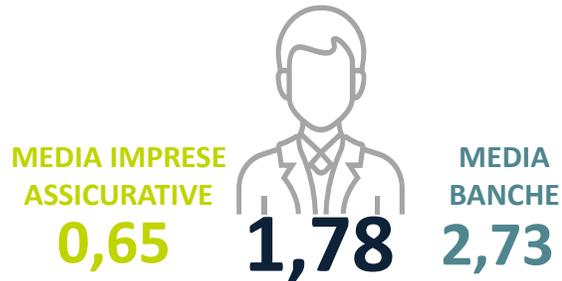


## 2. LA FUNZIONE COMPLIANCE

## LE RISORSE DELLA FUNZIONE COMPLIANCE

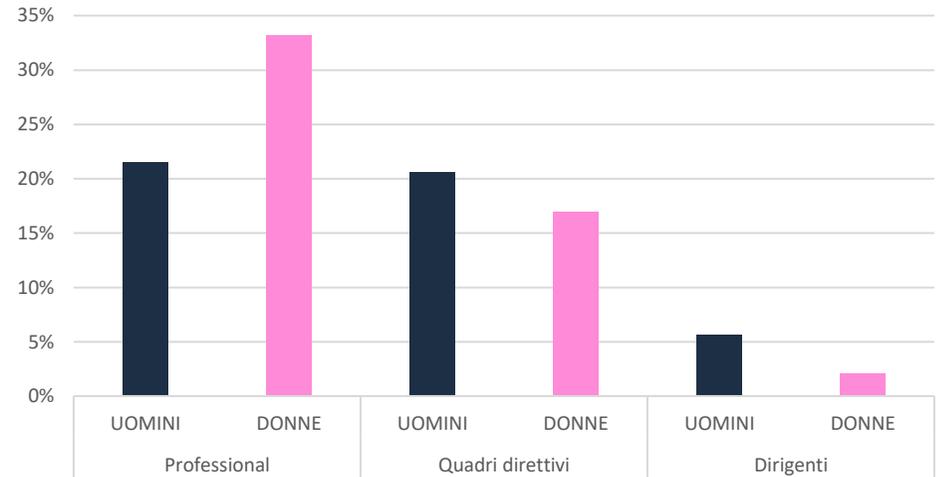
Gli istituti bancari occupano per la Compliance quattro volte più risorse rispetto alle imprese assicurative. Tra le risorse di Compliance c'è un'uguaglianza di genere, anche se persiste un elevato gender gap nelle posizioni dirigenziali

Numero di risorse (FTE) medio, impiegate nella  
Funzione compliance, ogni 100.000 clienti



Considerando in aggregato l'intero sistema finanziario, composto sia da imprese assicurative, sia da istituzioni bancarie, **il mercato impiega nella funzione Compliance in media 1,78 risorse, ogni 100.000 clienti**. Questo dato non tiene conto della diversità e della frammentazione del sistema finanziario, dove soprattutto le istituzioni bancarie hanno un'organizzazione solitamente più complessa, rispetto alle imprese assicurative. Pertanto, considerare le risorse mediamente impiegate separatamente per i due settori, può essere un indicatore che rappresenta efficacemente la realtà del sistema. Infatti, in questo modo si osserva che **il settore assicurativo impiega mediamente 0,65 risorse ogni 100.000 clienti, contro le 2,73 risorse impiegate mediamente dagli istituti bancari, quindi circa 4 volte più di risorse delle imprese assicurative**.

Distribuzione delle risorse di Compliance per genere e inquadramento

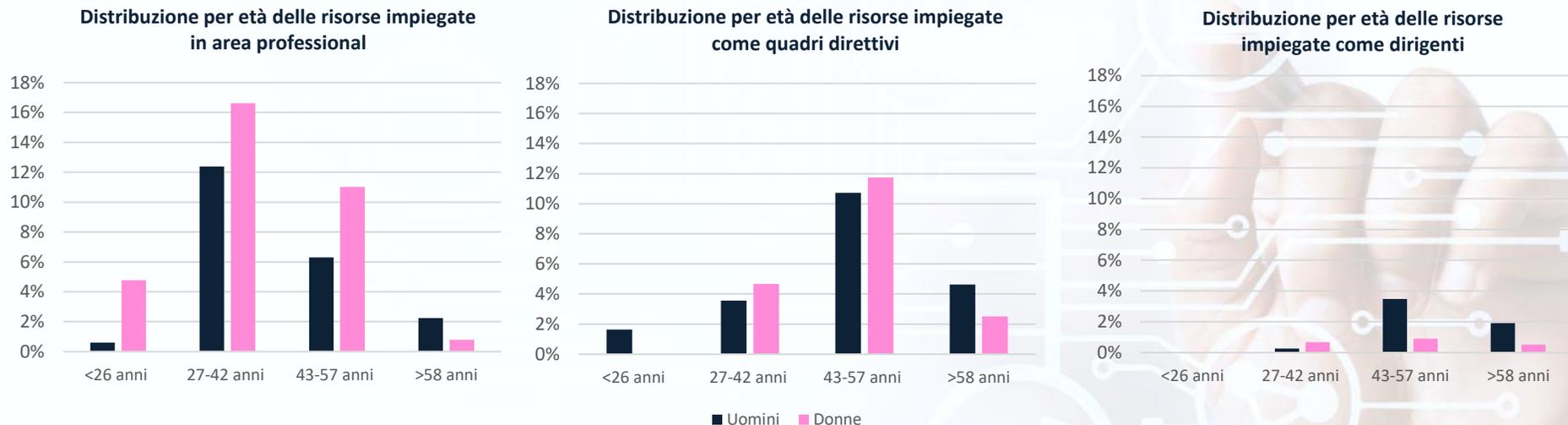


Questa **differenza può essere giustificata dal perimetro, solitamente più ampio, che la funzione Compliance ricopre all'interno degli istituti bancari**, a causa della presenza di funzioni di Non-Regulatory Compliance, come l'AML.

Le risorse sono quasi equamente distribuite per genere, con le donne leggermente più numerose (52%), rispetto agli uomini (48%), sebbene, analizzando come queste sono distribuite per inquadramento, si possa rilevare come **all'aumentare del livello di inquadramento, diminuisca il numero di donne**. Questo fenomeno è **indice di un elevato gender gap** presente per le posizioni dirigenziali. Infatti, il numero di donne occupate in area professional risulta essere quasi il doppio, rispetto al numero di uomini, ma già tra i quadri direttivi, il numero di uomini supera il numero di donne; fenomeno ancora più accentuato per i dirigenti, dove il numero di uomini rappresenta quasi il 75% del totale.

## DISTRIBUZIONE DELLE RISORSE DI COMPLIANCE PER ETÀ ED INQUADRAMENTO

Nella funzione di Compliance, all'aumentare dell'inquadramento, aumenta anche l'età media. Se per l'area professional l'età media delle risorse impiegate è compresa fra i 27 e i 42 anni, fra quadri direttivi e dirigenti prevalgono le risorse di età compresa fra i 43 e i 57 anni



Per quanto riguarda l'età delle risorse impiegate per la funzione Compliance, **l'età è mediamente più bassa nelle aree coincidenti ad un livello di inquadramento più basso**: all'aumentare dell'inquadramento è riscontrabile un incremento dell'età media.

