

Dipartimento di Impresa e Management

Cattedra di Economia e Gestione delle Imprese

L'Internal Audit come capability organizzativa e funzione strategica nei contesti regolamentati

Prof. Alfonso Luca Adinolfi

RELATORE

Irene Pronunzio Matr. 298401

CANDIDATO

Anno Accademico 2025/2026

Sommario

Introduzione	7
 Capitolo 1 - Strategia d'impresa e <i>corporate governance</i> nei contesti regolamentati	 8
1.1 Strategia d'impresa nei contesti regolamentati	8
1.1.1 Struttura istituzionale e vincoli nei settori regolamentati	8
1.1.2 Implicazioni strategiche della regolamentazione	9
1.1.3 Evoluzione dei sistemi di controllo nei contesti regolamentati	9
1.2 Teorie strategiche di riferimento	10
1.2.1 Le Cinque Forze di Porter e l' <i>Industry-Based View</i>	10
1.2.2 La <i>Resource-Based View</i>	12
1.2.3 La <i>Institution-Based View</i>	13
1.3 <i>Corporate governance</i> ed evoluzione delle funzioni di controllo	14
1.3.1 <i>Agency theory</i> e problemi di <i>governance</i>	14
1.3.2 Dalla funzione di <i>compliance</i> al ruolo strategico dei controlli	16
1.3.3 Le funzioni di controllo come <i>capability</i> organizzative	17
1.4 Il ruolo della vigilanza nei contesti iper-regolamentati	18
1.4.1 Il ruolo dei sistemi di controllo nella riduzione dei conflitti di interesse	18
1.4.2 I livelli del sistema dei controlli interni del settore bancario	19
 Capitolo 2 - Evoluzione strategica dell'<i>Internal Audit</i> e <i>driver</i> di cambiamento	 21
2.1 La funzione aziendale di controllo di terzo livello: l'<i>Internal Audit</i>	21
2.1.1 Definizione e finalità dell' <i>Internal Audit</i>	21
2.1.2 Collocazione organizzativa e indipendenza	22
2.2 Trade-off tra costi della <i>compliance</i> e benefici del controllo	23
2.2.1 I costi della <i>compliance</i> e dei sistemi di controllo	23

2.2.2 I benefici del controllo interno e dell' <i>audit</i>	25
2.2.3 Il <i>trade-off</i> efficienza-controllo	26
2.3 Il Framework COSO come modello integrato di controllo interno e gestione dei rischi	27
2.3.1 Origine, finalità e logica del COSO <i>Internal Control–Integrated Framework</i>	27
2.3.2 Le componenti del Framework: dal control environment al monitoring	28
2.3.3 Dal controllo interno alla gestione dei rischi di <i>compliance</i> : il collegamento tra COSO, ERM e <i>Internal Audit</i>	29
2.4 Driver di cambiamento e trasformazione delle funzioni nei contesti regolamentati	30
2.4.1 Innovazione tecnologica e digitalizzazione dei controlli.....	31
2.4.2 Sostenibilità e nuovi ambiti dell' <i>audit</i>	32
2.4.3 Implicazioni per l'evoluzione dell' <i>Internal Audit</i>	33
Capitolo 3 – Modelli di riferimento e applicazione a un caso bancario	35
3.1 Il framework Deloitte – <i>Internal Audit 3.0</i>	35
3.1.1 Origine del modello e limiti dell' <i>Internal Audit</i> tradizionale	35
3.1.2 Le tre dimensioni del valore: <i>Assure, Advise, Anticipate</i>	36
3.1.3 <i>Internal Audit 3.0</i> come modello evolutivo	37
3.2 Il contributo PwC: evidenze empiriche e approccio alla trasformazione	38
3.2.1 Il Global Internal Audit Study 2023	39
3.2.2 La trasformazione della funzione di <i>Internal Audit</i>	40
3.3 Integrazione dei framework in un modello evoluto di <i>Internal Audit</i>	42
3.3.1 Complementarità tra contenuto, metodo e struttura	42
3.3.2 Coerenza e compatibilità dei modelli	43
3.3.3 Proposta di un modello integrato di <i>Internal Audit</i>	44
3.4 Applicazione a un contesto bancario: caso studio simulato	46
3.4.1 Descrizione del contesto organizzativo e obiettivi del progetto: Banca Alfa	46
3.4.2 Analisi della situazione “ <i>as is</i> ” e valutazione del livello di maturità	48

3.4.3 Posizionamento della funzione e individuazione delle aree di miglioramento	49
3.4.4 Definizione dell' <i>Internal Audit Strategy</i> , <i>roadmap</i> evolutiva e KPI	51
3.4.5 Impatti strategici e organizzativi attesi	53
Conclusioni	55
Bibliografia	57

Introduzione

Negli ultimi decenni, l'evoluzione dei mercati, l'aumento della complessità organizzativa e il rafforzamento dei sistemi regolamentari hanno trasformato profondamente il ruolo dei sistemi di controllo interno e, in particolare, quello della funzione di *Internal Audit*. Da attività prevalentemente orientata alla verifica della conformità e alla prevenzione di errori o irregolarità, il sistema dei controlli interni ha progressivamente assunto una funzione più ampia, collegata alla gestione dei rischi, al supporto dei processi decisionali e al rafforzamento della *corporate governance*.

Tale evoluzione risulta particolarmente rilevante nei settori fortemente regolamentati, come quello bancario e finanziario, nei quali vincoli normativi, requisiti prudenziali e poteri di vigilanza richiedono assetti di controllo strutturati, indipendenti e integrati nei processi aziendali. In questi contesti, il controllo interno non può essere interpretato come un mero adempimento procedurale, ma rappresenta una componente essenziale dell'assetto organizzativo e strategico dell'impresa.

La presente tesi si propone quindi di analizzare l'evoluzione dell'*Internal Audit* verso un ruolo a forte valenza strategica, capace di fornire *assurance* indipendente sull'efficacia di tutti i processi aziendali e, in particolare, su quelli di *governance*, *risk management* e *compliance*, e di contribuire all'identificazione dei rischi emergenti, al miglioramento continuo dei processi e alla protezione del valore organizzativo. L'obiettivo della ricerca è comprendere in che modo l'*Internal Audit* possa configurarsi come una leva organizzativa a supporto della resilienza, della trasparenza e della sostenibilità dell'impresa.

Capitolo 1 - Strategia d'impresa e *corporate governance* nei contesti regolamentati

1.1 Strategia d'impresa nei contesti regolamentati

Lo sviluppo di una strategia è connesso al contesto competitivo e istituzionale in cui l'impresa opera, elementi che impongono vincoli operativi e ne condizionano profondamente le opportunità. In molti settori economici, le imprese operano in contesti relativamente aperti, nei quali le scelte strategiche sono principalmente influenzate dalle dinamiche di mercato e dalla competizione tra operatori. In altri ambiti, invece, l'attività delle imprese è fortemente influenzata dalla presenza di un articolato quadro regolamentare, che definisce limiti, requisiti operativi e poteri di vigilanza.

I settori regolamentati, come quello bancario, energetico o farmaceutico, rappresentano esempi emblematici nei quali la regolamentazione costituisce un elemento strutturale dell'ambiente competitivo. In tali contesti, le imprese sono chiamate a sviluppare strategie che tengano conto non solo delle logiche di mercato, ma anche dei vincoli e, in alcuni casi, delle opportunità derivanti dal quadro normativo. Comprendere il ruolo della regolamentazione diventa quindi fondamentale per analizzare come le imprese definiscono le proprie scelte strategiche e organizzative.

1.1.1 Struttura istituzionale e vincoli nei settori regolamentati

La presenza di un quadro regolamentare definito dalle autorità pubbliche all'interno dei cosiddetti settori regolamentati si esplica in un insieme di norme, vincoli e requisiti che disciplinano l'accesso al mercato, le modalità operative delle imprese, i sistemi di controllo a cui queste devono sottostare, l'uscita ordinata dal mercato.

La regolamentazione trova generalmente giustificazione nella presenza di specifiche caratteristiche economiche o sociali dei mercati. In molti casi essa è introdotta per garantire la stabilità del sistema economico, tutelare i consumatori o prevenire comportamenti opportunistici da parte degli operatori. In altri casi, la regolamentazione è necessaria per gestire settori caratterizzati da elevata complessità tecnica, rilevanza sistemica o potenziali fallimenti di mercato.

Tra gli esempi più rilevanti di settori regolamentati si possono citare il settore bancario e finanziario, soggetto alla vigilanza delle autorità di supervisione e a stringenti requisiti prudenziali, il settore energetico e quello farmaceutico, nei quali l'attività delle imprese è fortemente influenzata da autorizzazioni, standard tecnici e controlli istituzionali. In tali contesti, la regolamentazione diventa

quindi una componente strutturale dell'ambiente competitivo, contribuendo a definire le condizioni entro cui le imprese possono sviluppare le proprie strategie.

1.1.2 Implicazioni strategiche della regolamentazione

Le modalità con le quali la regolamentazione può influenzare la strategia aziendale riguarda: le decisioni di investimento, i modelli di business adottati, la gestione dei rischi e l'articolazione dell'assetto organizzativo. In molti casi, il rispetto delle normative richiede l'implementazione di idonee strutture organizzative e di adeguati sistemi di controllo, capaci di garantire la conformità alle disposizioni vigenti e di monitorare i principali rischi tipici dell'industria di appartenenza.

In questo senso, la regolamentazione diventa una componente strutturale dell'ambiente competitivo e contribuisce a definire il perimetro entro cui le imprese possono sviluppare le proprie strategie. Le imprese operanti in contesti regolamentati sono quindi chiamate non solo a competere sul mercato, ma anche a sviluppare capacità organizzative e sistemi di *governance* in grado di gestire in modo efficace i vincoli e le complessità derivanti dal contesto normativo.

1.1.3 Evoluzione dei sistemi di controllo nei contesti regolamentati

Nei contesti caratterizzati da una forte regolamentazione, l'esigenza di garantire il rispetto delle normative (*compliance risk*) e di gestire in modo efficace i rischi (ad esempio quelli operativi e finanziari) ha portato le imprese a sviluppare strutture organizzative e sistemi di controllo sempre più articolati. In tali realtà, i meccanismi di *governance* e i sistemi di controllo interno assumono un ruolo centrale nel garantire l'efficacia e l'affidabilità dei processi aziendali, nonché nel monitorare il rispetto delle disposizioni normative.

Tradizionalmente, tali sistemi erano concepiti principalmente come strumenti di conformità, finalizzati ad assicurare il rispetto delle regole imposte dalle autorità di vigilanza. Nel tempo, tuttavia, la crescente complessità dei contesti competitivi e l'evoluzione dei sistemi di *governance* hanno progressivamente ampliato il ruolo delle funzioni di controllo all'interno delle organizzazioni.

Oggi, i sistemi di controllo interno tendono a essere integrati nei più ampi assetti di *governance* e gestione dei rischi, assumendo un ruolo rilevante nel garantire l'affidabilità dei processi aziendali e la coerenza dell'organizzazione con il proprio contesto regolamentare.

1.2 Teorie strategiche di riferimento

Le dinamiche analizzate nei paragrafi precedenti, relative al ruolo della regolamentazione, dei sistemi di *governance*, delle funzioni di controllo e delle attività di vigilanza, possono essere interpretate alla luce delle principali prospettive teoriche dello *strategic management*. In particolare, la letteratura ha sviluppato tre prospettive fondamentali per spiegare la performance delle imprese: la *industry-based view*, la *resource-based view* e la *institution-based view*. L'integrazione di tali prospettive consente di costruire un quadro interpretativo unitario, in grado di spiegare come fattori competitivi, risorse interne e contesto istituzionale interagiscano nel determinare le scelte strategiche e organizzative delle imprese.

1.2.1 Le Cinque Forze di Porter e l'*Industry-Based View*

Le funzioni di controllo non si limitano più a verificare la conformità delle procedure, ma hanno il compito di valutare e gestire i rischi che l'impresa fronteggia e supportano il *management* nel conseguire in modo efficace ed efficiente gli obiettivi. Nel sistema dei controlli interni, la verifica dei processi aziendali è condotta dall'*Internal Audit*. Il modello delle "*Five Forces*" aiuta a comprendere dove si generano i rischi competitivi, quali pressioni esterne possono influenzare la *performance* aziendale, quali aree operative presentano una più elevata esposizione al rischio, consentendo quindi di mappare i fabbisogni in termini di controlli. Dunque, le Cinque Forze permettono di mappare il rischio competitivo dell'industria, che poi diventa input per il piano di *audit*. Nel *risk-based internal audit*, il piano di *audit* viene costruito proprio partendo dai principali rischi aziendali.

Il modello delle *Five Forces* si inserisce all'interno della cosiddetta *Industry-Based View* della strategia aziendale. Secondo questa prospettiva teorica, la *performance* delle imprese dipende in larga misura dalla struttura del settore in cui esse operano e dalle pressioni competitive esercitate dall'ambiente esterno. In questo senso, la redditività di un'impresa non è determinata esclusivamente dalle sue risorse interne, ma anche dalle caratteristiche del contesto in cui essa si trova a operare.

Il modello delle Cinque Forze, sviluppato da Michael Porter nel 1979, rappresenta uno dei contributi più influenti nel campo dello *strategic management*, introducendo un *framework* analitico utilizzato per comprendere la struttura competitiva di un settore e le determinanti della redditività delle imprese che vi operano. Porter parte dall'osservazione che molte analisi strategiche si concentrano esclusivamente sui concorrenti diretti, trascurando altri attori che esercitano pressioni competitive rilevanti. In realtà, la redditività di un'industria dipende dalla configurazione complessiva delle forze competitive che operano al suo interno. Il modello identifica cinque forze

fondamentali che determinano il livello di competizione e la distribuzione del valore economico tra le imprese. Tali forze sono: la rivalità tra concorrenti esistenti, la minaccia di nuovi entranti, il potere contrattuale dei fornitori, il potere contrattuale dei clienti, la minaccia di prodotti sostitutivi. Secondo Porter, l'analisi combinata di queste cinque forze consente di comprendere la struttura economica di un settore e di individuare le opportunità strategiche per ottenere un vantaggio competitivo. L'obiettivo della strategia non è soltanto competere con i rivali diretti, ma anche posizionarsi favorevolmente rispetto alle forze competitive. In questo modo, il modello delle *Five Forces* diventa uno strumento fondamentale per analizzare l'attrattiva di un'industria e guidare la formulazione della strategia aziendale.

Tuttavia, negli ultimi decenni diversi studiosi hanno messo in discussione l'efficacia del modello nel contesto dei mercati moderni. Una delle principali critiche riguarda il fatto che il *framework* è stato sviluppato in un periodo in cui le industrie erano relativamente stabili e caratterizzate da strutture competitive ben definite. Oggi, invece, molti settori sono caratterizzati da rapida innovazione tecnologica, convergenza tra industrie e nuovi modelli di *business*. Un'altra critica riguarda la natura relativamente statica del modello, che tende a descrivere la struttura di un'industria in un determinato momento senza considerare pienamente i cambiamenti dinamici nel tempo. Inoltre, il modello è stato accusato di trascurare il ruolo delle collaborazioni strategiche, delle piattaforme digitali e degli ecosistemi di innovazione.

Nonostante queste critiche, il modello delle *Five Forces* rimane uno strumento utile per comprendere le dinamiche competitive dei mercati. Piuttosto che essere abbandonato, il *framework* potrebbe essere integrato con altri approcci teorici, come la *Resource-Based View*, che enfatizza il ruolo delle risorse interne dell'impresa, o la *Blue Ocean Strategy*, che propone la creazione di nuovi spazi di mercato attraverso innovazione e differenziazione. In questa prospettiva, l'analisi della struttura competitiva dell'industria rappresenta un primo livello di comprensione dei rischi strategici che possono influenzare la *performance* aziendale. Per l'*internal audit*, tali analisi costituiscono un importante punto di partenza per l'identificazione dei rischi esterni e per la definizione delle priorità nel piano di *audit*.

Dunque, il modello di Porter continua a rappresentare una base importante per l'analisi strategica, ma la sua applicazione andrebbe adattata alle caratteristiche dei mercati contemporanei, integrandolo con altre prospettive teoriche.

1.2.2 La *Resource-Based View*

Secondo la *Resource-Based View* (RBV), sviluppata da Birger Wernerfelt nel 1984 e successivamente formalizzata da Jay Barney nel 1991, le differenze di *performance* tra imprese non dipendono solo dalla struttura del settore, ma soprattutto dalle risorse e capacità interne dell'organizzazione. Le imprese ottengono un vantaggio competitivo quando possiedono risorse che creano valore economico (*valuable*), non sono diffuse tra i concorrenti (*rare*), sono difficili da imitare (*inimitable*) e sono gestite in modo efficace dall'organizzazione (*organized*). Le risorse strategiche possono includere *asset* tangibili, ma spesso riguardano soprattutto risorse intangibili, come conoscenze organizzative, capitale umano, tecnologia proprietaria, reputazione o cultura aziendale.

La *Resource-Based View* nasce anche come risposta alle teorie strategiche tradizionali che spiegavano la *performance* delle imprese principalmente attraverso la struttura dell'industria, come nel caso del modello delle *Five Forces*. Questo approccio propone invece una prospettiva alternativa, secondo cui le differenze di performance tra imprese dipendono soprattutto dalle risorse e competenze interne. In questa prospettiva, il vantaggio competitivo sostenibile deriva dalla capacità dell'organizzazione di sviluppare e combinare risorse che non sono facilmente replicabili dai concorrenti, tra cui conoscenze organizzative, competenze manageriali, reputazione e sistemi organizzativi.

Un contributo rilevante della RBV riguarda inoltre il concetto di *capabilities*, ovvero le capacità dell'organizzazione di coordinare e integrare risorse diverse per svolgere attività complesse. Tali capacità sono spesso incorporate nelle *routine* organizzative e si sviluppano nel tempo attraverso processi di apprendimento. Questo approccio ha contribuito a spostare l'attenzione della strategia aziendale dalla semplice analisi del mercato alla comprensione delle fonti interne di vantaggio competitivo, ponendo maggiore enfasi su innovazione, conoscenza organizzativa e sviluppo delle competenze.

In questa prospettiva teorica, l'*internal audit* assume un ruolo importante perché contribuisce a preservare e migliorare l'utilizzo delle risorse che generano vantaggio competitivo. Attraverso le attività di *assurance* e consulenza, l'*internal audit* verifica che le risorse strategiche siano protette da rischi operativi o finanziari, che i processi aziendali permettano di sfruttare efficacemente tali risorse, che i sistemi di controllo interno supportino la creazione di valore nel lungo periodo.

La connessione tra RBV e *internal audit* diventa ancora più evidente nel modello di *risk-based internal auditing*. Questo approccio prevede che l'*audit* concentri le proprie attività sulle aree che rappresentano i rischi più rilevanti per il raggiungimento degli obiettivi strategici. Poiché le risorse

strategiche sono alla base del vantaggio competitivo, eventuali inefficienze o vulnerabilità nella loro gestione rappresentano rischi critici per l'organizzazione.

1.2.3 La *Institution-Based View*

La *Institution-Based View* rappresenta una prospettiva teorica che enfatizza il ruolo delle istituzioni nel determinare il comportamento delle imprese e le loro *performance*. Secondo questo approccio, le strategie aziendali non sono influenzate esclusivamente dalle caratteristiche dell'industria o dalle risorse interne dell'impresa, ma anche dal contesto istituzionale in cui l'organizzazione opera. In questa prospettiva, l'analisi strategica non può essere spiegata esclusivamente attraverso due prospettive tradizionali: la *industry-based view*, che analizza la struttura competitiva del settore, e la *resource-based view*, che si concentra sulle risorse interne dell'impresa. Per comprendere pienamente il comportamento strategico delle imprese è quindi necessario integrare una terza prospettiva, quella istituzionale. Questa integrazione ha portato allo sviluppo del cosiddetto *strategy tripod*, un modello teorico che considera congiuntamente tre dimensioni fondamentali della strategia: struttura del settore, risorse e capacità dell'impresa, contesto istituzionale in cui essa opera.

Le istituzioni possono essere definite come l'insieme delle regole formali e informali che strutturano le interazioni economiche e sociali, includendo elementi quali leggi, regolamenti, politiche pubbliche, norme sociali, valori culturali e pratiche consolidate. La prospettiva istituzionale evidenzia inoltre che imprese operanti in contesti istituzionali differenti tendono a sviluppare strategie diverse, anche quando operano nello stesso settore o possiedono risorse simili. In altre parole, il contesto normativo, politico e sociale contribuisce a spiegare perché imprese apparentemente comparabili adottino scelte strategiche differenti e ottengano performance diverse.

Il quadro istituzionale rappresenta una fonte rilevante di vincoli e opportunità per le imprese. Cambiamenti delle normative, nelle politiche pubbliche o nelle aspettative sociali possono generare rischi significativi per l'organizzazione, influenzando le decisioni strategiche e le modalità operative dell'impresa. La gestione di tali rischi richiede un sistema di *governance* e di controllo capace di monitorare l'evoluzione dell'ambiente istituzionale e di assicurare che i processi aziendali rimangano coerenti con le normative e le aspettative degli *stakeholder*.

In tale contesto, l'*Internal Audit* rileva soprattutto come presidio indipendente sull'adeguatezza dei controlli rispetto ai rischi derivanti dall'ambiente istituzionale e regolamentare. In questo modo, la prospettiva istituzionale completa le altre principali teorie della strategia aziendale. Se la *industry-*

based view consente di analizzare i rischi derivanti dalla struttura competitiva del settore e la *resource-based view* permette di comprendere quelli legati alla gestione delle risorse strategiche dell'impresa, la *institution-based view* consente di considerare i rischi derivanti dal contesto normativo, politico e sociale in cui l'impresa opera. L'integrazione di queste tre prospettive offre quindi un quadro analitico più completo per l'identificazione e la gestione dei rischi strategici.

1.3 Corporate governance ed evoluzione delle funzioni di controllo

La *corporate governance* e i sistemi di controllo interno rappresentano elementi fondamentali per il funzionamento delle organizzazioni, in quanto definiscono i meccanismi attraverso i quali vengono prese, monitorate e valutate le decisioni aziendali. In contesti caratterizzati dalla separazione tra proprietà e controllo e da una crescente complessità operativa e regolamentare, tali sistemi assumono un ruolo centrale nel garantire l'allineamento tra gli interessi dei diversi attori coinvolti e nel presidiare i rischi connessi all'attività d'impresa.

Nel tempo, l'evoluzione dei sistemi di *governance* ha ampliato il rilievo delle funzioni di controllo, rendendole componenti sempre più integrate nei meccanismi di supervisione, gestione dei rischi e *accountability*.

1.3.1 Agency theory e problemi di governance

Uno dei principali riferimenti teorici per comprendere il ruolo dei sistemi di *governance* e di controllo nelle organizzazioni è rappresentato dalla teoria dell'agenzia. Questo filone di ricerca è stato sviluppato in modo sistematico a partire dagli anni Settanta, in particolare con il contributo di Michael C. Jensen e William H. Meckling, che nel celebre articolo "*Theory of the Firm: Managerial Behavior, Agency Costs and Ownership Structure*" (1976) hanno analizzato le implicazioni economiche derivanti dalla separazione tra proprietà e controllo nelle imprese moderne. Secondo gli autori, nelle organizzazioni complesse si instaura frequentemente una relazione di agenzia, definita come un rapporto contrattuale nel quale uno o più soggetti, detti *principals*, delegano a un altro soggetto, detto *agent*, lo svolgimento di un'attività e il potere di prendere decisioni per loro conto. Nel contesto delle imprese societarie, questa relazione si manifesta tipicamente tra azionisti e *management*, dove i primi affidano ai secondi la gestione operativa dell'impresa. La delega decisionale comporta tuttavia l'emergere di potenziali conflitti di interesse, poiché *principals* e *agents* possono perseguire obiettivi differenti. Jensen e Meckling evidenziano come tali divergenze generino i cosiddetti costi di agenzia, che rappresentano il costo economico della delega e comprendono tre componenti principali: i costi

di monitoraggio sostenuti dai *principals* per controllare il comportamento degli *agents*, i costi di vincolo (*bonding costs*) sostenuti dagli *agents* per garantire l'allineamento degli interessi, e la perdita residua (*residual loss*) che permane anche dopo l'introduzione di meccanismi di controllo. Un ulteriore contributo rilevante della teoria dell'agenzia riguarda la concezione dell'impresa come rete di relazioni contrattuali (*nexus of contracts*) tra diversi soggetti economici, tra cui azionisti, *manager*, creditori e altri *stakeholder*. In questa prospettiva, i problemi di *governance* derivano dalla necessità di coordinare interessi potenzialmente divergenti tra tali soggetti.

Questi temi sono stati ulteriormente sviluppati da Eugene F. Fama e Michael C. Jensen nel lavoro "*Agency Problems and Residual Claims*" (1983), nel quale gli autori analizzano il ruolo dei diritti sui flussi di cassa residui (*residual claims*) nelle diverse forme organizzative. In particolare, nelle grandi società per azioni si osserva una separazione tra coloro che sopportano il rischio economico residuo, ossia gli azionisti, e coloro che esercitano il potere decisionale, cioè i *manager*. In tali contesti diventa quindi fondamentale distinguere tra *decision management*, che comprende l'iniziativa e l'implementazione delle decisioni operative, e *decision control*, che consiste nella ratifica e nel monitoraggio delle decisioni stesse. I sistemi di *corporate governance* e i sistemi di controllo interno assumono un ruolo centrale, poiché rappresentano gli strumenti attraverso i quali l'organizzazione cerca di ridurre i costi di agenzia e di assicurare un comportamento coerente con gli interessi dei proprietari e degli altri *stakeholder*. Tali sistemi comprendono, tra l'altro, meccanismi di supervisione da parte degli organi societari, sistemi di incentivazione manageriale, procedure di gestione del rischio e strutture organizzative dedicate al controllo.

All'interno del sistema dei controlli, la funzione di *internal audit* rappresenta uno dei principali strumenti attraverso cui l'organizzazione realizza concretamente le attività di monitoraggio previste dalla teoria dell'agenzia. L'*internal audit* svolge infatti un ruolo indipendente di valutazione dell'efficacia dei sistemi di controllo interno, di gestione dei rischi e di *governance* aziendale. Attraverso verifiche sistematiche e attività di *assurance*, tale funzione contribuisce a ridurre le asimmetrie informative tra *management* e organi di governo, rafforzando i meccanismi di *accountability* e limitando i comportamenti opportunistici che potrebbero emergere nelle relazioni di agenzia. La teoria dell'agenzia, dunque, fornisce una solida base teorica per comprendere l'importanza dei sistemi di controllo all'interno delle organizzazioni. Le strutture di *governance*, i meccanismi di monitoraggio e le funzioni di controllo non rappresentano semplicemente strumenti amministrativi, ma costituiscono elementi essenziali per garantire il corretto funzionamento delle imprese, in particolar modo di quelle caratterizzate dalla separazione tra proprietà e gestione.

1.3.2 Dalla funzione di *compliance* al ruolo strategico dei controlli

Tradizionalmente, le funzioni di controllo all'interno delle organizzazioni sono state concepite principalmente come strumenti volti a garantire il rispetto delle normative e delle procedure interne. In questa prospettiva, il loro ruolo era prevalentemente orientato alla verifica della conformità (*compliance*), attraverso attività di monitoraggio e controllo svolte spesso *ex post* rispetto ai processi decisionali e operativi. Le funzioni di controllo erano quindi considerate come presidi di natura prevalentemente amministrativa, finalizzati a ridurre il rischio di violazioni normative, errori operativi o comportamenti opportunistici all'interno dell'organizzazione. In questa visione tradizionale, il controllo interno rappresenta un insieme di procedure e meccanismi destinati a fornire una ragionevole sicurezza circa il raggiungimento degli obiettivi aziendali in termini di affidabilità delle informazioni, efficacia operativa e conformità alle normative.

Nel tempo, tuttavia, l'evoluzione dei contesti economici e istituzionali ha profondamente modificato questo approccio. L'aumento della complessità organizzativa, l'internazionalizzazione delle imprese, la crescente articolazione dei mercati e il rafforzamento dei sistemi regolatori hanno reso sempre più evidente la necessità di integrare i sistemi di controllo all'interno dei processi di gestione e di governo dell'impresa. In particolare, nelle industrie fortemente regolamentate, le funzioni di controllo hanno assunto un ruolo centrale nel presidiare i rischi operativi, finanziari e regolamentari, contribuendo alla stabilità e alla sostenibilità dell'attività aziendale. In questo contesto, i sistemi di controllo interno sono progressivamente diventati parte integrante dei più ampi sistemi di *governance*.

Alla luce di tali trasformazioni, il controllo non viene più interpretato esclusivamente come un'attività di verifica della conformità, ma come uno strumento di supporto alla gestione dei rischi e al miglioramento dei processi organizzativi. Le funzioni di controllo possono infatti contribuire a identificare potenziali criticità nei processi aziendali, a rafforzare i meccanismi di *governance* e il presidio dei rischi aziendali. In questa prospettiva, il controllo assume progressivamente una dimensione più proattiva e integrata rispetto alla gestione dell'impresa, affiancando le attività di verifica tradizionali con funzioni di monitoraggio continuo e di supporto ai processi decisionali.

La letteratura manageriale sottolinea come i sistemi di controllo possano svolgere un ruolo rilevante non solo nella prevenzione dei rischi, ma anche nel supporto all'implementazione della strategia aziendale. In particolare, essi consentono di monitorare l'allineamento tra gli obiettivi strategici definiti dal *management* e le attività operative svolte all'interno dell'organizzazione, contribuendo a migliorare la coerenza tra strategia e operatività. Pertanto, i sistemi di controllo non

rappresentano più soltanto strumenti di verifica, ma costituiscono meccanismi fondamentali attraverso i quali le imprese guidano e coordinano l'attuazione delle proprie strategie.

Ne deriva una concezione più ampia dei controlli interni, non più limitata alla verifica formale delle procedure, ma orientata anche al rafforzamento dell'affidabilità informativa, della gestione dei rischi e della coerenza tra strategia e operatività.

1.3.3 Le funzioni di controllo come *capability* organizzative

La letteratura di strategia aziendale ha progressivamente riconosciuto il ruolo delle risorse e delle competenze interne come fattori determinanti del vantaggio competitivo. In particolare, secondo la prospettiva della *Resource-Based View* (par. 1.2.2), le imprese sono in grado di generare valore e ottenere *performance* superiori quando possiedono risorse e capacità difficilmente imitabili dai concorrenti e in grado di sostenere nel tempo la strategia aziendale. In questo quadro teorico, le *capability* organizzative rappresentano l'insieme di competenze, *routine* e sistemi che consentono all'impresa di coordinare e integrare le proprie risorse in modo efficace.

Nel contesto delle organizzazioni contemporanee, caratterizzate da elevata complessità operativa e da un crescente livello di regolamentazione, le funzioni di controllo tendono a essere interpretate non soltanto come strumenti di verifica o di conformità normativa, ma come vere e proprie *capability* organizzative. Attraverso procedure, strumenti di monitoraggio e flussi informativi strutturati, essi permettono all'organizzazione di raccogliere e analizzare informazioni rilevanti per la gestione delle attività aziendali. Tali sistemi contribuiscono inoltre a ridurre l'incertezza nei processi decisionali, a rafforzare il coordinamento tra le diverse unità organizzative e a migliorare la capacità dell'impresa di individuare tempestivamente eventuali criticità nei processi operativi.

Le funzioni di controllo assumono un ruolo particolarmente rilevante anche nel supportare l'attuazione della strategia aziendale. Come evidenziato nella letteratura sui sistemi di controllo strategico, tali strumenti consentono al *management* di monitorare il grado di avanzamento degli obiettivi strategici e di verificare la coerenza tra le decisioni operative e le priorità strategiche dell'organizzazione. I sistemi di controllo contribuiscono quindi non solo a prevenire comportamenti opportunistici o inefficienze operative, ma anche a favorire l'allineamento tra strategia, struttura organizzativa e processi decisionali.

Di conseguenza, quando sono progettate in modo coerente con la strategia aziendale, le funzioni di controllo possono essere interpretate come *capability* organizzative: non semplici presidi

procedurali, ma sistemi di competenze, *routine* e flussi informativi che rafforzano il coordinamento e la qualità delle decisioni.

1.4 Il ruolo della vigilanza nei contesti iper-regolamentati

Nei contesti economici caratterizzati da un elevato livello di regolamentazione, il ruolo delle autorità di vigilanza assume una rilevanza crescente nel definire le modalità di funzionamento e di governo delle organizzazioni. In tali ambiti, le imprese operano all'interno di un sistema istituzionale complesso, nel quale norme, autorità di controllo e meccanismi di supervisione contribuiscono a orientare i comportamenti organizzativi e a delimitare gli spazi di autonomia decisionale.

In questo scenario, i sistemi di controllo interno e i presidi di *governance* si inseriscono in un quadro più ampio di regole e vincoli, assumendo una funzione centrale nel garantire l'equilibrio tra obiettivi aziendali, gestione dei rischi e rispetto delle disposizioni normative. L'analisi del ruolo della vigilanza e della sua interazione con i meccanismi interni di controllo consente quindi di comprendere come le organizzazioni operanti in contesti iper-regolamentati strutturino i propri sistemi di governo e affrontino le complessità derivanti dall'ambiente esterno.

1.4.1 Il ruolo dei sistemi di controllo nella riduzione dei conflitti di interesse

Nell'analizzare il ruolo della teoria dell'agenzia è stato evidenziato come la separazione tra proprietà e gestione possa generare conflitti di interesse e asimmetrie informative tra i diversi soggetti coinvolti nella *governance* dell'impresa. In presenza di tali relazioni di agenzia, le organizzazioni tendono a sviluppare meccanismi istituzionali e organizzativi volti a limitare comportamenti opportunistici e a garantire un adeguato allineamento tra gli interessi del *management* e quelli dei proprietari. In questo contesto, i sistemi di controllo interno rappresentano uno degli strumenti principali attraverso cui le imprese cercano di ridurre i costi di agenzia e di assicurare una gestione efficiente e trasparente delle attività aziendali.

In generale, il sistema di controllo interno può essere definito come l'insieme di regole, procedure e strutture organizzative progettate per fornire una ragionevole sicurezza circa il corretto funzionamento dell'impresa e il raggiungimento degli obiettivi aziendali. In tale ambito, il sistema di controllo interno opera lungo diverse dimensioni, tra cui l'efficacia e l'efficienza delle operazioni, l'affidabilità delle informazioni finanziarie e il rispetto della normativa applicabile, svolgendo una funzione essenziale nel ridurre i costi di agenzia e nel limitare le asimmetrie informative tra i diversi soggetti coinvolti nella *governance* dell'impresa.

La rilevanza dei sistemi di controllo risulta particolarmente evidente nel settore bancario e finanziario, dove la complessità delle attività svolte e la presenza di rischi elevati richiedono strutture organizzative e meccanismi di supervisione particolarmente articolati. Le banche, infatti, gestiscono il risparmio del pubblico e svolgono un ruolo centrale nel funzionamento del sistema economico e in quello dei pagamenti, motivo per cui sono soggette a un quadro regolamentare particolarmente stringente. In questo contesto, la regolamentazione prudenziale attribuisce grande importanza alla presenza di sistemi di controllo interno efficaci e indipendenti, considerati uno strumento fondamentale per garantire una gestione sana e prudente degli intermediari finanziari.