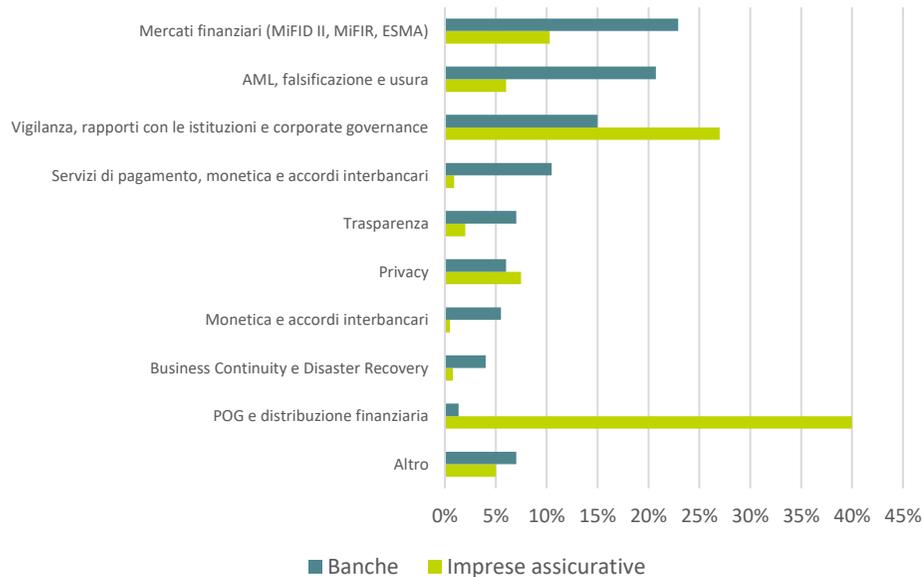
Pertanto, **nell'area professional l'età media** è relativamente più bassa, rispetto alle altre aree e **compresa fra i 27 e i 42 anni**. Inoltre, per lo stesso livello di inquadramento vi è una buona quantità di risorse, soprattutto di genere femminile, di età inferiore ai 26 anni, intorno al 5% del totale. In generale, nella stessa area e per tutte le fasce d'età, ad esclusione degli over 58 anni, la presenza di donne è nettamente superiore rispetto agli uomini.

Al contrario, **sia per i quadri direttivi, che per i dirigenti la fascia d'età prevalente è quella che va dai 43 ai 57 anni**. Inoltre, all'aumentare dell'inquadramento, aumenta la presenza di occupati over 58 anni, rappresentando il 30% circa del personale impiegato fra i dirigenti. Ancora una volta, si conferma la tendenza relativa alla presenza di un gender gap via via più elevato per le posizioni di vertice e tra le fasce d'età più elevate. Di fatto, tra i quadri direttivi le donne sono in maggioranza sia nella fascia d'età compresa fra i 27 e i 42 anni, che in quella 43-57 anni, ma per gli over 58 gli uomini sono la maggioranza. Ugualmente per i dirigenti, se tra i 27 e i 42 anni si osserva una prevalenza del genere femminile, vi è un capovolgimento nelle fasce d'età successive.

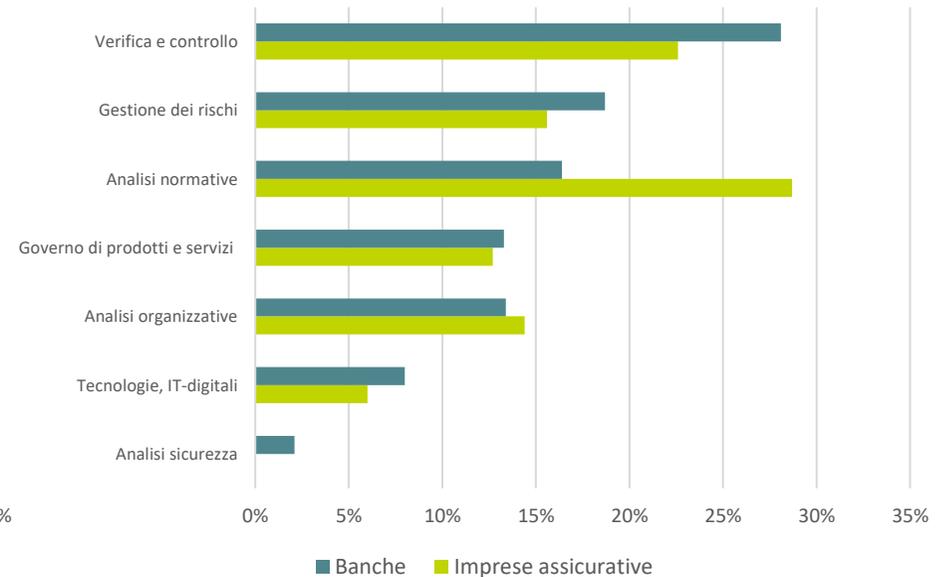
## DISTRIBUZIONE DELLE RISORSE E DELLE COMPETENZE DELLA FUNZIONE COMPLIANCE

Il settore bancario e quello assicurativo evidenziano differenze nella distribuzione sia delle risorse sia delle competenze. Le banche destinano più risorse per il presidio delle norme sui mercati finanziari e AML, mentre le assicurazioni per il presidio delle norme su POG e distribuzione assicurativa. Tra le competenze, per le banche prevalgono background di verifica e controllo e gestione dei rischi, per le assicurazioni background di natura legale per le analisi normative

Allocazione delle risorse rispetto agli ambiti specificati



Distribuzione delle competenze in area compliance



Analizzando gli ambiti nei quali sono impiegate le risorse di Compliance, emergono differenze fra le imprese assicurative e le istituzioni bancarie, a causa del modo in cui la funzione Compliance è strutturata nei due diversi settori. Come quanto accennato precedentemente, il perimetro più ampio ricoperto dalla Compliance di banche, implica una distribuzione delle risorse orientata su ambiti diversi.

Infatti, com'è possibile osservare dal grafico in alto a sinistra, le risorse bancarie sono distribuite in maniera più eterogenea, rispetto alle risorse del settore assicurativo che per il 60% sono allocate esclusivamente in due ambiti: la POG e la distribuzione finanziaria (40%) e Vigilanza, rapporti con le istituzioni e corporate governance (20%).

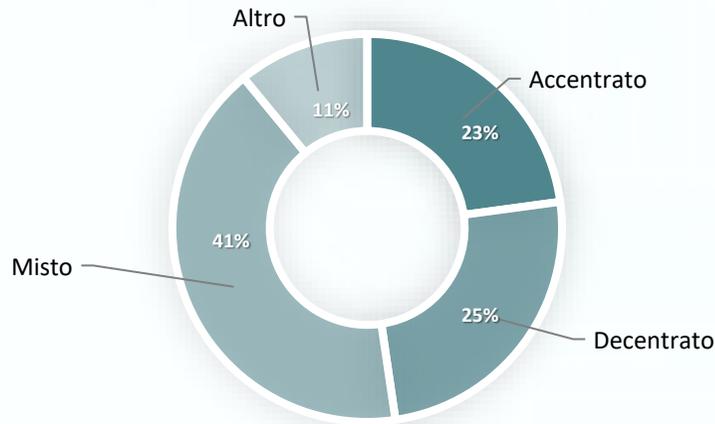
Nel settore bancario invece, le risorse sono prevalentemente impiegate per i mercati finanziari e per AML, falsificazione ed usura, per una quota pari al 20% in ciascuno degli ambiti indicati. Inoltre, tra gli ambiti indicati in altro, le istituzioni hanno individuato: l'analisi e la gestione dei dati, le normative di carattere residuale (FUG, CAI, ecc.) 231/2001, i rischi operativi di filiale e le sanzioni internazionali.

Per quanto concerne la distribuzione delle competenze, il settore assicurativo fa ancora molto ricorso alle analisi normative, competenza tradizionale della funzione Compliance, mentre nel settore bancario prevale la verifica e il controllo. Più per gli istituti bancari, che per le imprese di assicurazione, comincia ad emergere una forte componente di competenze legate alle nuove tecnologie, all'IT e al digitale, con l'8% di risorse bancarie di Compliance che possiede tali competenze, contro il 6% di quelle del settore assicurativo.

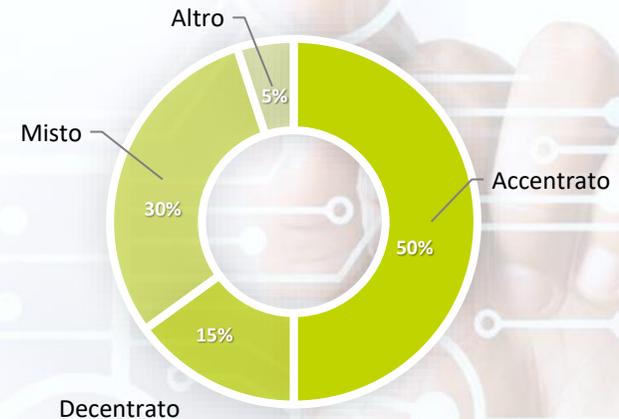
## IL MODELLO ORGANIZZATIVO DELLA FUNZIONE COMPLIANCE

Gli istituti bancari preferiscono organizzare la funzione Compliance secondo un modello misto: accentrato per alcuni ambiti normativi e decentrato per altri; al contrario delle imprese assicurative che preferiscono adottare un modello accentrato, in cui tutto il personale di Compliance è collocato in una medesima Funzione

Modello organizzativo adottato dalle banche



Modello organizzativo adottato dalle imprese assicurative



La selezione del modello organizzativo della funzione Compliance rappresenta, invece, una scelta strategica importante che varia solitamente in base alla specificità di ogni singola istituzione finanziaria. Un modello organizzativo caratterizzato da un'operatività decentrata, in cui sono presenti nelle principali unità organizzative referenti di Compliance che riportano alla funzione stessa, è in genere meno oneroso, in termini di risorse e di costi organizzativi, rispetto a quello accentrato, in cui tutto il personale di Compliance è collocato nella Funzione stessa. Infatti il primo è in generale di più facile applicazione e si può adattare meglio a un numero maggiore di strutture operative differenti, sebbene il secondo permetta un processo decisionale più rapido e immediato. Un modello di tipo "misto" è invece un modello che è accentrato per alcuni ambiti normativi e processi, solitamente attinenti alla fase di recepimento di nuove normative, che richiede un controllo più ristretto, mentre è decentrato per altri ambiti normativi e processi, spesso legati alle attività di gestione quotidiana.