1.4.2 I livelli del sistema dei controlli interni del settore bancario

Nel settore bancario, l'importanza dei sistemi di controllo interno è formalizzata nel quadro regolamentare definito dalla Circolare n. 285 della Banca d'Italia, che disciplina l'assetto organizzativo e il funzionamento dei sistemi di controllo degli intermediari. La complessità delle attività svolte dalle banche, l'elevata esposizione ai rischi finanziari e operativi e il ruolo centrale che tali istituzioni rivestono nel funzionamento del sistema economico rendono necessario un quadro regolamentare particolarmente rigoroso. La Circolare n. 285 della Banca d'Italia disciplina, tra le altre cose, l'assetto organizzativo e il funzionamento dei sistemi di controllo interno degli intermediari bancari, definendo principi e requisiti volti a rafforzare la solidità e la stabilità del sistema finanziario.

La normativa attribuisce un ruolo centrale al sistema dei controlli interni, inteso come l'insieme delle regole, delle procedure e delle strutture organizzative che concorrono ad assicurare il corretto funzionamento dell'impresa bancaria. Tale sistema è finalizzato a garantire il rispetto delle norme, la corretta gestione dei rischi, l'affidabilità delle informazioni aziendali e la tutela del patrimonio dell'intermediario. Dunque, il sistema dei controlli rappresenta uno strumento essenziale per sostenere il processo decisionale degli organi aziendali e per assicurare che l'attività della banca sia svolta in modo coerente con gli obiettivi strategici e con i principi di sana e prudente gestione.

La Circolare n. 285 prevede che il sistema dei controlli interni sia strutturato secondo un'architettura articolata su diversi livelli (*Three Lines Model*), ciascuno dei quali svolge funzioni specifiche ma complementari. Questa articolazione consente di distribuire le responsabilità di controllo all'interno dell'organizzazione e di garantire un monitoraggio continuo e indipendente dei processi aziendali.

Il primo livello di controllo è rappresentato dai cosiddetti controlli di linea, che sono integrati direttamente nei processi operativi e sono svolti dalle stesse unità organizzative responsabili delle attività aziendali. Tali controlli hanno lo scopo di assicurare il corretto svolgimento delle operazioni e di verificare che le attività siano svolte nel rispetto delle procedure interne e delle politiche di gestione dei rischi definite dalla banca. In questa prospettiva, i responsabili delle diverse aree operative sono i primi soggetti chiamati a presidiare i rischi connessi alle attività svolte.

Il secondo livello di controllo è costituito dalle funzioni aziendali specializzate nel monitoraggio e nella gestione dei rischi. Tra queste rientrano in particolare la funzione di *risk management* e la funzione di *compliance*, alle quali è affidato, rispettivamente, il compito di supportare gli organi aziendali nella definizione e nell'attuazione delle politiche di gestione dei rischi e di verificare il rispetto della normativa applicabile. Queste funzioni operano in modo indipendente rispetto alle unità operative e svolgono un ruolo fondamentale nel garantire che i rischi assunti dalla banca siano coerenti con le strategie e con il livello di rischio ritenuto accettabile dall'intermediario.

Il terzo livello di controllo è rappresentato dalla funzione di *internal audit*, alla quale è attribuito il compito di valutare in modo indipendente e sistematico l'adeguatezza e l'efficacia complessiva dei processi aziendali, incluso il sistema dei controlli interni. Attraverso attività di verifica e di analisi dei processi aziendali, l'*internal audit* fornisce agli organi di governo della banca un giudizio sull'effettivo funzionamento dei meccanismi di controllo e sull'efficacia delle procedure di gestione dei rischi. In questo modo, la funzione di revisione interna contribuisce a rafforzare la trasparenza e l'affidabilità del sistema di *governance*.

Nel loro insieme, i diversi livelli di controllo previsti dalla normativa consentono di creare un sistema di supervisione articolato e complementare, nel quale ciascuna funzione contribuisce al presidio dei rischi e alla corretta gestione dell'intermediario. L'adozione di un sistema dei controlli interni strutturato secondo tali principi rappresenta quindi uno degli elementi essenziali per assicurare la stabilità e la solidità delle istituzioni bancarie, nonché per tutelare la fiducia dei depositanti e degli altri *stakeholder* nel sistema finanziario.

Capitolo 2 - Evoluzione strategica dell'*Internal Audit* e driver di cambiamento

2.1 La funzione aziendale di controllo di terzo livello: l'*Internal Audit*

L'*Internal Audit* rappresenta una componente centrale nei moderni sistemi di *corporate governance*, il cui ruolo è progressivamente evoluto in risposta alla crescente complessità organizzativa e regolamentare. In particolare, la funzione si colloca all'intersezione tra controllo, gestione del rischio e supporto ai processi decisionali, contribuendo al corretto funzionamento dell'impresa.

Il presente paragrafo analizza l'*Internal Audit* come funzione aziendale, esaminandone dapprima la definizione e le finalità, per poi approfondirne la collocazione organizzativa e i requisiti di indipendenza.

2.1.1 Definizione e finalità dell'*Internal Audit*

L'*Internal Auditing* si definisce, secondo il quadro normativo dell'*Institute of Internal Auditors* (IIA), come un'attività indipendente e obiettiva di *assurance* e consulenza, finalizzata al miglioramento dei processi operativi e alla creazione di valore per l'organizzazione. Tale funzione opera attraverso un approccio sistematico e disciplinato, volto a valutare l'adeguatezza e l'efficacia dei sistemi di *governance*, di gestione dei rischi e di controllo interno. L'*Internal Audit* assume un ruolo centrale all'interno dell'assetto organizzativo dell'impresa, poiché contribuisce a rafforzare l'affidabilità dei processi decisionali e informativi. Attraverso le proprie attività di verifica, la funzione consente agli organi di governo e al *management* di disporre di una valutazione indipendente sul funzionamento dei principali presidi organizzativi. In tal modo, essa contribuisce a ridurre le asimmetrie informative tra i diversi livelli dell'organizzazione e a rafforzare i meccanismi di *accountability* e supervisione.

Le finalità dell'*Internal Audit* possono essere ricondotte a due principali ambiti di attività. Il primo riguarda l'attività di *assurance*, attraverso la quale la funzione valuta in modo indipendente l'adeguatezza dei sistemi di controllo interno, la correttezza dei processi di gestione dei rischi e la coerenza delle attività aziendali rispetto alle procedure e agli obiettivi dell'organizzazione. Tale attività consente di individuare eventuali criticità nei processi operativi, finanziari o di conformità, fornendo agli organi competenti elementi utili per intervenire in modo tempestivo. Il secondo ambito

riguarda l'attività di consulenza, che si sostanzia nel supporto al *management* attraverso analisi, raccomandazioni e suggerimenti volti al miglioramento dei processi aziendali. In questo caso, l'*Internal Audit* non sostituisce le funzioni operative né assume responsabilità gestionali, ma contribuisce a individuare aree di miglioramento e a rafforzare l'efficacia complessiva dell'organizzazione. Tale dimensione mostra come la funzione possa affiancare all'*assurance* tradizionale un contributo consulenziale, pur senza assumere responsabilità operative.

2.1.2 Collocazione organizzativa e indipendenza

L'efficacia operativa dell'*Internal Audit* è intrinsecamente legata alla sua capacità di operare con indipendenza e obiettività, pilastri fondamentali che ne garantiscono l'integrità e l'affidabilità agli occhi degli *stakeholder*.

Secondo gli standard professionali dell'IIA, l'indipendenza deve essere garantita a livello organizzativo, assicurando che il *Chief Audit Executive* (CAE) riferisca a un livello gerarchico tale da permettere alla funzione di adempiere alle proprie responsabilità senza restrizioni o condizionamenti. Questo requisito si traduce concretamente nell'adozione di una struttura di *reporting* duale, che bilancia le esigenze di supervisione strategica con quelle di gestione operativa quotidiana. Da un lato, il riporto funzionale verso l'organo di supervisione, come il comitato controllo e rischi o l'*audit committee*, consente di preservare l'autonomia della funzione e di garantire che il piano di *audit*, le principali risultanze delle verifiche e le eventuali criticità emerse siano portate all'attenzione degli organi competenti. Dall'altro lato, il riporto amministrativo verso l'alta direzione (solitamente il CEO o il CFO) permette alla funzione di disporre delle risorse organizzative necessarie allo svolgimento delle proprie attività ordinarie. La combinazione di questi due livelli di riporto consente quindi di bilanciare l'esigenza di indipendenza con quella di integrazione della funzione all'interno dell'organizzazione.

Accanto all'indipendenza organizzativa, assume rilievo anche il principio di obiettività. Gli *auditor* interni devono, infatti, mantenere un giudizio imparziale nello svolgimento delle proprie attività, evitando il coinvolgimento diretto in decisioni o responsabilità operative che potrebbero compromettere la neutralità delle valutazioni successive. In questa prospettiva, l'*Internal Audit* può supportare il *management* attraverso analisi e raccomandazioni, ma non deve sostituirsi alle funzioni operative né assumere responsabilità gestionali dirette. Il mantenimento di questa distinzione è essenziale per preservare la credibilità della funzione e la qualità dell'*assurance* fornita agli organi di governo.

La corretta collocazione dell'*Internal Audit* è inoltre coerente con l'architettura dei sistemi di controllo interno articolata su tre livelli, nella quale la funzione di *audit* rappresenta un presidio indipendente rispetto ai controlli di linea e alle funzioni di secondo livello. Dunque, l'*Internal Audit* non interviene direttamente nella gestione quotidiana dei rischi, ma valuta l'adeguatezza complessiva dei presidi adottati dall'organizzazione e la loro capacità di supportare il raggiungimento degli obiettivi aziendali.

L'indipendenza, tuttavia, non deve essere intesa come isolamento organizzativo. Affinché la funzione possa operare in modo efficace, è necessario che essa mantenga un'interazione costante con il *management* e con gli altri attori del sistema di *governance*, preservando al tempo stesso la propria autonomia di giudizio. Il supporto degli organi aziendali e dell'alta direzione contribuisce a rafforzare la legittimazione dell'*Internal Audit* all'interno dell'organizzazione e a favorire una cultura del controllo maggiormente integrata nei processi decisionali. In questo senso, la collocazione organizzativa della funzione rappresenta una condizione essenziale non solo per garantire l'indipendenza delle verifiche, ma anche per consentire all'*Internal Audit* di contribuire in modo più efficace al miglioramento dei processi e alla gestione dei rischi aziendali.

2.2 Trade-off tra costi della *compliance* e benefici del controllo

La progettazione dei sistemi di controllo interno implica un equilibrio tra l'esigenza di presidiare i rischi aziendali e quella di evitare un'eccessiva rigidità organizzativa. Nei contesti regolamentati, infatti, il controllo rappresenta una condizione essenziale per garantire conformità, affidabilità e stabilità, ma richiede anche risorse economiche, professionali e tecnologiche. Per questo motivo, il livello ottimale di controllo deve essere valutato in rapporto alla complessità dell'impresa, al suo profilo di rischio e ai benefici attesi in termini di riduzione delle criticità operative, regolamentari e reputazionali.

2.2.1 I costi della *compliance* e dei sistemi di controllo

L'implementazione di un sistema di controllo interno e il mantenimento della conformità normativa comporta per l'impresa un rilevante impiego di risorse economiche, organizzative e professionali. Tale investimento si traduce in una serie di oneri che possono essere distinti in costi diretti, facilmente quantificabili in termini monetari, e costi indiretti, legati alle dinamiche organizzative e all'efficienza operativa. In un'ottica di analisi marginale, all'aumentare della qualità dell'*audit* e della profondità delle verifiche, il prezzo unitario dell'assicurazione (*assurance*) tende a

crescere, riflettendo la maggiore complessità e lo sforzo richiesto per ridurre il rischio a livelli accettabili.

I costi diretti comprendono, in primo luogo, le risorse destinate alle funzioni di controllo, alla formazione del personale, all'adozione di sistemi informativi e strumenti tecnologici di monitoraggio, nonché alle attività di *audit* interno ed esterno. In organizzazioni complesse, tali attività richiedono competenze specialistiche e strutture dedicate, capaci di assicurare un controllo continuo sui processi aziendali e una corretta gestione degli adempimenti normativi. Di conseguenza, la *compliance* non rappresenta soltanto un obbligo formale, ma implica la costruzione di un assetto organizzativo in grado di sostenere nel tempo le attività di controllo e supervisione, nonché per implementare tecnologie avanzate di monitoraggio.

Accanto ai costi direttamente misurabili, assumono rilievo anche i costi indiretti, legati agli effetti che un sistema di controllo può produrre sul funzionamento dell'organizzazione. Un sistema di controllo eccessivamente rigido o caratterizzato da un'elevata burocratizzazione può indurre un rallentamento dei processi decisionali e una perdita di agilità organizzativa. La letteratura evidenzia il rischio di una "perdita secca" derivante dall'*over-regulation*, ovvero quando lo sforzo per implementare ulteriori controlli supera i benefici reali che questi possono produrre.

Un ulteriore rischio è rappresentato dall'adozione di un approccio meramente formale alla *compliance*, talvolta definito *check-the-box approach*. In tale prospettiva, l'attenzione dell'organizzazione si concentra prevalentemente sul rispetto formale delle procedure, piuttosto che sulla capacità effettiva dei controlli di individuare criticità, prevenire rischi e migliorare i processi aziendali. Il controllo, in questo modo, può perdere la propria funzione sostanziale e diventare un adempimento burocratico, con benefici limitati rispetto ai costi sostenuti.

Infine, non va trascurato l'onere in termini di tempo e distrazione del *management*. Le attività di verifica, documentazione e *reporting* richiedono infatti il coinvolgimento di diverse funzioni aziendali e possono assorbire risorse che potrebbero essere destinate ad attività operative o strategiche. In sintonia con la teoria dell'agenzia, i costi della *compliance* possono essere interpretati anche come costi di monitoraggio, necessari per ridurre le asimmetrie informative e limitare comportamenti opportunistici, ma che devono essere mantenuti entro livelli proporzionati alla complessità dell'organizzazione e al suo profilo di rischio.

2.2.2 I benefici del controllo interno e dell'*audit*

Il controllo interno non deve essere interpretato esclusivamente come un onere burocratico o una barriera all'operatività. Al contrario, esso può rappresentare una componente vitale per supportare le organizzazioni nel raggiungimento dei propri obiettivi strategici e nel miglioramento costante delle *performance*.

Un primo beneficio riguarda la capacità dei sistemi di controllo di ridurre l'esposizione dell'impresa ai principali rischi operativi, finanziari, regolamentari e reputazionali. Attraverso procedure, responsabilità definite e attività di monitoraggio, il controllo interno consente di individuare tempestivamente eventuali criticità e di intervenire prima che esse producano effetti negativi sull'organizzazione. Tale funzione assume particolare rilevanza nei contesti caratterizzati da elevata complessità e incertezza, nei quali la capacità di presidiare i rischi rappresenta una condizione essenziale per garantire la continuità e la stabilità dell'attività aziendale.

Un secondo beneficio riguarda la qualità delle informazioni disponibili per il *management*, per gli organi di governo e per gli *stakeholder* esterni. I sistemi di controllo interno contribuiscono infatti a rafforzare l'affidabilità dei flussi informativi e del *reporting* aziendale, riducendo il rischio che le decisioni siano assunte sulla base di dati incompleti, non aggiornati o non corretti. In tale ambito, l'*Internal Audit* svolge un ruolo rilevante, poiché valuta in modo indipendente l'adeguatezza dei processi informativi e dei presidi adottati dall'organizzazione. Alcuni studi empirici hanno inoltre evidenziato una relazione positiva tra la qualità della funzione di *Internal Audit* e l'accuratezza delle previsioni formulate dal *management*, come nel caso delle *management earnings forecasts*¹.

Un ulteriore beneficio riguarda la riduzione delle asimmetrie informative tra i diversi attori della *corporate governance*. Come evidenziato dalla teoria dell'agenzia, la separazione tra proprietà e gestione può generare conflitti di interesse tra il *management*, in qualità di *agent*, e gli azionisti o gli organi di governo, in qualità di *principal*. In questo contesto, l'*Internal Audit* agisce come un meccanismo di monitoraggio indipendente, contribuendo ad attenuare tali conflitti attraverso valutazioni oggettive sull'adeguatezza dei processi aziendali e sull'efficacia dei sistemi di gestione dei rischi. In tal modo, la funzione rafforza i meccanismi di *accountability* e limita il rischio di comportamenti opportunistici che potrebbero compromettere la creazione e la protezione del valore aziendale.

¹ Per *management earnings forecasts* si intendono le comunicazioni societarie volontarie attraverso le quali la direzione aziendale (*management*) diffonde stime e previsioni relative alle performance finanziarie future dell'impresa. Lo scopo primario di tali annunci è ridurre l'asimmetria informativa esistente tra i *manager*, che possiedono informazioni privilegiate sull'andamento aziendale, e gli azionisti o il mercato dei capitali.

Infine, la presenza di sistemi di controllo efficaci può contribuire a rafforzare la fiducia degli *stakeholder* interni ed esterni. Investitori, autorità di vigilanza, creditori e altri soggetti interessati attribuiscono infatti rilevanza alla capacità dell'impresa di dotarsi di presidi adeguati a prevenire rischi, garantire la correttezza delle informazioni e assicurare il rispetto delle normative. I controlli interni e l'*Internal Audit*, in particolare, non rappresentano soltanto strumenti di protezione del valore aziendale, ma anche elementi che contribuiscono alla credibilità, alla reputazione e alla sostenibilità dell'organizzazione nel lungo periodo.

2.2.3 Il *trade-off* efficienza-controllo

La progettazione dei sistemi di controllo interno richiede un equilibrio tra l'esigenza di presidiare i rischi aziendali e quella di preservare l'efficienza e la flessibilità dell'organizzazione. Il controllo, infatti, rappresenta uno strumento essenziale per garantire la conformità normativa, l'affidabilità dei processi e la corretta gestione dei rischi, ma comporta anche costi economici e organizzativi che devono essere attentamente valutati.

L'obiettivo dell'impresa non è quello di eliminare completamente il rischio, poiché tale risultato sarebbe difficilmente realizzabile e non sostenibile dal punto di vista economico. Al contrario, l'organizzazione deve individuare un livello di controllo coerente con la propria complessità, con il settore in cui opera e con il grado di rischio che è disposta ad assumere. Un sistema di controllo efficace, quindi, non coincide necessariamente con un sistema più esteso o più rigido, ma con un insieme di presidi proporzionati ai rischi effettivamente rilevanti per l'impresa.

Da un lato, un livello insufficiente di controllo può esporre l'organizzazione a rischi operativi, finanziari, regolamentari e reputazionali. In assenza di presidi adeguati, possono aumentare le probabilità di errori, inefficienze, violazioni normative o comportamenti opportunistici, con conseguenze negative sulla stabilità e sulla credibilità dell'impresa. Dall'altro lato, un sistema di controllo eccessivamente articolato può generare effetti contrari, determinando un aumento della burocratizzazione, un rallentamento dei processi decisionali e una riduzione della capacità dell'organizzazione di adattarsi rapidamente ai cambiamenti dell'ambiente esterno.

Il *trade-off* tra efficienza e controllo evidenzia quindi la necessità di evitare sia una sottovalutazione dei rischi sia un'eccessiva formalizzazione delle procedure. In particolare, quando i controlli sono progettati o applicati in modo puramente formale, essi rischiano di perdere la propria funzione sostanziale e di trasformarsi in meri adempimenti amministrativi. In questi casi, il controllo

non contribuisce realmente al miglioramento dei processi o alla gestione dei rischi, ma produce principalmente costi e rigidità organizzative.

Per questo motivo, la qualità del sistema di controllo dipende dalla sua capacità di essere proporzionato, selettivo e coerente con gli obiettivi aziendali. I presidi devono essere sufficientemente robusti da garantire trasparenza, affidabilità e conformità, ma anche abbastanza flessibili da non ostacolare l'operatività dell'impresa e la sua capacità di innovare. L'*Internal Audit* assume un ruolo rilevante nel valutare se il sistema dei controlli interni sia adeguato rispetto al profilo di rischio dell'organizzazione e se i benefici generati dai controlli siano coerenti con i costi sostenuti per mantenerli.

2.3 Il *Framework* COSO come modello integrato di controllo interno e gestione dei rischi

Il presente paragrafo analizza il *Framework* COSO (*Internal Control – Integrated Framework*), ampiamente riconosciuto come uno dei principali standard di riferimento per la progettazione e la valutazione dei sistemi di controllo interno. Attraverso l'esame della sua struttura, verrà illustrato come tale modello si sia evoluto per rispondere alla crescente complessità tecnologica, organizzativa e regolamentare, proponendo un approccio *principle-based* che valorizza il giudizio professionale rispetto alla mera esecuzione procedurale.

L'analisi si pone l'obiettivo di contestualizzare il *Framework* non come un elemento isolato, ma come una componente centrale di un sistema di *governance* più ampio, capace di integrarsi con le logiche dell'*Enterprise Risk Management* (ERM) e con l'attività dell'*Internal Audit*. In questa prospettiva, l'indagine verterà sulla capacità del modello di concepire il controllo interno come un processo dinamico e sistemico, essenziale per la tutela del valore aziendale e per il conseguimento di una ragionevole sicurezza rispetto agli obiettivi operativi, di *reporting* e di *compliance*.

2.3.1 Origine, finalità e logica del COSO *Internal Control–Integrated Framework*

Il *Framework* denominato *Internal Control – Integrated Framework*, elaborato dal *Committee of Sponsoring Organizations of the Treadway Commission* (COSO), costituisce uno dei riferimenti internazionali più autorevoli per la progettazione, l'implementazione e la valutazione dei sistemi di controllo interno. Pubblicato inizialmente nel 1992 e sottoposto a un rilevante aggiornamento nel 2013, il modello nasce con l'intento di offrire alle organizzazioni una struttura flessibile, capace di

applicarsi a entità di ogni tipologia, dimensione o assetto legale. L'evoluzione del 2013 ha mantenuto i pilastri fondamentali della versione originaria, introducendo tuttavia una formalizzazione dei concetti chiave attraverso diciassette principi associati alle componenti strutturali, al fine di rendere il modello più chiaro e favorire un'applicazione più agevole in contesti operativi caratterizzati da una crescente complessità tecnologica e regolamentare.

Al cuore del *Framework* risiede la definizione di controllo interno inteso come un processo, posto in essere dal Consiglio di Amministrazione, dal *management* e da tutto il personale dell'organizzazione, volto a fornire una ragionevole sicurezza (e non una garanzia assoluta) sul conseguimento degli obiettivi aziendali. Tali finalità sono articolate in tre macrocategorie che comprendono gli obiettivi operativi, relativi all'efficacia e all'efficienza delle attività e alla salvaguardia delle risorse, gli obiettivi di *reporting*, riguardanti l'attendibilità, la tempestività e la trasparenza delle informazioni finanziarie e non finanziarie, e infine gli obiettivi di *compliance*, attinenti al rispetto delle leggi e dei regolamenti applicabili all'ente.

Questa impostazione chiarisce come il controllo interno non debba essere ridotto a un mero adempimento procedurale, ma rappresenti un sistema organizzativo dinamico e integrato basato sulle persone e sulle azioni che esse compiono a ogni livello dell'organizzazione. In questa prospettiva, sebbene la creazione diretta di valore sia un concetto più propriamente legato ai modelli di *Enterprise Risk Management*, il sistema di controllo interno contribuisce in modo determinante alla tutela del valore stesso e al rafforzamento della *governance*.

2.3.2 Le componenti del *Framework*: dal *control environment* al *monitoring*

Il sistema di controllo interno delineato dal *Framework* COSO si articola in cinque componenti interrelate, che operano in modo integrato per supportare il raggiungimento degli obiettivi aziendali. L'efficacia del modello risiede proprio nella natura sistemica di tali elementi, i quali non devono essere considerati come compartimenti stagni, bensì come parti di un processo dinamico e interdipendente in cui le componenti agiscono in modo coordinato. In questa prospettiva, una carenza significativa nella presenza o nel funzionamento di una componente può impedire di qualificare il sistema come pienamente efficace. L'ambiente di controllo costituisce il pilastro fondamentale e la base culturale dell'organizzazione, stabilendo il complesso di standard, processi e strutture che forniscono le basi per l'esercizio del controllo interno a ogni livello dell'ente. Su questa base si innesta la valutazione del rischio, un processo dinamico e iterativo volto a identificare e analizzare le potenziali minacce che potrebbero ostacolare il conseguimento degli obiettivi aziendali.

Una volta identificati e analizzati i rischi, le attività di controllo intervengono per tradurre le risposte del *management* ai rischi in politiche e procedure concrete, garantendo che le direttive necessarie per mitigare tali rischi entro livelli accettabili siano effettivamente eseguite in tutta l'organizzazione. Il corretto funzionamento di queste dinamiche è sostenuto dalla componente di informazione e comunicazione, che assicura la generazione e la circolazione tempestiva di informazioni rilevanti e di qualità, permettendo a tali informazioni di fluire verso l'alto, verso il basso e trasversalmente all'ente, a supporto delle responsabilità di controllo. Infine, le attività di monitoraggio svolgono una funzione di supervisione essenziale attraverso valutazioni continuative o periodiche, verificando nel tempo che ciascuna delle componenti del sistema rimanga presente e funzionante e permettendo di comunicare e correggere tempestivamente eventuali carenze rilevate.

L'intera struttura del *Framework* è formalizzata attraverso diciassette principi fondamentali associati a ogni componente, offrendo un modello *principles-based* che non impone una struttura rigida, ma risulta altamente adattabile alla dimensione, al settore e alla complessità dell'organizzazione. Questa impostazione garantisce al *management* la flessibilità necessaria per applicare il sistema di controllo interno a diverse realtà aziendali, permettendo un esercizio del giudizio professionale nel progettare controlli proporzionati ai rischi specifici. In contesti caratterizzati da una crescente pressione regolamentare, tale approccio consente al sistema di controllo interno di evolversi e rispondere ai cambiamenti dell'ambiente operativo, assicurando che esso rimanga un presidio costante ed efficace per il raggiungimento degli obiettivi dell'organizzazione.

2.3.3 Dal controllo interno alla gestione dei rischi di *compliance*: il collegamento tra COSO, ERM e *Internal Audit*

Il sistema di controllo interno delineato nel *Framework* COSO non deve essere considerato come un'entità isolata, ma come un elemento che si collega sistematicamente al modello di *Enterprise Risk Management* (ERM), il quale adotta una prospettiva più ampia rivolta alla strategia, alla *performance* e alla creazione e preservazione del valore aziendale. Mentre il controllo interno si focalizza principalmente sulla ragionevole sicurezza nel raggiungimento degli obiettivi di *operations*, *reporting* e *compliance*, l'ERM incorpora concetti quali il *risk appetite*², la strategia e la formulazione degli obiettivi di *business*, ponendosi come un quadro più ampio e complementare, che si sovrappone

² Il *risk appetite* (propensione al rischio) è il livello e la tipologia di rischio che un'organizzazione è disposta ad accettare per raggiungere i propri obiettivi strategici. Definisce l'area di rischio in cui l'azienda desidera operare, bilanciando potenziali ricompense e minacce.

parzialmente al sistema di controllo interno senza sostituirlo. In questa architettura integrata, la gestione del rischio di conformità assume una rilevanza centrale, poiché l'efficacia dei programmi di *compliance* contribuisce alla preservazione del valore aiutando a proteggere l'organizzazione da rischi legali, sanzionatori e reputazionali che potrebbero produrre impatti finanziari e regolamentari anche molto rilevanti.

L'applicazione dei principi del COSO ERM alla gestione dei rischi di *compliance* permette alle organizzazioni di identificare, valutare, prioritizzare e gestire proattivamente i rischi di violazione di leggi, regolamenti, standard o *policy* interne. Questo approccio risulta particolarmente coerente con le dinamiche dei settori iper-regolamentati, come quello bancario e finanziario, dove la *compliance* non rappresenta un elemento accessorio, ma una condizione indispensabile per la sostenibilità operativa e la tutela della reputazione dell'impresa. All'interno di tali contesti, sebbene il *Framework* COSO definisca con precisione "cosa" debba essere presidiato per garantire un sistema efficace, la sua effettiva traduzione operativa richiede una chiara attribuzione delle responsabilità organizzative che chiarisca chi debba presidiare i diversi rischi.

In questa fase operativa, il modello delle *Three Lines* (vedi par. 1.4.2) funge da collegamento cruciale, definendo i ruoli dei vari attori aziendali per evitare lacune o inutili duplicazioni di sforzi. La prima linea, costituita dal *management* operativo e dai proprietari dei processi, detiene la proprietà dei rischi e ha il compito di progettare ed eseguire i controlli quotidiani. La seconda linea, che include funzioni specialistiche come il *risk management* e la *compliance*, supporta il *management* attraverso il monitoraggio dell'adeguatezza dei controlli e la fornitura di competenze tecniche. Infine, la terza linea è rappresentata dall'*Internal Audit*, il quale, operando in una posizione di indipendenza e obiettività e mantenendo un rapporto diretto con gli organi di governo, fornisce *assurance* indipendente sull'efficacia complessiva del sistema di *governance*, della gestione dei rischi e del controllo interno, contribuendo a verificare che i processi aziendali siano coerenti con le aspettative del Consiglio di Amministrazione, del *senior management* e, nei contesti regolamentati, delle autorità di vigilanza.

2.4 Driver di cambiamento e trasformazione delle funzioni nei contesti regolamentati

L'evoluzione dell'*Internal Audit* è strettamente legata ai cambiamenti che interessano l'ambiente competitivo, tecnologico e regolamentare in cui operano le imprese. Nei contesti caratterizzati da elevata complessità, le funzioni di controllo sono chiamate ad adattarsi a nuovi rischi,

a nuove esigenze informative e a forme di rendicontazione sempre più articolate. Tali trasformazioni incidono non solo sulle attività svolte dall'*Internal Audit*, ma anche sulle competenze richieste alla funzione e sul suo contributo ai sistemi di *governance* e di gestione dei rischi.

In particolare, l'innovazione tecnologica e la crescente rilevanza dei temi ESG rappresentano due ambiti nei quali si manifesta con maggiore evidenza l'ampliamento del ruolo dell'*Internal Audit*. Da un lato, la digitalizzazione modifica le modalità di raccolta, analisi e controllo delle informazioni; dall'altro, la sostenibilità estende il perimetro dell'*audit* verso dati e processi non finanziari. L'analisi di tali *driver* consente quindi di comprendere come la funzione stia evolvendo verso un ruolo più proattivo, trasversale e integrato nei processi aziendali.

2.4.1 Innovazione tecnologica e digitalizzazione dei controlli

L'innovazione tecnologica e la digitalizzazione dei processi aziendali rappresentano uno dei principali fattori di cambiamento per le funzioni di controllo e, in particolare, per l'*Internal Audit*. L'evoluzione dei sistemi informativi, l'aumento della disponibilità di dati e lo sviluppo di strumenti avanzati di analisi stanno modificando sia l'oggetto delle attività di *audit* sia le modalità con cui tali attività vengono svolte. L'*Internal Audit* è chiamato non solo a valutare nuovi rischi connessi all'utilizzo della tecnologia, ma anche a integrare strumenti digitali nei propri processi di verifica e monitoraggio.

Tradizionalmente, molte attività di *audit* si basavano su verifiche periodiche e su analisi campionarie svolte *ex post* rispetto ai processi aziendali. La digitalizzazione consente invece di sviluppare modalità di controllo più continue e tempestive, attraverso l'utilizzo di strumenti di *continuous auditing* e *continuous monitoring*. Tali strumenti permettono di analizzare un volume più ampio di dati, individuare anomalie nei processi e segnalare potenziali criticità con maggiore rapidità rispetto ai controlli tradizionali. In questo modo, l'attività di *audit* può diventare più aderente all'evoluzione dei rischi aziendali e meno dipendente da verifiche occasionali o meramente retrospettive.

Un ruolo particolarmente rilevante è assunto dagli strumenti di *data analytics*, che consentono all'*Internal Audit* di elaborare grandi quantità di informazioni e di individuare relazioni, anomalie o tendenze non immediatamente rilevabili attraverso tecniche di controllo tradizionali. L'utilizzo di tali strumenti può migliorare l'efficienza delle attività di verifica, riducendo il ricorso a controlli manuali e permettendo alla funzione di concentrare le proprie risorse su aree caratterizzate da maggiore esposizione al rischio. Allo stesso tempo, l'automazione di alcune attività di controllo, come

riconciliazioni, verifiche incrociate o controlli autorizzativi, può contribuire a rendere i processi più efficaci e tempestivi.

Tuttavia, l'efficacia della digitalizzazione dei controlli dipende dalla qualità dei dati e dalla solidità dei sistemi informativi utilizzati dall'organizzazione. La presenza di dati incompleti, non aggiornati o non correttamente strutturati può infatti compromettere l'affidabilità delle analisi svolte e ridurre il valore informativo degli strumenti digitali. Per questo motivo, la *data governance* assume un ruolo centrale, poiché consente di definire responsabilità, procedure e criteri volti a garantire la qualità, la tracciabilità e la sicurezza dei flussi informativi utilizzati nei processi di controllo.

La trasformazione digitale modifica, inoltre, il ruolo dell'*Internal Audit* rispetto alla gestione dei rischi. L'utilizzo di strumenti analitici avanzati consente alla funzione di passare da un approccio prevalentemente descrittivo, basato sull'analisi di eventi già verificatisi, a una prospettiva maggiormente orientata all'identificazione preventiva delle criticità. In questo senso, l'*Internal Audit* può contribuire non solo alla verifica del corretto funzionamento dei controlli esistenti, ma anche all'individuazione di rischi emergenti legati all'evoluzione tecnologica, alla sicurezza informatica, alla protezione dei dati e alla continuità operativa.

2.4.2 Sostenibilità e nuovi ambiti dell'*audit*

L'integrazione dei criteri ESG (*Environmental, Social and Governance*) e l'evoluzione della rendicontazione di sostenibilità rappresentano un ulteriore fattore di cambiamento per l'*Internal Audit*. Negli ultimi anni, la crescente attenzione verso gli impatti ambientali, sociali e di *governance* delle imprese ha ampliato il perimetro informativo richiesto agli operatori economici, affiancando alle tradizionali informazioni finanziarie una serie di dati e indicatori non finanziari. In questo contesto, la funzione di *audit* è progressivamente chiamata a valutare anche processi, controlli e flussi informativi relativi alla sostenibilità.

Nel contesto europeo, la *Corporate Sustainability Reporting Directive*³ (CSRD) ha rafforzato il ruolo della rendicontazione di sostenibilità, prevedendo obblighi più strutturati in materia di informazioni ambientali, sociali e di *governance* per le imprese rientranti nel relativo ambito di applicazione. Tale evoluzione riflette la crescente esigenza di rendere le informazioni di sostenibilità più affidabili, comparabili e utili per gli *stakeholder*. Per le organizzazioni, ciò comporta la necessità

³ La *Corporate Sustainability Reporting Directive* (CSRD), ovvero la Direttiva UE 2022/2464, è la nuova normativa europea in vigore dal 2023 che obbliga le aziende a pubblicare report dettagliati sul loro impatto ambientale, sociale e di *governance* (ESG). Sostituisce la precedente NFRD, rendendo i dati di sostenibilità confrontabili e verificabili, allineati agli standard ESRS (*European Sustainability Reporting Standards*).

di sviluppare sistemi interni capaci di raccogliere, verificare e comunicare dati non finanziari in modo coerente con i requisiti normativi e con le aspettative del mercato.