Dall'analisi effettuata, sono state riscontrate notevoli differenze fra i due settori finanziari, con il settore

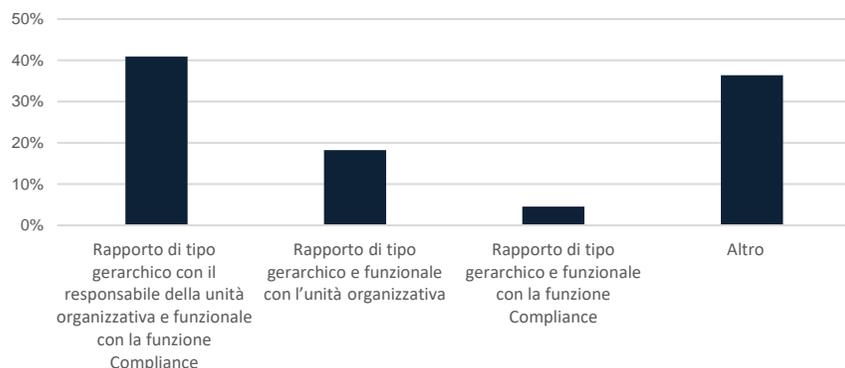
bancario che preferisce adottare un modello misto (41%), anche se un quarto degli istituti bancari predilige un sistema decentrato (25%), mentre solo il 23% adotta un modello accentrato. Quest'ultimo modello, è invece quello preferito dal mercato assicurativo, in cui un'impresa assicurativa su due sostiene di adottarlo, contro il 30% delle altre imprese che preferisce un modello organizzativo di tipo misto, mentre il 15% adotta un modello decentrato.

Inoltre, l'ampiezza della funzione Compliance e il numero di risorse impiegate spesso possono dipendere dal numero di legal entity per cui la Compliance svolge l'attività. Secondo la nostra analisi, la funzione Compliance svolge in media l'attività per circa 4,4 legal entity del medesimo gruppo. E' utile sottolineare, come ai fini del calcolo, per una maggiore omogeneità dei dati, siano stati esclusi i gruppi bancari federati, la cui funzione Compliance, spesso accentrata, svolge l'attività per un numero medio di società del medesimo gruppo molto più elevato (es. fino a 70 società), rispetto a banche e imprese assicurative dall'assetto più tradizionale.

## IL MODELLO ORGANIZZATIVO MISTO E LE METODOLOGIE DI LAVORO UTILIZZATE

In un modello organizzativo misto, il rapporto che intercorre fra i referenti di Compliance presenti in altre unità organizzative e la Funzione Compliance, è tipicamente di tipo gerarchico con il responsabile dell'unità organizzativa e funzionale con la Funzione Compliance. Inoltre, il 30% del mercato utilizza o sta sperimentando metodologie di lavoro agile, contro il 53% che utilizza metodologie di lavoro flessibile

Tipologia di rapporto che esiste tra i referenti di Compliance presenti in altre unità organizzative e la funzione Compliance

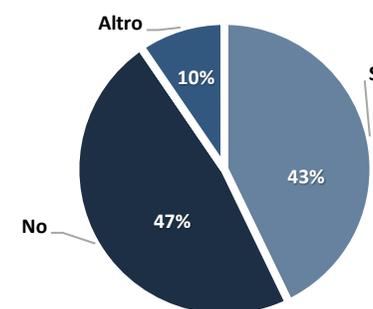


Le istituzioni che scelgono un modello organizzativo misto, solitamente nominano dei referenti di Compliance in altre *business unit*, che hanno il compito di collaborare funzione Compliance centrale. Analizzando il tipo di rapporto che intercorre tra loro, si evidenzia come generalmente viene preferito un rapporto di tipo gerarchico con il responsabile dell'unità organizzativa e funzionale con la funzione compliance, scelto da più del 40% del mercato. Sono molte anche le istituzioni che preferiscono però un rapporto gerarchico e funzionale con l'unità organizzativa (20%), mentre poco meno del 4% afferma di avere un rapporto di tipo gerarchico e funzionale con la funzione Compliance. Numerose istituzioni sostengono, invece, di non avere dei responsabili di Compliance in altre unità organizzative (35%).

L'utilizzo di metodologie di lavoro Agile per la compliance



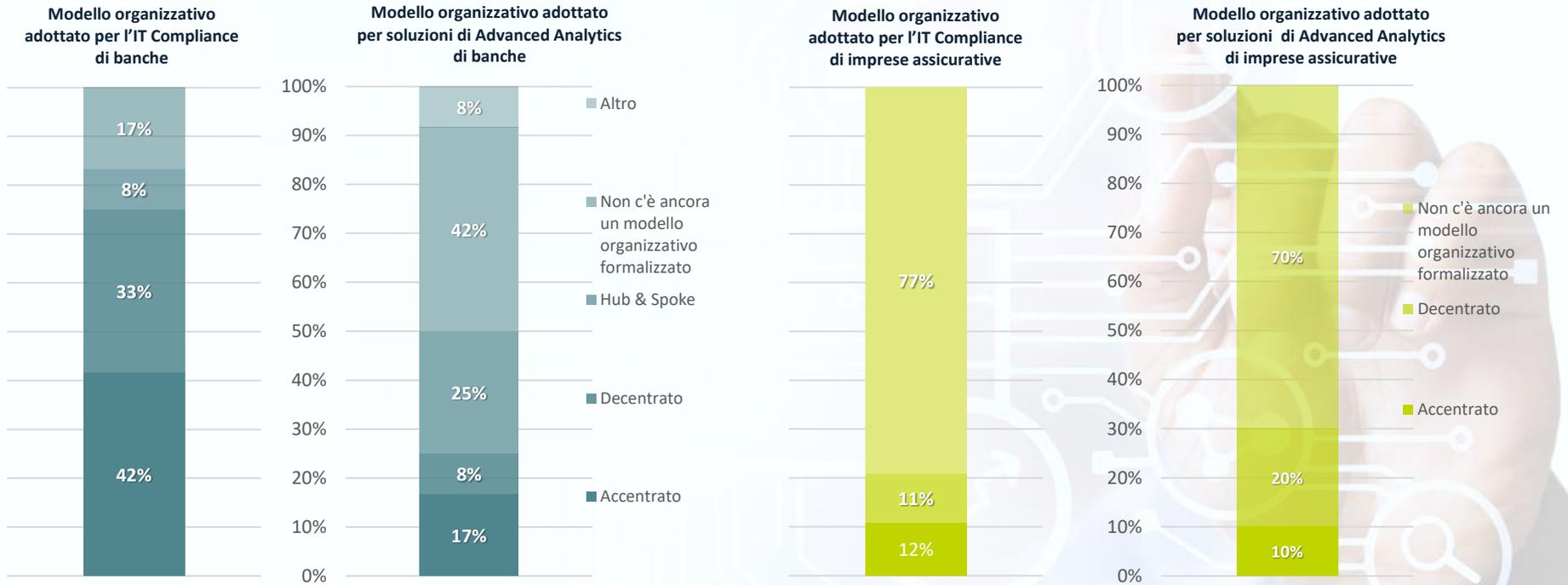
L'utilizzo di metodologie di lavoro Flessibile per la compliance



Osservando l'utilizzo di metodologie di lavoro agile o flessibile all'interno della funzione Compliance, si rileva che il 20% del mercato sostiene di utilizzare metodologie di lavoro agile, come *scrum*, *kanban* e *lean*, mentre il 10% le sta sperimentando. Nonostante queste percentuali possano sembrare relativamente basse, se si considera l'assoluta novità di queste metodologie di lavoro, entrate a far parte dei modelli organizzativi solo da pochissimi anni, il risultato è tuttavia soddisfacente. Per quanto riguarda l'adozione di metodologie di lavoro flessibile per la funzione Compliance, emerge che il 53% del mercato sostiene di adottarle, soprattutto in forma di *smart working*. Questo valore rappresenta un ottimo risultato, sicura conseguenza della crisi pandemica che ha costretto gli istituti a cambiare improvvisamente le proprie metodologie di lavoro.