L'ampliamento del perimetro dell'*audit* verso i temi ESG risponde anche alla necessità di ridurre le asimmetrie informative tra impresa e *stakeholder*. Investitori, creditori, autorità di vigilanza e altri soggetti interessati attribuiscono crescente rilevanza alla qualità delle informazioni sulla sostenibilità, poiché tali informazioni possono incidere sulla valutazione dei rischi, sulla reputazione dell'impresa e sulle decisioni di allocazione delle risorse. In assenza di adeguati presidi di controllo, tuttavia, aumenta il rischio che le informazioni comunicate non rappresentino correttamente le performance ambientali, sociali o di *governance* dell'organizzazione, dando luogo a fenomeni di rappresentazione distorta o incompleta, come nel caso del *greenwashing*⁴.

In tale ambito, l'*Internal Audit* può svolgere un ruolo rilevante nel valutare l'adeguatezza dei processi attraverso cui l'impresa identifica, misura e comunica le informazioni ESG. La funzione può contribuire a verificare la qualità dei dati utilizzati nella rendicontazione di sostenibilità, la coerenza tra obiettivi dichiarati e procedure interne, nonché l'efficacia dei controlli posti a presidio dei rischi ESG. In questo modo, l'*audit* interno non si limita a verificare la conformità formale agli obblighi informativi, ma contribuisce a rafforzare l'affidabilità complessiva dei processi di *reporting* non finanziario.

L'ingresso dei temi ESG nel perimetro dell'*Internal Audit* comporta inoltre un'evoluzione delle competenze richieste alla funzione. Gli *auditor* sono chiamati a comprendere non solo i tradizionali profili contabili, operativi e regolamentari, ma anche aspetti legati alla sostenibilità ambientale, alla gestione dei rischi sociali, alla *governance* aziendale e alla relazione tra informazioni finanziarie e non finanziarie. Tale trasformazione rende necessario un approccio multidisciplinare, capace di integrare competenze normative, analitiche e organizzative.

2.4.3 Implicazioni per l'evoluzione dell'*Internal Audit*

L'innovazione tecnologica, la digitalizzazione dei controlli e l'ampliamento del perimetro informativo legato ai temi ESG contribuiscono a modificare progressivamente il ruolo dell'*Internal Audit* all'interno delle organizzazioni. Tali trasformazioni non incidono soltanto sugli strumenti utilizzati dalla funzione, ma anche sulle sue finalità, sulle competenze richieste e sul rapporto con i sistemi di *governance* e di gestione dei rischi.

⁴ Il *greenwashing* (in italiano "ecologismo di facciata") è una strategia di *marketing* ingannevole utilizzata da aziende o istituzioni per presentarsi come ecosostenibili, nascondendo l'impatto ambientale negativo delle proprie attività.

Dunque, l'*Internal Audit* tende a superare una funzione prevalentemente retrospettiva, per assumere un ruolo maggiormente orientato all'identificazione preventiva dei rischi e al miglioramento dei processi aziendali. La funzione continua a svolgere un'attività essenziale di *assurance* indipendente, ma viene progressivamente chiamata anche a fornire analisi e raccomandazioni utili al *management* e agli organi di governo per affrontare rischi emergenti e contesti operativi più complessi.

L'evoluzione descritta comporta un ampliamento delle competenze professionali richieste agli *auditor* interni. Accanto alle tradizionali conoscenze contabili, procedurali e regolamentari, assumono crescente rilevanza competenze relative all'analisi dei dati, ai sistemi informativi, alla sicurezza informatica, alla sostenibilità e alla gestione integrata dei rischi. L'*Internal Audit* deve quindi sviluppare una capacità di lettura trasversale dei processi aziendali, in grado di collegare informazioni finanziarie e non finanziarie, rischi operativi e strategici, esigenze di conformità e obiettivi di lungo periodo.

Questa trasformazione rafforza il ruolo dell'*Internal Audit* come funzione integrata nei sistemi di *governance*. La sua attività non si limita alla segnalazione di carenze o irregolarità, ma contribuisce alla valutazione dell'adeguatezza complessiva dei presidi organizzativi e alla diffusione di una maggiore consapevolezza del rischio all'interno dell'impresa. In tale prospettiva, l'*Internal Audit* può supportare il miglioramento continuo dei processi decisionali, pur mantenendo la propria indipendenza e senza assumere responsabilità operative dirette.

Capitolo 3 – Modelli di riferimento e applicazione a un caso bancario

3.1 Il *framework* Deloitte – *Internal Audit* 3.0

Il presente paragrafo analizza il framework *Internal Audit* 3.0 proposto da Deloitte, interpretandolo come un modello evolutivo della funzione di *Internal Audit*. Dopo aver evidenziato nei capitoli precedenti il ruolo dell'*Internal Audit* nei sistemi di *governance*, controllo interno e gestione dei rischi, l'attenzione si sposta ora sulle modalità attraverso cui tale funzione può adattarsi a un contesto aziendale sempre più complesso, dinamico e regolamentato. In particolare, il modello Deloitte consente di superare una visione puramente tradizionale e retrospettiva dell'*audit*, introducendo una logica più ampia fondata su tre dimensioni integrate: *Assure*, *Advise* e *Anticipate*.

3.1.1 Origine del modello e limiti dell'*Internal Audit* tradizionale

Il framework *Internal Audit* 3.0 proposto da Deloitte nasce dalla consapevolezza che il modello tradizionale di *Internal Audit*, pur mantenendo un ruolo essenziale nei sistemi di controllo interno, non sia più pienamente adeguato a rispondere alla crescente complessità dei rischi contemporanei. La crescente interdipendenza tra rischi operativi, tecnologici, regolamentari e reputazionali richiede una funzione capace non solo di valutare il passato, ma anche di supportare il *management* nella lettura dei rischi emergenti.

Le radici del modello tradizionale, definibile attraverso le fasi evolutive "*Internal Audit* 1.0" e "2.0", risalgono alla fondazione dell'*Institute of Internal Auditors* nel 1941 e si sono consolidate in risposta a pilastri normativi come il *Sarbanes-Oxley Act*⁵. In questa veste, l'*Internal Audit* è considerato una colonna portante della *corporate governance*, con il compito primario di supportare l'*Audit Committee* e il *top management* attraverso attività di *assurance* e *advisory* sul sistema di controllo interno, sui processi di gestione dei rischi e sui meccanismi di *governance*. Secondo gli standard professionali, la funzione deve operare in modo indipendente e obiettivo, portando un approccio sistematico e disciplinato per migliorare l'efficacia dei processi aziendali. Storicamente, l'attività si è concentrata su verifiche *ex post*, analisi del rispetto di regolamenti e *reporting* di criticità già emerse, agendo come un garante dell'integrità delle informazioni finanziarie e operative.

⁵ Il *Sarbanes-Oxley Act* è una legge federale statunitense del 2002 che rafforza la trasparenza finanziaria, la responsabilità dei dirigenti e la *governance* aziendale per prevenire frodi contabili.

Nonostante l'indubbia utilità, questo approccio mostra limiti evidenti nell'attuale scenario competitivo, poiché rischia di rimanere ancorato a una visione puramente ispettiva che genera spesso delusione tra gli *stakeholder*. Il limite maggiore del modello tradizionale è la sua natura eccessivamente retrospettiva, che porta la funzione a "inseguire" gli sviluppi strategici e tecnologici invece di precederli. Un *Internal Audit* focalizzato esclusivamente sull'efficacia tecnica dei controlli può non riuscire a tradurre i propri risultati in una reale rilevanza organizzativa, rischiando di essere percepita come una funzione troppo generica o marginale rispetto alle sfide decisionali dell'impresa. In un contesto in cui il valore della funzione è multidimensionale e dovrebbe includere il supporto alla *governance* e alla gestione proattiva dei rischi, un orientamento focalizzato solo sul passato risulta strutturalmente limitato.

L'esigenza di evolvere verso l'*Internal Audit* 3.0 scaturisce quindi dai cambiamenti radicali che caratterizzano l'attuale contesto aziendale, tra cui digitalizzazione, intelligenza artificiale, rischi *cyber*, pressione regolamentare e crescente attenzione ai profili ESG. Questi fattori aumentano la velocità con cui i rischi si manifestano e rendono necessario un modello di *audit* più dinamico, prospettico e integrato nei processi decisionali. Il nuovo *framework* mira così a superare una visione puramente ispettiva della funzione, proponendo una triade di valore fondata su tre dimensioni: *Assure*, *Advise* e *Anticipate*. Attraverso tale evoluzione, l'*Internal Audit* non abbandona il proprio ruolo di controllo, ma lo rafforza e lo amplia, diventando una funzione capace di proteggere e creare valore nel lungo periodo.

3.1.2 Le tre dimensioni del valore: *Assure*, *Advise*, *Anticipate*

La dimensione *Assure* rappresenta il nucleo tradizionale e imprescindibile dell'*Internal Audit*, finalizzato a fornire valutazioni indipendenti e obiettive sull'efficacia dei controlli, dei processi di gestione del rischio e dei meccanismi di *governance*. Nel *framework Internal Audit* 3.0, questa componente non viene meno, ma si consolida come la base fondamentale della funzione, evolvendo verso una portata più ampia e un monitoraggio più vicino al tempo reale rispetto alle metodologie del passato. L'attività di *assurance* permette di accrescere il livello di fiducia degli *stakeholder* nei processi di governo e controllo, contribuendo direttamente al valore complessivo dell'organizzazione attraverso la verifica sistematica della tenuta del sistema di controllo interno lungo l'intera catena del valore.

La dimensione *Advise* amplia significativamente il perimetro d'azione della funzione, introducendo una capacità di supporto consultivo e di *advisory* nei confronti del *management*. Tale contributo non comporta l'assunzione di responsabilità operative o decisionali, che restano in capo

alle prime due linee di difesa, ma consiste nell'offrire prospettive indipendenti su rischi, controlli e processi decisionali durante le fasi di trasformazione o cambiamento organizzativo. In conformità con i principi del *Three Lines Model*, l'*Internal Audit* può supportare attivamente il *management* nel miglioramento delle proprie capacità di *assurance*, a patto di mantenere la necessaria indipendenza e obiettività per evitare situazioni di auto-revisione che potrebbero compromettere l'integrità e l'autorità della funzione. In questa veste, l'*Internal Audit* agisce come un catalizzatore di cambiamento e un *partner* strategico capace di generare *insight* di valore e favorire l'apprendimento organizzativo.

L'elemento di maggiore innovazione e rottura rispetto al modello tradizionale è rappresentato dalla dimensione *Anticipate*, che sposta l'*Internal Audit* da una logica prevalentemente retrospettiva a una prospettica e predittiva. La funzione è chiamata a intercettare segnali deboli, aree di vulnerabilità e rischi emergenti prima che questi si traducano in impatti rilevanti per l'organizzazione, operando come un presidio capace di leggere tempestivamente le dinamiche evolutive del contesto competitivo. Questo pilastro richiede l'adozione di strumenti avanzati di *risk sensing* e l'applicazione di logiche di *risk learning* per comprendere le relazioni causali tra gli eventi e anticipare minacce complesse legate alla trasformazione digitale, all'intelligenza artificiale, ai rischi *cyber* e ai cambiamenti regolamentari o ESG. Attraverso questa capacità di anticipazione, l'*Internal Audit* abilita il *management* a intervenire proattivamente, proteggendo e creando valore nel lungo periodo.

Le tre dimensioni descritte non devono essere considerate come attività alternative, ma come componenti integrate di una funzione più matura. L'*Internal Audit* evoluto continua a fornire *assurance* indipendente, ma al tempo stesso rafforza la propria capacità di supportare il *management* e di anticipare rischi futuri, mantenendo sempre una posizione autonoma rispetto alle responsabilità operative.

3.1.3 *Internal Audit* 3.0 come modello evolutivo

In questa prospettiva, *Internal Audit* 3.0 può essere interpretato come un modello evolutivo, poiché ridefinisce il contributo della funzione all'interno dell'organizzazione. Il *framework* proposto da Deloitte non rappresenta una semplice ridenominazione dell'attività di *audit*, ma un modello operativo evoluto volto ad ampliare il ruolo della funzione in risposta alla crescente complessità dei rischi aziendali. Rispetto a un'impostazione tradizionale orientata prevalentemente alla verifica *ex post*, il paradigma 3.0 amplia il mandato professionale dell'*Internal Audit*, trasformandolo in una *capability* organizzativa capace di combinare controllo, consulenza e anticipazione. L'*Internal Audit* non viene quindi concepito esclusivamente come un presidio di controllo retrospettivo, ma come una

funzione integrata e prospettica che, senza eliminare le verifiche di conformità, le integra con attività di *advisory* e con una maggiore capacità di intercettare minacce emergenti.

Questa trasformazione incide profondamente sulla creazione di valore, che assume una connotazione multidimensionale che va oltre la mera identificazione di errori. Il valore dell'*Internal Audit* evoluto risiede nella sua capacità di aiutare gli *stakeholder* a contrastare gli effetti dei rischi lungo l'intera *value chain*, rafforzando contemporaneamente la *corporate governance* e aumentando la fiducia nell'integrità dell'organizzazione. Integrando la visione di Deloitte con le evidenze sulla rilevanza organizzativa, emerge come l'*Internal Audit* 3.0 debba essere valutato non solo per l'efficacia tecnica dei controlli, ma per la sua capacità di generare apprendimento organizzativo e supportare decisioni più consapevoli e di alta qualità. La funzione supera così la percezione di essere un presidio puramente difensivo per posizionarsi come un partner strategico capace di produrre *insight* tempestivi e utili per il *senior management* e l'*Audit Committee*.

Il successo operativo del modello *Internal Audit* 3.0 richiede tuttavia specifiche condizioni organizzative. In primo luogo, la funzione deve sviluppare nuove competenze, combinando conoscenze di *audit*, comprensione del *business*, capacità analitiche e familiarità con strumenti digitali. In secondo luogo, l'utilizzo di tecnologie come *data analytics*, intelligenza artificiale e *robotic process automation* può migliorare l'efficienza e la copertura delle attività di *audit*, favorendo forme di monitoraggio più continuo e tempestivo. Tali strumenti consentono di analizzare volumi di dati più ampi, individuare anomalie con maggiore rapidità e orientare l'*audit* verso una logica più proattiva. Tuttavia, l'innovazione tecnologica non sostituisce il giudizio professionale dell'*auditor*: al contrario, lo rafforza, a condizione che siano preservati indipendenza, obiettività e qualità metodologica.

3.2 Il contributo PwC: evidenze empiriche e approccio alla trasformazione

Dopo aver analizzato il modello *Internal Audit* 3.0 di Deloitte, il contributo di PwC consente di approfondire l'evoluzione dell'*Internal Audit* da una prospettiva più empirica e operativa. Il *Global Internal Audit Study 2023* mostra, infatti, come il cambiamento della funzione non riguardi soltanto il suo ruolo teorico, ma anche le modalità concrete attraverso cui essa può rafforzare la propria rilevanza all'interno dell'organizzazione. In questa prospettiva, PwC offre un utile punto di collegamento tra l'esigenza di un *Internal Audit* più strategico e le condizioni necessarie per realizzare tale trasformazione nella pratica.

3.2.1 Il Global Internal Audit Study 2023

Il *Global Internal Audit Study 2023* di PwC analizza l'evoluzione della funzione di *Internal Audit* in un contesto caratterizzato da rischi sempre più complessi, dinamici e interconnessi. Lo studio si fonda sulla *survey* globale più ampia mai condotta da PwC sul tema, coinvolgendo 4.680 rispondenti tra cui *Internal Audit leaders*, membri del *board*, *business executives* e responsabili delle funzioni di rischio e *compliance* in 81 Paesi. L'obiettivo centrale del *report* è comprendere come la funzione possa rafforzare la propria rilevanza ed evolvere per generare valore in un ambiente in cui silos funzionali, barriere interne e difficoltà di coordinamento possono impedire una visione chiara e integrata dei rischi. Secondo PwC, l'*Internal Audit* può contribuire a superare tali limiti sfruttando la propria indipendenza e obiettività per aiutare l'organizzazione a interpretare i rischi emergenti e supportare decisioni più consapevoli.

Uno dei contributi principali del *report* è l'introduzione del concetto di "*risk multiverse*", con cui PwC descrive un ambiente in cui i *megatrend* (tecnologia, geopolitica, ESG, *supply chain*, ecc.) generano rischi che non si manifestano più in modo isolato, ma si sovrappongono e si influenzano reciprocamente. In tale scenario, l'*Internal Audit* non può limitarsi a verifiche frammentate o puramente retrospettive, ma deve sviluppare una visione trasversale capace di connettere informazioni provenienti da diverse aree aziendali e cogliere le interdipendenze tra le diverse dimensioni del rischio. Questo approccio è pienamente coerente con la dimensione "*Anticipate*" del modello Deloitte, poiché rafforza l'idea di un *Internal Audit* capace di agire come funzione *forward-looking*, promuovendo la consapevolezza di ciò che potrebbe accadere e aiutando il *management* a intervenire prima che i rischi si materializzino.

Un secondo elemento centrale evidenziato da PwC riguarda la necessità di un maggiore coinvolgimento dell'*Internal Audit* nelle aree strategiche. Lo studio rileva infatti uno scarto tra i rischi che minacciano la strategia aziendale (come inflazione, volatilità macroeconomica e trasformazione digitale) e quelli effettivamente coperti dai piani di *audit* tradizionali. Ne deriva l'esigenza di un piano di *audit* più dinamico, capace di includere temi quali l'utilizzo dell'intelligenza artificiale, la resilienza della *supply chain* e la sostenibilità. Questa prospettiva trova riscontro nell'analisi di Eulerich & Eulerich (2020), i quali sostengono che il valore dell'*Internal Audit* sia un concetto multidimensionale che va oltre il semplice "trovare errori". Secondo gli autori, la funzione crea valore strategico quando supporta i processi di *governance* e aiuta gli *stakeholder* a contrastare gli effetti dei rischi lungo l'intera catena del valore, aumentando la fiducia nell'integrità dell'organizzazione.

Il *report* attribuisce inoltre all'*Internal Audit* un ruolo di forza unificante (*unifying force*) all'interno dell'organizzazione. Grazie alla propria posizione indipendente e trasversale, la funzione può contribuire a collegare le informazioni prodotte dalle diverse aree aziendali, ridurre i silos organizzativi e favorire un migliore coordinamento tra prima, seconda e terza linea. Tale ruolo si inserisce pienamente nella logica del *Three Lines Model* dell'IIA, secondo cui l'*Internal Audit*, in qualità di terza linea, fornisce *assurance* e consulenza indipendenti sui processi di *governance*, gestione dei rischi e controllo interno, senza assumere responsabilità operative proprie del *management* o delle altre funzioni aziendali.

Per agire efficacemente come forza unificante, PwC sottolinea la necessità di investire nelle cosiddette "*human superpowers*": non solo competenze tecniche, ma capacità relazionali, scetticismo professionale, empatia, pensiero critico, solida conoscenza del business e abilità comunicative. Tali attributi umani sono indispensabili per trasformare le evidenze tecniche dell'*audit* in *insight* e *foresight* realmente utili per il *management*, supportando la creazione e la protezione del valore organizzativo, in linea con i nuovi *Global Internal Audit Standards*.

3.2.2 La trasformazione della funzione di *Internal Audit*

La trasformazione della funzione di *Internal Audit* richiede innanzitutto la definizione di una *roadmap* strategica, capace di collegare il mandato della funzione agli obiettivi e ai rischi prioritari dell'organizzazione. In questa prospettiva, l'*audit plan* non dovrebbe essere concepito come un documento statico, definito su base annuale, ma come uno strumento dinamico, aggiornabile tempestivamente in risposta all'evoluzione del profilo di rischio aziendale e dei cambiamenti nel contesto operativo. Secondo i nuovi *Global Internal Audit Standards*, la pianificazione deve basarsi su una valutazione documentata delle strategie e dei rischi, integrando il contributo del *board* e del *senior management*. La *roadmap* dovrebbe quindi individuare le aree di maggiore esposizione, le competenze necessarie, le tecnologie da adottare e le modalità con cui l'*Internal Audit* intende rafforzare il proprio contributo alla *governance* e ai processi decisionali, assicurando un allineamento costante con le aspettative degli *stakeholder* e con le priorità strategiche dell'organizzazione.

Un secondo elemento centrale riguarda la misurazione della *performance* della funzione, che deve superare un approccio puramente quantitativo. La trasformazione dell'*Internal Audit* richiede infatti KPI capaci di valutare non solo l'efficienza operativa, ma anche il valore generato. Indicatori tradizionali, come il numero di *audit* completati, il grado di completamento dell'*audit plan* o il tasso di implementazione delle raccomandazioni, pur rimanendo utili per misurare la "produzione" della

funzione, non sono sufficienti a coglierne il contributo strategico. Come evidenziato da dati empirici⁶, il valore dell'*audit* è un concetto multidimensionale che deve includere indicatori qualitativi relativi alla rilevanza degli *insight* prodotti, alla soddisfazione degli *stakeholder*, alla copertura dei rischi e al miglioramento effettivo dei processi di controllo lungo la catena del valore. I nuovi standard professionali ribadiscono la necessità di sviluppare una metodologia di misurazione della *performance* orientata al miglioramento continuo e basata sugli obiettivi concordati con il *board* e il *senior management*.

La tecnologia rappresenta una leva centrale della trasformazione, ma il suo valore dipende dalla capacità della funzione di integrarla in modo coerente nei processi di *audit*. PwC evidenzia che molte funzioni di *Internal Audit* non ottengono pienamente i benefici attesi dagli investimenti tecnologici, spesso perché gli strumenti vengono adottati senza una chiara strategia o senza adeguati KPI di misurazione. Tecnologie come *data analytics*, intelligenza artificiale e *robotic process automation* possono aumentare la copertura delle verifiche, ridurre le attività manuali, individuare anomalie con maggiore tempestività e favorire il passaggio a modelli di *assurance* più automatizzati e forme di monitoraggio continuo. Tuttavia, secondo il modello *Internal Audit* 3.0, tale evoluzione richiede non solo strumenti digitali, ma lo sviluppo di nuove competenze professionali. In questo senso, Deloitte richiama la figura dei cosiddetti *purple people*, ossia *auditor* capaci di combinare conoscenze di *business*, competenze tecnologiche e capacità analitiche. Allo stesso tempo, la tecnologia non sostituisce il giudizio professionale dell'*auditor*, ma lo rafforza, a condizione che le anomalie rilevate siano interpretate criticamente e contestualizzate rispetto ai rischi aziendali. In linea con gli standard professionali, il *Chief Audit Executive* ha il compito di garantire che la funzione disponga delle risorse tecnologiche necessarie, delle competenze e della formazione adeguata a un utilizzo efficace ed efficiente.

Infine, la trasformazione della funzione richiede un adeguato processo di *change management* e un maggiore coinvolgimento degli *stakeholder*. L'*Internal Audit* evoluto deve rafforzare il dialogo con l'*Audit Committee*, il *senior management* e le altre funzioni di controllo (quali *risk management*, *compliance*, IT e sostenibilità) per costruire una visione condivisa dei rischi e delle priorità. Questo approccio si fonda sul principio di coordinamento e allineamento del *Three Lines Model*, volto a eliminare duplicazioni e silos informativi, favorendo una maggiore integrazione tra le diverse componenti del sistema di *governance*. In tale prospettiva, il valore della funzione dipende in modo cruciale dalla capacità di comunicare i risultati in maniera efficace: le evidenze raccolte devono essere

⁶ Eulerich, A., & Eulerich, M. (2020). *What is the value of internal auditing? – A literature review on qualitative and quantitative perspectives*.

trasformate in raccomandazioni accurate, obiettive, tempestive e, soprattutto, orientate all'azione. Un solido *stakeholder engagement*, supportato da una reputazione di indipendenza e competenza, permette all'*Internal Audit* di agire come un vero *partner* strategico e un catalizzatore per il miglioramento dei processi di *governance*, *risk management* e controllo interno.

3.3 Integrazione dei framework in un modello evoluto di *Internal Audit*

Dopo aver analizzato il modello *Internal Audit 3.0* di Deloitte e il contributo empirico del *Global Internal Audit Study 2023* di PwC, è possibile individuare una prospettiva integrata dell'evoluzione della funzione di *Internal Audit*. I due approcci, infatti, non devono essere considerati alternativi, ma complementari: Deloitte fornisce una rappresentazione concettuale del nuovo ruolo della funzione, mentre PwC individua le principali condizioni operative necessarie per realizzare tale trasformazione. L'integrazione con i riferimenti professionali dell'IIA e con il *framework* COSO permette di collocare questa evoluzione all'interno di una struttura coerente di *governance*, controllo interno e gestione dei rischi, evitando che l'ampliamento del ruolo dell'*Internal Audit* comprometta i principi di indipendenza, obiettività e rigore metodologico.

3.3.1 Complementarità tra contenuto, metodo e struttura

L'integrazione di diversi *framework* consente di delineare un modello di *Internal Audit* evoluto, in cui i vari approcci si completano a vicenda perché rispondono a esigenze diverse ma complementari: la definizione del ruolo, la metodologia di trasformazione e la solidità della struttura di *governance*.

Il contributo di Deloitte (2018) può essere interpretato come la componente “contenutistica” del modello integrato, poiché individua le tre dimensioni evolutive attraverso cui l'*Internal Audit* genera valore. La funzione *Assure* preserva il nucleo tradizionale della funzione, fornendo *assurance* indipendente e oggettiva sui processi, sui controlli e sui rischi principali. La dimensione *Advise* permette all'*Internal Audit* di supportare il *management* attraverso raccomandazioni e *insight* indipendenti, senza tuttavia assumere responsabilità operative. Infine, la capacità di *Anticipate* introduce una prospettiva più proattiva e orientata al futuro, consentendo alla funzione di identificare rischi emergenti e vulnerabilità prima che si traducano in impatti significativi per l'organizzazione.

Il contributo di PwC (2023) assume invece una funzione prevalentemente metodologica e trasformativa, indicando come rendere concreto il modello evolutivo. Lo studio evidenzia che il passaggio verso un *Internal Audit* ad alte prestazioni richiede una *roadmap* strategica chiara e un *audit plan* dinamico, capace di adattarsi all'evoluzione del contesto aziendale e del profilo di rischio dell'organizzazione. PwC sottolinea inoltre l'importanza di un utilizzo consapevole della tecnologia, come *data analytics* e intelligenza artificiale, per aumentare l'efficienza e la copertura delle attività di *audit*. A ciò si aggiungono l'adozione di KPI adeguati alla misurazione della *performance* e il rafforzamento del dialogo con gli *stakeholder*, elementi necessari per mantenere la funzione rilevante e coerente con le priorità strategiche dell'organizzazione.

L'evoluzione della funzione non può prescindere da una solida base professionale e di *governance*, capace di preservare indipendenza, obiettività e rigore metodologico. In questo senso, il *Three Lines Model* dell'IIA fornisce la collocazione strutturale dell'*Internal Audit* come terza linea indipendente, distinta dalle funzioni operative e di controllo di prima e seconda linea. I *Global Internal Audit Standards* (2024) dell'IIA integrano questa struttura definendo i principi professionali, i requisiti di qualità e gli obiettivi di *performance* necessari per una pratica di *audit* efficace. Infine, il *framework* COSO fornisce la base concettuale indispensabile entro cui collocare il sistema di controllo interno, articolato nelle sue componenti chiave: ambiente di controllo, *risk assessment*, attività di controllo, informazione e comunicazione, e attività di monitoraggio. Questa combinazione assicura che l'orientamento strategico e consulenziale non comprometta mai la qualità e il rigore metodologico tipici della professione.

3.3.2 Coerenza e compatibilità dei modelli

L'integrazione di approcci più orientati alla strategia e alla consulenza solleva una questione centrale: a quali condizioni l'*Internal Audit* possa mantenere la propria autonomia pur ampliando il proprio ruolo all'interno dell'organizzazione. Tuttavia, la coerenza del modello integrato dimostra che l'evoluzione della funzione può essere compatibile con il rigore professionale, purché siano preservati indipendenza, obiettività e chiara separazione delle responsabilità.

La principale criticità nell'integrazione dei modelli riguarda il rapporto tra le attività di *advisory* e il mantenimento dell'indipendenza della funzione. L'ampliamento del mandato verso la dimensione *Advise* può generare il rischio di una sovrapposizione con le responsabilità operative del *management*. Questa tensione si manifesta soprattutto quando l'*Internal Audit* partecipa a progetti di trasformazione o fornisce raccomandazioni specifiche su controlli e processi che, in un secondo momento, sarà chiamato a valutare in modo imparziale. È quindi fondamentale distinguere tra un supporto

consulenziale legittimo, basato su analisi indipendenti e raccomandazioni, e l'assunzione di ruoli decisionali o esecutivi che competono alla dirigenza.

Tale criticità può essere gestita attraverso la logica del *Three Lines Model*, che consente all'*Internal Audit* di fornire *assurance* e consulenza indipendenti, a condizione che non assuma responsabilità gestionali proprie della prima o della seconda linea. In questo schema, l'*Internal Audit* opera come una terza linea distinta, la cui indipendenza è garantita dal rapporto diretto con gli organi di governo e dall'assenza di compiti esecutivi. Il ruolo consultivo è dunque compatibile con la professione solo se resta fondato sull'obiettività, sull'autonomia organizzativa e su una chiara separazione delle responsabilità, evitando che l'*auditor* diventi responsabile della progettazione o dell'implementazione dei sistemi e dei controlli che dovrà successivamente verificare.

In questa prospettiva, i diversi *framework* risultano coerenti e complementari tra loro. Deloitte (2018) amplia il perimetro d'azione della funzione verso l'*advisory* e l'anticipazione dei rischi, mentre lo studio di PwC (2023) individua le condizioni operative e le leve tecnologiche per concretizzare tale trasformazione. L'IIA (2024) definisce i confini professionali e i principi etici entro cui questa evoluzione deve avvenire, assicurando che la qualità dell'*assurance* e l'autonomia di giudizio rimangano centrali. Infine, il *framework* COSO fornisce il riferimento strutturale per collegare il sistema di controllo interno, il *risk management* e il monitoraggio continuo. La compatibilità dei modelli dipende quindi dalla capacità di integrare innovazione strategica e rigore professionale, garantendo che l'ampliamento del contributo dell'*Internal Audit* non comprometta mai l'autonomia di giudizio né la credibilità della funzione.

3.3.3 Proposta di un modello integrato di *Internal Audit*

Alla luce dell'analisi dei *framework* internazionali e degli studi di settore, si propone un modello integrato di *Internal Audit* fondato su quattro pilastri fondamentali: *assurance* indipendente e *risk-based*, *advisory* controllata, anticipazione dei rischi emergenti e misurazione del valore generato. Tali pilastri sintetizzano le dimensioni contenutistiche, metodologiche e strutturali emerse nei paragrafi precedenti.

Il primo pilastro del modello integrato è rappresentato dall'*assurance* indipendente e *risk-based*. L'*Internal Audit* deve continuare a garantire valutazioni obiettive sull'efficacia del sistema di controllo interno, dei processi di *governance* e della gestione dei rischi, fornendo un ragionevole livello di *assurance* sul raggiungimento degli obiettivi aziendali. Tuttavia, tale attività deve superare la logica puramente rotazionale per adottare un approccio dinamico, orientato alle aree di maggiore

esposizione e aggiornato in funzione dell'evoluzione del profilo di rischio dell'organizzazione. L'integrazione di dati e tecnologia consente di rafforzare l'attività di *assurance*, aumentando la copertura delle verifiche, migliorando la tempestività dell'analisi e liberando risorse per i rischi più critici.

Il secondo pilastro riguarda l'*advisory* controllata. La funzione *Internal Audit* agisce come un *partner* strategico che contribuisce al miglioramento dei processi aziendali fornendo raccomandazioni, *insight* e prospettive indipendenti, specialmente durante fasi di trasformazione organizzativa o tecnologica. Secondo la logica del *Three Lines Model*, tale contributo deve avvenire senza assumere responsabilità operative o decisionali. Questa distinzione è fondamentale per preservare l'indipendenza e l'obiettività professionale, permettendo alla funzione di valutare in futuro i processi su cui ha fornito supporto consulenziale senza conflitti di interesse o rischi di auto-riesame.

Il terzo pilastro è costituito dalla capacità di anticipazione. L'*Internal Audit* evoluto deve sviluppare strumenti e competenze per intercettare rischi emergenti e segnali deboli in un contesto di *risk multiverse* caratterizzato da minacce interconnesse come *cyber risk*, ESG, intelligenza artificiale, dipendenza da terze parti e volatilità macroeconomica. Attraverso l'integrazione di tecniche di *risk sensing*, analisi avanzata dei dati e monitoraggio continuo, la funzione può passare da una logica reattiva ed *ex-post* a una logica prospettica. In questo modo, l'*audit* non si limita a valutare eventi già verificatisi, ma aiuta il *management* a comprendere le vulnerabilità future e possibili aree di esposizione, contribuendo alla resilienza dell'organizzazione.

Il quarto pilastro riguarda la misurazione del valore e il coinvolgimento degli *stakeholder*. Un modello evoluto non può essere valutato solo attraverso indicatori quantitativi di *output*, come il numero di *audit* completati, che da soli non catturano il valore effettivamente prodotto. È necessario adottare una prospettiva multidimensionale che includa indicatori qualitativi relativi alla rilevanza degli *insight*, alla qualità delle raccomandazioni, alla soddisfazione degli *stakeholder*, alla copertura dei rischi strategici e al contributo al miglioramento dei processi decisionali. Il successo della funzione non dipende quindi soltanto da ciò che l'*Internal Audit* produce, ma dalla sua capacità di generare apprendimento organizzativo, rafforzare la fiducia nella *governance* e rendere l'attività di *audit* significativa per la strategia aziendale.

Il modello integrato così delineato consente di collegare le principali dimensioni di valore emerse dai diversi *framework* e studi analizzati, integrando componenti contenutistiche, metodologiche e strutturali. Deloitte fornisce il contenuto del ruolo evoluto, PwC individua le leve operative della trasformazione, mentre IIA e COSO assicurano il presidio professionale e strutturale necessario a mantenere indipendenza, obiettività e coerenza con il sistema di controllo interno. Ne

deriva una concezione dell'*Internal Audit* come funzione capace di fornire *assurance* indipendente, supportare il *management* senza sostituirsi a esso, anticipare rischi emergenti e misurare il valore generato attraverso un dialogo continuo con gli *stakeholder*.

Tale impostazione costituisce la base concettuale per la successiva applicazione al contesto bancario simulato, in cui la funzione di *Internal Audit* dovrà confrontarsi con una fitta rete di rischi regolamentari, operativi, tecnologici e reputazionali, in un settore nel quale la qualità dei controlli interni incide direttamente sulla resilienza organizzativa e sulla stabilità dell'intermediario.

3.4 Applicazione a un contesto bancario: caso studio simulato

Il presente paragrafo applica il modello integrato delineato nella sezione precedente a un caso studio simulato, con l'obiettivo di mostrare come la trasformazione dell'*Internal Audit* possa essere impostata in modo progettuale. In particolare, il caso consente di tradurre in termini applicativi i *framework* analizzati nei paragrafi precedenti: la triade *Assure*, *Advise* e *Anticipate* proposta da Deloitte viene utilizzata per definire il ruolo evolutivo della funzione; il contributo PwC orienta la costruzione della roadmap, dei KPI e del percorso di *stakeholder engagement*; mentre i riferimenti IIA e COSO forniscono la cornice professionale e strutturale entro cui preservare indipendenza, obiettività e coerenza con il sistema di controllo interno. L'analisi non intende fornire evidenza empirica, ma costruire un percorso illustrativo che, partendo dalla valutazione dello stato attuale della funzione, consenta di individuare le principali aree di sviluppo e di formalizzare una strategia evolutiva coerente con le esigenze di *governance*, gestione dei rischi e creazione di valore. In questo modo, il caso permette di verificare la traducibilità operativa dei *framework* analizzati, evidenziandone benefici attesi, condizioni abilitanti e principali criticità applicative.