## IL MODELLO ORGANIZZATIVO PER L'IT COMPLIANCE E PER LE SOLUZIONI DI ADVANCED ANALYTICS

Le banche preferiscono adottare un modello accentrato per l'IT compliance, mentre non prevedono ancora un modello organizzativo formalizzato per lo sviluppo di soluzioni di Advanced Analytics; le imprese assicurative in entrambi i casi non hanno ancora un modello formalizzato



Nello sviluppo di soluzioni di Digital Compliance, molte istituzioni hanno costituito unità organizzative interne alla funzione, come l'IT Compliance e un'unità dedicata finalizzata allo sviluppo e al monitoraggio di soluzioni di Advanced Analytics. Per quanto riguarda il **modello organizzativo adottato dal mercato bancario per l'IT Compliance**, le istituzioni preferiscono adottare un modello **accentrato (42%)**, per cui la funzione centrale collabora con un team di IT che funge da collettore per tutta l'organizzazione. **Il 33% delle banche preferisce invece, un modello di tipo decentrato**, in cui la Compliance ha costituito un team di IT interno e autonomo rispetto agli altri team di IT. Solo l'8% delle banche sceglie un modello di tipo Hub&Spoke, contro il 17% di istituzioni che sostiene di non avere ancora un modello organizzativo formalizzato.

Per quanto riguarda, invece, **il modello organizzativo utilizzato nello sviluppo di soluzioni di Advanced**

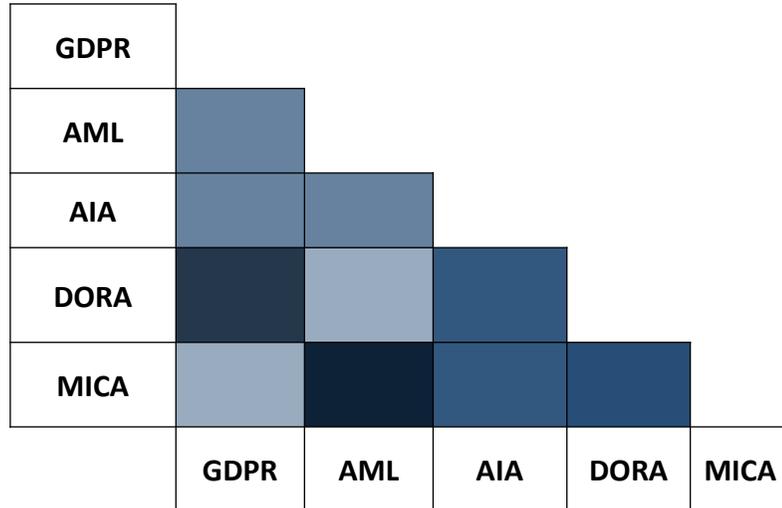
**Analytics, il 42% delle banche non ha un modello formalizzato**, mentre aumenta la quota di coloro che preferiscono un modello Hub&Spoke (25%) che consiste nella presenza di un team «Spoke» che sviluppa use case a seconda delle esigenze e collabora con un «Hub» centrale, con competenze di Advanced Analytics, che funge da coordinatore strategico. Al contrario, solo il 17% delle banche predilige un modello di tipo accentrato.

**Le imprese assicurative, invece, non sembrano essere ancora così strutturate** in entrambi i casi, in quanto prevalentemente **non hanno modelli organizzativi formalizzati**. Infatti, per l'IT Compliance solo il 23% del mercato ha un modello organizzativo formalizzato, mentre la quota è del 30% nello sviluppo di soluzioni di Advanced Analytics. Questo fenomeno può essere dovuto al fatto che le imprese assicurative, essendo ancora indietro nello sviluppo di progetti di Digital Compliance, non sono ancora strutturalmente ben organizzate.

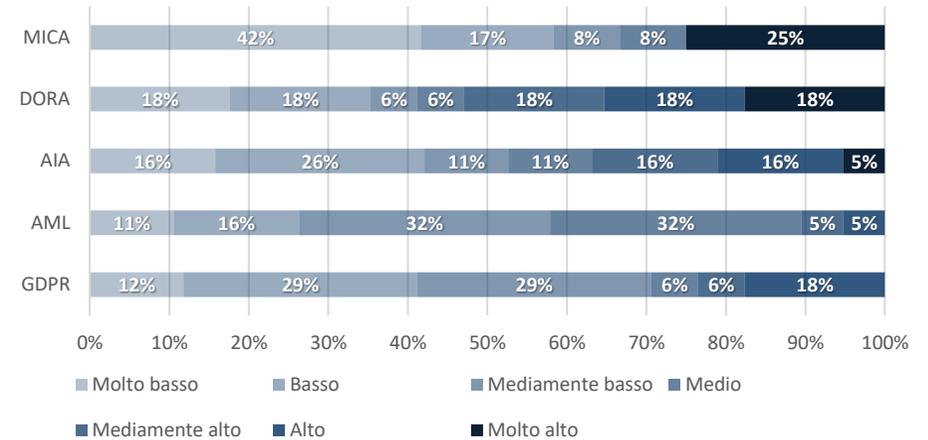
## L'IMPATTO DELLE NUOVE NORMATIVE IN AMBITO DIGITALE

Le norme tra loro più correlate sono AML-MICA e GDPR- DORA. Il Risk Management e la funzione Compliance stanno collaborando molto soprattutto su MICA e DORA

La correlazione fra norme



La collaborazione tra la funzione compliance e il risk management rispetto alle principali norme in materia digitale



Diverse normative stanno cambiando e cambieranno il framework regolamentare, all'interno del quale dovranno divincolarsi le istituzioni finanziarie. Le principali normative in ambito digitale dal forte impatto sono sicuramente: l'AIA (Artificial Intelligence Act), la MICA (Markets in Crypto-Assets), la DORA (Digital Resilience Operation Act), l'AML (Anti Money Laundering), la GDPR (General Data Protection Regulation) e la normativa ESG (Environmental Social and Governance),

E' stato analizzato quanto le principali normative in materia digitale sono correlate fra loro. Questa valutazione può essere molto interessante per la Funzione Compliance, in quanto molto spesso le istituzioni finanziarie organizzano la propria Compliance per normative, in cui ogni divisione si occupa di analizzare, interpretare e controllare la conformità per una o più norme simili fra loro. In particolare, il mercato ha evidenziato un'alta correlazione soprattutto fra le normative AML e MICA.

Entrambe infatti riguardano aspetti simili del mercato, come, ad esempio, il riciclaggio di denaro sporco che sempre più viene effettuato attraverso l'utilizzo di cripto-attività. Allo stesso tempo, anche le normative DORA e GDPR presentano un alto livello di correlazione, al contrario di DORA e AML che rappresentano, con MICA e GDPR, quelle con il livello di correlazione più basso.

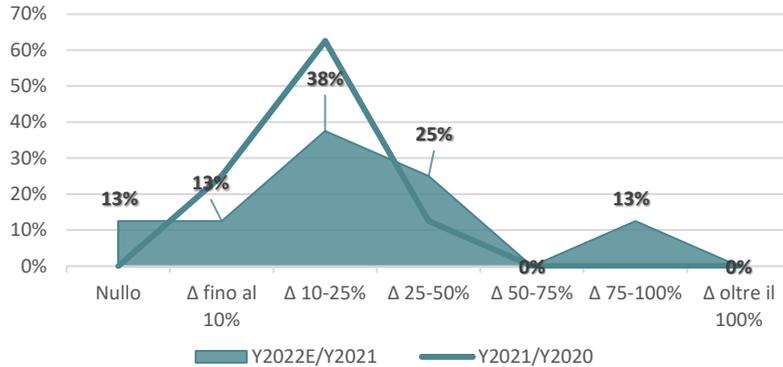
Spesso per le normative più complesse e di maggiore impatto, la funzione Compliance nelle sue attività di controllo collabora attivamente con un'altra struttura interna come il Risk Management. Si rileva che ciò oggi avviene soprattutto sulle normative MICA, DORA e AIA. Questo può essere dovuto alle caratteristiche delle normative, in quanto quelle più complesse, di maggiore impatto e che comportano più rischi possono richiedere un alto livello di collaborazione tra le due strutture.