3.4.1 Descrizione del contesto organizzativo e obiettivi del progetto: Banca Alfa

Il caso studio prende in esame una banca simulata, denominata Banca Alfa, costruita a fini esclusivamente illustrativi come contesto applicativo del modello integrato di *Internal Audit* sviluppato nel paragrafo 3.3. La scelta di un intermediario bancario consente infatti di verificare come i principi di *assurance* indipendente, *advisory* controllata, anticipazione dei rischi e misurazione del valore possano essere tradotti in un percorso concreto di trasformazione della funzione.

Banca Alfa è un istituto di credito operante nel mercato italiano caratterizzato da un modello di *business* diversificato che include attività di *retail banking* per famiglie e piccole imprese, unitamente

a segmenti di *private e corporate banking*. La banca ha adottato una strategia orientata all'innovazione e alla progressiva digitalizzazione dei servizi, tramite canali digitali evoluti, determinando una significativa esposizione e dipendenza da infrastrutture ICT⁷ critiche e interconnesse. La struttura organizzativa è complessa e prevede una *governance* articolata con funzioni di controllo formalmente definite, rendendo l'ente un ambiente idoneo per l'analisi di un sistema di governo dei rischi multidimensionale.

Banca Alfa opera in un contesto fortemente regolamentato, nel quale il principio della sana e prudente gestione costituisce il canone fondamentale dell'attività aziendale. In conformità alle disposizioni della Circolare 285/2013 della Banca d'Italia e alle linee guida EBA⁸ sulla *governance* interna, l'istituto deve garantire un sistema dei controlli interni completo, funzionale e affidabile. Tale sistema, coerente con il *framework* COSO, è progettato per fornire una ragionevole *assurance* sul conseguimento degli obiettivi legati all'operatività, al *reporting* e alla *compliance* normativa. Il quadro regolamentare attuale pone inoltre sfide cruciali in termini di resilienza operativa digitale, in linea con i requisiti del regolamento DORA (EU 2022/2554)⁹, volte a rafforzare la capacità delle entità finanziarie di prevenire, gestire e superare incidenti connessi alle tecnologie dell'informazione e della comunicazione. Parallelamente, l'evoluzione della disciplina sulla sostenibilità introdotta dalla direttiva CSRD (EU 2022/2464) richiede una crescente attenzione alla qualità dei dati ESG, ai processi di *reporting* non finanziario e ai rischi reputazionali connessi alla sostenibilità.

Il progetto di trasformazione oggetto dell'analisi si propone di analizzare il livello attuale di maturità della funzione di *Internal Audit* di Banca Alfa, valutandone il posizionamento rispetto alle *best practice* nel mercato, nonché ai nuovi *Global Internal Audit Standards* del 2024. Gli obiettivi principali includono l'individuazione di aree di miglioramento e la formalizzazione di una *Internal Audit Strategy* dinamica e *risk-based*, capace di supportare gli obiettivi strategici e la resilienza della banca. Il progetto mira a definire una *roadmap* evolutiva e un sistema di indicatori quali-quantitativi (KPI) per monitorare l'avanzamento delle iniziative e misurare il valore generato dalla funzione. In tale prospettiva, l'*Internal Audit* è chiamato a rafforzare il proprio ruolo non solo come presidio di *assurance* indipendente, ma anche come funzione capace di fornire *advisory* controllata, anticipare

⁷ Le infrastrutture ICT (*Information and Communication Technology*) rappresentano l'insieme di hardware, software, reti e servizi che permettono la gestione, l'elaborazione e la trasmissione delle informazioni all'interno di un'organizzazione.

⁸ Le linee guida EBA (*European Banking Authority*) sono raccomandazioni tecniche e standard prudenziali emanati dall'Autorità Bancaria Europea per armonizzare la vigilanza bancaria nell'UE. Il loro obiettivo è garantire solidità finanziaria, prevenire crediti deteriorati e uniformare la gestione dei rischi, inclusi quelli ESG e di credito, obbligando le banche a valutazioni prospettiche della sostenibilità finanziaria dei clienti.

⁹ Il DORA (Regolamento UE 2022/2554) è un regolamento dell'Unione Europea che stabilisce requisiti vincolanti per la resilienza operativa digitale nel settore finanziario.

rischi emergenti e favorire un maggiore coordinamento tra organi di governo, *management* e funzioni di controllo.

3.4.2 Analisi della situazione “*as is*” e valutazione del livello di maturità

L’analisi dello stato attuale della funzione di *Internal Audit* di Banca Alfa evidenzia un presidio formalmente solido e già inserito in un percorso di evoluzione, pur non avendo ancora raggiunto una piena maturità rispetto al modello integrato delineato nei paragrafi precedenti. Nell’ultimo triennio, la funzione ha avviato diverse iniziative di rafforzamento metodologico, organizzativo e operativo, con l’obiettivo di rendere l’attività di *audit* maggiormente coerente con il profilo di rischio della banca. In particolare, è stato consolidato un approccio *risk-based*, volto ad allineare il piano di *audit* annuale alle principali aree di esposizione individuate nel *Risk Appetite Framework* (RAF) della banca. Tale evoluzione ha prodotto benefici in termini di maggiore focalizzazione sui rischi rilevanti e migliore allocazione delle risorse, riducendo progressivamente il peso di attività a minore valore aggiunto. Sotto il profilo organizzativo, il riporto diretto agli organi di governo e il rafforzamento del dialogo con il vertice aziendale hanno contribuito a consolidare l’indipendenza della funzione, in coerenza con le indicazioni delle linee guida EBA e degli standard professionali internazionali.

In ambito digitale, Banca Alfa ha introdotto prime applicazioni di *data analytics* a supporto delle verifiche, con l’obiettivo di superare gradualmente un approccio basato esclusivamente su test campionari manuali. Tali strumenti hanno consentito di migliorare la qualità delle analisi, ampliare la base informativa utilizzata negli *audit* e liberare risorse da alcune attività ripetitive. Tuttavia, l’utilizzo delle tecnologie digitali risulta ancora selettivo e non pienamente integrato nei processi ordinari della funzione. Parallelamente, sono stati avviati programmi di formazione finalizzati allo sviluppo di competenze ibride, capaci di combinare conoscenze di *audit*, comprensione del *business* e familiarità con strumenti tecnologici. Anche sul fronte della sostenibilità, la funzione ha iniziato a includere nei propri programmi di *audit* alcuni profili connessi ai rischi ESG, con particolare attenzione alla qualità dei dati non finanziari, ai processi di *reporting* e ai potenziali rischi reputazionali. Questi interventi hanno favorito una maggiore consapevolezza del rischio all’interno delle *business unit*, pur rimanendo ancora in una fase di consolidamento.

Nel complesso, la funzione può essere collocata a un livello di maturità “strutturato”: essa dispone di processi formalizzati, di un piano di *audit risk-based* e di un assetto organizzativo coerente con i principali requisiti professionali e regolamentari, ma presenta ancora margini di evoluzione verso un modello pienamente dinamico, tecnologico e orientato al valore. Dal punto di vista metodologico, il piano di *audit* rimane prevalentemente annuale e non sempre consente un

aggiornamento tempestivo rispetto all'emergere di nuovi rischi o cambiamenti improvvisi nel contesto operativo. Sul piano operativo, la funzione mantiene una buona capacità di rilevare anomalie e formulare raccomandazioni correttive, ma la produzione di *insight* prospettici a supporto del *top management* risulta ancora limitata. Anche la digitalizzazione appare parziale: l'analisi dei dati è presente in alcune aree, ma non è ancora estesa a logiche sistematiche di *continuous monitoring*, mentre l'intelligenza artificiale e l'automazione avanzata non rappresentano ancora strumenti pienamente incorporati nel modello operativo dell'*Internal Audit*.

Ulteriori aree di miglioramento riguardano il capitale umano, lo *stakeholder engagement* e la capacità della funzione di incidere sulla cultura del rischio. Sebbene siano stati avviati percorsi di formazione tecnica e digitale, permane la necessità di rafforzare competenze legate al pensiero critico, alla capacità di anticipazione e alla comunicazione verso gli organi di governo e il *management*. Lo *stakeholder engagement*, pur essendo formalmente presente, non consente ancora all'*Internal Audit* di essere percepito in modo pieno come una funzione capace di collegare le informazioni provenienti dalle diverse aree aziendali e di favorire un coordinamento più efficace tra funzioni di controllo e *business unit*. Infine, nonostante l'aumento della consapevolezza sui rischi, il contributo dell'*Internal Audit* all'apprendimento organizzativo e al miglioramento dei processi decisionali non risulta ancora pienamente istituzionalizzato. Da questa analisi emerge quindi l'esigenza di una fase successiva di evoluzione, orientata a rafforzare il ruolo della funzione non solo come presidio di *assurance*, ma anche come soggetto capace di generare *insight*, supportare il cambiamento e contribuire alla protezione del valore aziendale.

3.4.3 Posizionamento della funzione e individuazione delle aree di miglioramento

Il posizionamento attuale dell'*Internal Audit* di Banca Alfa riflette una funzione caratterizzata da un'elevata efficacia tecnica, ma da una significatività organizzativa ancora non pienamente sviluppata. La funzione è percepita dagli *stakeholder* principalmente come un solido presidio di conformità e un fornitore di *assurance* periodica e prevalentemente retrospettiva, piuttosto che come un partner strategico capace di incidere stabilmente sui processi decisionali. Pur risultando coerente con i principali requisiti regolamentari e professionali, l'*Internal Audit* opera ancora in larga parte come una funzione di controllo *ex post*, con una capacità di anticipazione dei rischi emergenti non ancora pienamente riconosciuta dal *top management*. Questo posizionamento genera il rischio che la funzione venga percepita come necessaria ma non ancora decisiva per la resilienza organizzativa e per la protezione del valore nel lungo periodo.

Ai fini dell’individuazione delle aree di miglioramento, il posizionamento di Banca Alfa può essere posto a confronto con un *benchmark* di mercato (*leading practice*). Tale confronto non ha finalità empiriche o statistiche, ma consente di evidenziare gli scarti principali tra il livello di maturità attuale della funzione e il modello evoluto delineato nei paragrafi precedenti.

Confronto tra Banca Alfa e leading practice di mercato			
Area di confronto	Leading practice / peer evoluti	Posizionamento di Banca Alfa	Gap individuato
Governance e stakeholder engagement	Dialogo strutturato e continuativo con Board, Audit Committee, top management e funzioni di controllo	Dialogo presente, ma ancora prevalentemente formale	Rafforzare il confronto continuativo e orientarlo alla produzione di insight
Metodologia e audit plan	Audit plan dinamico, aggiornato periodicamente in base all’evoluzione del profilo di rischio	Piano risk-based, ma ancora prevalentemente annuale	Rendere il piano più flessibile e aggiornabile rispetto ai rischi emergenti
Digitalizzazione e data analytics	Utilizzo sistematico di data analytics, automazione e continuous monitoring su processi core	Prime applicazioni selettive di data analytics	Estendere l’utilizzo degli strumenti digitali e dei dati a processi più ampi
People excellence e competenze	Profili ibridi con competenze di audit, business, ICT, ESG e data analytics	Percorsi formativi avviati, ma non ancora pienamente strutturati	Definire una skill matrix e rafforzare programmi di upskilling mirati
KPI e misurazione del valore	KPI quantitativi e qualitativi collegati a insight, impatto, risk culture e miglioramento dei processi	KPI ancora prevalentemente operativi	Misurare meglio qualità, rilevanza e valore generato dalla funzione

FIGURA 1 - CONFRONTO TRA BANCA ALFA E LEADING PRACTICE DI MERCATO

FONTE: ELABORAZIONE PROPRIA SULLA BASE DI DELOITTE (2018), PWC (2023), IIA (2024) E DEL MODELLO INTEGRATO SVILUPPATO NEL PARAGRAFO 3.3.

Nel confronto con le *best practice* dei principali operatori bancari italiani ed europei, Banca Alfa evidenzia alcuni margini di miglioramento nel livello di digitalizzazione e nella copertura dei rischi strategici. Le funzioni di *Internal Audit* più evolute, che PwC identifica come *Pioneers*, si distinguono per una maggiore attenzione ai rischi strategici, un utilizzo più maturo della tecnologia e una più forte capacità di produrre *insight* rilevanti per il *management*. Rispetto a tali pratiche, Banca Alfa mostra un approccio ancora parzialmente tradizionale, soprattutto per quanto riguarda l’utilizzo sistematico di *data analytics*, *continuous monitoring* e strumenti di *risk sensing*. Le *leading practice* evidenziano inoltre una maggiore integrazione tra *Internal Audit* e funzioni di controllo di seconda linea, quali *Risk Management* e *Compliance*, attraverso strumenti come *assurance map*, momenti strutturati di coordinamento e condivisione delle priorità di rischio. In Banca Alfa, invece, la collaborazione tra le funzioni è presente, ma risulta ancora prevalentemente formale e non sempre supportata da una visione integrata dei rischi.

La percezione del ruolo da parte degli *stakeholder* rappresenta un ulteriore fattore critico. Sebbene il *Board* e l'*Audit Committee* riconoscano l'indipendenza e l'obiettività della funzione, emerge una crescente aspettativa di ricevere *insight* strategici più profondi, oltre alla tradizionale rappresentazione dei *finding* e delle raccomandazioni correttive. Il *top management* e le *business unit* tendono ancora a vedere l'*auditor* come un valutatore esterno, più che come un soggetto capace di stimolare apprendimento organizzativo e miglioramento dei processi decisionali. Questo scarto deriva dalla crescente complessità delle sfide attuali, tra cui *cyber risk*, resilienza operativa digitale, requisiti DORA, rischi ESG e sostenibilità, rispetto a un'attività di *audit* ancora percepita come prevalentemente orientata alla verifica della conformità procedurale. Per rafforzare la propria influenza, la funzione deve quindi dimostrare non solo competenze tecniche, ma anche capacità relazionali, pensiero critico, conoscenza del *business* e capacità di sfida costruttiva, cioè quelle competenze che PwC riconduce alle cosiddette *human superpowers*.

Le aree di miglioramento individuate per Banca Alfa richiedono un intervento multidimensionale volto ad accrescere il valore prodotto dalla funzione. In primo luogo, appare prioritario rendere l'*audit plan* più dinamico e flessibile, aumentando la copertura dei rischi strategici, della resilienza operativa digitale e dei fattori ESG, superando progressivamente una logica fondata sulla sola rotazione periodica delle aree da verificare. Sotto il profilo tecnologico, è necessario rafforzare l'utilizzo di *data analytics* e strumenti di monitoraggio continuo, estendendoli gradualmente a processi e *dataset* più ampi, senza tuttavia trascurare la qualità dei dati e il giudizio professionale dell'*auditor*. Parallelamente, la funzione deve investire nella formazione di profili con competenze ibride e rafforzare lo *stakeholder engagement*, strutturando un dialogo più continuo con *Board*, *Audit Committee*, *top management*, funzioni di controllo e *business unit*. Infine, l'adozione di KPI più evoluti, sia quantitativi sia qualitativi, consentirebbe di misurare e comunicare meglio il contributo effettivo dell'*Internal Audit* al rafforzamento della *risk culture*, al miglioramento dei processi decisionali e alla qualità complessiva del sistema di *governance* della banca.

3.4.4 Definizione dell'*Internal Audit Strategy*, roadmap evolutiva e KPI

La formalizzazione della *Internal Audit Strategy* di Banca Alfa rappresenta il punto di raccordo tra le evidenze emerse dall'analisi *as is* e la definizione del modello evolutivo desiderato. Essa costituisce un piano d'azione orientato al medio-lungo periodo, volto ad allineare l'evoluzione della funzione alle aspettative del *Board*, dell'*Audit Committee* e del *Senior Management*. Tale documento definisce una visione della funzione su un orizzonte di tre-cinque anni, individuando priorità, iniziative, risorse necessarie e modalità di monitoraggio del percorso di trasformazione. La missione

dell'*Internal Audit* viene quindi progressivamente orientata al rafforzamento della *governance*, del *risk management* e dei processi di controllo, attraverso un modello capace di combinare *assurance* indipendente, supporto consulenziale e capacità di anticipazione dei rischi emergenti. Le priorità strategiche includono la copertura sistematica dei rischi più significativi, con particolare attenzione alla resilienza operativa digitale, ai rischi ICT, ai fattori ESG e alla qualità dei dati, nonché lo sviluppo di competenze ibride e l'utilizzo più maturo di tecnologie a supporto dell'attività di *audit*.

A fini illustrativi, la *roadmap* seguente sintetizza le principali iniziative evolutive previste per la funzione *Internal Audit* di Banca Alfa, articolandole per area di intervento e fase progettuale.