# 3. DIGITAL COMPLIANCE

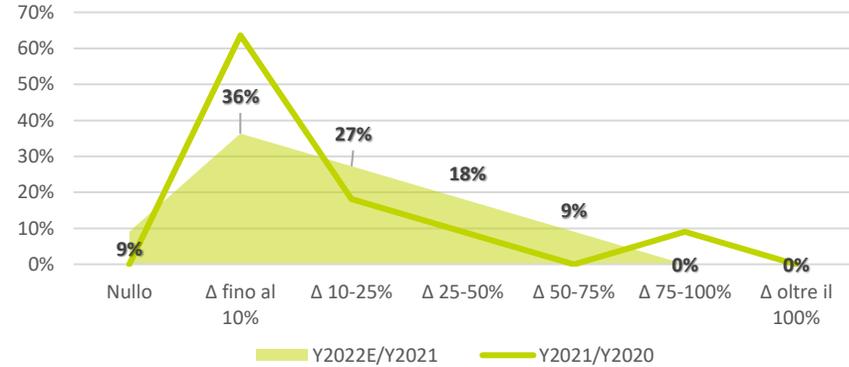
## IL TREND DI INVESTIMENTO IN DIGITAL COMPLIANCE

Nel settore bancario il trend di investimento per la digital Compliance è in crescita: il 40% del mercato prevede di investire oltre il 25% in più nel 2022, rispetto all'anno precedente, mentre la stessa quota sarà investita dal 27% del mercato assicurativo.

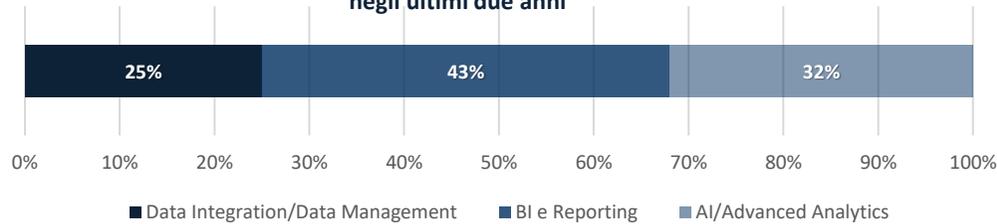
**Trend di investimento del mercato bancario  
y/y 2022E/2021 e 2021/2020**



**Trend di investimento del mercato assicurativo  
y/y 2022E/2021 e 2021/2020**



**Tecnologie utilizzate a supporto di progetti di digital Compliance  
negli ultimi due anni**



Per capire quanto il mercato sta implementando progetti di Digital Compliance è necessario analizzare il trend di investimento negli ultimi due anni del mercato bancario e assicurativo. **Per entrambi i settori emerge come il trend di investimento in Digital Compliance è sicuramente in costante crescita**, infatti una buona fetta di mercato ha deciso di accelerare lo sviluppo di progetti di Digital Compliance negli ultimi due anni.

In particolare, **nel 2022 il 40% del settore bancario e il 27% del mercato assicurativo hanno previsto di voler investire oltre il 25% in più, rispetto all'anno precedente**. Come accennato, il trend è in costante crescita e ciò è confermato considerando che nel 2021, rispetto al 2020, solo il 13% del mercato bancario aveva investito una quota oltre il 25%. Anche per il mercato assicurativo, come precedentemente

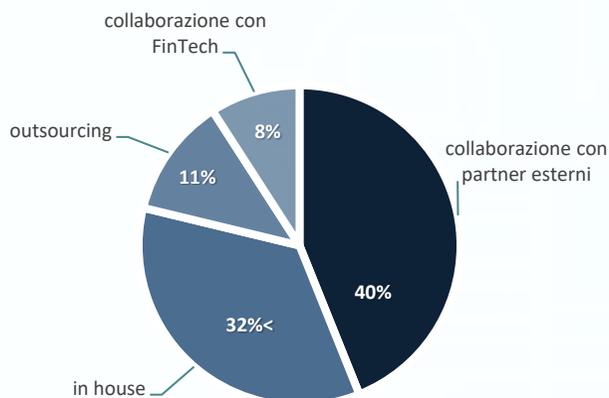
accennato, il trend di investimento per lo sviluppo di progetti di Digital Compliance è in forte aumento. Infatti se nel 2021/2020 solo il 18% del mercato aveva deciso di investire oltre il 25% in più, nel 2022 lo faranno 27% delle imprese assicurative. Inoltre, **nel 2022E/2021 non vi sono imprese assicurative che avranno variazioni nulle, quindi gli investimenti in progetti di Digital Compliance sono in aumento per ogni singola impresa assicurativa**.

In particolare, **la principale tecnologia utilizzata a supporto di progetti di Digital Compliance**, su cui le istituzioni finanziarie hanno investito negli ultimi due anni, è stata prevalentemente l'Advanced Analytics nel 45% dei casi, mentre il 32% dei progetti sono stati sviluppati utilizzando la Business Intelligence, il 19% attraverso il Data Management e solo il 3% attraverso il Data Reporting.

## LA COLLABORAZIONE CON LE FINTECH PER PROGETTI DI DIGITAL COMPLIANCE

Sia la collaborazione con partner esterni, che lo sviluppo interno, rappresentano le principali modalità di realizzazione dei progetti di Digital Compliance. Solo l'8% del mercato decide di sviluppare questi progetti attraverso la collaborazione con FinTech, a causa di diverse criticità, come l'integrazione con i sistemi legacy.

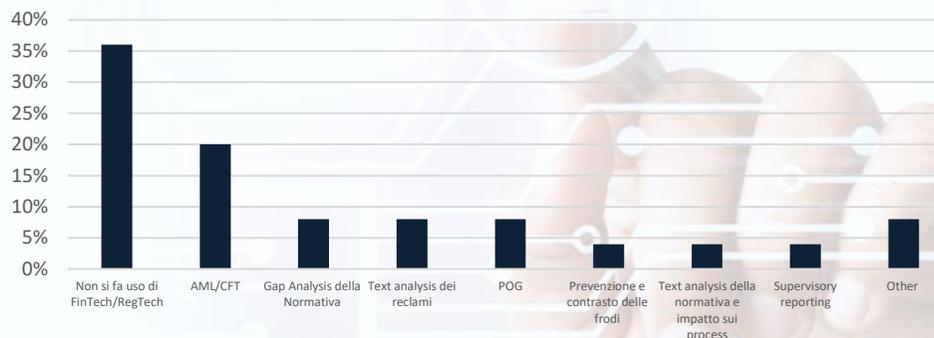
Modalità di realizzazione dei progetti di Digital Compliance



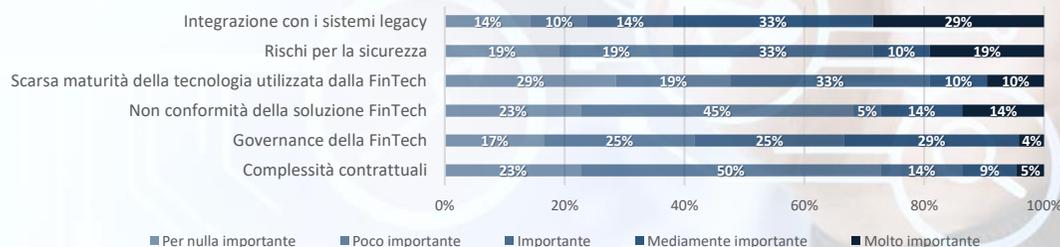
Come precedentemente analizzato, i principali progetti di digital Compliance sviluppati negli ultimi due anni si sono avvalsi prevalentemente di tecnologie di Advanced Analytics, ma focalizzandosi sulle modalità di realizzazione degli stessi progetti, emergono principalmente due direttrici. **Prevalentemente il mercato finanziario si è avvalso della collaborazione con partner esterni, con cui sono stati sviluppati il 40% dei progetti negli ultimi due anni, mentre il 32% dei progetti sono stati sviluppati internamente. Un progetto su dieci è invece stato sviluppato in outsourcing, mentre solo l'8% dei progetti totali sono stati sviluppati attraverso la collaborazione con FinTech.**

In particolare, se si analizza il ricorso che le istituzioni finanziarie fanno in merito a servizi offerti da FinTech o RegTech, solo il 64% del mercato sostiene di averne fatto uso, contro il 36% sostiene di non

Gli ambiti e le aree all'interno delle quali si fa ricorso a servizi offerti da FinTech/RegTech



Le maggiori criticità che nascono dalla collaborazione con FinTech/RegTech:



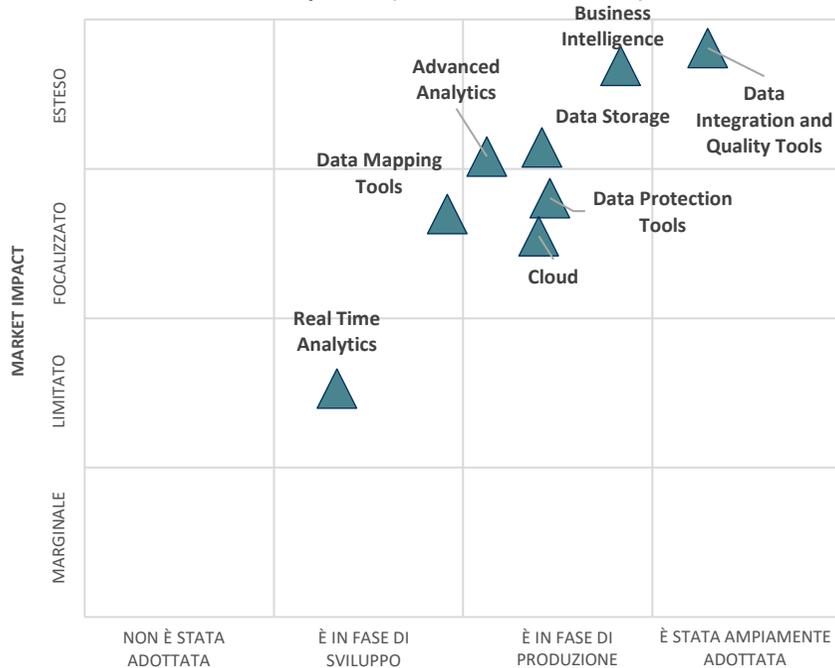
far ricorso a questi servizi. In particolare, le istituzioni finanziarie ricorrono all'uso del RegTech soprattutto in alcuni ambiti ed aree particolari, come: AML/CFT (il 20% del mercato), Gap Analysis della normativa (8%), POG (8%) e text analysis dei reclami (8%).

**La scarsa collaborazione tra istituzioni finanziarie e FinTech nei progetti di Digital Compliance può essere legata ad una serie di criticità provocate dall'utilizzo di FinTech o RegTech. In primis, il mercato ritiene molto difficoltoso integrare strumenti FinTech/RegTech con i sistemi legacy, segnalando anche che un'eventuale collaborazione potrebbe comportare rischi per la sicurezza. Allo stesso modo emerge tra le criticità anche la scarsa maturità tecnologica delle Fintech ed una bassa disponibilità di strumenti FinTech sul mercato, già pronti e disponibili ad essere utilizzate in processi di Compliance.**

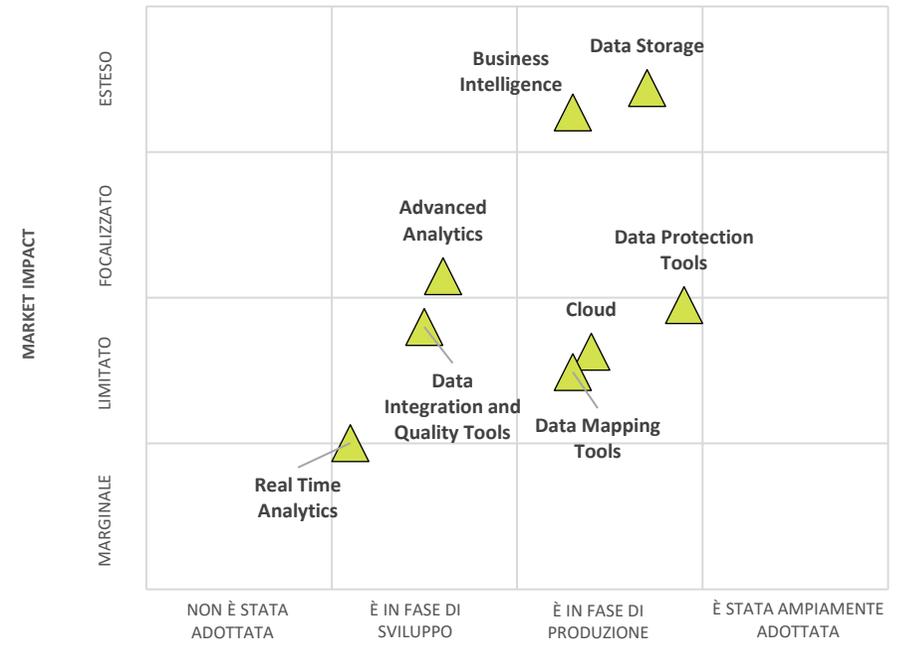
## L'ADOZIONE DELLE TECNOLOGIE NEI PROCESSI DI COMPLIANCE

Per le banche, il livello di adozione di tecnologie a supporto dei processi di compliance si rivela essere ad un livello più elevato rispetto alle imprese assicurative che scontano un gap dovuto principalmente a carenze sui dati. Le tecnologie in fase di adozione più avanzata sono la Data Integration e la Business Intelligence per il mercato bancario; Data Storage e Business intelligence per quello assicurativo

Livello di adozione delle tecnologie nella digital Compliance (Settore bancario, 2022)



Livello di adozione delle tecnologie nella digital Compliance (Settore assicurativo, 2022)



Come emerso dall'analisi del trend degli investimenti per il 2021/2020 e 2022E/2021 il settore bancario ha investito maggiormente, rispetto al settore assicurativo. Questo ha contribuito a fare in modo che le banche siano più avanti nell'adozione delle tecnologie, anche in termini di impatto di mercato, come rappresentato dai grafici in alto. Le banche, rappresentate sulla sinistra, sono più avanti sia nel livello medio di adozione, che per l'impatto di mercato. Infatti, **nel settore bancario, la maggior parte delle tecnologie indicate si trovano in fase di produzione, o sono state ampiamente adottate. Inoltre, anche lo stesso impatto di mercato (misurato in termini di quanti clienti beneficeranno dall'implementazione di una tecnologia) è generalmente più elevato per ogni singola tecnologia.**

**In particolare, nel settore bancario le tecnologie di Data integration and Quality Tools, così come la Business Intelligence, sono quelle sia a più alto impatto, che quelle in fase più avanzata di adozione.**

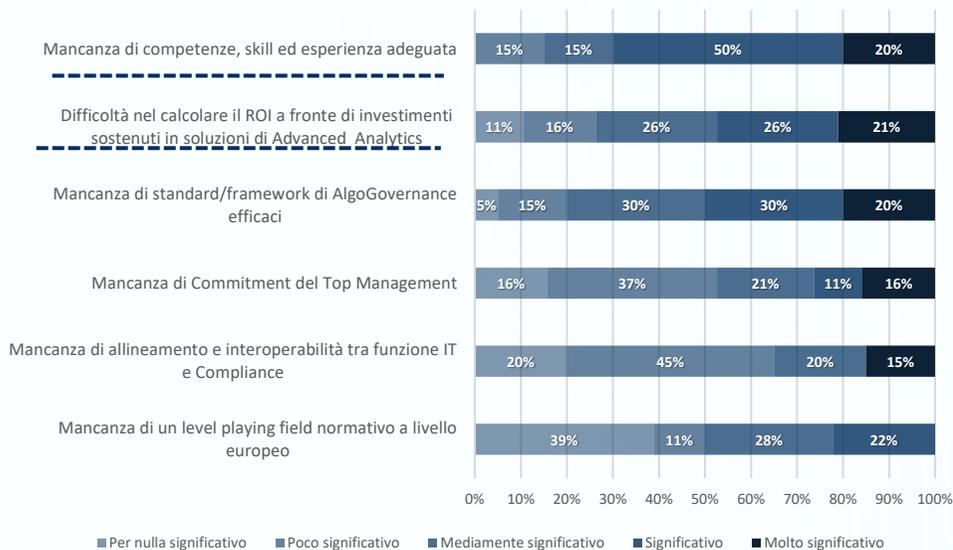
Si nota, inoltre una crescita degli Analytics, i quali si trovano in una fase di sviluppo ma destinati a crescere nei prossimi anni.