Roadmap evolutiva della funzione Internal Audit di Banca Alfa				
Area di intervento	Fase 1: Analisi as-is e maturity assessment	Fase 2: Definizione Internal Audit Strategy	Fase 3: Implementazione delle iniziative evolutive	Fase 4: Monitoraggio e consolidamento
Governance e stakeholder engagement	Mappatura stakeholder	Allineamento con Board e Audit Committee	Tavoli periodici con funzioni di controllo	Valutazione soddisfazione stakeholder
Metodologia e audit plan	Analisi piano attuale	Revisione in ottica risk-based	Introduzione audit plan dinamico	Aggiornamento periodico su rischi emergenti
Digitalizzazione e data analytics	Assessment strumenti esistenti	Selezione use case data analytics	Pilot data analytics su processi core	Estensione continuous monitoring
People excellence e competenze	Skill gap analysis	Definizione skill matrix e piano formativo	Formazione su ICT, ESG e analytics	Valutazione competenze acquisite
KPI e misurazione del valore	Identificazione KPI iniziali	Definizione KPI quali-quantitativi	Monitoraggio avanzamento roadmap	Reporting sul valore generato dalla funzione
Benchmark e posizionamento	Raccolta best practice e peer benchmark	Gap analysis rispetto ai peer	Integrazione dei gap nella roadmap	Rivalutazione periodica del posizionamento

FIGURA 2 - ROADMAP EVOLUTIVA DELLA FUNZIONE INTERNAL AUDIT DI BANCA ALFA PER AREA DI INTERVENTO E FASE PROGETTUALE

FONTE: ELABORAZIONE PROPRIA SULLA BASE DEL MODELLO INTEGRATO SVILUPPATO NEL PARAGRAFO 3.3.

La *roadmap* evolutiva si articola su quattro orizzonti temporali, al fine di garantire un percorso di crescita graduale, sostenibile e misurabile. La prima fase ha una funzione prevalentemente diagnostica, poiché consente di valutare il livello di maturità della funzione, individuare le principali aree di esposizione e raccogliere elementi utili dal confronto con le *leading practice* di mercato. La seconda fase traduce tali evidenze nella definizione della strategia, attraverso l'individuazione delle priorità evolutive, delle competenze necessarie, degli strumenti tecnologici da introdurre e degli indicatori di monitoraggio. La terza fase riguarda l'attuazione concreta delle iniziative, con

particolare attenzione al rafforzamento dell'*audit plan*, all'utilizzo progressivo di *data analytics*, allo sviluppo delle competenze e all'integrazione dei *gap* emersi dal *benchmark*. Infine, la quarta fase è orientata al monitoraggio e al consolidamento del modello, affinché la trasformazione non rimanga un intervento isolato, ma diventi un processo continuativo di aggiornamento, misurazione del valore e riallineamento rispetto all'evoluzione dei rischi e delle aspettative degli *stakeholder*.

Il monitoraggio della strategia richiede un set bilanciato di KPI quantitativi e qualitativi, in grado di valutare non solo l'efficienza operativa della funzione, ma anche la qualità e la rilevanza del contributo prodotto. Sotto il profilo quantitativo, Banca Alfa può monitorare la percentuale di completamento del piano di *audit*, il tasso di implementazione delle raccomandazioni, il tempo medio di chiusura dei *finding*, la quota di *audit* dedicati a rischi strategici o emergenti e la percentuale di attività supportate da strumenti di *data analytics*. Parallelamente, la valutazione deve estendersi a indicatori qualitativi, quali la qualità percepita degli *insight* prodotti, la soddisfazione del *Board* e del *top management*, la rilevanza delle raccomandazioni formulate e il contributo alla diffusione di una più solida cultura del rischio. Ulteriori metriche possono riguardare il livello di coordinamento con le funzioni di *Risk Management*, *Compliance*, *ICT* e *Sustainability*, al fine di ridurre duplicazioni, migliorare la copertura complessiva dei rischi e individuare eventuali aree non adeguatamente presidiate.

L'allineamento degli *stakeholder* costituisce una fase essenziale del progetto, poiché consente di rafforzare la legittimazione della funzione e di ridurre possibili resistenze al cambiamento. La strategia deve essere condivisa e discussa con l'*Audit Committee*, il *Senior Management* e i responsabili delle principali funzioni aziendali coinvolte. Tale confronto permette di raccogliere *feedback*, verificare la coerenza tra priorità di *audit* e obiettivi strategici della banca e costruire una visione condivisa del percorso evolutivo. In questo modo, l'*Internal Audit* può rafforzare la propria autorevolezza interna, non limitandosi a svolgere un ruolo di controllo *ex post*, ma contribuendo in modo più strutturato al miglioramento dei processi decisionali, alla qualità del sistema di *governance* e alla resilienza complessiva dell'istituto.

3.4.5 Impatti strategici e organizzativi attesi

L'attuazione della nuova *Internal Audit Strategy* di Banca Alfa può generare benefici significativi che si riflettono, in primo luogo, sulla *governance*. Un dialogo più strutturato e trasparente con il *Board* e il Comitato Controllo e Rischi consente infatti di rafforzare la qualità delle informazioni disponibili per gli organi di governo e di aumentare la fiducia degli *stakeholder* nell'integrità del sistema dei controlli interni. Sotto il profilo del *risk management*, il passaggio a un

piano di *audit* più dinamico e l'adozione di strumenti di *risk sensing* permettono una copertura più tempestiva dei rischi emergenti e interconnessi, con particolare attenzione alla resilienza operativa digitale, ai rischi ICT e ai fattori ESG. A livello organizzativo, la funzione può contribuire a ridurre i silos informativi e a promuovere una cultura del rischio più consapevole, migliorando il coordinamento tra funzioni di *business*, funzioni di controllo e organi di governo. Infine, l'integrazione di tecnologie come *data analytics* e *continuous monitoring* può accrescere la tempestività e la qualità degli *insight* prodotti, favorendo un *reporting* meno descrittivo e più orientato al supporto dei processi decisionali.

Tuttavia, questa evoluzione comporta *trade-off* e criticità che devono essere gestiti per garantire la sostenibilità del modello. L'adozione di strumenti di intelligenza artificiale, automazione e analisi avanzata dei dati richiede investimenti rilevanti in infrastrutture ICT, competenze specialistiche e formazione continua, oltre alla necessità di superare possibili resistenze culturali e organizzative al cambiamento. Esiste inoltre il rischio che un coinvolgimento più ampio in attività di *advisory* e in progetti strategici possa compromettere, o essere percepito come idoneo a compromettere, l'indipendenza e l'obiettività degli *auditor*, qualora non siano applicati adeguati presidi di salvaguardia e una chiara separazione delle responsabilità. La *performance* della funzione diventa inoltre più dipendente dalla qualità, affidabilità e disponibilità dei dati aziendali: se i dati di *input* sono incompleti, non aggiornati o distorti, gli strumenti automatici possono produrre analisi imprecise o poco significative. Per questo motivo, l'innovazione tecnologica deve essere accompagnata da una solida *governance* dei dati e dal mantenimento del giudizio professionale e dello scetticismo dell'*auditor*.

Il successo del progetto è subordinato a precise condizioni abilitanti. In primo luogo, è necessaria una forte *sponsorship* del *Board* e del Comitato Controllo e Rischi, chiamati a sostenere il ruolo evolutivo dell'*Internal Audit* e a garantire risorse adeguate al raggiungimento degli obiettivi strategici. Un ruolo centrale è ricoperto dal *Chief Audit Executive*, che deve guidare il percorso di trasformazione, assicurare l'allineamento con il *top management* e promuovere lo sviluppo di competenze ibride all'interno del *team*. È inoltre essenziale mantenere una chiara separazione delle responsabilità rispetto alle funzioni di prima e seconda linea, in modo da evitare sovrapposizioni operative e preservare l'autonomia di giudizio della funzione. Infine, una comunicazione efficace e il monitoraggio sistematico di KPI quantitativi e qualitativi consentono di dimostrare il valore generato dall'*Internal Audit*, rafforzandone la legittimazione interna e la significatività organizzativa.

Conclusioni

L'analisi svolta nel corso della tesi ha evidenziato come la funzione di *Internal Audit* stia attraversando una trasformazione profonda, che ne modifica progressivamente ruolo, finalità e contributo all'interno dell'organizzazione. Da funzione tradizionalmente associata alla verifica della conformità, alla prevenzione di errori e al controllo *ex post* dei processi aziendali, l'*Internal Audit* si configura oggi come un presidio sempre più integrato nei sistemi di *governance*, gestione dei rischi e controllo interno. Tale evoluzione risulta particolarmente rilevante nei contesti fortemente regolamentati, come quello bancario, nei quali la complessità normativa, la rilevanza sistemica degli intermediari e la crescente esposizione a rischi operativi, tecnologici, reputazionali e di sostenibilità rendono indispensabile un sistema di controllo solido, indipendente e dinamico.

La conclusione principale che emerge dalla tesi è che l'*Internal Audit* evoluto non sostituisce il proprio ruolo tradizionale, ma lo supera ampliandolo. L'*assurance* indipendente rimane il fondamento della funzione, ma non ne esaurisce più il valore. In un ambiente caratterizzato da rischi interconnessi, trasformazione digitale, pressioni regolamentari e nuove aspettative degli *stakeholder*, l'*Internal Audit* deve essere in grado di guardare oltre la semplice verifica della conformità. Deve saper interpretare segnali deboli, collegare informazioni provenienti da aree diverse dell'organizzazione, formulare raccomandazioni realmente utili e contribuire a decisioni più tempestive e consapevoli.

Tale evoluzione, tuttavia, non è priva di criticità. L'ampliamento del ruolo della funzione richiede investimenti in tecnologia, nuove competenze professionali, maggiore qualità dei dati e una forte *sponsorship* da parte degli organi di governo. Richiede inoltre una chiara separazione delle responsabilità, affinché l'attività di *advisory* non comprometta l'indipendenza e l'obiettività dell'*audit*. Il valore dell'*Internal Audit* non dipende quindi soltanto dagli strumenti adottati, ma dalla capacità dell'organizzazione di integrare tali strumenti in un modello coerente di *governance*, controllo e gestione dei rischi.

Bibliografia

- Alzeban, A. (2020). *Internal audit as an antecedent of economic growth*. Journal of Economic Studies, 48(7), 1267-1283
- Anderson, D. J., & Eubanks, G. (2015). *Leveraging COSO across the three lines of defense*. Committee of Sponsoring Organizations of the Treadway Commission
- Arena, M., & Azzone, G. (2009). *Identifying organizational drivers of internal audit effectiveness*. International Journal of Auditing, 13(1), 43-60.
- Banca d'Italia. (2013). *Circolare n. 285 del 17 dicembre 2013. Disposizioni di vigilanza per le banche e successive modifiche e integrazioni*. Banca d'Italia.
- Banca d'Italia. (2025). *Relazione sulla gestione e sulla sostenibilità: Anno 2024*. Banca d'Italia.
- Barbe, O., Raimbault, S., & Roussy, M. (2019). *Internal audit: from effectiveness to organizational significance*. Managerial Auditing Journal, 35(2), 322-342
- Bardhan, I., Lins, S., & Hao, L. (2023). *Internal audit function and the precision and accuracy of management forecasts*. Journal of Management and Governance, 27(4), 1339-1365
- Barney, J. (1991). *Firm resources and sustained competitive advantage*. Journal of Management, 17(1), 99-120.
- Barney, J. B., Wright, M., & Ketchen, D. J. (2001). *The resource-based view of the firm: Ten years after 1991*. Journal of Management, 27(6), 625-641.
- Besanko, D., Dranove, D., Shanley, M., & Schaefer, S. (2017). *Economics of strategy* (7th ed.). Wiley.
- Cawman, M. W., & Liu, M. (2020). *External factors and risk considerations: Applying the institution-based view of management*. Academy of Strategic Management Journal, 19(4), 1-16.
- Committee of Sponsoring Organizations of the Treadway Commission (COSO). (2013). *Internal control - Integrated framework*. COSO.
- Committee of Sponsoring Organizations of the Treadway Commission. (2013). *Internal control—Integrated framework: Executive summary*.
- Committee of Sponsoring Organizations of the Treadway Commission. (2013). *COSO internal control—Integrated framework: I principi*

- Cruz, L. B., & Cabral, S. (2010). *A culturally informed resource-based view of the firm: Toward a theoretical integration of culture and competitive advantage*. *Strategic Management Journal*, 31(8), 795-815.
- Deloitte. (2018). *Internal audit 3.0: The future of internal audit is now*. Deloitte.
- De Zwaan, L., Stewart, J., & Subramaniam, N. (2011). *Internal audit involvement in enterprise risk management*. *Managerial Auditing Journal*, 26(7), 586-604
- Dobbs, M. E. (2014). *Guidelines for applying Porter's five forces framework: A set of industry analysis templates*. *Competitiveness Review*, 24(1), 32-45.
- Johnson, G., Scholes, K., & Whittington, R. (2017). *Exploring strategy* (11th ed.). Pearson.
- Eulerich, A., & Eulerich, M. (2020). *What is the value of internal auditing? – A literature review on qualitative and quantitative perspectives*. *Maandblad Voor Accountancy en Bedrijfseconomie*, 94(3/4), 83–92.
- Eulerich, M., & Lenz, R. (2020). *Defining, measuring, and communicating the value of internal auditing*.
- Eulerich, M., Eulerich, A., & Bonrath, A. (2025). *Technology and internal auditing: An overview of performance effects*. *Maandblad Voor Accountancy en Bedrijfseconomie*, 99(4), 181–193.
- European Banking Authority. (2021). *Guidelines on internal governance under Directive 2013/36/EU*. EBA/GL/2021/05. EBA.
- European Union. (2022). *Regulation (EU) 2022/2554 on digital operational resilience for the financial sector*. Official Journal of the European Union.
- European Union. (2022). *Directive (EU) 2022/2464 as regards corporate sustainability reporting*. Official Journal of the European Union.
- Fama, E. F., & Jensen, M. C. (1983). *Agency problems and residual claims*. *Journal of Law and Economics*, 26(2), 327-349.
- Francis, J. R. (2025). *Why regulate auditing? Externalities and the limits of regulation*. *International Journal of Auditing*, 29(3), 366-375
- Garrido, E., Gómez, J., Maicas, J. P., & Orcos, R. (2016). *The institution-based view of strategy: How to measure it*. *BRQ Business Research Quarterly*, 21(2), 82-101.
- Grant, R. M. (2022). *Contemporary strategy analysis* (11th ed.). Wiley.

- Grant Thornton LLP. (2009). *Guidance on monitoring internal control systems: Introduction*. Committee of Sponsoring Organizations of the Treadway Commission.
- Grundy, T. (2006). *Rethinking and reinventing Michael Porter's five forces model*. *Strategic Change*, 15(5), 213-229.
- Hill, C. W. L., Jones, G. R., & Schilling, M. A. (2020). *Strategic management: Theory & cases: An integrated approach* (13th ed.). Cengage Learning.
- Institute of Internal Auditors (IIA). (2017). *International Professional Practices Framework (IPPF)*.
- Institute of Internal Auditors (IIA). (2020). *The three lines model: An update of the three lines of defense*. The Institute of Internal Auditors.
- Institute of Internal Auditors. (2024). *Global Internal Audit Standards*. The Institute of Internal Auditors.
- Isack, M., & Aschauer, E. (2024). *The role of CSR report assurance and ESG rating in bank manager's judgement on ESG lending decisions*. *International Journal of Auditing*, 29(2), 280-304.
- Ismael, H. R., & Kamel, H. (2021). *Internal audit quality and earnings management: evidence from the UK*. *Managerial Auditing Journal*, 36(7), 951-978
- Jensen, M. C., & Meckling, W. H. (1976). *Theory of the firm: Managerial behavior, agency costs and ownership structure*. *Journal of Financial Economics*, 3(4), 305-360.
- Klösch, M., & Kasmanhuber, A. (2025). *How sustainability audits impact audit effort choices*. *International Journal of Auditing*, 29(3), 436-453
- Peng, M. W., Wang, D. Y. L., & Jiang, Y. (2008). *An institution-based view of international business strategy: A focus on emerging economies*. *Journal of International Business Studies*, 39(5), 920-936.
- Peng, M. W., Sun, S. L., Pinkham, B., & Chen, H. (2009). *The institution-based view as a third leg for a strategy tripod*. *Academy of Management Perspectives*, 23(3), 63-81.
- Peng, M. W. (2002). *Towards an institution-based view of business strategy*. *Asia Pacific Journal of Management*, 19(2-3), 251-267.
- Porter, M. E. (1980). *Competitive strategy: Techniques for analyzing industries and competitors*. Free Press.
- Porter, M. E. (1979). *How competitive forces shape strategy*. *Harvard Business Review*, 57(2), 137-145.

- Porter, M. E. (2008). *The five competitive forces that shape strategy*. Harvard Business Review, 86(1), 78-93.
- PwC. (2023). *Global Internal Audit Study 2023: Seeing through walls to find new horizons*. PricewaterhouseCoopers.
- Rajgopal, S., Srinivasan, S., & Zheng, X. (2021). *Measuring audit quality*. Review of Accounting Studies, 26(2), 559-619
- Roussy, M., Barbe, O., & Raimbault, S. (2020). *Internal audit: from effectiveness to organizational significance*. Managerial Auditing Journal, 35 (2), 322–342.
- Sarens, G., & De Beelde, I. (2006). *The relationship between internal audit and senior management*. International Journal of Auditing, 10(3), 219-241.
- Scott, W. R. (2014). *Institutions and organizations: Ideas, interests, and identities* (4th ed.). Sage Publications.
- Shleifer, A., & Vishny, R. W. (1997). *A survey of corporate governance*. Journal of Finance, 52(2), 737-783.
- Simons, R. (1995). *Levers of control: How managers use innovative control systems to drive strategic renewal*. Harvard Business School Press.
- Society of Corporate Compliance and Ethics & Health Care Compliance Association. (2020). *Compliance risk management: Applying the COSO ERM framework*. Committee of Sponsoring Organizations of the Treadway Commission.
- Sun, S. L., & Ding, Z. (2012). *Institution-based view*. In C. L. Cooper (Ed.), Wiley Encyclopedia of Management (3rd ed., Vol. 6). Wiley.
- United States Congress. (2002). *Sarbanes–Oxley Act of 2002*, Pub. L. No. 107-204, 116 Stat. 745.
- Wang, P., & Liang, S. (2025). *Internal audit independence, legal person governance structure, and financial reporting quality*. International Review of Economics and Finance.
- Wernerfelt, B. (1984). *A resource-based view of the firm*. Strategic Management Journal, 5(2), 171-180.