Come emerso, il mercato assicurativo risulta essere generalmente più indietro nell'adozione delle nuove tecnologie. In particolare, gli Analytics si trovano ancora in un'iniziale fase di sviluppo e con basso *market impact*, mentre le altre tecnologie sono mediamente in fase di produzione. **Inoltre, ad esclusione di Data Storage e Business Intelligence, l'impatto di mercato rimane per tutte loro molto basso.** Secondo i nostri dati, si segnala una piccola regressione del livello di adozione della Business Intelligence tra 2022 e 2021. Sembra che le imprese assicurative stiano dismettendo questa tecnologia, probabilmente per far spazio alle tecnologie di *Analytics*, che nel 2022 crescono molto, così come la tecnologia di *Data Protection Tools*, il cui livello d'adozione è in fase più avanzata.

## L'ADOZIONE DI SOLUZIONI DI ADVANCED ANALYTICS PER LA FUNZIONE COMPLIANCE

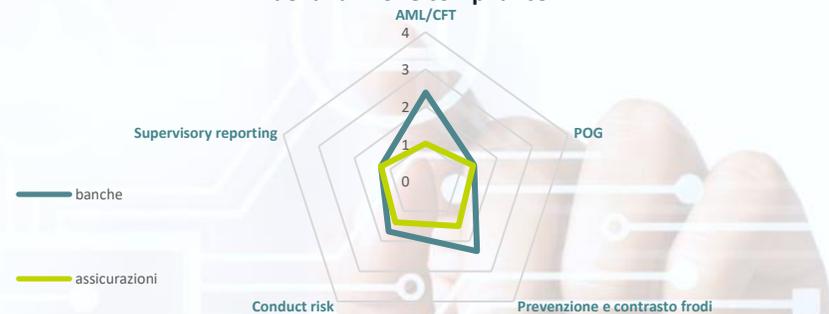
Mancanza di competenze e difficoltà nel calcolare il ROI dell'investimento sono i principali ostacoli nell'adozione e implementazione di soluzioni di Advanced Analytics per la funzione Compliance. La stessa Compliance si occupa di controllare internamente lo sviluppo di soluzioni di Advanced Analytics

I principali ostacoli relativi all'adozione e all'implementazione di soluzioni di Advanced Analytics

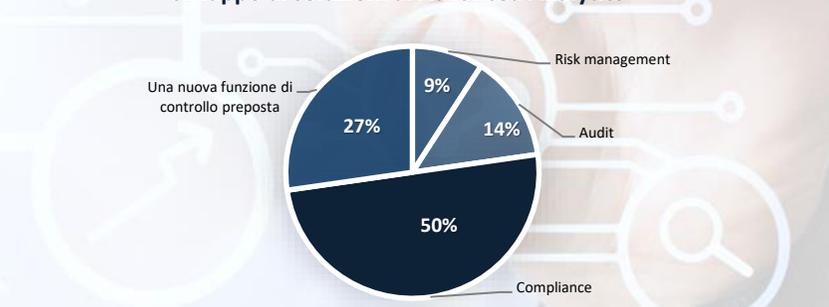


Nonostante gli investimenti in progetti di Digital Compliance siano in costante crescita negli ultimi due anni, **nell'adozione e sviluppo di soluzioni di Advanced Analytics per la Compliance, il sistema finanziario riscontra una serie di ostacoli e criticità. La principale** è costituita dalla **mancanza di competenze, skill ed esperienza adeguata**: è molto complesso per le istituzioni trovare ed assumere personale adeguatamente formato, o con un'esperienza rilevante, rispetto alle proprie necessità. Le istituzioni si trovano spesso costrette a rallentare i propri progetti di sviluppo e a formare internamente i propri lavoratori, promuovendo iniziative di upskilling e reskilling. **Una seconda criticità è legata alla difficoltà nel calcolo del ROI a fronte di investimenti sostenuti in soluzioni di Advanced Analytics.** Infatti nell'ambito della Compliance, è complesso valutare immediatamente il ritorno degli investimenti, in quanto spesso i benefici si sostanziano solitamente nel medio-lungo periodo, in una diminuzione dei costi e una maggiore efficacia dei processi di controllo. Inoltre, **nella valutazione del grado di maturità relativo all'utilizzo di tecniche di Advanced Analytics, rispetto agli ambiti e alle Aree proposte, le imprese assicurative, come confermato dal trend di investimento, hanno un livello di maturità medio**

Il grado di maturità degli Advanced Analytics in alcune aree della funzione compliance



La funzione di controllo interna preposta a monitorare lo sviluppo di soluzioni di Advanced Analytics



**generalmente molto basso, rispetto al settore bancario.** Infatti, in tutte le 5 aree considerate: AML/CFT, POG, Prevenzione e contrasto frodi, Conduct risk e Supervisory reporting, le imprese assicurative non hanno ancora adottato tecniche di Advanced Analytics, o si trovano in una fase iniziale di sviluppo. Le istituzioni bancarie sono in fase di produzione per tecniche di Advanced Analytics a supporto delle aree di prevenzione, contrasti frodi e AML/CFT.

**Invece, il controllo interno volto a monitorare, valutare gli algoritmi e porre in essere interventi correttivi connessi a errori, bias, o malfunzionamenti degli stessi nello sviluppo di soluzioni di Advanced Analytics per la funzione Compliance, esso è affidato nella maggior parte dei casi (50%) alla funzione Compliance stessa.** Al contrario, solo il **27% del mercato assegna tale compito ad una nuova funzione di controllo preposta**, mentre Audit e Risk Management se ne assumono la responsabilità rispettivamente nel 14% e nel 9% dei casi.



# BIBLIOGRAFIA

## BIBLIOGRAFIA

- A. Dania, C. Frigerio, F. Rajola, *Processi distributivi e controlli a distanza*, Cetif, Marzo 2022, Milano
- A. Dania, C. Frigerio, F. Rajola, *I nuovi rischi di sostenibilità e il sistema dei controlli interni*, Cetif, Maggio 2022, Milano
- A. Dania, C. Frigerio, G. Gatti, F. Rajola, *DORA e AIA at work: gli effetti sulla IT Compliance*, Settembre 2022, Milano
- A. Dania, C. Frigerio, G. Gatti, F. Rajola, *Next Generation Compliance: data, AI & Algo-Governance*, Ottobre 2022, Milano
- *The AI ACT*, <https://artificialintelligenceact.eu/>
- *Rilevazione tecnologica "La trasformazione digitale della banca" - Anno 2021*, CIPA e ABI, Luglio 2022
- *Rilevazione economica - Esercizio 2021 – Rapporto annuale*, CIPA e ABI,
- *Rilevazione tecnologica "La trasformazione digitale della banca" - Anno 2020*, CIPA e ABI, 2020
- Accenture, « Europeans are skeptical about their banks. Here's what the data tells us », Febbraio 2022
- Banca d'Italia Statistiche «Banche e Istituzioni Finanziarie: articolazione territoriale», 2020
- Banca d'Italia, «Orientamenti per gli intermediari relativi ai dispositivi di governance e di controllo sui prodotti bancari al dettaglio» (POG)
- Cetif Digital Banking HUB, Research Insight «Opti channel Experience: a new Branch Model & Phygital Customer Journey », Luglio 2021
- Cetif Digital Compliance HUB, Research Insight «La Compliance nel nuovo scenario digitale ed emergenziale», Luglio 2021
- Cetif Digital Compliance HUB, Research Insight « Ecosystem implications on Governance Risks», Luglio 2021
- Cetif Digital Insurance & Distribution HUB, Research Insight «A new era of Insurance Distribution: the bionic agent», Luglio 2021
- EIOPA, «Open Insurance: accessing and sharing insurance related data. Discussion paper», 2021
- FSB, « Regulatori and Supervisory Issues Relating to Outsourcing and Third Party Relationships Discussion paper » », Novembre 2020
- IVASS, «La Product Oversight Governance dei prodotti assicurativi Profili giuridici e operativi» 20 febbraio 2020
- S. Torrance, «Embedded Insurance: a \$3 Trillion market opportunity, that could also help close the protection gap», Dicembre 2020
- Osservatorio Nomisma Crif , *The world after Lockdown*, Ottobre 2020

# APPENDICE METODOLOGICA

## APPENDICE METODOLOGICA

Il Digital Compliance HUB si inserisce all'interno dei 13 Research HUB di Cetif, che nel 2022 hanno contato ben 195 relatori e 2255 partecipazioni, di cui 496 hanno preso parte al Digital Compliance HUB.

L'HUB si rivolge alle aree Controlli Interni, Compliance, Legale e AML delle Istituzioni finanziarie. La Community aggrega competenze di aree specialistiche al fine di rendere efficace il networking e proficuo lo scambio di know-how tra pari. Le competenze ed esperienze dei partecipanti in progetti strategici e di trasformazione digitale contribuiscono a creare il valore dei tavoli operativi e degli output dell'HUB. Nel corso del 2022, nell'ambito dell'Hub, si sono svolte 4 giornate di ricerca, ognuna delle quali è stata suddivisa tra una sessione mattutina (Community Event) e una pomeridiana (Research Meeting).

I Community Event sono seminari di presentazione e approfondimento dei temi e dei contenuti di ogni singola giornata, in cui la testimonianza e la partecipazione attiva di Authority, Istituzioni Finanziarie, Aziende e FinTech avvalorano i lavori ivi condotti. Tali Community Event presentano tutti la stessa struttura: il format è quello di un convegno in cui scambiare esperienze e favorire l'arricchimento di conoscenze tra tutti i partecipanti. Nel dettaglio, dopo uno scenario introduttivo, frutto della ricerca Cetif, segue solitamente un Research Partner Speech e un Legal Partner Speech, quindi l'analisi di uno Use Case (Participant or Guest) e infine Uno SteerCo Panel Discussion, seguito da un Open Session (momento di discussione tra tutti i partecipanti con Q&A circa le tematiche trattate) sono poste a chiusura dell'evento. Target di queste sessioni sono i Middle Manager, i Project Manager, i talenti e i Junior Professional.

La sessione pomeridiana del Research Meeting consiste in sessioni di lavoro finalizzate alla realizzazione di progetti di ricerca e dei suoi output. L'approccio è quello dell'Active Lab, che sfrutta analisi qualitative e metodologie collaborative per costruire output condivisi e concreti utili a supportare l'avvio di attività progettuali. E' rivolto ai Referenti dello Steering Committee e a specialisti con responsabilità su progetti di trasformazione. Esso ha l'obiettivo di stimolare il confronto tra i partecipanti attraverso metodologie di Design Thinking e Instant Survey, finalizzate alla definizione di output condivisi e utili a supportare l'avvio di attività progettuali.

In particolare, nel corso del 2022 durante i Community Event sono state approfondite tematiche quali: i processi distributivi, i controlli a distanza e i controlli interni, le nuove normative regolamentari in materia digitale, quali DORA e AIA, la next generation Compliance. I Research Meeting hanno invece riguardato la definizione del progetto di ricerca: dalla definizione degli obiettivi, alla presentazione dei risultati, passando per la somministrazione di una survey, attraverso il continuo confronto con le istituzioni partecipanti.

Di seguito un dettaglio relativo alle 4 giornate di ricerca:

- **10 Marzo**

**Community Event: Processi distributivi e controlli a distanza delle reti: what's new**

Sono state approfondite tematiche quali: il ruolo della POG & Business Conduct nei nuovi ecosistemi finanziari; gli ecosistemi finanziari e la governance; il ruolo del RegTech nel controllo dei processi distributivi.

**I Research Meeting: validazione degli obiettivi di ricerca**

- **10 Maggio:**

**Community Event: I nuovi rischi di sostenibilità e il sistema dei controlli interni**

Sono state approfondite tematiche quali: la classificazione delle attività secondo i criteri ESG; la trasparenza e l'informativa alla clientela; il Target Market, la distribuzione dei prodotti e l'adeguatezza per gli ESG.

**II Research Meeting: validazione dei modelli di input**

- **14 Settembre:**

**Community Event: DORA e AIA at work: gli effetti sulla IT compliance**

Sono state approfondite tematiche quali: l'Artificial Intelligence Act e l'impatto sui processi; il ruolo della DORA, i rischi informatici e gli impatti sull'IT Compliance; la sicurezza informatica e il ruolo della Compliance.

**III Research Meeting: validazione dei preliminary findings**

- **13 Ottobre:**

**Community Event: Next generation compliance: data, AI & Algo-Governance**

Sono state analizzate le tematiche quali: il ruolo della Data Driven Compliance, la gestione e il presidio del Digital e del Tech Risk; la Digital Compliance, il RegTech e gli impatti sulle competenze della Compliance.

**IV Research Meeting: validazione dei risultati finali**

Nell'ambito del progetto di ricerca, è stata somministrata una Survey, composta da circa 40 domande e di tre diverse sezioni. La prima ha avuto l'obiettivo di analizzare strategicamente la funzione Compliance, andando ad indagare le principali caratteristiche della funzione in termini di strutture (personale, competenze, metodologie e approcci collaborativi e di risorse). La seconda sezione, invece, ha avuto l'obiettivo di misurare l'impatto normativo sui processi, analizzando in che modo le normative in materia digitale influiscono sia oggi, sia in prospettiva, sull'operatività della funzione Compliance, in termini di impegno del personale e di costi di non conformità. La terza sezione ha riguardato un'analisi sull'innovazione della funzione, cercando di identificare le principali applicazioni di carattere tecnologico utilizzate dalla Compliance, con un focus particolare sugli investimenti e le possibili integrazioni di soluzioni di terzi.

Il campione analizzato nel progetto di ricerca rappresenta l'80% del market share, pari a 450 bn di Asset under Management e composto per il 40% di imprese di assicurazione, per il 60% di istituti bancari, (l'85% dei quali riguardavano gruppi bancari Significant). Inoltre, il totale dei rispondenti rappresenta 44 legal entity, facenti riferimento a 17 capogruppo italiane e 5 internazionali.

Tutti i dati, ove non specificato, hanno riguardato la situazione al 31/12/2021.

## INNOVAZIONE, STRATEGIA, SVILUPPO MANAGERIALE PER L'ECOSISTEMA BANCARIO, FINANZIARIO E ASSICURATIVO

Cetif dal 1990 realizza studi e promuove ricerche sulle dinamiche di cambiamento strategico e organizzativo nei settori finanziario, bancario e assicurativo, cui partecipano gli oltre 20.000 professionisti del suo network. Tra i partner istituzionali di Cetif: Banca d'Italia, IVASS, ABI, ANBP, ANIA, AIPB, CLUSIT e CONSOB. Cetif è inoltre socio fondatore di FIT, il network europeo dei centri di ricerca sulla finanza e l'innovazione.

### Membership & Events

Oltre 60 events tra cui main events (workshop e summit) e community events (collegati alle attività di ricerca) e webinar: facciamo incontrare banche, assicurazioni e aziende per una crescita condivisa su trend e sfide per delineare strategie di sviluppo innovative.

### Research

14 Hub di ricerca focalizzati su dinamiche di evoluzione strategica, aggiornamenti normativi, prassi organizzative e di processo, effetti della digitalizzazione: studiamo trend di innovazione e best practice e li condividiamo con la nostra community.

### Academy

Oltre 40 percorsi di Executive Education, 4 Master e numerosi Company Specific Program: trasferiamo con approccio scientifico contenuti innovativi orientati al mondo finanziario.

### Advisory

Uno spin off di sperimentazione che unisce ricerca accademica e impostazione imprenditoriale: trasformiamo innovazione e digitalizzazione in un concreto vantaggio per le imprese.

**WE'RE COMMUNITY!**

CETIF |



UNIVERSITÀ  
CATTOLICA  
del Sacro Cuore

[www.cetif.it](http://www.cetif.it)

Università Cattolica del Sacro Cuore  
Via Olona, 2 – 20123 Milano